Workshop on Number Theory with a view towards Transcendence and Diophantine Approximation

In honor of
Michel Waldschmidt

University of Ottawa, Ottawa

June 2013

Stark-Heegner points

Henri Darmon

McGill University, Montreal

June 9, 2013

Remarks on transcendence

Given a real or p-adic number α, defined analytically (as the limit of a sequence, infinite series, integral, etc.)

$$\text{e.g.,,} \quad \alpha = \pi, \quad e, \quad e^{\pi}, \quad \zeta(3), \quad \sum_{n=1}^{\infty} \frac{1}{2^{n!}}, \quad \int_0^1 \frac{dt}{\sqrt{t^3 - t}},$$

one may try to

1. show that α is transcendental;
2. show that α is algebraic.

Some motivation is required to pursue direction 2: a real or p-adic number is *unlikely* to be algebraic, unless there is a "good reason".

Theme of this talk: Some instances of problem 2 related to Complex Multiplication and eventual generalisations.

An illustration of problem 2

Let K be a finite unramified extension of $\mathbb{Q}_2$ of degree $d > 2$, and let $a \in \mathcal{O}_K$ be an element satisfying $a \equiv 1 \pmod 4$. Consider the sequence defined inductively by

$$a_0 = a, \qquad a_{n+1} = \frac{1 + a_n}{2\sqrt{a_n}}.$$

Fact: The subsequence $(a_{nd})_n$ converges to a limit, $a_\infty \in K$. This limit is algebraic. More precisely, a_∞^2 belongs to a ring class field of some imaginary quadratic field.

Underlying reason: Elliptic curves, Serre-Tate canonical lifts, 2-adic AGM, Complex Multiplication, ...

Explicit class field theory

Theorem (Kronecker-Weber)

The values of the function $e^{2\pi iz}$ at rational arguments are algebraic, and generate the maximal abelian extension of $\mathbb{Q}$.

Theorem (Kronecker)

Let K be a quadratic imaginary field, and let $\mathcal{H}$ be the Poincaré upper half plane. The values $j(\tau)$, for $\tau \in K \cap \mathcal{H}$, are algebraic. More precisely they belong to abelian extensions of $\mathbb{Q}$.

Explicit class field theory

> *Finally, the extension of Kronecker's theorem to the case that, in place of the realm of rational numbers or of the imaginary quadratic field, any algebraic field whatever is laid down as realm of rationality, seems to me of the greatest importance. I regard this problem as one of the most profound and far reaching in the theory of numbers and of functions.* (Hilbert, Paris ICM, 1900)

Simplest case: What object plays the role of $j(z)$ if K is a *real quadratic field*?

Modular parametrisations

Let E be an elliptic curve over $\mathbb{Q}$, of conductor N.

Theorem (Wiles)

There is a non-constant analytic map

$$j_E : \Gamma_0(N)\backslash\mathcal{H} \longrightarrow E(\mathbb{C}).$$

Explicit formula for j_E:

$$L(E,s) =: \sum_{n=1}^{\infty} a_n n^{-s}, \qquad \omega_E := \sum_{n=1}^{\infty} a_n e^{2\pi i n z} dz \in \Omega^1(\Gamma_0(N)\backslash\mathcal{H}).$$

$$j_E(\tau) = \int_{i\infty}^{\tau} \omega_E = \sum_{n=1}^{\infty} \frac{a_n}{n} e^{2\pi i n\tau} \in \mathbb{C}/\Lambda_E = E(\mathbb{C}).$$

Complex multiplication points

Theorem

Let K be an imaginary quadratic field. If $\tau \in K \cap \mathcal{H}$, then $j_E(\tau)$ is an algebraic point *on E, defined over a class field of K.*

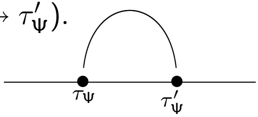
The points $j_E(\tau)$ are called *CM points* attached to K, or *Heegner points*.

The Stark-Heegner points of the title are conjectural generalisations of these points when K is replaced by a real quadratic field.

Quadratic cycles

Let $\Psi : K \hookrightarrow M_2(\mathbb{Q})$ be an embedding of a quadratic field (either imaginary, or real).

1. If K is imaginary, $\tau_\Psi :=$ fixed point of $\Psi(K^\times) \circlearrowleft \mathcal{H}$; $\Delta_\Psi := \{\tau_\Psi\}$.
2. If K is real, $\tau_\Psi, \tau'_\Psi :=$ fixed points of $\Psi(K^\times) \circlearrowleft (\mathcal{H} \cup \mathbb{R})$; $\Upsilon_\Psi = \mathrm{geodesic}(\tau_\Psi \to \tau'_\Psi)$.



$$\Delta_\Psi = \langle \Psi(\mathcal{O}_K^\times) \rangle \backslash \Upsilon_\Psi \simeq (\mathbb{R}/\mathbb{Z}) \subset \Gamma_0(N) \backslash \mathcal{H}.$$

Digression: elliptic curves over totally real fields

Let F be a totally real field of degree n,

$$v_1, \ldots, v_n : F \longrightarrow \mathbb{R}; \qquad \mathbf{SL}_2(\mathcal{O}_F) \circlearrowleft \mathcal{H}^n.$$

E an elliptic curve over F of conductor 1 (to simplify notations);

Definition

The elliptic curve E/F is *modular* if there is a Hilbert modular form $G \in S_2(\mathbf{SL}_2(\mathcal{O}_F))$ over F such that

$$L(E/F, s) = L(G, s).$$

Modularity is often known, and will be assumed from now on.

Geometric meaning of modularity

Geometrically, the Hilbert modular form G corresponds to a (2^n-dimensional) subspace

$$\Omega_G \subset \Omega^n_{\mathrm{har}}(\mathbf{SL}_2(\mathcal{O}_F)\backslash\mathcal{H}^n).$$

Goal: Produce algebraic points on $P \in E(\bar{F})$ by an analytic recipe involving integration of the harmonic n-forms in Ω_G.

ATR cycles

Definition. A quadratic extension K/F is called an *ATR extension* if all but exactly one of the real places of F are real in K/F:

$$\tilde{v}_1 : K \longrightarrow \mathbb{C}, \qquad \tilde{v}_2, \dots, \tilde{v}_n : K \longrightarrow \mathbb{R}.$$

ATR cycles: To each F-algebra embedding

$$\Psi : K \longrightarrow M_2(F),$$

we will attach a topological cycle

$$\Delta_\Psi \subset \mathbf{SL}_2(\mathcal{O}_F)\backslash\mathcal{H}^n$$

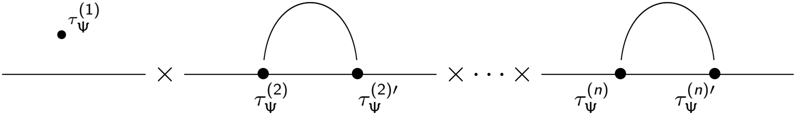
of real dimension $n-1$ which is analogous to a real quadratic cycle, but "behaves like a Heegner point".

ATR cycles

$\tau_\Psi^{(1)} :=$ fixed point of $\Psi(K^\times) \circlearrowleft \mathcal{H}_1$;

$2 \le j \le n$: $\tau_\Psi^{(j)}, \tau_\Psi^{(j)\prime} :=$ fixed points of $\Psi(K^\times) \circlearrowleft (\mathcal{H}_j \cup \mathbb{R})$;

$\Upsilon_\Psi = \{\tau_\Psi^{(1)}\} \times \mathrm{geodesic}(\tau_\Psi^{(2)} \to \tau_\Psi^{(2)\prime}) \times \cdots \times \mathrm{geodesic}(\tau_\Psi^{(n)} \to \tau_\Psi^{(n)\prime})$.



$$\Delta_\Psi = \Upsilon_\Psi / \langle \Psi(\mathcal{O}_K^\times) \rangle \simeq (\mathbb{R}/\mathbb{Z})^{n-1} \subset \mathbf{SL}_2(\mathcal{O}_F) \backslash \mathcal{H}^n.$$

Key fact: The cycles Δ_Ψ are *null-homologous*.

Stark-Heegner Points attached to ATR cycles

Abel-Jacobi map: Choose an n-form $\omega_G \in \Omega_G$,

$$P_{\Psi}^{?}(\omega_G) := \int_{\partial^{-1}\Delta_{\Psi}} \omega_G \quad \in \quad \mathbb{C}/\Lambda_G.$$

Conjecture (Oda,1982)

For a suitable choice of ω_G, we have $\mathbb{C}/\Lambda_G \sim E(\mathbb{C})$. In particular $P_{\Psi}^{?}(\omega_G)$ can then be viewed as a point in $E(\mathbb{C})$.

Conjecture (Logan, D, 2003)

The points $P_{\Psi}^{?}(\omega_G)$ are algebraic, and belong to $E(K^{\mathrm{ab}})$.

They are called *Stark-Heegner points* attached to ATR cycles.

Numerical evidence (Xavier Guitart, Marc Masdeu)

$F = \mathbb{Q}(\omega), \qquad \omega = \frac{1+\sqrt{509}}{2};$

$E : y^2 - xy - \omega y = x^3 + (2 + 2\omega)x^2 + (162 + 3\omega)x + (71 + 34\omega);$

$K = F(\sqrt{98577 + 9144\omega}).$

For suitable (well-chosen) embeddings $\Psi_1, \Psi_2 : \mathcal{O}_K \longrightarrow M_2(\mathcal{O}_F)$,

$$P_{\Psi_1}(\omega_G) + P_{\psi_2}(\omega_G) \stackrel{?}{=} 4\left(\omega + 17, \frac{17}{2} + \omega + \frac{\sqrt{98577 + 9144\omega}}{2}\right).$$

This identity was verified to many decimal digits of accuracy.

A critique of the ATR setting

1. Like the original Stark conjectures, the conjecture on "Stark-Heegner points attached to ATR cycles" seems to lie very deep; we lack (to the speaker's understanding!) theoretical tools with which to tackle it.

2. The ATR setting is somewhat recundite, and does not capture the more natural "simplest setting" of elliptic curves over $\mathbb{Q}$, and class fields of real quadratic fields.

Back to "Heegner points attached to real quadratic fields"

Simplest setting:

$E/\mathbb{Q}$ is an elliptic curve of prime conductor p;

K is a real quadratic field in which the prime p is inert.

$$\mathcal{H}_p = \mathbb{P}_1(\mathbb{C}_p) - \mathbb{P}_1(\mathbb{Q}_p),$$

$$\mathbf{SL}_2(Z[1/p]) \circlearrowleft \mathcal{H}_p \times \mathcal{H}.$$

A dictionary between the two settings

ATR cycles ($n = 2$)	Real quadratic points
F real quadratic	$\mathbb{Q}$
∞_0, ∞_1	p, ∞
E/F of conductor 1	$E/\mathbb{Q}$ of conductor p
$\mathbf{SL}_2(\mathcal{O}_F)\backslash(\mathcal{H} \times \mathcal{H})$	$\mathbf{SL}_2(\mathbb{Z}[1/p])\backslash(\mathcal{H}_p \times \mathcal{H})$
K/F ATR	$K/\mathbb{Q}$ real quadratic, with p inert
ATR cycles $\Delta_\Psi \simeq (\mathbb{R}/\mathbb{Z}) \subset \mathbf{SL}_2(\mathcal{O}_F)\backslash(\mathcal{H} \times \mathcal{H})$	Cycles $\Delta_\Psi \simeq (\mathbb{R}/\mathbb{Z}) \subset \mathbf{SL}_2(\mathbb{Z}[1/p])\backslash(\mathcal{H}_p \times \mathcal{H})$

A dictionary between the two settings

One can develop the notions in the right-hand column to the extent of

1. Attaching to $f \in S_2(\Gamma_0(p))$ a "Hilbert modular form" G on $\mathbf{SL}_2(\mathbb{Z}[1/p])\backslash(\mathcal{H}_p \times \mathcal{H})$.
2. Making sense of the expression

$$\int_{\partial^{-1}\Delta_\Psi} \omega_G \quad \in \quad K_p^\times/q^{\mathbb{Z}} = E(K_p)$$

   for any real quadratic cycle Δ_Ψ on $\mathcal{H}_p \times \mathcal{H}$.

The resulting local points are defined (*conjecturally*) over ring class fields of K. They are called "Stark-Heegner points attached to cycles on $\mathcal{H}_p \times \mathcal{H}$".

p-adic versus ATR Stark-Heegner points

The fact that Stark-Heegner points arising from cycles on $\mathcal{H}_p \times \mathcal{H}$ involve a mixture of complex and p-adic integration makes them appear somewhat more exotic than their ATR counterparts.

On the other hand, p-adic variants of the Stark conjecture seem more tractable than the complex conjectures, thanks to the possibility of attacking them using powerful tools based on *p-adic variation* of motives and congruences between modular forms.

The p-adic Gross-Stark conjecture

New cases of the p-adic Gross-Stark conjecture:

Samit Dasgupta, Robert Pollack, HD, *Hilbert modular forms and the Gross-Stark conjecture*, Annals of Math. (2) 174 (2011),

proved by exploiting ideas used by Wiles to prove the Iwasawa Main Conjecture for totally real fields.

Recent work (joint with Victor Rotger) suggests that likewise, the algebraicity of the Stark-Heegner points arising from cycles on $\mathcal{H}_p \times \mathcal{H}$ may be *more tractable* than the analogous problem for ATR cycles.

The approach followed here is guided by the seminal ideas of Kato and Perrin-Riou on Euler systems and p-adic Hodge theory.

Heegner points and the BSD conjecture

Theorem (Gross-Zagier (1985), Kolyvagin (1987))

Let E be a (modular) elliptic curve over $\mathbb{Q}$. If $\mathrm{ord}_{s=1} L(E/K, s) \leq 1$, then $Ш(E/K)$ is finite, and

$$\mathrm{rank}(E(K)) = \mathrm{ord}_{s=1} L(E/K, s).$$

This result is still the best theoretical evidence for the BSD conjecture.

Key ingredient in the proof: the collection of Heegner points which is used to mediate between $L(E/K, s)$ (via the theorem of Gross-Zagier) and the arithmetic of E/K (via the theorem of Kolyvagin).

Heegner points and the BSD conjecture

Theorem (Bertolini, D, Nekovar, Rotger, Seveso, Vigni, Zhang, ...)

Let χ be a ring class character of K. If $\mathrm{ord}_{s=1} L(E/K, \chi, s) \leq 1$, then

$$\dim_{\mathbb{C}}(E(H_\chi) \otimes \mathbb{C})^\chi = \mathrm{ord}_{s=1} L(E/K, \chi, s),$$

as predicted by a natural Galois-equivariant refinement of the BSD conjecture.

This theorem has been proved in gradually increasing generality, over the last 20 or so years.

Until very recently, Heegner points supplied the *only available approach* to proving this result, when χ is non-quadratic.

A conditional result

Theorem (Bertolini, Dasgupta, D, 2006)

Assume that the Stark-Heegner points attached to real quadratic cycles on $\mathcal{H}_p \times \mathcal{H}$ enjoy the predicted algebraicity properties. Let χ be a ring class character of a real quadratic *$F/\mathbb{Q}$. If $L(E/F, \chi, s) \neq 0$, then*

$$\dim_{\mathbb{C}}(E(H_\chi) \otimes \mathbb{C})^\chi = 0,$$

as predicted by a natural Galois-equivariant refinement of the BSD conjecture.

One thus has a (not so surprising, in light of Kolyvagin's work) arithmetic application of Stark-Heegner points to the Birch and Swinnerton-Dyer conjecture over ring class fields of real quadratic fields.

This result is now unconditional!

Theorem (Victor Rotger, D)

Let χ be a ring class character of a real quadratic $F/\mathbb{Q}$*. If $L(E/F, \chi, s) \neq 0$, then*

$$\dim_{\mathbb{C}}(E(H_\chi) \otimes \mathbb{C})^\chi = 0,$$

as predicted by a natural Galois-equivariant refinement of the BSD conjecture.

The methods used to prove this theorem *completely avoid* the conjectural Stark-Hegner points.

We hope that they will, eventually, give information about the global properties of these mysterious objects, which are defined *purely analytically*.

A more general result

Theorem (Victor Rotger, D)

Let $E/\mathbb{Q}$ be an elliptic curve, and let ρ_1 and ρ_2 be odd, irreducible, two-dimensional Artin representations of $\mathbb{Q}$, satisfying

$$\det(\rho_1) = \chi, \qquad \det(\rho_2) = \chi^{-1}.$$

If $L(E, \rho_1 \otimes \rho_2, 1) \neq 0$, then

$$\dim_{\mathbb{C}} \hom_{G_{\mathbb{Q}}}(V_{\rho_1} \otimes V_{\rho_2}, E(K_{\rho_1 \otimes \rho_2}) \otimes \mathbb{C}) = 1.$$

If $\rho_1 = \mathrm{Ind}_F^{\mathbb{Q}} \chi_1$, $\rho_2 = \mathrm{Ind}_F^{\mathbb{Q}} \chi_2$, then

$$(\mathrm{Ind}_F^{\mathbb{Q}} \chi_1) \otimes (\mathrm{Ind}_F^{\mathbb{Q}} \chi_2) = (\mathrm{Ind}_F^{\mathbb{Q}} \psi_1) \oplus (\mathrm{Ind}_F^{\mathbb{Q}} \psi_2),$$

where $\psi_1 = \chi_1\chi_2, \quad \psi_2 = \chi_1\chi_2'$.

Gross-Kudla-Schoen diagonal cycles

The *Gross-Kudla-Schoen* cycle:

$$\Delta = X_0(N) \subset X_0(N)^3, \qquad \Delta \in \mathrm{CH}^2(X_0(N)^3)_0,$$

modified in a simple way so as to become null-homologous.

The p-adic étale Abel-Jacobi map:

$$\begin{aligned} \mathrm{AJ}_{\mathrm{et}} : \mathrm{CH}^2(X_0(N)^3) &\longrightarrow H^1(\mathbb{Q}, H^3_{\mathrm{et}}(X_0(N)^3_{\bar{\mathbb{Q}}}, \mathbb{Z}_p)(2)) \\ &\longrightarrow H^1(\mathbb{Q}, V_f \otimes V_g \otimes V_h(2)), \end{aligned}$$

V_f, V_g and V_h: Deligne-Serre representations attached to weight two forms f, g, and h.

The BSD cohomology class

We have global cohomology classes

$$\kappa(f, g, h) := \mathrm{AJ}_{\mathrm{et}}(\Delta) \in H^1(\mathbb{Q}, V_f \otimes V_g \otimes V_h(2)),$$

indexed by triples of modular forms (f, g, h) of weight two.

For the application to the BSD conjecture, one rather needs to construct global classes with values in $V_f \otimes V_{g_1} \otimes V_{h_1}$, where

f is a form of weight two, attached to an elliptic curve;

g_1 and h_1 are forms of weight one, attached to Artin representations ρ_{g_1} and ρ_{h_1}.

The theme of p-adic variation

Basic idea:

1. p-adically interpolate the classes $\kappa(f, g, h)$ as g and h vary over the weight two specialisations of suitable Hida families specialising to g_1 and h_1 in weight one.

2. Study the weight one specialisation $\kappa(f, g_1, h_1)$ of the resulting family, and relate its *local behaviour at p* to the central critical value $L(E, \rho_{g_1} \otimes \rho_{h_1}, 1)$.

The global reciprocity law

The following result is the technical core of the proof:

Theorem (Rotger, D)

The class $\kappa(f, g_1, h_1)$ is cristalline at p if and only if $L(E, \rho_{g_1} \otimes \rho_{h_1}, 1) \neq 0$.

When $L(E, \rho_{g_1} \otimes \rho_{h_1}, 1) \neq 0$, the ramified classes $\kappa(f, g_1, h_1)$ can be used to bound the associated Selmer group, by the standard "Euler system approach" exploiting local and global Tate duality.

The global classes $\kappa(f, g_1, h_1)$ obtained by p-adically deforming the p-adic étale Abel-Jacobi images of diagonal cycle classes, are the objects which play the role of the (Kummer images of) Heegner points in Kolyvagin's original argument.

A question

Question: When ρ_{g_1} and ρ_{h_1} are induced from characters χ_1 and χ_2 of the same real quadratic field F, can one relate the *global* cohomology class

$$\kappa(f, g_1, h_1) \in H^1(\mathbb{Q}, V_p(E) \otimes (\mathrm{Ind}_F^{\mathbb{Q}} \psi_1)) \oplus H^1(\mathbb{Q}, V_p(E) \otimes (\mathrm{Ind}_F^{\mathbb{Q}} \psi_2))$$

to the Stark-Heegner points attached to cycles on $\mathcal{H}_p \times \mathcal{H}$, which are conjecturally defined over the abelian extensions of F cut out by ψ_1 and ψ_2?

Thank you for your attention