Rational Points on Modular Elliptic Curves

II. Modular Forms

Hedrick Lecture Series

MAA MathFest
Boulder, Colorado
August 2003

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

Recall

Last time, we introduced

- Elliptic curves;

- Their L-functions

$$L(E, s) = \sum_n a_n n^{-s},$$

where $a_p = p - N_p$;

- The Birch and Swinnerton-Dyer conjecture:

$$\text{ord}_{s=1} L(E, s) = \text{rank}(E(\mathbf{Q})).$$

To control $L(E, s)$ (and its arithmetically defined coefficients) we will relate it to *modular forms*.

Modular forms

They are functions on the Poincaré upper half-plane:

$$\mathcal{H} = \{z : \Im(z) > 0\}$$

The group

$$\mathbf{SL}_2(\mathbf{Z}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbf{Z}, ad - bc = 1 \right\}$$

acts on $\mathcal{H}$ by Möbius transformations.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (z) = \frac{az + b}{cz + d}.$$

Given N fixed, we will also consider the subgroups

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbf{Z}) : N \text{ divides } c \right\}.$$

Modular forms

Definition. A *modular form* (of weight 2, level N) is a holomorphic function f on $\mathcal{H}$ satisfying

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

for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$.

Fourier expansion: $f(z+1) = f(z)$, so

$$f(z) = \sum_{n=0}^{\infty} \lambda_n q^n, \qquad q = e^{2\pi i z}.$$

L-**functions**: To the modular form $f(z)$ we associate the L-function

$$L(f,s) = \sum_n \lambda_n n^{-s}.$$

Hecke's Theorem

Theorem (Hecke). The L-function $Lf, s)$ has an analytic continuation to $s \in \mathbf{C}$.

Idea of Proof. Integral representation

$$(2\pi)^s \Gamma(s) L(E, s) = \int_0^\infty f(iy) y^s \frac{dy}{y}.$$

The symmetry satisfied by f under

$$z \leftrightarrow \frac{-1}{Nz}$$

makes it possible to rewrite the right-hand side as a sum of two integrals which converge *for all* $s \in \mathbf{C}$:

$$\int_{1/\sqrt{N}}^\infty f(iy) y^s \frac{dy}{y} \pm \int_{1/\sqrt{N}}^\infty f(iy) y^{2-s} \frac{dy}{y}$$

In fact one gets a *functional equation*

$$L(f, s) \leftrightarrow L(f, 2-s).$$

Wiles' theorem

Returning to E, and the *arithmetically defined* coefficients a_n;

These coefficients can be *packaged* into a *generating series*:

$$f_E(z) := \sum_{n=1}^{\infty} a_n e^{2\pi i n z}.$$

Obvious relation:

$$f_E(z+1) = f_E(z).$$

Modularity conjecture / Wiles' Theorem. The function $f_E(z)$ satisfies *extra, non-obvious* symmetries: it is a *modular form* of weight two and level N, for some N.

More precise form: The integer N is the arithmetic conductor of E, which can be calculated easily in terms of E.

An example

$E =$ an elliptic curve of conductor 11.

$$E : y^2 + y = x^3 - x^2 - 10x - 20$$

Setting $q = e^{2\pi i z}$,

$$\begin{aligned} f_E(z) &= q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 \\ &\quad -2q^7 - 2q^9 - 2q^{10} + q^{11} + \cdots \end{aligned}$$

$g(z) =$ the *unique* modular form of weight 2, level 11,

$$\boxed{g(z) = \eta(z)^2\eta(11z)^2}$$

$$\begin{aligned} g(z) &= q\left(\prod_{n=1}^{\infty}(1-q^n)(1-q^{11n})\right)^2 \\ &= q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 \\ &\quad -2q^7 - 2q^9 - 2q^{10} + q^{11} + \cdots \end{aligned}$$

These two series are equal!

Remarks on Wiles' Theorem

• Wiles' theorem effectively *tames* the coefficients N_p in the same way that the quadratic reciprocity law sheds light on the N_p's in the simpler case of the circle and Pell equations of the previous lecture.

• It lies *much deeper* than quadratic reciprocity, but is part of the same borad current of ideas.

• Amazingly, it implies Fermat's Last Theorem.

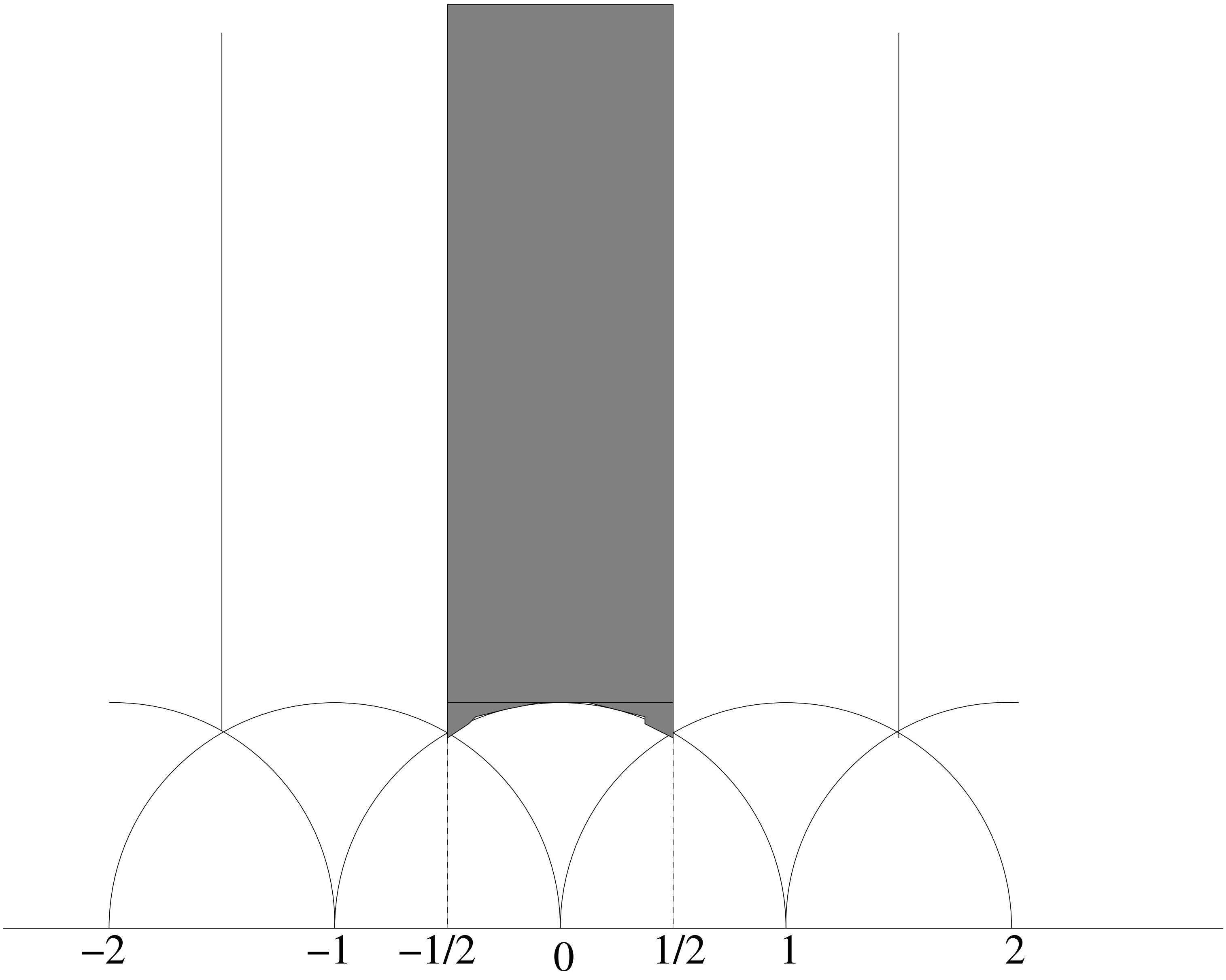
• More germane to this lecture are its applications to the theory of elliptic curves.

1. The L-function $L(E, s)$ has an analytic continuation;

2. The curve E is endowed with a *modular parametrisation*.

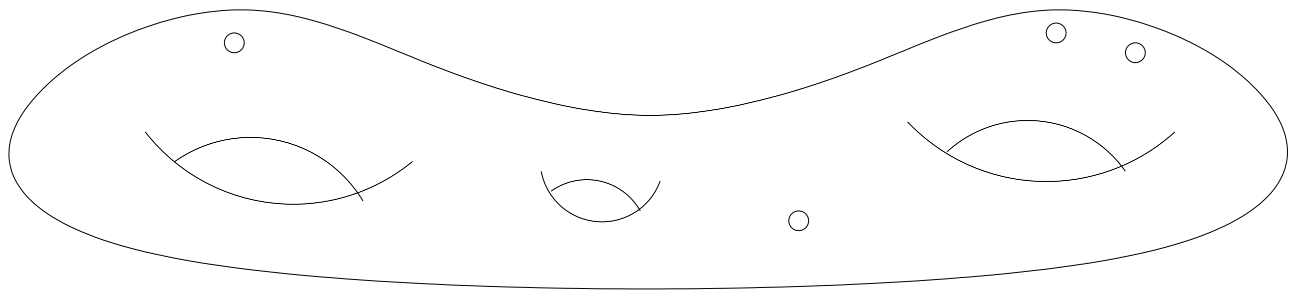
Quotients of $\mathcal{H}$

The quotient $\mathcal{H}/\mathbf{SL}_2(\mathbf{Z})$ is isomorphic to the complex plane (punctured Riemann sphere).



The quotient $\mathcal{H}/\Gamma_0(N)$

Likewise $\mathcal{H}/\Gamma_0(N)$ is a Riemann surface



Remarkably, it can be described by polynomial equations with *rational* coefficients.

This is one reason why this quotient, the so-called *modular curve* $X_0(N)$, is of such interest to number theorists!

Restatement of modularity: There is a non-constant algebraic map from $X_0(N)$ to the elliptic curve E.

Modular parametrisations

The expression $2\pi i f_E(z)z$ is a differential form on $\mathcal{H}$ which is *invariant* under $\Gamma_0(N)$, i.e., a differential on $\mathcal{H}/\Gamma_0(N)$.

Given $\tau \in \mathcal{H}$, set

$$J_\tau := \int_{i\infty}^{\tau} 2\pi i f(z)dz = \sum_n \frac{a_n}{n} e^{2\pi i n\tau} \in \mathbf{C}.$$

$$\exp_E : \mathbf{C} \longrightarrow E(\mathbf{C}) \quad \text{(Exponential map).}$$

$$P_\tau := \exp_E(J_\tau) \in E(\mathbf{C}).$$

The assignment

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

defined by

$$\Phi(\tau) = P_\tau$$

is called the *modular parametrisation* attached to E.

Complex multiplication

Note that the modular parametrisation Φ is transcendental as a function of $\tau \in \mathcal{H}$. In fact,

Theorem. If $\tau \in \mathcal{H} \cap \bar{\mathbf{Q}}$, then $\Phi(\tau)$ has transcendental coordinates, *with one crucial exception*.

Complex multiplication theorem. If τ is a quadratic irrationality then $\Phi(\tau)$ is *algebraic* as well.

More precisely, if τ belongs to $\mathcal{H} \cap K$, where K is a quadratic (imaginary) extension of $\mathbf{Q}$, then $\Phi(\tau)$ belongs to $E(K^{\mathrm{ab}})$.

$$K^{\mathrm{ab}} := \text{ maximal abelian extension of } K.$$

An example

Returning to the elliptic curve

$$E : y^2 + y = x^3 - x^2 - 10x - 20$$

of conductor $N = 11$, set

$$\tau = \frac{-3 - \sqrt{-2}}{11}$$

$$J_\tau = 0.1269209304\ldots - 0.5360796103\ldots i$$

$$\begin{aligned} P_\tau &= (-3.000000\ldots + 1.4142135\ldots i, \\ &\qquad 3.000000\ldots + 4.2426406\ldots i) \\ &= (-3 + \sqrt{-2}, 3 + 3\sqrt{-2}) \end{aligned}$$

Heegner points

Fix a quadratic imaginary field $K \subset \mathbf{C}$.

Definition A point of the form

$$\Phi(\tau), \text{ with } \tau \in \mathcal{H} \cap K$$

is called a *Heegner point* (attached to K.)

$$\boxed{\mathrm{HP}_K := \text{Group generated by } \Phi(\mathcal{H} \cap K).}$$

$\mathrm{HP}_K \subset E(K^{\mathrm{ab}})$ is called the *Heegner subgroup* attached to K.

Questions.

- How big is HP_K?

- What about $\mathrm{HP}_K \cap E(K)$ or $\mathrm{HP}_K \cap E(\mathbf{Q})$?

Some “elementary” facts

• Good news: for any K, rank(HP_K) $= \infty$;

• Bad news: rank($\mathsf{HP}_K \cap E(K)$) ≤ 1, and hence

$$\mathrm{rank}(\mathsf{HP}_K \cap E(\mathbf{Q})) \leq 1.$$

Question. When is rank($\mathsf{HP}_K \cap E(K)$) $= 1$?

• If there is a prime $\ell | N$ which is inert in K, then $\mathsf{HP}_K \cap E(K)$ is trivial.

Assume from now on: all primes dividing N are split in K.

The Gross-Zagier theorem

Given $K = \mathbf{Q}(\sqrt{D})$, $E : y^2 = x^3 + ax + b$, define

$$E^{(D)} : Dy^2 = x^3 + ax + b.$$

$$L(E/K, s) := L(E, s)L(E^{(D)}, s).$$

Theorem (Gross-Zagier) $\mathrm{HP}_K \cap E(K)$ is infinite if and only if $\mathrm{ord}_{s=1} L(E/K, s) = 1$.

Proof: a (very) involved calculation which relates $L'(E/K, 1)$ to the *Néron-Tate canonical height* of a generator of $\mathrm{HP}_K \cap E(K)$.

Conclusion: The "Heegner point approach" produces a point of infinite order on $E(K)$, if and only if

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

Kolyvagin's Theorem

Kolyvagin's Theorem. If $\mathrm{HP}_K \cap E(K)$ is infinite, then $E(K)$ has rank one and $Ш_E$ is finite.

Proof. The *purely algebraic* proof does not involve $L(E,s)$ at all.

It uses the *entire collection* HP_K to bound the size of $E(K)$ under the hypothesis that $\mathrm{HP}_K \cap E(K)$ is non-trivial.

Note the apparently paradoxical nature of this result...

Proof of the Gross-Zagier-Kolyvagin Theorem

Theorem. If $\mathrm{ord}_{s=1} L(E,s) \leq 1$, then

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

and $Ш_E$ is finite.

Proof. There exists K such that

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

By Gross-Zagier,

$$\mathrm{HP}_K \cap E(K) \text{ is infinite.}$$

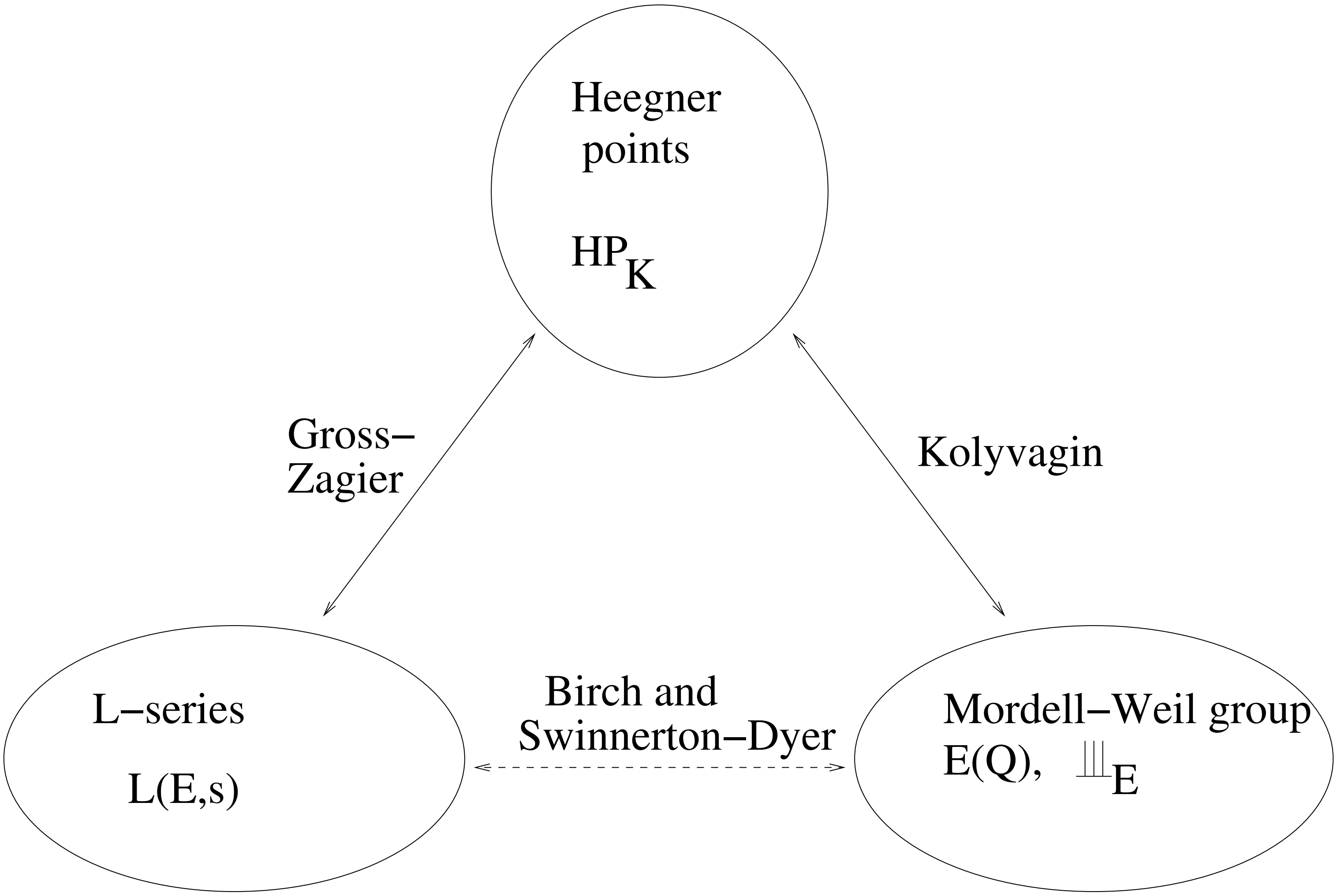
By Kolyvagin's theorem,

$$\mathrm{rank}(E(K)) = 1 \text{ and } Ш_E \text{ is finite.}$$

Hence BSD is true for E/K.

A more careful analysis yields BSD for $E/\mathbf{Q}$.

Summary



Heegner points
HP$_K$
Gross–Zagier
Kolyvagin
L–series
L(E,s)
Birch and Swinnerton–Dyer
Mordell–Weil group
E(Q), Ш$_E$

Next lecture

In the next lecture, I will discuss possible generalisations (conjectural, and otherwise) of the Heegner point construction.