

Stark-Heegner points

Course and Student Project description
Arizona Winter School 2011

Henri Darmon and Victor Rotger

1 Heegner points and Stark-Heegner points

1.1 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

$$L(E, s) = L(f, s), \quad (1)$$

where

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

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

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

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 $\{s \in \mathbb{C}, \operatorname{Re}(s) > 3/2\}$ 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 $s = 1$:

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

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 $\mathcal{H} = \{z \in \mathbb{C}, \text{Im}(z) > 0\}$ by the Hecke congruence subgroup of level N

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

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}/Λ_f where

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

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:

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

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.

1.2.1 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].

1.2.2 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

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

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

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

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

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

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 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

$$V = X_0(N) \times \mathcal{E}_r \times \mathcal{E}_r,$$

where \mathcal{E}_r is the r th 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].

2 The student project

The aim of the lectures delivered in the mornings by the authors at the Arizona Winter School 2011 and of the afternoon student project is to make a careful study of rational points on elliptic curves arising from null-homologous algebraic cycles in $\mathrm{CH}^2(V)_0$, where $V = X_0(N) \times X_0(N) \times X_0(N)$ as explained in Chapter 7 of [DR]. The reader is referred to these notes for a more careful explanation of the necessary background, the precise definitions and the notation employed below.

In particular, the following general questions will be considered:

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

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

by complex analytic means.

2. Producing tables of the Chow-Heegner points

$$P_r = \mathrm{AJ}(\Delta), \quad P_{g,g,f}$$

arising in equations (7.6) and (7.7) of [DR], with the goal of generating conjectures about their behaviour. These conjectures could focus on the precise 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.

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 treatment of Stark-Heegner points and Chow-Heegner points which is somewhat more elaborate than Section 1 (but still written in the style of an *executive summary* with almost no proofs or detailed calculations) can be found in [Da3].

Most of all, the notes of the course [DR] on *Algebraic cycles and Stark-Heegner points* which are now available in the web site of the Arizona Winter School (particularly the first seven chapters), although still quite rough and containing many inaccuracies, can serve as a road map for what will be discussed during the AWS.

The exercises we propose below for the afternoon sessions have both a theoretical and computational flavor and should be solved by the students in small groups, combining the insights of those students with a stronger background on each of the several topics we will be touching, with the assistance of those students who are more computationally oriented. Since many of the exercises include numerical calculations on the computer, we encourage all students to bring their laptop with them and to acquire some familiarity with symbolic algebra software like

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

The first requires a license, while the second and third can be freely downloaded from the respective web sites.

2.1 Warm-up: classical Heegner points

On Saturday afternoon we shall begin by briefly discussing the following classical questions, which should serve as source of motivation and inspiration for the main student project, to which we will quickly move.

- (1) Familiarise yourself with Cremona's tables of elliptic curves [Cr] of small conductor, which are available on the web.
- (2) Write a short program (in MAGMA, PARI, SAGE or any other language) which takes as input

- An elliptic curve E over \mathbb{Q} , in the form of a vector $[a_1, a_2, a_3, a_4, a_6]$ of coefficients following the standard conventions of the Cremona tables;
- a (fundamental, or not) negative discriminant D ,

and returns as output a vector of $h = h(D)$ complex points on $E(H_D)$ corresponding to the Heegner points attached to the discriminant D . Here $h(D)$ is the class number of D and H_D is the ring class field attached to this discriminant. (So that, for example, H_D is the Hilbert class field of $K = \mathbb{Q}(\sqrt{D})$ when D is fundamental.)

- (3) Explain how you would go about recognizing the complex points that your program computes as algebraic points.
- (4) Test your program on a few elliptic curves of conductor ≤ 100 taken from Cremona's tables, and for the values $D = -3, -4, -7, -11$, and -23 . (Or any other values that strike your fancy.)
- (5) In the special cases where $h(D) = 1$, when is the Heegner point you compute of infinite order? Explain how what you observe is consistent with the Gross-Zagier formula.
- (6) In the case where $N = pq$ is a product of two distinct primes modulo which D is *not* a quadratic residue, how would you go about calculating a point on $E(\mathbb{Q}(\sqrt{D}))$ using the Heegner point program you have written?

2.2 Working tools

The numerical approach we propose towards the computation of Chow-Heegner points arising from diagonal cycles on triple products of modular curves requires a plethora of working tools, most of them very classical, which need to be understood in detail and, in many cases, to be efficiently implemented.

For this reason, we propose below a series of tasks or mini-projects, to be assigned and developed separately in small groups. These projects are arranged in no particular order: rather than being part of a chronological sequence, they each develop an aspect that will be needed to understand (both from a theoretical and practical point of view) the calculation of Chow-Heegner points. In particular, discussions and expositions of the progress made by each of the groups is highly encouraged during the afternoon sessions. The final project will be the reunion of each of the pieces and can not be understood without all of them.

This also means that every time you implement any of the algorithms suggested below, you should discuss with the groups working on the other projects which is the most suitable way of introducing your input, as they will probably have to use some of yours, and conversely.

As a way of example, let us all agree (unless you discuss and suggest anything better) that all meromorphic differential forms on the classical modular curve $X = X_0(N)$ that we shall be considering are given as

$$\omega_f = f(q) \frac{dq}{q}$$

where $f(q) = \sum_{n \geq n_0} a_n q^n$ is a formal Laurent series in the variable q such that the function

$$\mathcal{H} = \{\tau \in \mathbb{C} : \text{Im}(\tau) > 0\} \rightarrow \mathbb{C} \quad \tau \mapsto \sum_{n \geq n_0} a_n e^{2\pi i n \tau}$$

is absolutely convergent and yields an holomorphic function on \mathcal{H} .

Finally, questions below labelled with one star (\star) are considered basic steps towards the final implementation of the whole algorithm. Those labelled as ($\star \star \star$) are the main computational goal of each of the projects A, B and C.

(A) **The geometry of modular curves: cusps and modular units.** Let $N \geq 1$ be a positive integer and let $\Gamma_0(N)$ denote the usual congruence subgroup of level N . Let $Y_0(N) \subset X_0(N)$ be the classical (affine and complete, respectively) modular curves attached to this group.

- (a) (\star) Find a complete system of representatives in $\mathbf{P}^1(\mathbb{Q})$ of the set $\Gamma_0(N) \backslash \mathbf{P}^1(\mathbb{Q})$ of cusps of $X_0(N)$.
- (b) Define the group $W_N \subseteq \text{Aut}(X_0(N))$ of Atkin-Lehner involutions of $X_0(N)$. Is it always true that $W_N = \text{Aut}(X_0(N))$?
- (c) Does W_N leave the set of cusps invariant? If yes, describe the action of W_N on this set. Does $\text{Aut}(X_0(N))$ always leave the set of cusps invariant?
- (d) (\star) Let $q = q(\tau) := e^{2\pi i \tau}$. The classical eta function on \mathcal{H} is $\eta(q) = q^{1/24} \prod_{n>0} (1 - q^n)$. Explain its basic properties concerning convergence, meromorphy, zeros and poles.
- (e) Study the behavior of $\eta(q)$ under Moebius transformations and find in what ways the function $\eta(q)$ can be manipulated in order to give rise to well-defined meromorphic modular forms of even weight $k \in 2\mathbb{Z}$ on $X_0(N)$. Implement this on the computer.
- (f) Define $U_\eta \subseteq \mathcal{O}(Y_0(N))^\times \subseteq \mathbb{Q}(X_0(N))^\times$ to be the subgroup of those rational functions constructed in the previous point. What can you say about the first inclusion?
- (g) ($\star \star \star$) Given a divisor $D = \sum n_x \cdot x$ supported at the cusps, can you find a $u \in U_\eta$ such that $\text{div}(u) = D$? Such a function is called a *modular unit*. Write a program to construct u given D .

(B) **The Betti (co)homology of modular curves: modular symbols.** Let $N \geq 1$ be a positive integer and let $\Gamma_0(N)$ denote the usual congruence subgroup of level N . Let $Y_0(N) \subset X_0(N)$ be the classical (affine and complete, respectively) modular curves attached to this group. Let $Y := X_0(N) \setminus \{\infty\}$.

- (a) (\star) Describe the relationship between the first homology groups of $Y_0(N)$, Y and $X_0(N)$.

- (b) (★) Define modular symbols with respect to $\Gamma_0(N)$, establish their basic properties and compute some examples with any of the above software packages. You may wish to familiarise yourself with the extensive library of software for calculating with modular symbols that are already in the public domain, and can be found, notably, on William Stein's web page.
- (c) Describe $H_1(X_0(N), \mathbb{Z})$ in terms of the group $\Gamma_0(N) \backslash \text{Div}^0(\mathbf{P}^1(\mathbb{Q}))$ of modular symbols.
- (d) (★) Describe $H_1(X_0(N), \mathbb{Z})$ as a quotient of the group $\Gamma_0(N)$. Make this description computable on the computer: given $\gamma \in \Gamma_0(N)$, compute a modular symbol m_γ such that $m_\gamma = [\gamma] \in H_1(X_0(N), \mathbb{Z})$. And conversely: given a modular symbol $m_\gamma \in H_1(X_0(N), \mathbb{Z})$ find an element $\gamma \in \Gamma_0(N)$ such that $m_\gamma = [\gamma]$.
- (e) (★) Given a modular form $f \in S_2(\Gamma_0(N))$, let $\omega_f = f(q) \frac{dq}{q}$ its associated regular differential 1-form on $X_0(N)$. Define what is the line integral of ω_f along a path $c \in H_1(X_0(N), \mathbb{Z})$ and study its basic properties, particularly those related to the dependence of this integral on the various choices made. Implement its computation and study how the various choices can be optimized in order to make it more efficient.
- (f) (★) Define what does it mean for an element $\gamma \in H_1(X_0(N), \mathbb{C})$ to be *Poincaré dual* to ω_f and implement its computation.
- (g) Implement an algorithm which takes as input a modular form $f \in S_2(\Gamma_0(N))$ with *integral* fourier coefficients and outputs the lattice Λ_f of the elliptic curve E_f associated to f via the Eichler-Shimura construction. Compute several examples.
- (h) (★ ★ ★) What is the answer to the questions in (e) when we replace ω_f by an arbitrary meromorphic differential form η of the *second kind* on $X_0(N)$? How can one explicitly write down meromorphic (non-holomorphic) 1-forms of the second kind on $X_0(N)$? Implement all this.

(C) **Applications of the theorem of Riemann-Roch.**

Let X be a smooth projective curve over the field \mathbb{Q} of rational numbers and let $Y = X \setminus \{\infty\}$ for some point $\infty \in X(\mathbb{Q})$. Let $\tilde{X} \xrightarrow{\pi} X$ denote the universal covering of X .

- (a) Define $H_{dR}^1(Y)$ and of $H_{dR}^1(X)$ in terms of differential forms of the *second kind*. Use Riemann-Roch to prove that there is a natural isomorphism $\varphi : H_{dR}^1(Y) \xrightarrow{\sim} \frac{\Omega^1(Y)}{d\mathcal{O}(Y)}$.
- (b) (★) Implement the map φ when $X = X_0(N)$ and ∞ is the cusp at infinity.
- (c) (★) Describe the Poincaré pairing on $H_{dR}^1(X)$ and prove its basic properties. Implement it when $X = X_0(N)$.
- (d) Let $\omega \in \Omega^1(X)$ and $\eta \in \Omega^1(Y)$ be regular differential forms on X and Y , respectively. Show that the form η gives rise to a differential of the second kind on X . Let F_η denote the primitive of that form in \tilde{X} . Use Riemann-Roch to prove

that there exists a holomorphic differential form α on Y such that $\omega \cdot F_\eta - \alpha$ is holomorphic on $\tilde{X} \setminus \pi^{-1}(\infty)$ and has at worst a pole of order 1 at any point in the fiber at ∞ .

(e) ($\star\star\star$) Implement (d) on the computer when $X = X_0(N)$.

2.3 Chow-Heegner points

This is last stage of the student project, in which most of the basic ingredients needed for the computation of the Chow-Heegner points P_{f_1, f_2, f_3} introduced in [DR, Ch. 7] should be already available. However, having the ingredients is not enough: we still must discuss the recipe.

Share all the background accumulated during the elaboration of projects A, B, C together with the material explained in our lectures and use it to discuss the following questions.

- Write down diagram (5.4) of [DR, Ch. 5] in the particular setting of the variety $V = X_0(N) \times X_0(N) \times X_0(N)$ and an elliptic curve E/\mathbb{Q} of conductor N , recalling the definition of the four maps involved in the diagram.
- Given three modular eigenforms $f_1, f_2, f_3 \in S_2(N)$ of weight 2 and square-free level N , describe what we *mean* precisely by the point P_{f_1, f_2, f_3} .
- Design a recipe for the numerical computation of the Chow-Heegner points P_{f_1, f_2, f_3} when
 1. $N = 37$
 2. f_1, f_2 and f_3 are *newforms* and have *integral* coefficients.
 3. f_1, f_2 and f_3 are *newforms* but do not necessarily have *integral* coefficients.

3 Other exercises

The following is a short list of exercises which we find interesting and that we encourage the reader to solve, though most probably won't be discussed because of lack of time.

3.1 A concrete example: the curve $X_0(37)$

Once all tasks posed in the previous section have been accomplished and shared with all the participants, make a complete and detailed study of the modular curve $X = X_0(37)/\mathbb{Q}$, particularizing all the answers and computations that were obtained there to this curve.

Once this is done, use all this information to work on the following further questions:

1. Compute an equation for $X_0(37)$ over \mathbb{Q} .
2. Compute $X_0(37)(\mathbb{Q})$.

3. Compute an equation and the basic arithmetic data of the two curves E_f and E_g of level 37, and equations of the modular parametrisations

$$\pi_f : X \longrightarrow E_f, \quad \pi_g : X \longrightarrow E_g.$$

4. Let K denote the canonical divisor on X . Compute the image on E_f and on E_g of the divisor $K - 2\infty$.

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.
- [DR] H. Darmon and V. Rotger, *Algebraic cycles and Stark-Heegner points*, available at <http://math.arizona.edu/swc>.
- [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.