数理解析研究所講究録 1324 巻 2003 年 153-160

Heegner points and Hilbert modular forms

Henri Darmon
Adam Logan

The following is a report on work in progress; full details will appear in [DL].

1 Background and motivation

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

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

be its Hasse-Weil L-series. Thanks to the work of Wiles as completed by Breuil, Conrad, Diamond and Taylor, the curve E is known to be *modular*: the function

$$f(\tau)=\sum_{n}a_n e^{2\pi i n\tau}\quad(\tau\in\mathcal{H},\ \text{the Poincaré upper half-plane})$$

is a cusp form of weight 2 relative to the Hecke congruence group $\Gamma_0(N)$, so that the differential $\omega_f:=2\pi i f(\tau)d\tau$ is invariant under this group. The modularity of E has a number of useful consequences, such as the analytic continuation and functional equation of $L(E,s)$ (Hecke) and the existence of an explicitly computable *modular parametrisation*

$$\Phi:\mathcal{H}/\Gamma_0(N)\longrightarrow\mathbb{C}/\Lambda_E=E(\mathbb{C}),\qquad\text{where }\Phi(\tau):=\int_{i\infty}^{\tau}\omega_f=\sum_{n=1}^{\infty}\frac{a_n}{n}e^{2\pi i n\tau}.\quad(1)$$

(Here Λ_E is a suitable period lattice commensurable with the Néron lattice of E.) The function Φ, which is transcendental as a function of τ, enjoys the following notable algebraicity property, a consequence of the theory of complex multiplication:

Theorem HP: *Let $K\subset\mathbb{C}$ be a quadratic imaginary extension of $\mathbb{Q}$, and let K^{ab} denote its maximal abelian extension. If τ belongs to $\mathcal{H}\cap K$, then $\Phi(\tau)$ belongs to $E(K^{\mathrm{ab}})$.*

The points in $E(K^{\mathrm{ab}})$ arising from theorem HP are sometimes called *Heegner points* (although it is customary to place further restrictions on the values of τ that are allowed). Theorem HP admits a more precise formulation, given

by the *Shimura reciprocity law* expressing the action of Frobenius elements in $G_K^{\mathrm{ab}} = \mathrm{Gal}(K^{\mathrm{ab}}/K)$ on the collection of all $\Phi(\tau)$. This reciprocity law reflects the fact that we have an *explicit class field theory* for imaginary quadratic fields.

At present, theorem HP (and its extensions to Shimura curve parametrisations discussed below) supply *essentially the only known* method for systematically constructing algebraic points on elliptic curves over a field which is given in advance (other than direct computer search based on Fermat's descent, which is not known to yield an effective algorithm in general).

The importance of this method to the Birch and Swinnerton-Dyer conjecture is underscored by the key role it plays in the proof of the following theorem of Gross-Zagier and Kolyvagin.

Theorem GZK *Suppose that* $\mathrm{ord}_{s=1} L(E,s) \leq 1$. *Then*

$$\mathrm{rank}(E(\mathbb{Q})) = \mathrm{ord}_{s=1} L(E,s),$$

as predicted by the Birch and Swinnerton-Dyer conjecture, and the Shafarevich-Tate group of E is finite.

Remark: When $\mathrm{ord}_{s=1} L(E,s) = 0$, theorem GZK can also be proved by other methods which do not rely on CM points, using an Euler system discovered by Kato. This is not so when $\mathrm{ord}_{s=1} L(E,s) = 1$. At present, all known results on the Birch and Swinnerton-Dyer conjecture for elliptic curves in the analytic rank one case rely on theorem HP.

The goal of this lecture is to describe a conjectural extension of theorem HP in which E is defined over a totally real field and classical modular forms are replaced by Hilbert modular forms.

2 Elliptic curves over totally real fields

Let F be a totally real field of degree $n+1$, assumed for simplicity to be of narrow class number one. Fix an ordering $v_0, \ldots, v_n$ for the $n+1$ distinct real embeddings of F and write x_j for $v_j(x)$. We will occasionally denote by $|x| := x_0 x_1 \ldots x_n$ the norm of an element or of an integral ideal of F.

Let E be an elliptic curve over F with arithmetic conductor N. Denote by E_j the elliptic curve over $\mathbb{R}$ obtained from E by applying to it the embedding v_j. For each prime ideal $\mathfrak{p}$ of F let $a_{\mathfrak{p}}$ be the coefficient attached to E by the rule

$$a_{\mathfrak{p}} = |\mathfrak{p}| + 1 - \#E(\mathcal{O}_F/\mathfrak{p}) \quad \text{for } \mathfrak{p} \not| N.$$

(One completes this definition at the bad primes by setting $a_{\mathfrak{p}} = 0, 1$, or -1 depending on whether E has additive, split multiplicative, or non-split multiplicative reduction at $\mathfrak{p}$.) Let

$$L(E,s) = \prod_{\mathfrak{p}|N} (1 - a_{\mathfrak{p}}|\mathfrak{p}|^{-s})^{-1} \prod_{\mathfrak{p}\not|N} (1 - a_{\mathfrak{p}}|\mathfrak{p}|^{-s} + |\mathfrak{p}|^{1-2s})^{-1} =: \sum_{\nu} a_\nu |\nu|^{-s} \quad (2)$$

be the Hasse-Weil L-function attached to E, where the product (resp. the sum) is taken over the prime (resp. all) ideals of $\mathcal{O}_F$.

Write $\Gamma = \Gamma_0(N)$ for the Hecke-type congruence subgroup of $\mathbf{SL}_2(\mathcal{O}_F)$ consisting of matrices of determinant one which are upper-triangular modulo N. The actions of $v_j(\Gamma)$ on $\mathcal{H}$ by Möbius tranformations can be combined to yield a discrete action of Γ on the $n+1$-fold product of $\mathcal{H}$. Write $\mathcal{H}^{n+1}$ as $\mathcal{H}_0 \times \cdots \times \mathcal{H}_n$, with the obvious convention that Γ acts on $\mathcal{H}_j$ via the real embedding v_j.

The modularity conjecture for E predicts the existence of a Hilbert modular form

$$f(\tau_0, \ldots, \tau_n) \quad \text{on} \quad (\mathcal{H}_0 \times \cdots \times \mathcal{H}_n)/\Gamma$$

of parallel weight 2 which is a simultaneous eigenform for the Hecke operators and satisfies

$$T_{\mathfrak{p}} f = a_{\mathfrak{p}} f \text{ for all } \mathfrak{p} \not| N.$$

This modular form has Fourier expansion given by

$$f(\tau_0, \ldots, \tau_n) = \sum_{\nu \gg 0} a_{(\nu)} e^{2\pi i(\nu_0/d_0\tau_0 + \cdots + \nu_n/d_n\tau_n)},$$

where the sum is taken over all totally positive elements ν of $\mathcal{O}_F$ and d is a totally positive generator of the *different ideal* of F.

Many cases of this Shimura-Taniyama conjecture are known, thanks to the work of Diamond, Fujiwara, Skinner-Wiles, and others.

The difficulty in extending the Heegner point construction to the setting where $n > 0$ is that f now corresponds to a holomorphic $(n+1)$-form

$$\omega_f := f(\tau_0, \ldots, \tau_n) d\tau_0 \cdots d\tau_n \tag{3}$$

on the $(n+1)$-dimensional Hilbert modular variety whose complex points are identified with the analytic quotient $\mathcal{H}^{n+1}/\Gamma$. There seems to be no obvious modular parametrisation in this context.

The traditional way around this difficulty has been to exploit Shimura curves instead of Hilbert modular varieties, relying on the following (loosely stated) fact based on deep results of Jacquet-Langlands and Shimura:

Fact. *Suppose that $n+1$ is odd, or that there is a prime of F which exactly divides N. Then there exists a discrete arithmetic subgroup $\Gamma \subset \mathbf{SL}_2(\mathbb{R})$ and a non-trivial "modular parametrisation"*

$$\Phi : \mathrm{Div}^0(\mathcal{H}/\Gamma) \longrightarrow E(\mathbb{C}) \tag{4}$$

generalising (1).

The group Γ is a subgroup of the multiplicative group of an appropriate quaternion algebra over F which is definite at all but one of the archimedean places. Shimura has shown that the quotient $\mathcal{H}/\Gamma$ can be identified with the complex points of a curve admitting a canonical model over F – a so-called *Shimura*

Shimura curves are equipped with a well-behaved collection of CM points generalising those of theorem HP. It is thanks to this structure that the proof of theorem GZK has been extended to (many, but not all) modular elliptic curves over totally real fields. (For further background and precise statements in this direction, see [Zh], which supplies the most difficult missing ingredient, an appropriate generalisation of the analytic formula of Gross and Zagier for Shimura curves.)

There are certain elliptic curves not expected to have a Shimura curve parametrisation, the first examples occuring when F is real quadratic and E has everywhere good reduction over F. Even when a Shimura curve parametrisation is available, the resulting Heegner points are always defined over ring class fields of certain quadratic CM extensions of F. From the point of view of explicit class field theory (and Hilbert's twelfth problem) it would be desirable to go beyond the realm of CM fields.

The basic insight made explicit in [Dar] and [DL] is that it should be possible to construct algebraic points on E directly from the periods of the associated Hilbert modular form, without resorting to Shimura curve parametrisations. We will report on some experimental evidence which supports this insight.

3 ATR points

It is convenient to view F as a subfield of $\mathbb{C}$ via the distinguished real embedding v_0 that was singled out previously. Likewise all algebraic extensions of F will be viewed as subfields of the complex numbers. We begin with the following simple lemma.

Lemma. *Let τ be an element of $\mathcal{H}_0$ and let Γ_τ be the stabiliser of τ in Γ. Then Γ_τ is an abelian group of rank at most n, and the following two properties are equivalent.*

1. *Γ_τ has rank n;*
2. *The field $K = F(\tau)$ is a quadratic extension of F satisfying*

$$K \otimes_F \mathbb{R} \simeq \mathbb{C}, \qquad \text{and} \qquad K \otimes_{F,v_j} \mathbb{R} \simeq \mathbb{R} \oplus \mathbb{R} \quad \text{for} \quad j = 1, \ldots, n.$$

For a proof of this lemma, which is based on the Dirichlet unit theorem, see [Dar], section 7.6. A point $\tau \in \mathcal{H}_0$ satisfying the two equivalent properties of the lemma is called an ATR point.

Remark. The acronym ATR stands for "Almost Totally Real". This terminology refers to the fact that the quadratic extension K of F, although not a subfield of $\mathbb{R}$, is otherwise as close to being totally real as possible, since the n remaining real embeddings of F extend to real embeddings of K.

Denote by $\mathcal{H}_0'$ the collection of all ATR points in $\mathcal{H}_0$, equipped with its natural discrete topology. This set is preserved under the action of Γ by Möbius

transformations. The main construction of chapters 7 and 8 of [Dar] yields a map

$$\Phi : \mathcal{H}_0'/\Gamma \longrightarrow E_0(\mathbb{C}) \tag{5}$$

which is defined purely in terms of appropriate integrals of the differential form ω_f of (3), and could be viewed as a *natural substitute* for the modular parametrisations of (1) and (4). The main conjecture to be formulated below will lend weight to that assertion by predicting that the image of Φ consists of algebraic points defined over class fields of ATR extensions of F.

Note that the group Γ acts on $\mathcal{H}_0$ with dense orbits. The quotient $\mathcal{H}_0/\Gamma$ can be endowed with the structure of a "non-commutative space" (cf. [Ma] for example). We do not know what relations (if any) might exist between the map Φ of (5) and Manin's program of tackling Hilbert's twelfth problem through a suitable arithmetisation of non-commutative geometry.

We give a brief sketch of the construction of Φ in the simplest case where F is a real quadratic field of narrow class number one and E has everywhere good reduction over F. This is also the setting considered in [DL]; we refer the reader to chapters 7 and 8 of [Dar] for further generality, and to [DL] for the complete details.

Let ϵ be a fundamental unit of F, chosen so that $\epsilon_0 > 0$ and $\epsilon_1 < 0$. The Γ-invariant differential two-form ω_f can be used to define two differential forms ω_f^+ and ω_f^-, which are holomorphic in τ_0 but not in τ_1, by the rule

$$\omega_f^{\pm} := -4\pi^2\sqrt{|d|}^{-1}\left\{ f(\tau_0,\tau_1)d\tau_0 d\tau_1 \pm f(\epsilon_0\tau_0,\epsilon_1\bar{\tau}_1)d(\epsilon_0\tau_0)d(\epsilon_1\bar{\tau}_1)\right\}. \tag{6}$$

For conciseness, we will confine our remarks to the form ω_f^+. This form can be used to attach to f, and to $\tau \in \mathcal{H}_0$, a basic two-cocycle $\kappa_\tau \in Z^2(\Gamma,\mathbb{C})$ by choosing an arbitrary $x \in \mathcal{H}_1$ and setting

$$\kappa_\tau(\gamma_0,\gamma_1) = \int_\tau^{\gamma_0\tau}\int_{\gamma_0 x}^{\gamma_0\gamma_1 x}\omega_f^+.$$

The image of κ_τ in $H^2(\Gamma,C)$ depends only on f, not on the choice of x – or, for that matter, of τ – that was made in defining it. Choose a real invariant differential ω_E on E_0, and let Λ_E be the associated period lattice. In [DL] it is conjectured that there exists a lattice $\Lambda_0 \subset \mathbb{C}$ satisfying

1. the cocycle κ_τ becomes cohomologous to 0 modulo this lattice.

2. Λ_0 is homothetic to a lattice which is commensurable to Λ_E.

The conjecture formulated in [DL] is somewhat more precise, suggesting a precise choice of real differential ω_E to be made so that $\Lambda_0 \subset \Lambda_E$. Suppose from now on that such a choice has been made, and let

$$\eta_0 : \mathbb{C}/\Lambda_0 \longrightarrow E_0(\mathbb{C})$$

be the Weierstrass uniformisation attached to ω_E, composed with the natural projection $\mathbb{C}/\Lambda_0 \longrightarrow \mathbb{C}/\Lambda_E$.

Letting $\bar{\kappa}_\tau$ be the natural image of κ_τ in $Z^2(\Gamma, \mathbb{C}/\Lambda_0)$, we express $\bar{\kappa}_\tau$ as a coboundary:

$$\bar{\kappa}_\tau = d\xi_\tau.$$

The element ξ_τ belongs to $C^1(\Gamma, \mathbb{C}/\Lambda_0)$, and is well-defined up to elements of $Z^1(\Gamma, \mathbb{C}/\Lambda_0)$. This ambiguity is not serious, because it can be shown that the abelianisation of Γ is finite; hence

$$Z^1(\Gamma, \mathbb{C}/\Lambda_0) = \hom(\Gamma, \mathbb{C}/\Lambda_0) \text{ is a finite group.}$$

It is possible to estimate the order of this group fairly precisely. Replacing ξ_τ by an appropriate integer multiple of it yields a well-defined invariant in $C^1(\Gamma, \mathbb{C}/\Lambda_0)$, which will be denoted again ξ_τ by abuse of notation.

The class ξ_τ is not a cocycle, but its restriction to Γ_τ is. Moreover, the image of this restriction in $H^1(\Gamma_\tau, \mathbb{C}/\Lambda_0)$ does not depend on the choice of base point $x \in \mathcal{H}_1$ that was made to define κ_τ. Of course, the invariant J_τ yields no information when τ is not an ATR point, since the group Γ_τ is then trivial. When τ is ATR, it yields a canonical invariant

$$J_\tau \in \hom(\Gamma_\tau, \mathbb{C}/\Lambda_0) = \hom(\mathbb{Z}, \mathbb{C}/\Lambda_0) = \mathbb{C}/\Lambda_0,$$

where the first identification depends of course on the choice of a generator of Γ_τ.

We now define the parametrisation Φ alluded to in equation (5) by the rule

$$\Phi(\tau) := \eta_0(J_\tau).$$

The main conjecture that was tested numerically in [DL] can now be stated as follows.

Main Conjecture. *If τ is an ATR point, and $K = F(\tau)$, then $\Phi(\tau)$ is defined over an abelian extension of K.*

Chapters 7 and 8 of [Dar], and [DL], give a more precise version of this conjecture, with a more careful description of the map Φ and an explicit Shimura reciprocity law describing the action of Frobenius elements of K on the collection of points $\Phi(\tau)$ as τ ranges over $\mathcal{H}_0 \cap K$. The reader is invited to consult those references for further details.

4 Numerical examples

The smallest real quadratic field of narrow class number one which possesses an elliptic curve with everywhere good reduction is the field $F = \mathbb{Q}(\sqrt{29})$. Let $\epsilon = (5 + \sqrt{29})/2$ denote its fundamental unit of norm -1. There is (up to

isogeny) a single elliptic curve with everywhere good reduction over F, which has been found by Tate. Its minimal Weierstrass equation is given by

$$E : y^2 + xy + \epsilon^2 y = x^3, \tag{7}$$

and its discriminant is equal to $-\epsilon^{10}$. It has a rational subgroup of order 3 generated by the point $(0,0)$, and is of rank 0 over F.

Fix v_0 and v_1 so that v_0 sends $\sqrt{29}$ to the negative square root, and set $\omega = \frac{1+\sqrt{29}}{2}$. The field $K = F(\sqrt{4+2\omega})$ is an ATR extension (relative to this chosen ordering). Let

$$\tau = \sqrt{v_0(4+2\omega)} \in \mathcal{H}_0'.$$

(Here of course one takes the square root with strictly positive imaginary part.) A direct calculation using the definitions above and the algorithm explained in [DL] shows that

$$J_\tau = 5.43973608624\ldots + +12.1797882505\ldots i$$

and that

$$\eta_0(J_\tau) = (-0.13256917899\ldots, 0.0477405984\ldots + 0.0071192599\ldots i). \tag{8}$$

Although only the first ten digits are displayed above, these calculations were actually performed on the computer to roughly 200 digits of numerical accuracy. The more precise form of the main conjecture formulated in [DL] leads to the prediction that $\eta_0(J_\tau)$ is defined over the field $K = F(\tau)$, a (non-Galois) algebraic extension of degree 4 over $\mathbb{Q}$. Let x and y denote the x and y-coordinates of the complex point (8). The Pari commands `algdep(x,4)` and `algdep(y,4)` yield the following suggested algebraic relations satisfied by x and y respectively.

$$p_x = 802816x^2 - 300672x - 53969,$$

$$\begin{aligned} p_y = {} & 5174257739848744 96y^4 + 1416428306964047 4624y^3 \\ & - 1423403547411611648y^2 + 39557777686183936y \\ & - 157192967652209. \end{aligned}$$

The small coefficients in these relations (relative to the 200 digits of numerical accuracy that were calculated) suggests strongly that x and y are the roots of p_x and p_y respectively. This guess is confirmed by noting that p_x has a root defined over F and that p_y has a root defined over K. Assuming that x and y are algebraic numbers satisfying p_x and p_y respectively, we find that

$$\eta_0(J_\tau) = 2\left(-\frac{1}{4}, \frac{-53+10\sqrt{29}}{8} + \frac{17-3\sqrt{29}}{8}\sqrt{5-\sqrt{29}}\right) \tag{9}$$

is a point of infinite order in $E(K)$. That an identity like (9) can be verified to 200 digits of numerical accuracy provides convincing evidence for our main conjecture.

More experiments of the same sort are performed in [DL], with three elliptic curves having everywhere good reduction over the real quadratic fields $F = \mathbb{Q}(\sqrt{29})$, $\mathbb{Q}(\sqrt{37})$, and $\mathbb{Q}(\sqrt{41})$. In [DL] we numerically verify the main conjecture for five to eleven ATR extensions of each of these three fields, to roughly 20 digits of accuracy. In all cases the experimental data agrees with theoretical predictions.

References

[Dar] H. Darmon. *Rational points on modular elliptic curves.* NSF-CBMS notes. To appear.

[DL] H. Darmon, A. Logan. *Periods of Hilbert modular forms and rational points on elliptic curves.* In progress.

[Ma] Yu.I. Manin. *Real multiplication and noncommutative geometry (ein Alterstraum).* Preprint.

[Zh] S. Zhang. *Heights of Heegner points on Shimura curves.* Ann. of Math. (2) **153** (2001), no. 1, 27–147.