Stark-Heegner points

Course and Student Project description
Arizona Winter School 2011

Henri Darmon and Victor Rotger

1. Background: Elliptic curves, modular forms, and Heegner points

Let $E_{/\mathbb{Q}}$ be an elliptic curve over the field of rational numbers, of conductor N. Thanks to the proof of the Shimura-Taniyama conjecture, the curve E is known to be *modular*, i.e., there is a normalised cuspidal newform $f = \sum_{n=1}^{\infty} a_n(f)q^n$ of weight 2 on $\Gamma_0(N)$ satisfying

$$L(E,s) = L(f,s), \tag{1}$$

where

$$L(E,s) = \prod_{p \text{ prime}} (1 - a_p(E)p^{-s} + \delta_p p^{1-2s})^{-1} = \sum_{n=1}^{\infty} a_n(E)n^{-s} \tag{2}$$

is the *Hasse-Weil L-series* attached to E, whose coefficients with prime index are given by the formula

$$(a_p(E), \delta_p) = \begin{cases} (p+1-|E(\mathbb{F}_p)|, 1) & \text{if } p \nmid N; \\ (1,0) & \text{if } E \text{ has split multiplicative reduction at } p; \\ (-1,0) & \text{if } E \text{ has non-split multiplicative reduction at } p; \\ (0,0) & \text{if } E \text{ has additive reduction at } p, \text{ i.e., } p^2|N, \end{cases}$$

and

$$L(f,s) = \sum_{n=1}^{\infty} a_n(f)n^{-s} \tag{3}$$

is the *Hecke L-series* attached to the eigenform f. Hecke's theory shows that $L(f,s)$ has an Euler product expansion identical to (2), and also that it admits an integral representation as a Mellin transform of f. This extends $L(f,s)$ analytically to the whole complex plane and shows that it satisfies a functional equation relating its values at s and $2-s$.

The modularity of E thus implies that $L(E,s)$, which a priori is only defined on the right half-plane $\{s \in \mathbb{C}, \mathrm{Re}(s) > 3/2\}$ of absolute convergence for (2), enjoys a similar analytic continuation and functional equation. This fact is of great importance for the theory of elliptic curves. For example, the Birch and Swinnerton-Dyer conjecture equates the rank of the Mordell-Weil group $E(\mathbb{Q})$ to the order of vanishing of $L(E,s)$ at $s=1$:

$$\mathrm{rank}(E(\mathbb{Q})) \stackrel{?}{=} r_{\mathrm{an}}(E/\mathbb{Q}) := \mathrm{ord}_{s=1}(L(E,s)). \tag{4}$$

Equation (1) lends unconditional meaning to the right-hand side of (4).

Another important consequence of modularity is the existence of a so-called *modular parametrisation*—a non-constant map

$$\varphi : X_0(N) \longrightarrow E \tag{5}$$

of algebraic curves defined over $\mathbb{Q}$. Here $X_0(N)_{/\mathbb{Q}}$ stands for the classical modular curve whose underlying Riemann surface

$$X_0(N)(\mathbb{C}) = \Gamma_0(N)\backslash(\mathcal{H} \cup \mathbb{P}_1(\mathbb{Q})) \tag{6}$$

is the quotient of the upper-half plane $\mathcal{H} = \{z \in \mathbb{C}, \mathrm{Im}(z) > 0\}$ by the Hecke congruence subgroup of level N

$$\Gamma_0(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) : N \mid c\} \subset \mathbf{SL}_2(\mathbb{Z}),$$

suitably compactified by adding the finite set of cusps.

The fact that geometric modularity implies modularity ((5) $\Rightarrow$ (1)) is a direct consequence of the theory of Eichler-Shimura. The reverse implication is more delicate, and follows from Faltings' proof of the Tate conjectures for abelian varieties over global fields.

The modular parametrisation in (5) allows the construction of a systematic supply of algebraic points on E defined over certain abelian extensions of imaginary quadratic subfields K of $\mathbb{C}$. These are the classical Heegner points, which can be defined complex analytically using (6) as

$$P_\tau = \varphi([\tau]) \in E, \tag{7}$$

where $\tau \in \mathcal{H} \cap K$ is imaginary quadratic. The theory of complex multiplication shows that P_τ is defined over the maximal abelian extension K^{ab} of K. Up to replacing E by an isogenous elliptic curve if necessary, the underlying complex torus of E is $\mathbb{C}/\Lambda_f$ where

$$\Lambda_f = \{2\pi i \int_\gamma f(z)dz, \gamma \in H_1(X_0(N), \mathbb{Z})\},$$

and the Heegner point P_τ can be computed explicitly by the formula

$$P_\tau = 2\pi i \int_\infty^\tau f(z)dz \in \mathbb{C}/\Lambda_f. \tag{8}$$

Heegner points are the main actors in the proof of the celebrated theorem of Gross-Zagier-Kolyvagin, which establishes the following special case of the Birch and Swinnerton-Dyer conjecture:

$$\mathrm{rank}(E(\mathbb{Q})) = r_{\mathrm{an}}(E/\mathbb{Q}) \quad \text{ when } r_{\mathrm{an}}(E/\mathbb{Q}) \leq 1.$$

2. Stark-Heegner points

Heegner points arise from (the image under φ of) certain distinguished 0-dimensional algebraic cycles on modular curves—those supported on the moduli of elliptic curves with complex multiplication. The theory of *Stark-Heegner points* represents an attempt to construct algebraic points on elliptic curves—ideally, in settings that go well beyond what can be achieved through the theory of complex multiplication—by adapting the Heegner point

construction to distinguished higher-dimensional algebraic or topological cycles on appropriate "modular varieties". The notion of "Stark-Heegner point" is still too fluid to admit a clear-cut mathematical definition, but one can nonetheless distinguish two broad types of approaches.

2.1. Topological constructions

These are *completely conjectural* analytic constructions of points on elliptic curves arising from topological cycles on modular varieties. Some basic examples are the so-called ATR cycles on Hilbert modular varieties [DL] and the "p-adic ATR cycles on $\mathcal{H}_p \times \mathcal{H}$" attached to ideal classes of real quadratic orders [Da1].

2.2. Constructions via algebraic cycles

Given a variety V defined over $\mathbb{Q}$, let $\mathrm{CH}^j(V)(F)$ denote the Chow group of codimension j algebraic cycles on V defined over a field (or $\mathbb{Q}$-algebra) F modulo rational equivalence, and let $\mathrm{CH}^j(V)_0(F)$ denote the subgroup of null-homologous cycles. The assignments $F \mapsto \mathrm{CH}^j(V)(F)$ and $F \mapsto \mathrm{CH}^j(V)_0(F)$ are functors on $\mathbb{Q}$-algebras, and there is a natural equivalence $\mathrm{CH}^1(X_0(N))_0 = J_0(N)$. The modular parametrisation φ of (5) can thus be viewed as a natural transformation

$$\varphi : \mathrm{CH}^1(X_0(N))_0 \longrightarrow E. \tag{9}$$

The modular parametrisation (5) can therefore be generalised by replacing $X_0(N)$ with a variety V over $\mathbb{Q}$ of dimension $d > 1$, and $\mathrm{CH}^1(X_0(N))_0$ by $\mathrm{CH}^j(V)_0$ for a suitable $0 \leq j \leq d$. Any element Π of the Chow group $\mathrm{CH}^{d+1-j}(V \times E)(\mathbb{Q})$ induces a natural transformation

$$\varphi : \mathrm{CH}^j(V)_0 \longrightarrow E \tag{10}$$

sending $\Delta \in \mathrm{CH}^j(V)_0(F)$ to

$$\varphi_F(\Delta) := \pi_{E,*}(\pi_V^*(\tilde{\Delta}) \cdot \tilde{\Pi}), \tag{11}$$

where π_V and π_E denote the natural projections from $V \times E$ to V and E respectively. When V is a *modular variety* (for instance, the universal object or a self-fold fiber product of the universal object over a Shimura variety of PEL type), the natural transformation Φ is called the *modular parametrisation of* E attached to the pair (V, Π).

Modular parametrisations of this type are most useful when $\mathrm{CH}^j(V)_0(\bar{\mathbb{Q}})$ is equipped with a systematic supply of special elements, arising for example from from Shimura subvarieties of V. The images in $E(\bar{\mathbb{Q}})$ of such special elements under $\varphi_{\bar{\mathbb{Q}}}$ can be viewed as "higher-dimensional" analogues of Heegner points: they are sometimes referred to, following the terminology of [BDP], as *Chow-Heegner points*.

Chow-Heegner points have been studied in the following two settings:

1. The case where E is an elliptic curve with complex multiplication and V is a suitable family of $2r$-dimensional abelian varieties fibered over a modular curve [BDP]. The existence of modular parametrisation in this case relies on the Hodge or Tate conjectures on algebraic cycles for the variety $V \times E$, and seems difficult to establish unconditionally even though the modularity of E is a classical and relatively easy result dating

back to Deuring. This setting was described in a mini-course at the CRM in Barcelona by the first speaker and Kartik Prasanna, and will only be touched upon briefly at the AWS.

2. The case where E is a modular elliptic curve of conductor N and

$$V = X_0(N) \times W_r \times W_r,$$

where W_r is the rth Kuga Sato variety over a modular curve, obtained by desingularising and compactifying the r-fold fiber product of the universal elliptic curve over an affine modular curve. The fact that points of infinite order on E can be constructed from certain diagonal cycles in $\mathrm{CH}^1(V)_0$ when $r = 0$ was first observed by Shouwu Zhang, and a more systematic study of cycles on V and the resulting points on E has been undertaken more recently by the two speakers in collaboration with Ignacio Sols [DRS]. Chow-Heegner points arising from diagonal cycles on V are relatively well-understood—for instance, their construction does not rely on unproven cases of the Hodge or Tate conjectures. While diagonal cycles are too limited to bear a direct relationship with the more mysterious cases of the Stark-Heegner point construction, there is encouraging evidence that p-adic deformations of these cycles (more precisely, of their images under p-adic étale Abel-Jacobi maps) could lead to new insights into the Stark-Heegner points of [Da1].

3. The goal of the AWS lectures

The aim of the lectures delivered by the authors at the Arizona Winter School 2011 is to make a careful study of rational points on elliptic curves arising from null-homologous algebraic cycles in $\mathrm{CH}^{r+2}(V)_0$, where $V = X_0(N) \times W_r \times W_r$. In particular, the following general questions will be considered:

1. The conception and implementation of efficient algorithms for calculating the modular parametrisation

$$\varphi_{\mathbb{C}} : \mathrm{CH}^{r+2}(V)_0(\mathbb{C}) \longrightarrow E(\mathbb{C})$$

by complex analytic means;

2. Producing tables of Chow-Heegner points, with the goal of generating conjectures about their behaviour. These conjectures could focus on the relation between Chow-Heegner points and special values of L-series in the spirit of the Gross-Zagier formula, or on whether the Chow-Heegner points are well-behaved with respect to congruences between modular forms.

4. Recommended reading and background preparation

Students are encouraged to get acquainted with the basic theory of elliptic curves, modular forms, and Heegner points sketched in section 1 above by reading some of the many manuscripts devoted to this topic (e.g. [Da2, Ch. I-IV] for the statements of the basic facts

with many proofs omitted, and [DS] [Sil, Ch. II], [Sh, Ch. V], and [St, Ch. III] for more detailed expositions).

A somewhat more elaborate treatment of the material in Section 2 on Stark-Heegner points and Chow-Heegner points (but still written in the style of an "executive sumary" with almost no proofs or detailed calculations) can be found in [Da3].

Since some of the exercises we will propose for the afternoon sessions, as well as the student projects, will include numerical calculations on the computer, we also recommend acquiring some familiarity with symbolic algebra software like

- Sage (www.sagemath.org),
- Magma (http://magma.maths.usyd.edu.au/magma), or
- Pari-GP (http://pari.math.u-bordeaux.fr).

5. Some warm-up exercises.

Let $E_{/\mathbb{Q}}$ be any of the elliptic curves in Cremona's tables [Cr] of conductor $N \leq 100$, $N = p$ or $p \cdot q$ with p and q different primes.

(1) For any $\tau \in \{\frac{1+\sqrt{3}i}{2}, i, \frac{1+\sqrt{7}i}{2}, \sqrt{2}i, \frac{1+\sqrt{11}i}{2}, \sqrt{6}i\}$, use (8) to compute P_τ on E.

(2) Over what number field K do numerical computations suggest P_τ is rational in each case? Give a coherent, uniform explanation of what is going on.

(3) Is P_τ torsion or is it of infinite order? Try again to give a coherent, uniform explanation of the dichotomy that you observe.

References

[BDP] M. Bertolini, H. Darmon, and K. Prasanna, *Chow-Heegner points on CM elliptic curves and values of p-adic L-functions*, submitted.

[Cr] J. E. Cremona, Algorithms for Modular Elliptic Curves, Cambridge University Press, 1997, available on-line at http://www.warwick.ac.uk/ masgaj/book/fulltext/

[Da1] H. Darmon, *Integration on $\mathcal{H}_p \times \mathcal{H}$ and arithmetic applications*, Annals of Mathematics **154** (2001) 589-639.

[Da2] H. Darmon, *Rational points on modular elliptic curves*, CBMS Regional Conference Series in Mathematics, **101**, American Mathematical Society, Providence, RI 2004.

[Da3] H. Darmon, *Cycles on modular varieties and rational points on elliptic curves*, Oberwolfach reports, 6:3 (2009), 1843–1920 Explicit Methods in Number Theory.

[DL] H. Darmon and A. Logan, *Periods of Hilbert modular forms and rational points on elliptic curves*, International Mathematics Research Notices (2003) no. 40, 2153-2180.

[DRS] H. Darmon, V. Rotger and I. Sols, *Diagonal cycles on triple products of Kuga-Sato varieties and rational points on elliptic curves*, in progress.

[DS] F. Diamond, J. Shurman, *A first course in modular forms*, Graduate Texts in Mathematics **228**, Springer 2005.

[Sh] G. Shimura, Introduction to the arithmetic theory of automorphic functions, Publications of the Math. Soc. Japan **11**, Princeton Univ. Press, 1971.

[Sil] J. H. Silverman, Advanced topics in the arithmetic of elliptic curves, Graduate Texts in Mathematics **151**, Springer 1994.

[St] W. Stein, *The Birch and Swinnerton-Dyer Conjecture, a Computational Approach*, 2007. Available at http://modular.math.washington.edu

[Vo] C. Voisin, *Hodge Theory and complex algebraic geometry I*, Cambridge University Press **77**, 2002.