Modularity

26/3/21
Chris Williams

Modularity: "$\exists$ a deep correspondence between elliptic curves and modular forms."

§1: Motivation & applications

1) **Proof of Fermat's last theorem:** suppose $X^n + Y^n = Z^n$, $n \geq 3$, $XYZ \neq 0$.

$\xrightarrow{\text{(Frey)}}$ $\exists$ associated elliptic curve $E/\mathbb{Q}$ ("Frey curve") conductor N

$\xrightarrow[\text{(wiles)}]{\text{Modularity}}$ $\exists$ associated wt 2 modular form $f \in S_2(\Gamma_0(N))$

$\xrightarrow[\text{(Ribet)}]{\text{level lowering}}$ $\exists$ non-zero $g \in S_2(\Gamma_0(2))$

$\rightsquigarrow$ Contradiction! $\dim S_2(\Gamma_0(2)) = \text{genus}(X_0(2))$ (Ben)

$= 0.$

2) **Stating BSD:** "$\text{rk}\, E(\mathbb{Q}) = \text{ord}_{s=1} L(E,s)$".

Drill a bit deeper. Relatively 'easy' to see $L(E,s)$ converges absolutely for $\text{Re}(s) > 3/2$...

... but $s = 1$ is not in this range, so a priori $\text{ord}_{s=1} L(E,s)$ is not well-defined!!

Modularity $\Rightarrow$ $\exists$ $f \in S_2(\Gamma_0(N))$ such that

$$L(E,s) = L(f,s)$$

$\uparrow$ has analytic continuation to $\mathbb{C}$ (Barna)

$\Rightarrow$ $L(E,s)$ has analytic continuation to $\mathbb{C}$

$\Rightarrow$ $\text{ord}_{s=1} L(E,s)$ is well-defined (phew!).

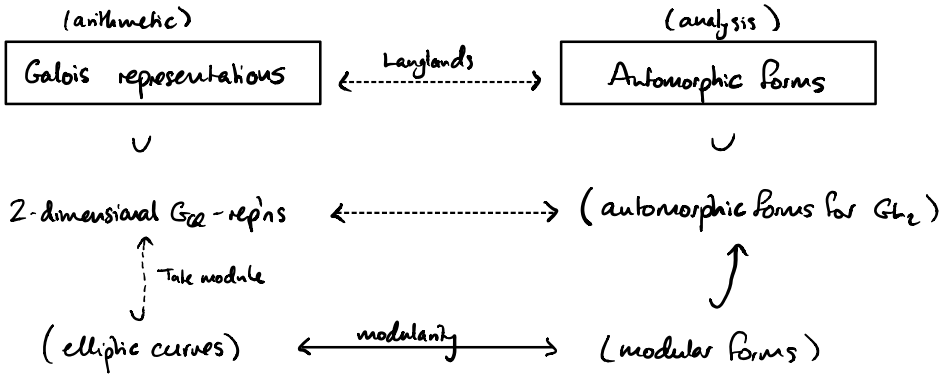
... this is NOT known without using modularity.

3) Proving cases of BSD : Modularity allows constructions of Heegner points, points of infinite order on elliptic curves (Gross-Zagier).

$\rightsquigarrow$ Led to Kolyvagin's proof of BSD in analytic rank 1.

(I'll come back to this).

4) GL_2-case of (global) Langlands :



"Modular forms, and their generalisation automorphic forms/representations, are a universal theory for algebraic number theory."

Note: Langlands for GL_1 is CFT. So modularity is like a "2-dimensional CFT".

§2: Modularity via modular curves

Let $E/\mathbb{Q}$ elliptic curve of conductor N. Then:

- (Diana) $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$ = compact Riemann surface,
- (Ben) $X_0(N) = \Gamma_0(N)\backslash\mathcal{H}$ = compact Riemann surface.

Modularity A: $\exists$ surjective map $X_0(N) \longrightarrow E(\mathbb{C})$ of cpct Riemann surfaces.

... but this isn't very arithmetic. Note:

- E is a variety $/\mathbb{Q}$ (def'n)
- $X_0(N)$ has a model $/\mathbb{Q}$ (Steven)

Modularity B: $\exists$ morphism $\pi: X_0(N) \longrightarrow E$ of varieties $/\mathbb{Q}$.

Note: we have $A \Leftrightarrow B$. $B \Rightarrow A$ is easy, $A \Rightarrow B$ is not.

§3: Application: Heegner points

Interested in rational points on elliptic curves. Modularity B gives a way of finding them:

- Suppose $x \in Y_0(N)(\mathbb{Q})$. Then $\pi(x) \in E(\mathbb{Q})$.
- (Philippe) $Y_0(N)$ has a moduli description: $K/\mathbb{Q}$ field,

$$Y_0(N)(K) = \left\{ \text{pairs } \left(\underbrace{A/K}_{\text{elliptic curve}}, \; \underbrace{C \subset A(K)[N]}_{\text{subgp exact order } N} \right) \right\} \Big/ \sim$$

- Heegner points: write down "good" pairs $(A, C) \in Y_0(N)$ using Complex multiplication.

CM: crash course (cf. Silverman, "Advanced topics...", §II)

Let K imaginary quadratic field, integers $\mathcal{O}_K \subset K$, $I \subset \mathcal{O}_K$ ideal. Fix $K \hookrightarrow \mathbb{C}$.

Then:

$$I \hookrightarrow \mathbb{C} \quad \text{is a lattice.}$$

Let $A_I := \mathbb{C}/I$, elliptic curve over $\mathbb{C}$.

Note: (Diana) $\mathrm{End}(A_I) = \{\alpha \in \mathbb{C} : \alpha I \subset I\}$
$= \mathcal{O}_K$ (I ideal).

We say A_I has <u>CM by $\mathcal{O}_K$</u>.

<u>Theorem</u>: (a) Let $I, J \subset \mathcal{O}_K$, then $A_I \cong A_J \iff [I] = [J]$ in Cl_K.

(b) $\exists$ bijection

$$\left\{ \begin{array}{l} \text{ell. curves } /\mathbb{C} \\ \text{w/ CM by } \mathcal{O}_K \end{array} \right\} \longleftrightarrow Cl_K,$$

$$A_I \longleftrightarrow [I].$$

(c) A_I has a model over the Hilbert class field H_K of K.

(Recall: $H_K :=$ max. abelian ext. of K unramified everywhere; $\mathrm{Gal}(H_K/K) \cong Cl_K$).

<u>Example</u>: Suppose K class number 1, eg. $\mathbb{Q}(i)$. Up to isomorphism, there is a unique ell. curve $A_{\mathcal{O}_K} = \mathbb{C}/\mathcal{O}_K$ with CM by $\mathcal{O}_K$. Also, $A_{\mathcal{O}_K}$ has a model over K.

Recall $E/\mathbb{Q}$ has conductor N. Suppose N has <u>squarefree</u> conductor. Assume:

<u>Heegner hypothesis</u>: every $p \mid N$ splits in K.

This implies $\exists$ ideal $\eta \subset \mathcal{O}_K$ with $\mathcal{O}_K/\eta \cong \mathbb{Z}/N\mathbb{Z}$.

(If $N = p_1 \cdots p_r$, $p_i \mathcal{O}_K = \mathfrak{p}_i \bar{\mathfrak{p}}_i$, then $\eta = \mathfrak{p}_1 \cdots \mathfrak{p}_r$).

Then $\eta^{-1}/\mathcal{O}_K \subset \mathbb{C}/\mathcal{O}_K = A_{\mathcal{O}_K}(\mathbb{C})[N]$.

$\eta^{-1}/\mathcal{O}_K \cong \mathbb{Z}/N\mathbb{Z}$

↑ Fact: $\eta^{-1}/\mathcal{O}_K \subset A_{\mathcal{O}_K}(K)[N]$ order N.

Corollary: $x_K := \left(A_{\mathcal{O}_K}, \eta^{-1}/\mathcal{O}_K\right) \in Y_0(N)(K) \subset X_0(N)(K)$.

↳ so under $\pi: X_0(N) \to E$, we have $P_K := \pi(x_K) \in E(K)$.

Theorem: (Gross-Zagier). $ht(P_K) = (\neq 0) \cdot L'(E/K, 1)$.

So: if $L(E/K, 1) = 0$, $L'(E/K, 1)$ (ie. $\operatorname{ord}_{s=1} L(E/K, 1) = 1$).

$\Rightarrow ht(P_K) \neq 0$;

$\Rightarrow P_K$ has infinite order

$\Rightarrow \operatorname{rk} E(K) \geq 1$! (ie. one inequality in BSD for E/K).

Remarks: (1) Can descend to $\mathbb{Q}$ (Murty-Murty): $E(K) = E(\mathbb{Q}) \cup E^{\chi_{K/\mathbb{Q}}}(\mathbb{Q})$,

$L(E/K, s) = L(E/\mathbb{Q}, s)\, L(E^{\chi_{K/\mathbb{Q}}}/\mathbb{Q}, s)$.

↑ Artin Formalism

(2) Heegner points can be made into an Euler system.

(3) All of this was key to Kolyvagin's proof of BSD in analytic rank 1.

§4: Modularity via modular forms

Slogan: "[arithmetic of $X_0(N)$] = $\bigoplus_{\substack{f \in S_2(\Gamma_0(N)) \\ \text{eigenform}}}$ [arithmetic of f]." (DRS, §6).

Precisely: Let

$$J_0(N) := \text{Jacobian}(X_0(N)) = \text{Pic}^0(X_0(N)) \qquad \text{(Muhammad)}$$
$$= \text{abelian variety}/\mathbb{Q} \text{ of dimension } g = \text{genus}(X_0(N)).$$

Modularity C: $\exists$ morphism

$$\begin{array}{ccc} \text{Pic}^0(X_0(N)) & \longrightarrow & \text{Pic}^0(E) \\ \| & & \| \\ J_0(N) & \longrightarrow & E \end{array}$$

of abelian varieties.

Want to control the kernel. Xenia, Barna, Muhammad: the Hecke operators T_ℓ act on $J_0(N)$. (by correspondences).

Definition: Let $f \in S_2(\Gamma_0(N))$ newform $T_\ell f = a_\ell f \ \forall \ell$. Let

$$A_f := J_0(N) \Big/ \{T_\ell - a_\ell : \ell\}.$$

= "piece of $J_0(N)$ where T_ℓ acts like it does on f".

Theorem: $\exists$ isogeny $J_0(N) \sim \bigoplus_{[f \text{ newform}, M \mid N]} A_f^{m_f}$,

m_f = multiplicity of f in $S_2(\Gamma_0(N))$
$= 1$ if $f \in S_2(\Gamma_0(N))^{\text{new}}$.

Fact: If f has Hecke eigenvalues in $\mathbb{Z}$, then A_f is an elliptic curve.

Modularity: $\exists\ f \in S_2(\Gamma_0(N))$ newform such that:

(D) $\exists$ isogeny $A_f \longrightarrow E$;

Combined with reduction mod p (Horatio) + Eichler–Shimura (Muhammad):

(E) $a_p(f) = a_p(E) \quad \forall p$;

(F) $L(f,s) = L(E,s)$;

ℓ-adic Galois representation of f is Tate module $V_\ell f := \varprojlim A_f[\ell^n] \otimes \mathbb{Q}$

" " of E " $V_\ell E := \varprojlim E[\ell^n] \otimes \mathbb{Q}$.

(G) $V_\ell f \sim V_\ell E$ are equivalent.

Remark: Version (G) was proved by Wiles, Breuil-Conrad-Diamond-Taylor.