Cycles on modular varieties and rational points on elliptic curves

Henri Darmon

July 31, 2009

This is a summary of a three-part lecture series given at the meeting on "Explicit methods in number theory" that was held in Oberwolfach from July 12 to 18, 2009. The theme of this lecture series was the explicit construction of algebraic points on elliptic curves from cycles on *modular varieties*. Given a fixed elliptic curve E over $\mathbb{Q}$, the goal is to better understand the group $E(\bar{\mathbb{Q}})$ of algebraic points on E by focusing on the following question:

Which points in $E(\bar{\mathbb{Q}})$ can be accounted for by a "modular construction"?

Heegner points arising from CM points on modular curves are the prototypical example of such a modular construction. While we do not dispose of a completely satisfactory general definition of modular points, fulfilling the conflicting requirements of flexibility and mathematical precision, several "test cases" that go beyond the setting of Heegner points have been studied over the last 10 years (cf. [Da01], [DL], [BDG], [Da04], [Tr], [Gre], [BDP2]). Three illustrative examples were touched upon in these lectures:

1. [BDP1], [BDP2]. "Chow-Heegner points" arising from algebraic cycles on higher dimensional varieties. The existence and key properties of Chow-Heegner points are typically conditional on the Hodge or Tate conjectures on algebraic cycles.

2. [DL], [BDG], [CD]. "Stark-Heegner points" arising from ATR ("Almost Totally Real") cycles on Hilbert modular varieties parametrising elliptic curves over totally real fields. These ATR cycles are not algebraic, and the expected algebraicity properties of the associated Stark-Heegner points do not seem (for now) to be part of a systematic philosophy.

3. [Da01], [DP]. Stark-Heegner points attached to real quadratic cycles on the "mock Hilbert modular surface" $\mathbf{SL}_2(\mathbb{Z}[1/p])\backslash(\mathcal{H}_p \times \mathcal{H})$ parametrising an elliptic curve E over $\mathbb{Q}$ of prime conductor p. These real quadratic cycles are indexed by ideal classes of orders in a real quadratic field K, and are topologically isomorphic to $\mathbb{R}/\mathbb{Z}$. By an analytic process that combines complex and p-adic integration, they can be made to yield p-adic points on E which are expected to be defined over class fields of K. This setting leads to convincing experimental evidence for the existence of a theory of "complex multiplication for real quadratic fields".

1 Heegner Points

We begin with a brief sketch of the classical picture which we aim to generalize.

Modular parametrisations. Let E be an elliptic curve over $\mathbb{Q}$, and let N be its conductor. The classical construction of Heegner points is based on the modularity theorem of [Wi], [TW], as completed in [BCDT]. It asserts that

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

where $f(z) = \sum a_n e^{2\pi i n z}$ is a cusp form of weight 2 on the Hecke congruence group $\Gamma_0(N)$. The modularity of E is established by showing that the p-adic Galois representation

$$V_p(E) = \left(\lim_{\leftarrow,n} E[p^n]\right) \otimes \mathbb{Q}_p = H^1_{\text{et}}(\bar{E}, \mathbb{Q}_p)(1) \tag{2}$$

is a constituent of the first p-adic étale cohomology of the modular curve $X_0(N)$. The surjective $G_{\mathbb{Q}}$-equivariant projection of Galois representations

$$H^1_{\text{et}}(\overline{X_0(N)}, \mathbb{Q}_p) \longrightarrow H^1_{\text{et}}(\bar{E}, \mathbb{Q}_p) \tag{3}$$

gives rise to a non-trivial *Tate cycle*

$$\Pi_p \in H^2_{\text{et}}(\overline{X_0(N) \times E}, \mathbb{Q}_p)(1)^{G_{\mathbb{Q}}}. \tag{4}$$

By the Tate conjecture for curves over number fields that was proved by Faltings, there is therefore a non-constant morphism over $\mathbb{Q}$

$$\Phi : J_0(N) \longrightarrow E, \tag{5}$$

where $J_0(N)$ is the Jacobian of $X_0(N)$. This stronger, "geometric" form of modularity is crucial for the Heegner point construction.

CM points. The modular curve $X_0(N)$ is equipped with a distinguished supply of 0-dimensional cycles $\mathrm{CM}_K \subset \mathrm{Div}^0(X_0(N)(K^{\mathrm{ab}}))$ attached to any imaginary quadratic field K. The group CM_K consists of degree zero divisors supported on CM points attached to the moduli of elliptic curves with complex multiplication by an order in K. It is not hard to show that $\Phi(\mathrm{CM}_K)$ is an infinitely generated subgroup of $E(K^{\mathrm{ab}})$; it will be referred to as the group of *Heegner points* on E attached to K. The importance of Heegner points can be justified on (at least) three grounds.

1. The Gross-Zagier formula [GZ] relates the heights of certain points in $\Phi(\mathrm{CM}_K)$ to the central critical derivatives of the Hasse-Weil L-series of E over K, twisted by abelian characters of K, and thus supplies a link between the arithmetic of E and its Hasse-Weil L-series.

2. Following a method of Kolyvagin (cf. [Gr2]), the non-triviality of certain Heegner points can be used to bound the Selmer group of E (and therefore, its rank and Shafarevich-Tate group). Combined with the Gross-Zagier formula, this has led to the strongest

known results on the Birch and Swinnerton-Dyer conjecture, most notably the theorem that

$$\mathrm{rank}(E(\mathbb{Q})) = \mathrm{ord}_{s=1} L(E,s) \ \text{ and } \ \#\text{Ш}(E/\mathbb{Q}) < \infty, \qquad \text{when } \mathrm{ord}_{s=1}(L(E,s)) \leq 1.$$

3. Heegner points can be computed efficiently in practice by analytic methods. After identifying the set $Y_0(N)(\mathbb{C})$ of complex points on the open modular curve with the quotient $\Gamma_0(N)\backslash\mathcal{H}$, and replacing $E(\mathbb{C})$ by the isogenous torus $\mathbb{C}/\Lambda_f$ for an appropriate period lattice Λ_f attached to f, one has

$$\Phi(\tau) = \int_{i\infty}^{\tau} 2\pi i f(z) dz = \sum_{n=1}^{\infty} \frac{a_n}{n} e^{2\pi i n\tau} \pmod{\Lambda_f}.$$

This formula leads to efficient algorithms for computing Heegner points numerically, which have been implemented in software systems like Pari-GP, Magma, and SAGE.

2 Chow-Heegner points

Chow Groups. Given a variety V of dimension d defined over a field F, let

$$\begin{aligned} \mathrm{CH}^j(V)(F) &= \left\{ \begin{array}{c} \text{Codimension } j \text{ algebraic cycles on } V \text{ over } F \\ \text{modulo rational equivalence} \end{array} \right\}, \\ \mathrm{CH}^j(V)_0(F) &= \text{the subgroup of null-homologous cycles.} \end{aligned}$$

Modular parametrisations. Any element Π of the Chow group $\mathrm{CH}^{d+1-j}(V \times E)(\mathbb{Q})$ induces homomorphisms

$$\Phi_F : \mathrm{CH}^j(V)_0(F) \longrightarrow E(F) \tag{6}$$

for any $F \supset \mathbb{Q}$, by the rule

$$\Phi_F(\Delta) := \pi_E(\pi_V^{-1}(\tilde{\Delta}) \cdot \tilde{\Pi}), \tag{7}$$

where π_V and π_E denote the natural projections from $V \times E$ to V and E respectively and $\tilde{\Delta}$ and $\tilde{\Pi}$ are representatives of the class of Δ and Π, chosen so that $\pi_V^{-1}(\tilde{\Delta})$ and $\tilde{\Pi}$ intersect transversally. The assignment $\Phi : F \mapsto \Phi_F$ is a natural transformation from $\mathrm{CH}^j(V)_0$ to E, viewed as functors on $\mathbb{Q}$-algebras. This leads to the following informal definition:

Definition 2.1. A *modular parametrisation* of E is a triple (V, Π, j) where

1. V is a "modular variety" of dimension d;
2. Π is a cycle class in $\mathrm{CH}^{d+1-j}(V \times E)(\mathbb{Q})$;
3. the induced morphism $\Phi : \mathrm{CH}^j(V)_0 \longrightarrow E$ is *non trivial*.

The non-triviality condition on Φ merits some clarification. The most obvious notion of non-triviality is to require the existence of a cycle $\Delta \in \mathrm{CH}^j(V)_0(\bar{\mathbb{Q}})$ for which $\Phi(\Delta)$ is non-zero in $E(\bar{\mathbb{Q}}) \otimes \mathbb{Q}$. A second notion rests on the fact that the correspondence Π induces a functorial map on deRham cohomology:

$$\Phi^*_{\mathrm{dR}} : H^1_{\mathrm{dR}}(E/\mathbb{Q}) \longrightarrow H^{2d-2j+1}_{\mathrm{dR}}(V/\mathbb{Q}).$$

The modular parametrisation Φ will be said to be non-trivial if the class of $\Phi^*_{\mathrm{dR}}(\omega_E)$ is non-zero, where ω_E is a non-zero regular differential on E. We will henceforth work with this cohomological notion of non-triviality.

Modular varieties. Definition 2.1 above falls short of being mathematically precise because we have not explained what is meant by "modular variety". Loosely speaking, such a variety is one which can be related to a Shimura variety in a reasonably direct way. For instance, a Shimura variety is a modular variety, as is the universal object or the r-fold fiber product of the universal object over a Shimura variety of PEL type. Examples include modular and Shimura curves, Kuga-Sato varieties, Hilbert modular varieties, Siegel modular varieties, Shimura varieties attached to the the orthogonal group $O(2,n)$ or the unitary group $U(p,q)$, etc. For the purposes of these lectures, the term "modular variety" is best interpreted informally in the broadest possible sense, as any variety whose cohomology is related to modular forms.

Chow-Heegner points. Modular varieties frequently contain a plentiful supply of arithmetically interesting algebraic cycles. The images in $E(\bar{\mathbb{Q}})$ of such special cycles under a modular parametrisation can be viewed as "higher-dimensional" analogues of Heegner points: they will be referred to as *Chow-Heegner points*.

The general program. Given an elliptic curve E, it would be of interest to construct modular parametrisations to E in the greatest possible generality, study their basic properties, and explore the relations (if any) between the resulting systems of Chow-Heegner points and values of L-series attached to E.

3 Generalised Heegner cycles

We flesh out the loosely formulated program of the previous paragraph in a simple but non-trivial setting, in which $E = A$ is an elliptic curve with complex multiplication by an imaginary quadratic field K, and V is a suitable family of $2r$-dimensional abelian varieties fibered over a modular curve. This construction (to which two of the lectures in the series ended up being devoted to) is part of a work in progress with Massimo Bertolini and Kartik Prasanna [BDP1], [BDP2].

The setting. Fix a quadratic imaginary field K, and let A be an elliptic curve with complex multiplication by the maximal order in K. In order to simplify the presentation of the main results, we make the following assumptions:

Assumption 3.1. *1. The field K has class number one, unit group of order two, and* *odd discriminant. This implies that* $D := -\operatorname{Disc}(K)$ *is one of the following* 6 *primes:*

$$D = 7, 11, 19, 43, 67, \text{ or } 163.$$

2. *The elliptic curve* A *is defined over* $\mathbb{Q}$ *and has conductor* D^2.

These assumptions are of course very restrictive; they are only made to ease the exposition, and the main results of [BDP1] and [BDP2] are obtained under more general conditions in which K is not assumed to have class number one.

Let $\epsilon_D : (\mathbb{Z}/D\mathbb{Z})^\times \longrightarrow \pm 1$ be the quadratic Dirichlet character of conductor D attached to K. Because A has complex multiplication, its modularity follows from the fact (known much before the work of Wiles, of course) that

$$L(A, s) = L(\psi, s),$$

where ψ is the Hecke character of K of infinity type $(1, 0)$ defined on (principal) ideals by the rule

$$\psi((a)) = \epsilon_D(a \bmod \sqrt{D})a.$$

The theta-series

$$\theta_\psi := \frac{1}{2}\sum_{a\in\mathcal{O}_K} \psi(a)q^{a\bar{a}} \in S_2(\Gamma_0(D^2)) \qquad (q = e^{2\pi i\tau})$$

is the weight two normalised eigenform of level D^2 attached to A.

Fix an integer $r \geq 0$, and consider the higher weight theta series

$$\theta_{\psi^{r+1}} := \frac{1}{2}\sum_{a\in\mathcal{O}_K} \psi(a)^{r+1}q^{a\bar{a}} = \sum_{n=1}^{\infty} a_n q^n \in \begin{cases} S_{r+2}(\Gamma_0(D^2)) \text{ if } r \text{ is even;} \\ S_{r+2}(\Gamma_0(D), \epsilon_K) \text{ if } r \text{ is odd.} \end{cases} \tag{8}$$

Set

$$\Gamma = \begin{cases} \Gamma_0(D) \text{ if } r \text{ is odd,} \\ \Gamma_0(D^2) \text{ if } r \text{ is even,} \end{cases}$$

and write C for the modular curve attached to Γ. Let W_r be the Kuga-Sato variety obtained by taking a canonical desingularisation of the r-fold fiber product

$$\mathcal{E} \times_C \mathcal{E} \times_C \cdots \times_C \mathcal{E}$$

of the universal (generalised) elliptic curve $\mathcal{E}$ over C. The locus $W_r^0 \subset W_r$ that lies over the open modular curve admits an explicit complex uniformisation

$$W_r^0(\mathbb{C}) = (\mathbb{Z}^{2r} \rtimes \Gamma)\backslash(\mathbb{C}^r \times \mathcal{H}).$$

The theta series $\theta_{\psi^{r+1}}$ has a geometric interpretation as a regular $(r+1)$-form on W_r given on $W_r^0(\mathbb{C})$ by

$$\omega_{\psi^{r+1}} = (2\pi i)^{r+1}\theta_{\psi^{r+1}}(\tau)dz_1 \cdots dz_r d\tau,$$

where $(z_1, \ldots, z_r, \tau)$ are the standard coordinates on $\mathbb{C}^r \times \mathcal{H}$. The q-expansion principle implies that

$$\omega_{\psi^{r+1}} \text{ belongs to } \Omega^{r+1}(W_r/\mathbb{Q}) = \mathrm{Fil}^{r+1} H^{r+1}_{\mathrm{dR}}(W_r/\mathbb{Q}).$$

The Deligne-Scholl motive associated to ψ^{r+1} corresponds to the piece of the $(r{+}1)$-st cohomology of W_r on which the nth Hecke correspondence T_n acts (for each n) as multiplication by the Fourier coefficient a_n of (8). It can be shown that the étale realisations of this motive are isomorphic to a specific piece of the middle cohomology of A^{r+1}:

$$H^{r+1}_{\mathrm{et}}(\bar{W}_r, \mathbb{Q}_p)^{\theta_{\psi^{r+1}}} = H^{r+1}_{\mathrm{et}}(\bar{A}^{r+1}, \mathbb{Q}_p)^{\psi^{r+1}}.$$

This isomorphism gives a non-trivial Tate cycle

$$\Pi_p \in H^{2r+2}(\overline{W_r \times A^{r+1}}, \mathbb{Q}_p)(r{+}1)^{G_{\mathbb{Q}}}.$$

The existence of this Tate cycle suggests the following conjecture which is the basis for the definition of Chow-Heegner points on A.

Conjecture 3.2. *There is an algebraic cycle class* $\Pi^? \in \mathrm{CH}^{r+1}(W_r \times A^{r+1})(K) \otimes \mathbb{Q}$ *satisfying*

$$\Pi^{?*}_{\mathrm{dR}}([\omega_A^{r+1}]) \sim [\omega_{\psi^{r+1}}], \qquad \Pi^{?*}_{\mathrm{dR}}([\omega_A^j \bar{\omega}_A^{r+1-j}]) = 0, \qquad \textit{for all } 1 \le j \le r,$$

where

$$\Pi^{?*}_{\mathrm{dR}} : H^{r+1}_{\mathrm{dR}}(A^{r+1}/\mathbb{C}) \longrightarrow H^{r+1}_{\mathrm{dR}}(W_r/\mathbb{C})$$

is the map on deRham cohomology induced by $\Pi^?$*, and the symbol* $\sim$ *denotes equality up to multiplication by a non-zero scalar of* $\mathbb{Q}^\times$*.*

Notice that the putative cycle $\Pi^?$ is also an element of $\mathrm{CH}^{r+1}(X_r \times A)$, where X_r is the $(2r{+}1)$-dimensional variety

$$X_r := W_r \times A^r.$$

Viewed in this way, the cycle $\Pi^?$ gives rise to a modular parametrisation

$$\Phi^? : \mathrm{CH}^{r+1}(X_r)_0 \longrightarrow A$$

defined over K. It is not hard to see that $\Phi^?$ is non-trivial. More precisely, a direct calculation reveals that

$$\Phi^{?*}_{\mathrm{dR}}(\omega_A) = \omega_{\psi^{r+1}} \wedge \eta_A^r, \tag{9}$$

where η_A is a suitably normalised class in $H^{0,1}_{\mathrm{dR}}(A/\mathbb{C})$. (The fact that A has complex multiplication implies that the class η_A can be chosen to belong to $H^1_{\mathrm{dR}}(A/K)$.)

Generalised Heegner cycles on X_r. The article [BDP1] introduces and studies a collection of null-homologous, r-dimensional algebraic cycles on X_r, referred to as *generalised Heegner cycles*. These cycles, which extend the notion of Heegner cycles on Kuga-Sato varieties considered in [Scho], [Ne] and [Zh], are indexed by isogenies $\varphi : A \longrightarrow A'$, and are defined over abelian extensions of K. The cycle Δ_φ attached to φ is essentially equal to the r-fold product of the graph of φ:

$$\Delta_\varphi := \epsilon_r(\mathrm{Graph}(\varphi)^r) \subset (A \times A')^r = (A')^r \times A^r \overset{(*)}{\subset} W_r \times A^r = X_r, \tag{10}$$

where the inclusion (*) arises by embedding $(A')^r$ in W_r as a fiber for the natural projection $W_r \longrightarrow C$. The projector ϵ_r that appears in (10) is a suitable idempotent in the ring of algebraic correspondences on X_r, which has the effect of making the cycle Δ_φ homologically trivial.

It can be shown, by adapting an argument of Schoen [Scho], that the cycles Δ_φ generate a subgroup of $\mathrm{CH}^{r+1}(X_r)_0(K^{\mathrm{ab}})$ of infinite rank. The conjectural map $\Phi^?_{K^{\mathrm{ab}}}$ sends these generalised Heegner cycles to points in $A(K^{\mathrm{ab}})$. The resulting collection

$$\{\Phi^?_{K^{\mathrm{ab}}}(\Delta_\varphi)\}_{\varphi: A \longrightarrow A'} \tag{11}$$

of Chow-Heegner points should generate an infinite rank subgroup of $A(K^{\mathrm{ab}})$, and should give rise to an "Euler system" in the sense of Kolyvagin. In the classical situation where $r = 0$, the variety X_r is just a modular curve and the existence of $\Pi^?$ follows from Faltings' proof of the Tate conjecture for curves. When $r \geq 1$, the very existence of the collection of Chow-Heegner points relies, ultimately, on producing the algebraic cycle $\Pi^?$ unconditionally.

Complex calculations. Since this is a workshop about explicit methods, we hasten to point out that even when the modular parametrisation $\Phi^?$ cannot be shown to exist, *it can still be computed efficiently in practice*, by complex analytic means.

The numerical calculation of $\Phi^?$ rests on the complex Abel-Jacobi map

$$\mathrm{AJ}_{X_r} : \mathrm{CH}^{r+1}(X_r)_0(\mathbb{C}) \longrightarrow \frac{\mathrm{Fil}^{r+1} H^{2r+1}_{\mathrm{dR}}(X_r/\mathbb{C})^{\mathrm{dual}}}{\mathrm{Im} H_{2r+1}(X_r(\mathbb{C}), \mathbb{Z})} \tag{12}$$

of Griffiths and Weil, which is defined by the rule:

$$\mathrm{AJ}_{X_r}(\Delta)(\omega) = \int_{\tilde{\Delta}} \omega, \qquad \text{(for any } (2r{+}1)\text{-chain } \tilde{\Delta} \text{ with } \partial\tilde{\Delta} = \Delta). \tag{13}$$

This is a natural generalisation of the usual Abel-Jacobi map for elliptic curves:

$$\mathrm{AJ}_A : A(\mathbb{C}) = \mathrm{CH}^1(A)_0(\mathbb{C}) \longrightarrow \frac{\Omega^1(A/\mathbb{C})^{\mathrm{dual}}}{\mathrm{Im} H_1(A(\mathbb{C}), \mathbb{Z})}, \tag{14}$$

which one recovers from (12) after replacing X_r by A and setting $r = 0$. The image of the Chow-Heegner point $\Phi^?(\Delta_\varphi)$ under the Abel-Jacobi map (14) is computed by noting that:

$$\mathrm{AJ}_A(\Phi^?(\Delta_\varphi))(\omega_A) = \mathrm{AJ}_{X_r}(\Delta_\varphi)(\Phi^{?*}_{\mathrm{dR}}(\omega_A)) = \mathrm{AJ}_{X_r}(\Delta_\varphi)(\omega_{\psi^{r+1}} \wedge \eta_A^r), \tag{15}$$

where the first equality follows from the functorial properties of the Abel-Jacobi maps, and the second follows from (9).

Let $N = D$ or D^2 (depending on whether r is odd or even) and let $\varphi : A \longrightarrow A'$ be an isogeny from A to some elliptic curve A'. Suppose that $A'(\mathbb{C})$ is described as $A' = \mathbb{C}/\langle 1, \tau\rangle$, and that $(A')^r$ is embedded in W_r as the fiber above the point of C corresponding to the pair $(\mathbb{C}/\langle 1, \tau\rangle, 1/N)$. Suppose also that

$$\varphi^*(2\pi i dz) = \omega_A,$$

where z is the standard coordinate on $\mathbb{C}/\langle 1, \tau\rangle = A'(\mathbb{C})$. The last expression in (15) can be calculated from the following proposition, which is established in [BDP1], Thm. 3.14:

Proposition 3.3. *Let $0 \le j \le r$ be an integer. For a complex isogeny φ as above, modulo the appropriate period lattice,*

$$\mathrm{AJ}_{X_r}(\Delta_\varphi)(\omega_{\theta_{\psi^{r+1}}} \wedge \omega_A^j \eta_A^{r-j}) = \frac{(-d_\varphi)^j (2\pi i)^{j+1}}{(\tau - \bar\tau)^{r-j}} \int_{i\infty}^{\tau} (z-\tau)^j (z - \bar\tau)^{r-j} \theta_{\psi^{r+1}}(z) dz.$$

Setting $j = 0$, we find that $\Phi^?_{\mathbb{C}} = \Phi_{\mathbb{C}}$, where

$$\Phi_{\mathbb{C}} : \mathrm{CH}^{r+1}(X_r)_0(\mathbb{C}) \longrightarrow A(\mathbb{C})$$

is given by the explicit formula

$$\Phi_{\mathbb{C}}(\Delta_\varphi) = \frac{2\pi i}{(\tau - \bar\tau)^r} \int_{i\infty}^{\tau} (z - \bar\tau)^r \theta_{\psi^{r+1}}(z) dz \pmod{\Lambda_A},$$

for an appropriate period lattice Λ_A attached to the elliptic curve A. Conjecture 3.2 on the existence of the modular parametrisation $\Phi^?$ implies the following explicit algebraicity statement:

Conjecture 3.4. *Let H be a subfield of K^{ab} and let $\Delta_\varphi \in \mathrm{CH}^{r+1}(X_r)_0(H)$ be a generalised Heegner cycle defined over H. Then (after fixing an an embedding of K^{ab} into $\mathbb{C}$),*

$$\Phi_{\mathbb{C}}(\Delta_\varphi) \text{ belongs to } A(H) \otimes \mathbb{Q},$$

and

$$\Phi_{\mathbb{C}}(\Delta_\varphi^\sigma) = \Phi_{\mathbb{C}}(\Delta_\varphi)^\sigma \quad \text{for all } \sigma \in \mathrm{Gal}(H/K).$$

While ostensibly weaker than Conjecture 3.2, Conjecture 3.4 has the virtue of being more readily amenable to experimental verification. A number of such verifications—which can be viewed as indirect numerical "tests" of the Tate conjectures for $W_r \times A^{r+1}$—are documented in [BDP2]. In these experiments, the complex points $\Phi_{\mathbb{C}}(\Delta_\varphi)$ attached to a few generalised Heegner cycles Δ_φ are calculated to high accuracy and recognized as algebraic points defined over the predicted class fields.

***p*-adic methods**. Aside from such numerical explorations, the main theoretical evidence for the existence of the modular parametrisation $\Phi^?$ arises from p-adic methods.

If F is any field, then the Abel-Jacobi map admits an analogue in étale cohomology:

$$\mathrm{AJ}_F^{\mathrm{et}} : \mathrm{CH}^{r+1}(X_r)_0(F) \longrightarrow H^1(F, H_{\mathrm{et}}^{2r+1}(\bar{X}_r, \mathbb{Q}_p)(r+1)). \tag{16}$$

The image of the conjectural algebraic cycle $\Pi^?$ under the étale cycle class map is a Tate cycle

$$\Pi_{\mathrm{et}} \in H_{\mathrm{et}}^{2r+2}(\overline{X_r \times A}, \mathbb{Q}_p)(r+1)^{G_{\mathbb{Q}}},$$

which in turn gives rise to a surjective, $G_{\mathbb{Q}}$-equivariant projection

$$\pi_r : H_{\mathrm{et}}^{2r+1}(\bar{X}_r, \mathbb{Q}_p)(r+1) \longrightarrow H_{\mathrm{et}}^1(\bar{A}, \mathbb{Q}_p)(1) = V_p(A).$$

Applying π_r to the target of (16) gives a map

$$\pi_r \circ \mathrm{AJ}_F^{\mathrm{et}} : \mathrm{CH}^{r+1}(X_r)_0(F) \longrightarrow H_{\mathrm{Sel}}^1(F, V_p(A)), \tag{17}$$

where $H_{\mathrm{Sel}}^1(F, V_p(A))$ is the pro-p *Selmer group* of A over F. This Selmer group consists cohomology classes whose restrictions to each completion F_v of F belongs to the image of the local connecting homomorphism

$$\delta_v : (\lim_{\leftarrow} A(F_v)/p^n A(F_v)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \longrightarrow H^1(F_v, V_p(A))$$

arising from the p-power descent exact sequence of Kummer theory for A over F_v. When F is a global field, this is the "usual" pro-p Selmer group of A over F, and when F is a local field of residue characteristic p, the $\mathbb{Q}_p$-vector space $H_{\mathrm{Sel}}^1(F, V_p(A))$ is identified with the Lie algebra $A^1(F) \otimes \mathbb{Q}_p$ of the p-adic Lie group $A(F)$.

Remark: The system $\{\mathrm{AJ}_{F_\varphi}^{\mathrm{et}}(\Delta_\varphi)\}_\varphi$ (as φ ranges over all isogenies from A, and F_φ is the field of definition of φ) is an infinite collection of global cohomology classes defined over finite abelian extensions of K, satisfying various norm compatibility and Selmer conditions. This collection obeys (a simple variant of) the axioms of an Euler system, as they are spelled out in [Ru] for example.

In the case where F is a finite extension of $\mathbb{Q}_p$, equation (17) can be used to define a p-adic parametrisation

$$\Phi_F := \pi_r \circ \mathrm{AJ}_F^{\mathrm{et}} : \mathrm{CH}^{r+1}(X_r)_0(F) \longrightarrow A(F) \otimes \mathbb{Q},$$

which is a p-adic counterpart of the map $\Phi_{\mathbb{C}}$, is defined *independently* of the Hodge or Tate conjectures, and agrees with $\Phi_F^?$ when the latter exists. The main theorem of [BDP2] is the following p-adic analogue of Conjecture 3.4, which shows that the images of generalised Heegner points under Φ_F have the expected algebraicity properties, and can be related to the L-series of A. Assume for simplicity that the integer r is odd.

Theorem 3.5. *Let $p = \mathfrak{p}\bar{\mathfrak{p}}$ be a rational prime which splits in $K/\mathbb{Q}$. Let $H \subset K^{ab}$ be a finite extension of $\mathbb{Q}$ which is unramified at p, let $\Delta \in \mathrm{CH}^{r+1}(X_r)_0(H)$ be a generalised Heegner cycle defined over this field, and let $H_{\mathfrak{p}} \supset H$ be the completion of H at a prime above $\mathfrak{p}$. Then*

$$\Phi_{H_{\mathfrak{p}}}(\Delta) \text{ belongs to } A(H) \otimes \mathbb{Q}.$$

In particular, the cycle $\Delta_1 \in \mathrm{CH}^{r+1}(X_r)_0(K)$ *attached to the identity isogeny* $1 : A \longrightarrow A$ *maps to a rational point on* $A(K) \otimes \mathbb{Q}$ *under* $\Phi_{K_{\mathfrak{p}}}$. *This point is of infinite order if and only if*

$$L(\psi^{2r+1}, r+1) \neq 0, \qquad \textit{and} \qquad L'(\psi, 1) \neq 0.$$

The idea of the proof of Theorem 3.5 is to express the local points $\Phi_{H_{\mathfrak{p}}}(\Delta_\varphi)$ in terms of special values of the p-adic L-functions studied in [BDP1] which are attached to the Rankin convolution of $\theta_{\psi^{r+1}}$ with Hecke characters of K. The resulting formulae for the local points $\Phi_F(\Delta_\varphi)$ (for F any p-adic field over which Δ_φ can be defined) allows one to *compare* these points for different values of r, and thereby reduce the case $r > 0$ of Theorem 3.5 to the case $r = 0$, where it follows from the Tate conjecture for curves proved by Faltings.

The very possibility of such a proof reveals that the Chow-Heegner points constructed in this setting are not *genuinely new*, since they can ultimately be related to CM points on modular curves. The set-up involving the CM elliptic curve A and the variety X_r—a simple but non-trivial "toy model" for the notion of Chow-Heegner points—is perhaps most noteworthy for bringing the Hodge and Tate conjectures, which are notoriously difficult to test numerically, a bit closer to the realm of "explicit methods".

4 ATR cycles

Of course, the hope is that higher-dimensional cycles will lead to points on E that cannot already be obtained by more classical approaches based on Heegner points. We will take a first step in this direction by considering certain *non-algebraic* cycles on Hilbert modular varieties.

The setting. Let F be a totally real field of degree $r+1$, and fix an ordering $v_0, v_1, \ldots, v_r$ of the r+1 distinct real embeddings of F. Let E be an elliptic curve over F, and let

$$E_j := E \otimes_{v_j} \mathbb{R} \qquad (0 \leq j \leq r)$$

be the r+1 elliptic curves over $\mathbb{R}$ obtained by taking the base change of E to $\mathbb{R}$ via the embedding v_j. To ease the exposition, we will make the following inessential assumptions:

1. The field F has narrow class number one;

2. the conductor of E/F is equal to 1 (i.e., E has everywhere good reduction).

Remark 4.1. These hypotheses, although very restrictive, are satisfied in some examples. For example, when $D = 29, 37$ and 41, the real quadratic field $F = \mathbb{Q}(\sqrt{D})$ has narrow class number one, and there is an elliptic curve E of conductor one over F. This elliptic curve cannot be defined over $\mathbb{Q}$, but it is isogenous to its Galois conjugate, and is a quotient of the Jacobian $J_1(D)$. The elliptic modular form thus associated to E belongs to $S_2(\Gamma_0(D), \epsilon_D)$, where ϵ_D is the quadratic Dirichlet character of conductor D attached to F.

In general, the modularity conjecture asserts that E gives rise to a *Hilbert modular form* f on $\mathbf{SL}_2(\mathcal{O}_F)$. Such a form is a holomorphic function on the product $\mathcal{H}_0 \times \mathcal{H}_1 \times \cdots \times \mathcal{H}_r$

of $r+1$ copies of the complex upper half plane, which is of parallel weight $(2,2,\ldots,2)$ under the action of the Hilbert modular group $\mathbf{SL}_2(\mathcal{O}_F)$. The latter group acts discretely on $\mathcal{H}_0\times\cdots\times\mathcal{H}_r$ by Möbius transformations via the embedding

$$(v_0,\ldots,v_r):\mathbf{SL}_2(\mathcal{O}_F)\longrightarrow\mathbf{SL}_2(\mathbb{R})^{r+1}.$$

Because of this trasformation property, the Hilbert modular form f can be interpreted geometrically as a holomorphic differential $(r+1)$-form on the complex analytic quotient

$$X(\mathbb{C}):=\mathbf{SL}_2(\mathcal{O}_F)\backslash(\mathcal{H}_0\times\mathcal{H}_1\times\cdots\times\mathcal{H}_r), \tag{18}$$

by setting

$$\omega_f^{\mathrm{hol}}:=(2\pi i)^{r+1}f(\tau_0,\ldots,\tau_r)d\tau_0\cdots d\tau_r.$$

This quotient in (18) is identified with the complex points of the (open) *Hilbert modular variety* X attached to $\mathbf{GL}(2)_{/F}$, but this algebraic structure will not be exploited in our construction of Stark-Heegner points attached to ATR cycles.

It will be useful to replace ω_f^{hol} by a closed, but non-holomorphic differential $(r+1)$-form ω_f on $X(\mathbb{C})$. When $r=1$, the differential ω_f is defined by choosing a unit $\epsilon\in\mathcal{O}_F^\times$ of norm -1 satisfying

$$\epsilon_0:=v_0(\epsilon)>0,\qquad \epsilon_1:=v_1(\epsilon)<0,$$

and setting

$$\omega_f=(2\pi i)^2\left(f(\tau_0,\tau_1)d\tau_0d\tau_1-f(\epsilon_0\tau_0,\epsilon_1\bar\tau_1)d\tau_0d\bar\tau_1\right).$$

For general r, one defines ω_f similarly, but this time summing over the subgroup of $\mathcal{O}_F^\times/(\mathcal{O}_F^+)^\times$ of cardinality 2^r consisting of units ϵ with $v_0(\epsilon)>0$. Note that the closed $(r+1)$-form ω_f is holomorphic in τ_0, but only harmonic in the remaining variables $\tau_1,\ldots,\tau_r$. The justification for working with ω_f rather than ω_f^{hol} lies in the following statement which is a reformulation of a conjecture of Oda [Oda].

Conjecture 4.2 (Oda). *Let*

$$\Lambda_f:=\left\{\int_\gamma\omega_f,\quad \gamma\in H_r(X(\mathbb{C}),\mathbb{Z})\right\}.$$

Then Λ_f is a lattice in $\mathbb{C}$ and the elliptic curve $\mathbb{C}/\Lambda_f$ is isogenous to E_0.

This conjecture is known to hold for Hilbert modular forms which are base change lifts of classical elliptic modular forms. For example, in the setting of Remark 4.1, the Hilbert modular form attached to E is the Doi-Naganuma lift of an elliptic modular form in $S_2(\Gamma_1(D),\epsilon_D)$ and Conjecture 4.2 is known to hold in this case.

Let

$$\mathcal{Z}_r(X(\mathbb{C})):=\left\{\begin{array}{c}\text{Null-homologous cycles}\\ \text{of real dimension } r\\ \text{on } X(\mathbb{C})\end{array}\right\}.$$

Conjecture 4.2 makes it possible to define an "Abel-Jacobi map"

$$\mathrm{AJ}_f:\mathcal{Z}_r(X(\mathbb{C}))\longrightarrow E_0(\mathbb{C}), \tag{19}$$

by choosing an isogeny $\iota : \mathbb{C}/\Lambda_f \longrightarrow E_0(\mathbb{C})$, and setting

$$\mathrm{AJ}_f(\Delta) := \iota\left(\int_{\tilde{\Delta}} \omega_f\right), \qquad \text{(for any } \tilde{\Delta} \text{ with } \partial\tilde{\Delta} = \Delta). \tag{20}$$

Note that the domain $\mathcal{Z}_r(X(\mathbb{C}))$ of AJ_f has no natural algebraic structure, and that the map AJ_f bears no obvious relation (beyond an analogy in its definition) with the Griffiths-Weil Abel-Jacobi map on the Hilbert modular variety X.

ATR Cycles. A quadratic extension K of F is called an ATR extension if

$$K \otimes_{F,v_0} \mathbb{R} \simeq \mathbb{C}, \qquad K \otimes_{F,v_j} \mathbb{R} \simeq \mathbb{R} \oplus \mathbb{R}, \ \ (1 \leq j \leq r).$$

The acronym ATR stands for "Almost Totally Real"; an ATR extension of F is "as far as possible" from being a CM extension, without being totally real.

Fix an ATR extension K of F, and let $\Psi : K \longrightarrow M_2(F)$ be an F-algebra embedding. Then

1. Since $K \otimes_{F,v_0} \mathbb{R} \simeq \mathbb{C}$, the torus $\Psi(K^\times)$ has a unique fixed point $\tau_0 \in \mathcal{H}_0$.
2. For each $1 \leq j \leq r$, the fact that $K \otimes_{F,v_j} \mathbb{R} \simeq \mathbb{R} \oplus \mathbb{R}$ shows that $\Psi(K^\times)$ has two fixed points τ_j and τ_j' on the boundary of $\mathcal{H}_j$. Let $\Upsilon_j \subset \mathcal{H}_j$ be the hyperbolic geodesic joining τ_j to τ_j'.

An embedding $\Psi : K \longrightarrow M_2(F)$ has a *conductor*, which is defined to be the unique $\mathcal{O}_F$-ideal c_Ψ for which

$$\Psi(K) \cap M_2(\mathcal{O}_F) = \Psi(\mathcal{O}_F + c_\Psi \mathcal{O}_K).$$

The $\mathcal{O}_F$-order $\mathcal{O}_\Psi := \mathcal{O}_F + c_\Psi \mathcal{O}_K$ is called the *order associated to* Ψ. By the Dirichlet unit theorem, the group

$$\Gamma_\Psi := \Psi((\mathcal{O}_\Psi^+)^\times) \subset \mathbf{SL}_2(\mathcal{O}_F)$$

is of rank r and preserves the region

$$R_\Psi := \{\tau_0\} \times \Upsilon_1 \times \cdots \times \Upsilon_r.$$

The ATR cycle associated to the embedding Ψ is defined to be the quotient

$$\Delta_\Psi := \Gamma_\Psi \backslash R_\Psi.$$

It is a closed cycle on $X(\mathbb{C})$ which is topologically isomorphic to an r-dimensional real torus. In many cases, one can show that Δ_Ψ is null-homologous, at least after tensoring with $\mathbb{Q}$. (This is the case, for instance, when $r = 1$, and it follows from the fact that the group cohomology $H^r(\mathbf{SL}_2(\mathcal{O}_F), \mathbb{C})$ is trivial.) Assume from now on that Δ_Ψ is homologically trivial, and therefore that it belongs to $\mathcal{Z}_r(X(\mathbb{C}))$.

The following conjecture lends arithmetic meaning to the Abel-Jacobi map AJ_f and to the ATR cycles Δ_Ψ.

Conjecture 4.3. *Let $\Psi : K \longrightarrow M_2(F)$ be an F-algebra embedding of an ATR extension K of F. Then the complex point $\mathrm{AJ}_f(\Delta_\Psi) \in E_0(\mathbb{C})$ is algebraic. More precisely, the isogeny ι in the definition (20) of AJ_f can be chosen so that, for all Ψ,*

$$\mathrm{AJ}_f(\Delta_\Psi) \text{ belongs to } E(H_{c_\Psi}),$$

where H_{c_Ψ} is the ring class field of K of conductor c_Ψ.

This conjecture has been tested numerically in [DL], for the three elliptic curves mentionned in Remark 4.1. A key ingredient in [DL] is the formulation of an efficient algorithm for calculating AJ_f numerically. This algorithm relies on group cohomology, and involves the manipulation of certain $(r+1)$-cochains on Γ which are defined by integrating ω_f over appropriate regions. The algorithm described in [DL] also exploits the fact that the real quadratic field $K = \mathbb{Q}(\sqrt{D})$ for $D = 29, 37$, and 41, is Euclidean. It would be of interest to have algorithms to calculate AJ_f in more general settings, particularly in cases where $r > 1$.

Conjecture 4.3 is poorly understood at present. For instance, it is not clear whether the Tate conjecture sheds any light on it. On the positive side, the ATR points that are produced by Conjecture 4.3 are "genuinely new" and go beyond what can be obtained using only CM points on Shimura curves. Indeed, the former are defined over abelian extensions of ATR extensions of totally real fields, while the latter are defined over abelian extensions of CM fields.

5 Real quadratic cycles on $\mathbf{SL}_2(\mathbb{Z}[1/p])\backslash(\mathcal{H}_p \times \mathcal{H})$

The construction based on ATR cycles fails to cover some of the most basic settings where a modular construction might be expected to exist. The simplest non-trivial such setting arises when E is an elliptic curve over $\mathbb{Q}$ of prime conductor p, and K is a *real* quadratic field in which p is inert. In that case, a study of signs in functional equations reveals that

$$\mathrm{ord}_{s=1} L(E/H, s) \geq [H : K],$$

for any abelian extension H of K which is unramified at p and for which $\mathrm{Gal}(H/K)$ is isomorphic to a (generalised) dihedral group. (See the discussion in the introduction of [Da01] for example.) The Birch and Swinnerton-Dyer conjecture therefore predicts that

$$\mathrm{rank}(E(H)) \stackrel{?}{\geq} [H : K].$$

It is natural to ask whether this predicted systematic growth in Mordell-Weil rank can be accounted for by a modular construction.

Such a modular construction does appear to exist. It rests on the formal analogy between the Hilbert modular surface $\mathbf{SL}_2(\mathcal{O}_F)\backslash(\mathcal{H}_0 \times \mathcal{H}_1)$ (corresponding to the case $r = 1$ of the ATR construction described in the previous paragraph) and the quotient

$$\mathbf{SL}_2(\mathbb{Z}[1/p])\backslash(\mathcal{H}_p \times \mathcal{H}),$$

where $\mathcal{H}_p := \mathbf{P}_1(\mathbb{C}_p) - \mathbf{P}_1(\mathbb{Q}_p)$ is the p-adic upper half plane. Some of the terms that make up the analogy are listed in the table below.

ATR cycles	Real quadratic cycles
F real quadratic	$\mathbb{Q}$
v_0, v_1	p, ∞
Elliptic curve E/F of conductor 1	Elliptic curve $E/\mathbb{Q}$ of conductor p
$\mathbf{SL}_2(\mathcal{O}_F)\backslash(\mathcal{H}_0 \times \mathcal{H}_1)$	$\mathbf{SL}_2(\mathbb{Z}[1/p])\backslash(\mathcal{H}_p \times \mathcal{H})$
K/F ATR	$K/\mathbb{Q}$ real quadratic, with p inert
$\Psi : K \longrightarrow M_2(F)$	$\Psi : K \longrightarrow M_2(\mathbb{Q})$
$\langle\gamma\rangle := \Psi((\mathcal{O}_\Psi^+)^\times)$	$\langle\gamma\rangle := \Psi((\mathcal{O}_\Psi^+)^\times)$
$\Delta_\Psi = \{\tau_0\} \times (\Upsilon_1/\gamma), \quad \tau \in \mathcal{H}_0$	$\Delta_\Psi = \{\tau\} \times (\Upsilon_1/\gamma), \quad \tau \in \mathcal{H}_p.$
$\Downarrow \mathrm{AJ}_f$	$\Downarrow \mathrm{AJ}_f^{(p)}$
Points in $\mathbb{C}/\Lambda_f = E_0(\mathbb{C})$, defined over abelian extensions of K	Points in $K_p^\times/q^{\mathbb{Z}} = E(K_p)$, defined over abelian extensions of K.

The "real quadratic cycles" Δ_Ψ in $\mathbf{SL}_2(\mathbb{Z}[1/p])\backslash(\mathcal{H}_p \times \mathcal{H})$ are topologically isomorphic to $\mathbb{R}/\mathbb{Z}$, and $\mathrm{AJ}_f^{(p)}(\Delta_\Psi)$ belongs to $K_p^\times/q^{\mathbb{Z}} = E(K_p)$, where $q \in \mathbb{Q}_p^\times$ is the p-adic Tate period of E. Since the symmetric space $\mathcal{H}_p \times \mathcal{H}$ mixes a rigid analytic topology on the first factor with a complex analytic topology on the second, one cannot define $\mathrm{AJ}_f^{(p)}$ by directly integrating an appropriate differential on a two-dimensional region having Δ_Ψ as boundary, as in equation (20) defining AJ_f. The main steps that make it possible to define the p-adic analogue of AJ_f are:

1. To reinterpret the elliptic modular form $f \in S_2(\Gamma_0(p))$ attached to E as a "mock Hilbert modular form" on $\mathbf{SL}_2(\mathbb{Z}[1/p])\backslash\mathcal{H}_p \times \mathcal{H}$. This reinterpretation gives a precise meaning to certain 2-cochains on Γ with values in $\mathbb{C}_p^\times$ which are the direct p-adic analogues of the corresponding cochains considered in the *ATR* setting in the algorithms of [DL].

2. With these cochains in hand, the algorithms of [DL] can be precisely mimicked, yielding invariants $\mathrm{AJ}_f^{(p)}(\Delta_\Psi) \in K_p^\times/q^{\mathbb{Z}}$.

For more details on this construction, and the precise definition of $\mathrm{AJ}_f^{(p)}$, see [Da01], [Da04]. The article [DP] describes the most efficient algorithms for computing the Stark-Heegner points $\mathrm{AJ}_f^{(p)}(\Delta_\Psi)$ attached to real quadratic fields. These algorithms have been implemented in MAGMA and can be downloaded from the web site

http://www.math.mcgill.ca/darmon/programs/shp/shp.html

References

[BCDT] Breuil, C., Conrad, B., Diamond, F., and Taylor, R., *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild 3-adic exercises.* J. Amer. Math. Soc. 14 (2001), no. 4, 843–939.

[BDG] Bertolini, M., Darmon, H., and Green, P. *Periods and points attached to quadratic algebras*. Heegner points and Rankin L-series, 323–367, Math. Sci. Res. Inst. Publ., 49, Cambridge Univ. Press, Cambridge, 2004.

[BDP1] Bertolini, M., Darmon, H., and Prasanna, K. *Generalised Heegner cycles and p-adic Rankin L-series*, submitted.

[BDP2] Bertolini, M., Darmon, H., and Prasanna, K., *Chow-Heegner points on CM elliptic curves and values of p-adic L-series*, in progress.

[CD] Charollois, P., Darmon, H. *Arguments des unités de Stark et périodes de séries d'Eisenstein*. Algebra Number Theory 2 (2008), no. 6, 655–688.

[Da01] Darmon, H., *Integration on $\mathcal{H}_p \times \mathcal{H}$ and arithmetic applications*. Ann. of Math. (2) 154 (2001), no. 3, 589–639.

[Da04] Darmon, H. Rational points on modular elliptic curves. CBMS Regional Conference Series in Mathematics, 101. Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 2004. xii+129 pp.

[Da06] Darmon, H., *Heegner points, Stark-Heegner points, and values of L-series*. International Congress of Mathematicians. Vol. II, 313–345, Eur. Math. Soc., Zürich, 2006.

[DG] Darmon, H., Green, P. Elliptic curves and class fields of real quadratic fields: algorithms and evidence. Experiment. Math. 11 (2002), no. 1, 37–55.

[DL] Darmon, H. and Logan, A. *Periods of Hilbert modular forms and rational points on elliptic curves*. Int. Math. Res. Not. 2003, no. 40, 2153–2180.

[DP] Darmon, H., Pollack, R. *Efficient calculation of Stark-Heegner points via overconvergent modular symbols*. Israel J. Math. 153 (2006), 319–354.

[Gre] Greenberg, Matthew. *Stark-Heegner points and the cohomology of quaternionic Shimura varieties*. Duke Math. J. 147 (2009), no. 3, 541–575.

[Gr2] Gross, B.H., *Kolyvagin's work on modular elliptic curves*. in L-functions and arithmetic (Durham, 1989), 235–256, London Math. Soc. Lecture Note Ser., 153, Cambridge Univ. Press, Cambridge, 1991.

[GZ] Gross, Benedict H. and Zagier, Don B. *Heegner points and derivatives of L-series*. Invent. Math. 84 (1986), no. 2, 225–320.

[Ne] Nekovar, Jan. *On the p-adic height of Heegner cycles*. Math. Ann. 302 (1995), no. 4, 609–686.

[Oda] Oda, Takayuki. Periods of Hilbert modular surfaces. Progress in Mathematics, 19. Birkhuser, Boston, Mass., 1982.

[Ru] Rubin, K., Euler systems. Annals of Mathematics Studies, 147. Hermann Weyl Lectures. The Institute for Advanced Study. Princeton University Press, Princeton, NJ, 2000. xii+227 pp.

[Scho] Schoen, Chad. *Complex multiplication cycles on elliptic modular threefolds*. Duke Math. J. 53 (1986), no. 3, 771–794.

[Tr] Trifkovic, M., *Stark-Heegner points on elliptic curves defined over imaginary quadratic fields*, Duke Math. J. 135 (2006), no. 3, 415–453.

[TW] Taylor, Richard; Wiles, Andrew Ring-theoretic properties of certain Hecke algebras. Ann. of Math. (2) 141 (1995), no. 3, 553–572.

[Wi] Wiles, A., *Modular elliptic curves and Fermat's last theorem*. Ann. of Math. (2) 141 (1995), no. 3, 443–551.

[Zh] Zhang, Shouwu. *Heights of Heegner cycles and derivatives of L-series*. Invent. Math. 130 (1997), no. 1, 99–152.