Rational Points on Modular Elliptic Curves

III. Hilbert's twelfth problem

Hedrick Lecture Series

MAA MathFest
Boulder, Colorado
August 2003

http://www.math.mcgill.ca/darmon
/slides/slides.html

Recall

Last time, we discussed:

- Wiles' theorem: every elliptic curve is modular.

- The modular parametrisation

$$\Phi : \mathcal{H}/\Gamma_0(N) \longrightarrow E(\mathbf{C}).$$

- The Heegner point construction

$$\mathrm{HP}_K := \Phi(\mathcal{H} \cap K).$$

- The key role played by HP_K in establishing the known cases of the BSD conjecture (when $\mathrm{ord}_{s=1}(L(E,s)) \leq 1$.)

Some questions

Q1. Can one construct a group GHP $\subset E(\bar{\mathbf{Q}})$ of *"generalised Heegner points"* such that

1. GHP is constructed "from modular forms";
2. rank(GHP $\cap E(\mathbf{Q})$) can be ≥ 2;
3. rank(GHP $\cap E(\mathbf{Q})$) can be related to

$$\text{ord}_{s=1} L(E,s)?$$

This is the \$1,000,000 question!

Q2. Generalise the Heegner point construction in other ways? E.g., define

$$\text{HP}_K \subset E(K^{\text{ab}})$$

for fields K *other* than imaginary quadratic fields?

Generating abelian extensions

When K is a *quadratic imaginary field*, the Heegner point construction – or rather, the theory of complex multiplication which underlies it – gives a beautiful solution to the following general problem:

Problem: Given a field K, give an *explicit construction*, from values of analytic functions evaluated at specific arguments, of all abelian extensions L/K.

The problem of extending this construction to other base fields is known as *Hilbert's twelfth problem*.

The prototype: $K = \mathbf{Q}$

Let $e(z) = e^{2\pi iz}$. (Note: e(z+1) = e(z).)

Easy fact: If $z = \frac{a}{b} \in \mathbf{Q}$, then $e(z)$ is a bth root of unity, and hence $\mathbf{Q}(e(z))$ is an abelian extension of $\mathbf{Q}$.

Theorem (Kronecker-Weber) Any abelian extension of $\mathbf{Q}$ is contained in an extension of the form $\mathbf{Q}(e(z))$ for some $z \in \mathbf{Q}$.

In other words,

$$\mathbf{Q}^{\text{ab}} = \cup_{z \in \mathbf{Q}} \mathbf{Q}(e(z)).$$

The modular function j

Recall: $\mathcal{H} = \{z \in \mathbf{C}, \text{such that } \mathrm{Im}(z) > 0\}$.

Theorem: There is a *unique* analytic function j on $\mathcal{H}$ satisfying

$$j(z+1) = j(z), \quad j(-1/z) = j(z),$$

admitting a Laurent series expansion in the variable $q = e^{2\pi iz}$ of the form

$$j(z) = \frac{1}{q} + a_1 q + \cdots + a_n q^n + \cdots$$

j has many remarkable properties:

- The coefficients a_i are integers.

- $a_1 = 196884 = 196883 + 1$.

John McKay: 196883 is the dimension of the smallest non-trivial irreducible representation of the Monster group.

K a quadratic imaginary field

The function j plays much the *same role* for K as the function e for $\mathbf{Q}$.

Main theorem of complex multiplication

If $K = \mathbf{Q}(\sqrt{-d})$, then

$$K^{\mathsf{ab}} \simeq \cup K(e(t), j(z)),$$

where the union is taken over

$$t \in \mathbf{Q}, \qquad z \in \mathcal{H} \cap K.$$

• The notation $M \simeq L$ means that M/L is a union of quadratic extensions.

General K?

For other K, a generalisation of the Kronecker-Weber Theorem and the main theorem of complex multiplication is *not known*.

Hilbert's twelfth problem (Hilbert, 1900):

> "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."

First open case: when K is a *real quadratic field*, $K = \mathbf{Q}(\sqrt{d})$ with $d > 0$.

The work of Shimura-Taniyama

$F =$ totally real field, of degree $n + 1$.

$K =$ totally imaginary extension of F.

Theorem (Shimura-Taniyama, 1960's) There exists

- An explicit discrete subgroup Γ of $\mathbf{SL}_2(\mathbf{R})$;
- Two Γ-invariant functions j_1 and j_2 on $\mathcal{H}$;
- An explicit subset $\mathcal{H}^K$ of $\mathcal{H}$;

such that

$$K^{\mathrm{ab}} \simeq \cup_{z \in \mathcal{H}^K} F^{\mathrm{ab}}(j_1(z), j_2(z)).$$

This solves the problem of constructing class fields of totally imaginary K, *modulo* the solution of the problem for the totally real subfield F.

The Shimura-Taniyama theory yields *very little* in the case where K is a real quadratic field.

Real quadratic fields

A *conjectural* approach to Heegner point construction for real quadratic fields is outlined in

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

• H. Darmon, P. Green. *Elliptic curves and class fields of real quadratic fields*, Experimental Mathematics **11:1** (2002) 37–55.

• H. Darmon, A. Logan. *Periods of Hilbert modular forms and rational points on elliptic curves*, IMRN, to appear.

They can be downloaded from

http://www.math.mcgill.ca/darmon

Hilbert modular forms

Idea #1: Exploit modular forms of several variables.

Hilbert, 1900: It will be seen that in the problem just sketched the three fundamental branches of mathematics, number theory, algebra and function theory, come into closest touch with one another, and I am certain that the theory of analytical functions of several variables in particular would be notably enriched if one should succeed in finding and discussing those functions which play the part for any algebraic number field corresponding to that of the exponential function in the field of rational numbers and of the elliptic modular functions in the imaginary quadratic number field.

Hilbert modular forms

$F =$ totally real field, of degree $n + 1$.

$v_0, \dots, v_n : F \hookrightarrow \mathbf{R}$.

$\mathbf{SL}_2(\mathcal{O}_F)$ acts discretely on $\mathcal{H}_0 \times \cdots \times \mathcal{H}_n$.

$E/F =$ elliptic curve of conductor N.

$\Gamma_0(N) \subset \mathbf{SL}_2(\mathcal{O}_F)$.

Conjecture (Shimura-Taniyama-Weil). There exists a holomorphic differential $(n+1)$-form ω_E on $\mathcal{H}_0 \times \cdots \times \mathcal{H}_n$ which is invariant under $\Gamma_0(N)$ and whose fourier coefficients are obtained from E as in the original Shimura-Taniyama-Weil conjecture.

Numerous cases of this conjecture have been proved (Wiles, Skinner-Wiles).

Periods of Hilbert Modular Forms

A quadratic extension K/F is called *almost totally real* (ATR) if it is imaginary at v_0 and real at $v_1, \ldots, v_n$.

$\mathcal{H}_0' =$ points in $\mathcal{H}_0$ with ATR coordinates.

Logan, Darmon:

• There is a *natural substitute* for the modular parametrisation

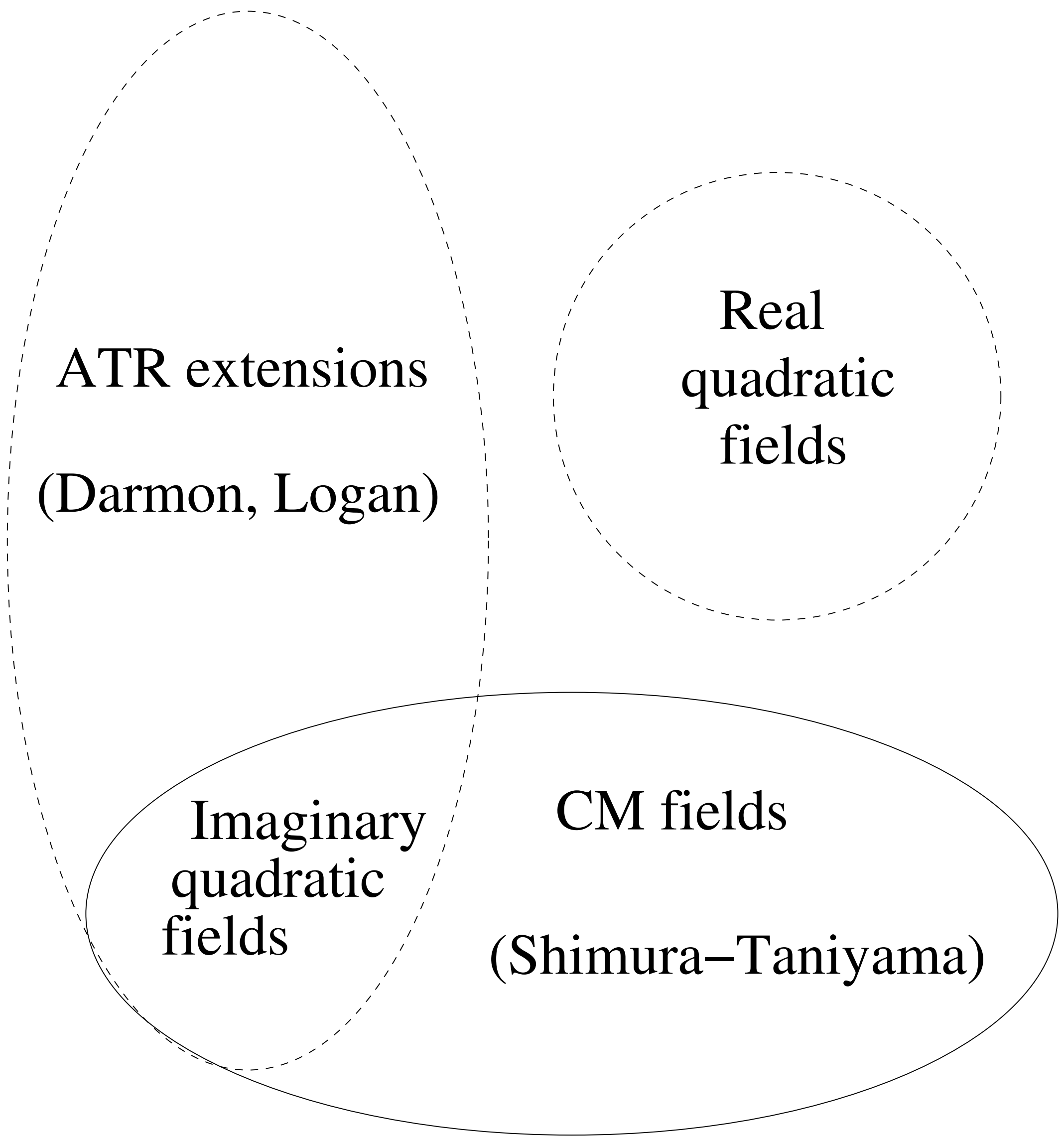
$$j_E : \mathcal{H}_0'/\Gamma_0(N) \longrightarrow E(\mathbf{C})$$

defined in terms of

$$\int \cdots \int \omega_E.$$

• **Conjecture** (Logan, Darmon) If z belongs to $\mathcal{H}_0 \cap K$, then $j_E(z)$ belongs to $E(K^{\mathrm{ab}})$

Remark: This conjecture does not cover real quadratic K, which are neither CM nor ATR...



p-adic integration

Idea #2: Replace complex by p-adic analysis.

Motivation: If K is real quadratic, then

$$K \cap \mathcal{H} = \emptyset.$$

To circumvent this problem, let

$\mathbf{Q}_p$= completion of $\mathbf{Q}$ with respect to the p-adic metric.

$\mathbf{C}_p$ = completion of $\bar{\mathbf{Q}}_p$.

$\mathcal{H}_p = \mathbf{C}_p - \mathbf{Q}_p$.

One can define on $\mathcal{H}_p$ a space of *rigid analytic functions* which plays the role of holomorphic functions in the p-adic realm. (Tate, Mumford).

Key benefit: $K \cap \mathcal{H}_p$ need not be empty!

Forms on $\mathcal{H}_p \times \mathcal{H}$

Crucial construction. To an elliptic curve E over $\mathbf{Q}$ of prime conductor p one may attach a "differential two-form" on $\mathcal{H}_p \times \mathcal{H}$, which is *invariant* under $\mathbf{SL}_2(\mathbf{Z}[1/p])$ and hence behaves *just like a Hilbert modular form*.

This is a kind of "modularity theorem", but is an *easy formal consequence* of the modularity theorem proved by Wiles.

Let us call this form ω.

(In fact, ω does not *really* exist, but one can still define *periods* – "double integrals" – attached to it.)

Integration on $\mathcal{H}_p \times \mathcal{H}$

Double Integrals:

$$\int_{\tau_1}^{\tau_2}\int_x^y \omega \in \mathbf{C}_p^\times.$$

Here τ_1, τ_2 belong to $\mathcal{H}_p$,

and x, y belong to $\mathbf{P}_1(\mathbf{Q})$.

Properties:

$$\int_{\tau_1}^{\tau_2}\int_x^y \omega \times \int_{\tau_2}^{\tau_3}\int_x^y \omega = \int_{\tau_1}^{\tau_3}\int_x^y \omega.$$

$$\int_{\tau_1}^{\tau_2}\int_x^y \omega \times \int_{\tau_1}^{\tau_2}\int_y^z \omega = \int_{\tau_1}^{\tau_2}\int_x^z \omega.$$

$$\int_{\gamma\tau_1}^{\gamma\tau_2}\int_{\gamma x}^{\gamma y} \omega = \int_{\tau_1}^{\tau_2}\int_x^y \omega$$

for all $\gamma \in \mathbf{SL}_2(\mathbf{Z}[1/p])$.

The function $j_E^{(p)}$

$\mathcal{H}_p' =$ points in $\mathcal{H}_p$ with *real quadratic coordinates*.

Replacing the complex multiple integrals used in the definition of j_E, by the p-adic double integral of the previous slide, yields

$$j_E^{(p)} : \mathcal{H}_p' \longrightarrow E(\mathbf{C}_p).$$

Conjecture (Darmon, Green). If $K/\mathbf{Q}$ is a real quadratic field, and τ belongs to $K \cap \mathcal{H}_p$, then $j_E^{(p)}(\tau)$ belongs to $E(K^{\mathrm{ab}})$. Furthermore

$$K^{\mathrm{ab}} \simeq \cup K(e(t), j_E^{(p)}(z)), \quad t \in \mathbf{Q}, \quad z \in K \cap \mathcal{H}_p.$$

Peter Green's example

$E =$ elliptic curve of conductor 43.

$$E : y^2 + y = x^3 + x^2.$$

Let $K = \mathbf{Q}(\sqrt{37})$.

$z_1 = \frac{-3+\sqrt{37}}{4}, z_2 = \frac{-3+\sqrt{37}}{7}, z_3 = -6 + \sqrt{37}$.

Compute $P_j = j_E^{(43)}(z_j) := (x_j, y_j)$ to 4 significant 43-adic digits.

$$P_1 = (1953822 + 3156001\sqrt{37},$$

$$1647778 + 1133177\sqrt{37})$$

$$P_2 = (1953822 + 262800\sqrt{37},$$

$$1647778 + 2285624\sqrt{37})$$

$$P_3 = (2929963, 123259).$$

Green's example (continued)

$$\prod_j (t - x_j) = t^3 - 5t^2 - 5t - 1 \pmod{43^4},$$

$$\prod_j (t - y_j) = t^3 + 17t^2 + 17t - 1 \pmod{43^4}.$$

The roots of the polynomials on the right do indeed give points $\tilde{P}_j$ on E, defined over a cyclic cubic extension of $\mathbf{Q}(\sqrt{37})$.

Difficult Problem: Show that the 43-adic points P_j are indeed *equal* to the global points $\tilde{P}_j$, not just modulo 43^4.

Some notations

• Given $\tau \in K \cap \mathcal{H}_p$ the quadratic form

$$(x - \tau y)(x - \tau' y)$$

is proportional to a *unique* negative-definite integral primitive binary quadratic form Q_τ.

$$Q_\tau(x, y) = ax^2 + bxy + cy^2,$$

with $a, b, c \in \mathbf{Z}, \quad a > 0, \quad \gcd(a, b, c) = 1$.

• Discriminant of $\tau :=$ discriminant of Q_τ,

$$D_\tau = b^2 - 4ac > 0.$$

• $\mathbf{SL}_2(\mathbf{Z})$ acts on all quadratic forms of a given discriminant D:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} Q(x, y) = Q(ax + cy, bx + dy).$$

• Class number of D = number of distinct primitive binary quadratic forms of discriminant D, modulo the action of $\mathbf{SL}_2(\mathbf{Z})$.

Some theoretical evidence

Theorem (Bertolini, Darmon, in progress)

Let $\tau \in \mathcal{H}_p \cap K$ and ssume that

- The discriminant of τ has class number one;

- E has split multiplicative reduction at p;

- both $L(E,s)$ and $L(E/K,s)$ have a simple zero at $s = 1$.

Then $j_E^{(p)}(\tau)$ is a point of infinite order in $E(\mathbf{Q})$.

Remark. The second assumption is made for technical reasons and can probably be relaxed. The first is *essential* to the method of proof.

The above result gives a p-adic construction of a point of infinite order in $E(\mathbf{Q})$; because of the key first assumption, it *sheds no new light* on Hilbert's twelfth problem.