Rational points on elliptic curves

and

cycles on Shimura varieties

Harvard-MIT-Brandeis-Northeastern
Joint Colloquium

Henri Darmon
McGill University
February 28, 2008

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

Diophantine equations

$$f_1, \ldots, f_m \in \mathbf{Z}[x_1, \ldots, x_n],$$

$$X : \begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \vdots \quad \vdots \quad \vdots \\ f_m(x_1, \ldots, x_n) = 0. \end{cases}$$

Question: What is an *interesting* Diophantine equation?

A "working definition". A Diophantine equation is *interesting* if it reveals or suggests a rich underlying mathematical structure.

(In other words, a Diophantine question is interesting if it has an interesting answer...!)

Some examples

Fermat, 1635: Pell's equation $x^2 - ny^2 = 1$ has infinitely many solutions because the class group of binary quadratic forms of discriminant $4n$ is finite.

Kummer, 1847: Fermat's equation $x^n + y^n = z^n$ has no non-zero solution for $2 < n < 37$ because all primes $p < 37$ are *regular*.

Mazur, Frey, Serre, Ribet, Wiles, Taylor, 1994: Fermat's equation $x^n + y^n = z^n$ has no non-zero solution for all $n > 2$ because all elliptic curves are *modular*.

Elliptic Curves

An *elliptic curve* is an equation of the form

$$\boxed{E : y^2 = x^3 + ax + b,}$$

with $\Delta := 4a^3 - 27b^2 \neq 0$.

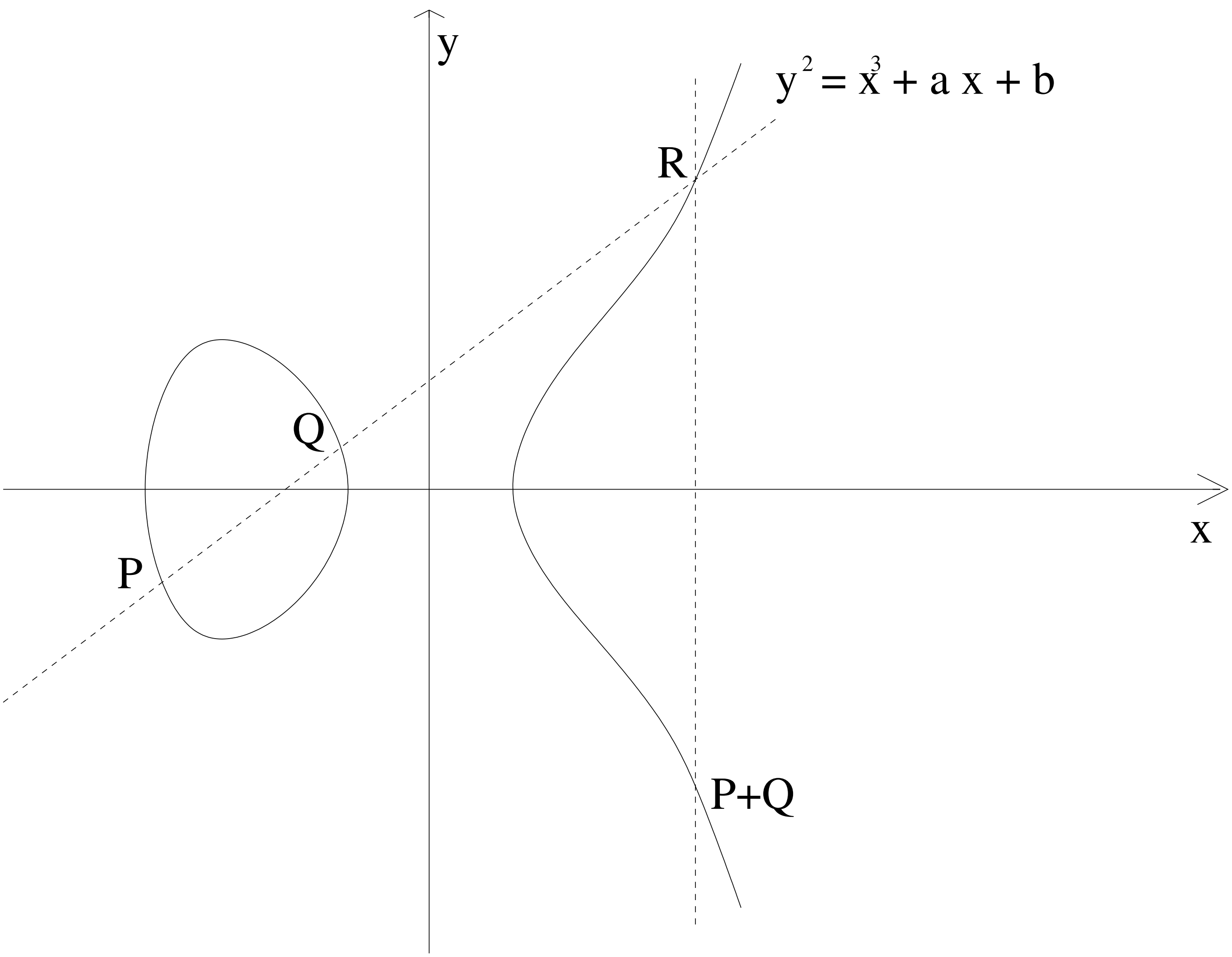
If F is a field,

$E(F) :=$ Mordell-Weil group of E over F.

Why elliptic curves?

The addition law

Elliptic curves are *algebraic groups*.



The addition law on an elliptic curve

Modularity

Let $N =$ *conductor* of E.

$$a(p) := \begin{cases} p+1-\#E(\mathbf{Z}/p\mathbf{Z}) & \text{if } p \nmid N; \\ 0, \pm 1 & \text{if } p \mid N. \end{cases}$$

$a(mn) = a(m)a(n)$ if $\gcd(m,n) = 1$,

$a(p^n) = a(p)a(p^{n-1}) - pa(p^{n-2})$, if $p \nmid N$.

Generating series:

$$f_E(z) = \sum_{n=1}^{\infty} a(n)e^{2\pi inz}, \quad z \in \mathcal{H},$$

$\mathcal{H} :=$ Poincaré upper half-plane

Modularity

Modularity: the series $f_E(z)$ satisfies a deep symmetry property.

$M_0(N) :=$ ring of 2×2 integer matrices which are *upper triangular* modulo N.

$\Gamma_0(N) := M_0(N)_1^{\times} =$ units of determinant 1.

Theorem: The series f_E is a *modular form of weight two on* $\Gamma_0(N)$.

$$f_E\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f_E(z).$$

In particular, the differential form $\omega_f := f_E(z)dz$ is defined on the quotient

$$X := \Gamma_0(N)\backslash\mathcal{H}.$$

Cycles and modularity

The Riemann surface X contains many natural *cycles*, which convey a *tremendous amount of arithmetic information* about E.

These cycles are indexed by the commutative subrings of $M_0(N)$: orders in $\mathbf{Q}[\epsilon]$, $\mathbf{Q} \times \mathbf{Q}$, or in a quadratic field.

Disc(R) := discriminant of R.

$\Sigma_D = \Gamma_0(N) \backslash \{R \subset M_0(N)$ with $\mathrm{Disc}(R) = D\}$.

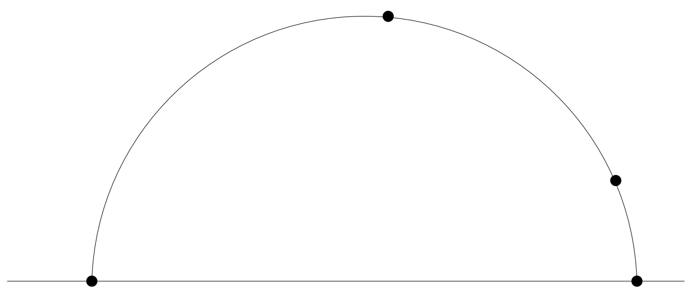
G_D := Equivalence classes of binary quadratic forms of discriminant D.

The set Σ_D, if non-empty, is equipped with an action of the class group G_D.

The special cycles $\gamma_R \subset X$

Case 1. Disc(R) > 0. Then $(R \otimes \mathbf{Q})^\times$ has *two real fixed points* $\tau_R, \tau'_R \in \mathbf{R}$.

$\Upsilon_R :=$ geodesic from τ_R to τ'_R;

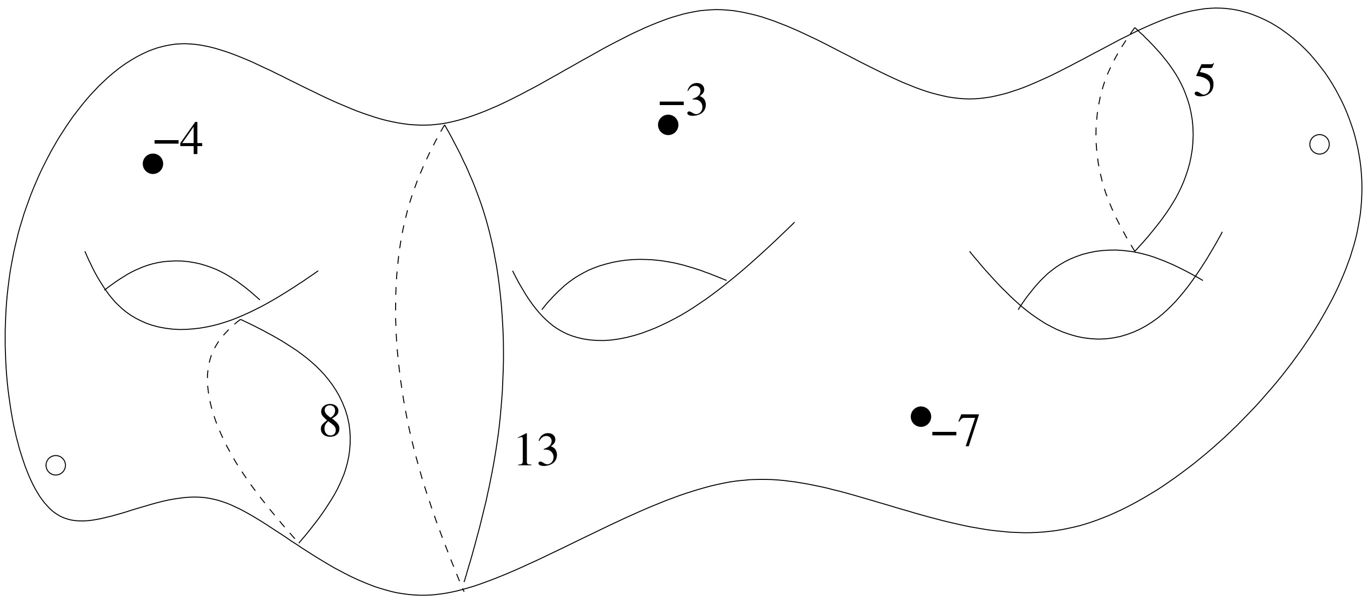


$$\boxed{\gamma_R := R_1^\times \backslash \Upsilon_R}$$

Case 2. Disc(R) < 0. Then $(R \otimes \mathbf{Q})^\times$ has *a single fixed point* $\tau_R \in \mathcal{H}$.

$$\boxed{\gamma_R := \{\tau_R\}}$$

An (idealised) picture



For each discriminant D, define:

$$\gamma_D = \sum \gamma_R,$$

the sum being taken over a G_D-orbit in Σ_D.

Convention: $\gamma_D = 0$ if Σ_D is empty.

Fact: The periods of ω_f against γ_R and γ_D convey alot of information about the arithmetic of E over quadratic fields.

Periods of ω_f: the case $D > 0$

Theorem (Eichler, Shimura) The set

$$\Lambda := \left\langle \int_{\gamma_R} \omega_f, \quad R \in \Sigma_{>0} \right\rangle \subset \mathbf{C}$$

is a lattice in $\mathbf{C}$, which is commensurable with the Weierstrass lattice of E.

Proof (Sketch)

1. **Modular curves**: $X = Y_0(N)(\mathbf{C})$, where $Y_0(N)$ is an algebraic curve over $\mathbf{Q}$, parametrising elliptic curves over $\mathbf{Q}$.

2. **Eichler-Shimura**: There exists an elliptic curve E_f and a quotient map

$$\Phi_f : Y_0(N) \longrightarrow E_f$$

such that

$$\int_{\gamma_R} \omega_f = \int_{\Phi(\gamma_R)} \omega_{E_f} \in \Lambda_{E_f}.$$

Hence, $\int_{\gamma_R} \omega_f$ is a *period* of E_f.

The curves E_f and E are related by:

$$a_n(E_f) = a_n(E) \text{ for all } n \geq 1.$$

3. **Isogeny conjecture for curves** (Faltings): E_f is isogenous to E over $\mathbf{Q}$.

Arithmetic information

Conjecture (BSD) Let $D > 0$ be a fundamental discriminant. Then

$$J_D := \int_{\gamma_D} \omega_f \neq 0 \quad \text{iff} \quad \#E(\mathbf{Q}(\sqrt{D})) < \infty.$$

"The position of γ_D in the homology $H_1(X, \mathbf{Z})$ encodes an *obstruction* to the presence of rational points on $E(\mathbf{Q}(\sqrt{D}))$. "

Gross-Zagier, Kolyvagin. If $J_D \neq 0$, then $E(\mathbf{Q}(\sqrt{D}))$ is finite.

Periods of ω_f: the case $D < 0$

The γ_R are 0-cycles, and their image in $H_0(X, \mathbf{Z})$ is *constant* (independent of R).

Hence we can produce many homologically trivial 0-cycles suppported on Σ_D:

$$\Sigma_D^0 := \ker(\mathrm{Div}(\Sigma_D) \longrightarrow H_0(X, \mathbf{Z})).$$

Extend $R \mapsto \gamma_R$ to $\Delta \in \Sigma_D^0$ by linearity.

$\gamma_\Delta^\#$:= any smooth one-chain on X having γ_Δ as boundary,

$$P_\Delta := \int_{\gamma_\Delta^\sharp} \omega_f \in \mathbf{C}/\Lambda_f \simeq E(\mathbf{C}).$$

CM points

CM point Theorem For all $\Delta \in \Sigma_D^0$, the point P_Δ belongs to $E(H_D) \otimes \mathbf{Q}$, where H_D is the Hilbert class field of $\mathbf{Q}(\sqrt{D})$.

Proof (Sketch)

1. **Complex multiplication**: If $R \in \Sigma_D$, the 0-cycle γ_R is a point of $Y_0(N)(\mathbf{C})$ corresponding to an elliptic curve with complex multiplication by $\mathbf{Q}(\sqrt{D})$. Hence it is defined over H_D.

2. **Explicit formula for** Φ: $\Phi(\gamma_\Delta) = P_\Delta$.

The systematic supply of *algebraic* points on E given by the CM point theorem is an *essential tool* in studying the arithmetic of E over K.

Generalisations?

Principle of functoriality: modularity admits many incarnations.

Simple example: **quadratic base change.**

Choose a fixed **real quadratic field** F, and consider E as an elliptic curve over this field.

Notation: $(v_1, v_2) : F \longrightarrow \mathbf{R} \oplus \mathbf{R}, \quad x \mapsto (x_1, x_2).$

Assumptions: $h^+(F) = 1$, $N = 1$.

Counting points mod $\mathfrak{p}$ yields $\mathfrak{n} \mapsto a(\mathfrak{n}) \in \mathbf{Z}$, on the integral ideals of $\mathcal{O}_F$.

Problem: To package these coefficients into a *modular generating series.*

Modularity

Generating series

$$G(z_1, z_2) := \sum_{n>>0} a((n)) e^{2\pi i \left(\frac{n_1}{d_1} z_1 + \frac{n_2}{d_2} z_2\right)},$$

where d := totally positive generator of the different of F.

Theorem: (Doi-Naganuma, Shintani).

$$G(\gamma_1 z_1, \gamma_2 z_2) = (c_1 z_1 + d_2)^2 (c_2 z_2 + d_2)^2 G(z_1, z_2),$$

for all

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathcal{O}_F).$$

Geometric formulation

The differential form

$$\alpha_G := G(z_1, z_2)dz_1dz_2$$

is a *holomorphic* (hence closed) 2-form defined on the quotient

$$X_F := \mathbf{SL}_2(\mathcal{O}_F)\backslash(\mathcal{H} \times \mathcal{H}).$$

It is better to work with the harmonic form

$$\omega_G := G(z_1, z_2)dz_1dz_2 + G(\epsilon_1 z_1, \epsilon_2 \bar{z}_2)dz_1d\bar{z}_2,$$

where $\epsilon \in \mathcal{O}_F^\times$ satisfies $\epsilon_1 > 0$, $\epsilon_2 < 0$.

ω_G is a closed two-form on the four-dimensional manifold X_F.

Question: What do the periods of ω_G, against various natural cycles on X_F, "know" about the arithmetic of E over F?

Cycles on the four-manifold X_F

The natural cycles on the four-manifold X_F are now indexed by commutative $\mathcal{O}_F$-subalgebras of $M_2(\mathcal{O}_F)$, i.e., by $\mathcal{O}_F$-orders in quadratic extensions of F.

D := Disc(R) := relative discriminant of R over F.

There are now *three cases* to consider.

1. $D_1, D_2 > 0$: the totally real case.

2. $D_1, D_2 < 0$: the complex multiplication (CM) case.

3. $D_1 < 0, D_2 > 0$: the "almost totally real" (ATR) case.

The special cycles $\gamma_R \subset X_F$

Case 1. Disc$(R) >> 0$. Then, for $j = 1, 2$,

$(R \otimes_{v_j} \mathbf{R})^\times$ has *two fixed points* $\tau_j, \tau_j' \in \mathbf{R}$.

Let $\Upsilon_j :=$ geodesic from τ_j to τ_j';

$$\boxed{\gamma_R := R_1^\times \backslash (\Upsilon_1 \times \Upsilon_2)}$$

Case 2. Disc$(R) << 0$. Then, for $j = 1, 2$,

$(R \otimes_{v_j} \mathbf{R})^\times$ has *a single fixed point* $\tau_j \in \mathcal{H}$.

$$\boxed{\gamma_R := \{(\tau_1, \tau_2)\}}$$

The ATR case

Case 3. $D_1 < 0, D_2 > 0$. Then

$(R \otimes_{v_1} \mathbf{R})^\times$ has a unique fixed point $\tau_1 \in \mathcal{H}$.

$(R \otimes_{v_2} \mathbf{R})^\times$ has two fixed points $\tau_2, \tau_2' \in \mathbf{R}$.

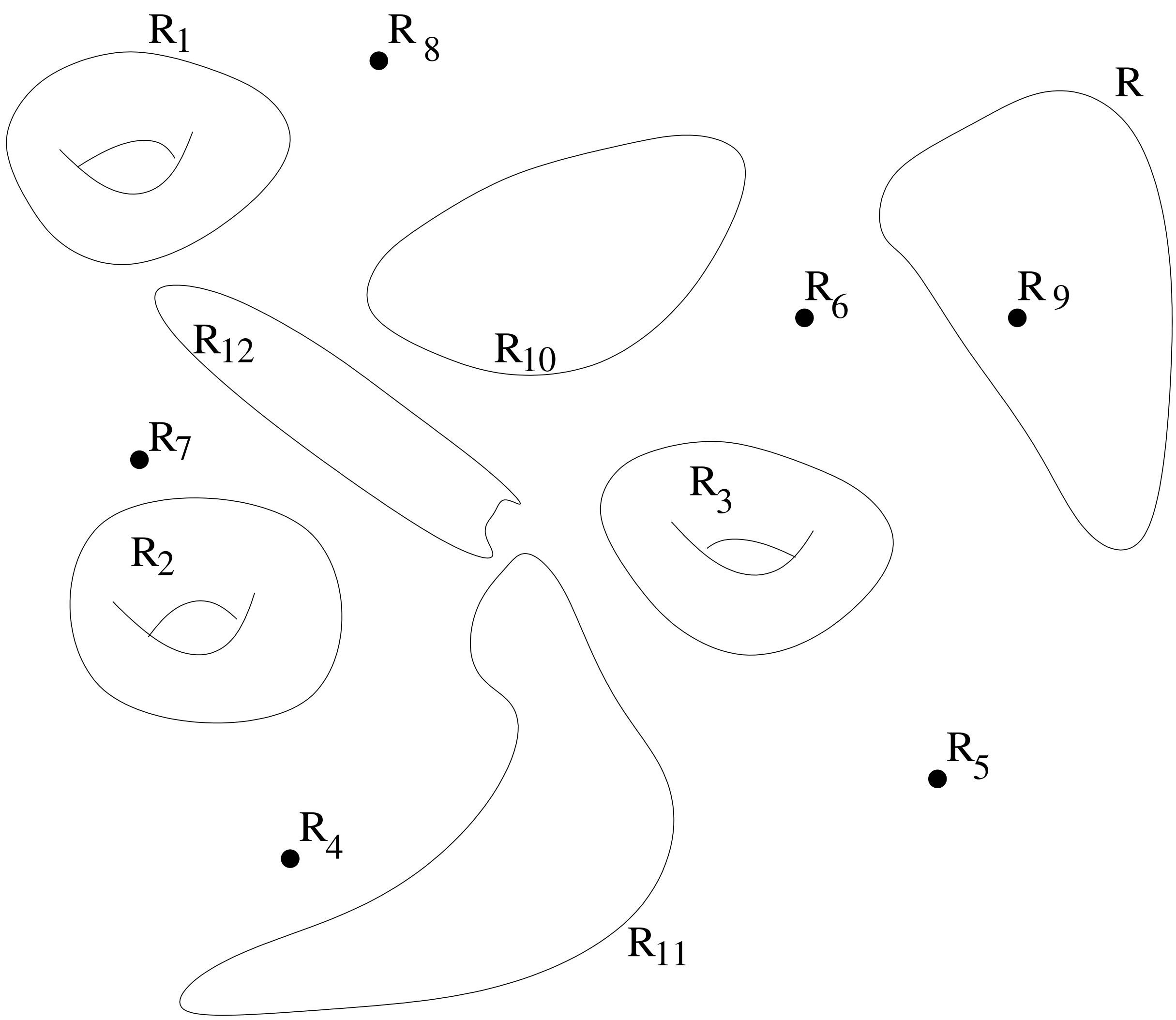
Let $\Upsilon_2 :=$ geodesic from τ_2 to τ_2';

$$\boxed{\gamma_R := R_1^\times \backslash (\{\tau_1\} \times \Upsilon_2)}$$

The cycle γ_R is a closed one-cycle in X_F.

It is called an *ATR cycle*.

An (idealised) picture



Cycles on the four-manifold X_F

Periods of ω_G: the case $D >> 0$

Conjecture (Oda) The set

$$\Lambda_G := \left\langle \int_{\gamma_R} \omega_G, \quad R \in \Sigma_{>>0} \right\rangle \subset \mathbf{C}$$

is a lattice in $\mathbf{C}$ which is commensurable with the Weierstrass lattice of E.

Conjecture (BSD) Let $D := \mathrm{Disc}(K/F) >> 0$. Then

$$J_D := \int_{\gamma_D} \omega_G \neq 0 \quad \text{iff} \quad \#E(K) < \infty.$$

"The position of γ_D in $H_2(X_F, \mathbf{Z})$ encodes an *obstruction* to the presence of rational points on $E(F(\sqrt{D}))$. "

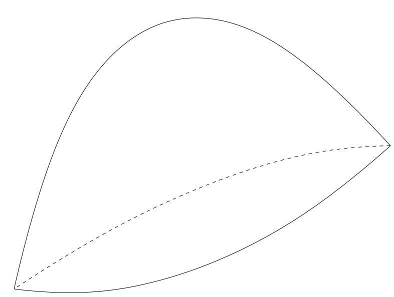
Periods of ω_G: the ATR case

Theorem: The cycles γ_R are *homologically trivial* (after tensoring with $\mathbf{Q}$).

This is because $H_1(X_F, \mathbf{Q}) = 0$.

Given $R \in \Sigma_D$, let

$\gamma_R^{\#}$:= any smooth two-chain on X_F having γ_R as boundary.



$$P_R := \int_{\gamma_R^{\sharp}} \omega_G \in \mathbf{C}/\Lambda_G \simeq E(\mathbf{C}).$$

The conjecture on ATR points

Assume still that $D_1 < 0$, $D_2 > 0$.

ATR points conjecture. If $R \in \Sigma_D$, then the point P_R belongs to $E(H_D) \otimes \mathbf{Q}$, where H_D is the Hilbert class field of $F(\sqrt{D})$.

Question: Understand the process whereby the one-dimensional ATR cycles γ_R on X_F lead to the construction of *algebraic points* on E.

Several potential applications:

a) Construction of algebraic points, and *Euler systems* attached to elliptic curves.

b) "Explicit" construction of class fields.

p-adic methods

Difficulty: One wants to relate a *complex analytic* invariant – the complex periods P_R – to an *arithmetic one* – points on E over abelian extensions of $\mathbf{Q}(\sqrt{D})$.

Simplification of the original question:

1. Replace the complex analytic periods by certain p-adic periods.

Advantage: These are easier to relate to p-adic Galois cohomology ("Selmer groups").

2. Replace the elliptic curve E by the *multiplicative group*.

Advantage: The connection between Selmer groups and rational/integral points (i.e., *units*) is better understood.

Work in progress: Dasgupta, Pollack.

Algebraic cycles

Replace "ATR cycles on the Hilbert modular surface X_F" by *algebraic cycles* on a higher-dimensional Shimura variety.

Basic example (Bertolini, Prasanna):

Let $K = \mathbf{Q}(\sqrt{-7})$, $E = \mathbf{C}/\mathcal{O}_K$,

$W =$ (uni)versal elliptic curve over $X_0(7)$,

$X = W \times E$ (a "Calabi-Yau threefold")

$$\mathrm{CH}^2(X)_0 = \left\{ \begin{array}{l} \text{null-homologous,} \\ \text{codimension two} \\ \text{algebraic cycles on } X \end{array} \right\} / \simeq .$$

“Exotic modular parametrisation”:

$$\Phi : \mathrm{CH}^2(X)_0 \longrightarrow E.$$

Theorem (Bertolini, Prasanna, D). The group $\Phi(\mathrm{CH}_2(X)_0(K^{\mathrm{ab}}))$ is a subgroup of $E(K^{\mathrm{ab}})$ of *infinite rank*, and gives rise to an *Euler system* of algebraic points on E.

The points in $E(K^{\mathrm{ab}})$ are tied to a rich geometric structure: an infinite collection of curves on a specific Calabi-Yau threefold.

A final question.

Vague Definition: A point $P \in E(\bar{\mathbf{Q}})$ is said to be *modular* if there exists: a Shimura(-like) variety X, an exotic modular parametrisation

$$\Phi : \mathrm{CH}^r(X)_0 \longrightarrow E,$$

and a "modular" cycle $\Delta \in \mathrm{CH}^r(X)$, such that

$$P = \lambda\Phi(\Delta), \qquad \text{for some } \lambda \in \mathbf{Q}.$$

Question. Given E, what points in $E(\bar{\mathbf{Q}})$ are modular?

Very optimistic: All algebraic points on E are modular.

Optimistic: All algebraic points on E satisfying a suitable "rank one hypothesis" are modular.

Legitimate question: Find a simple characterisation of the modular points.