Clemson ADM
Tonghai Yang
2-5-09

Solving Diophantine Equations with Analysis:

$E: y^2 = x^3 + ax + b \quad a, b \in \mathbb{Z}$ elliptic curve

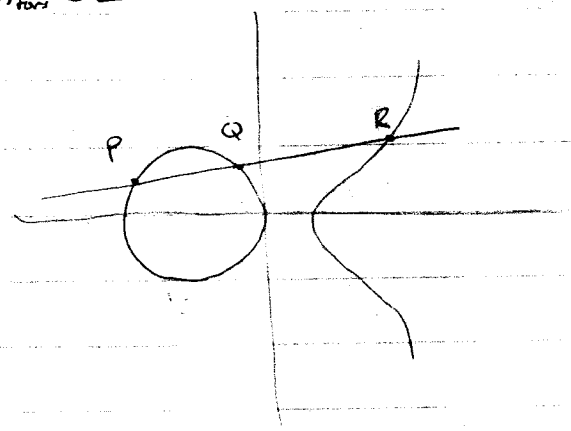
Why popular?

1. Wiles' proof of FLT.
2. BSD
3. Cryptography
4. Congruent number problem

Why interesting?

① $E(\mathbb{Q}) = \{$ all rational solutions $\} \cup \{\infty\}$ f.g. abelian group.

$= E(\mathbb{Q})_{tors} \oplus \mathbb{Z}^r$



$P+Q+R=0.$

r = rank of $E(\mathbb{Q})$

② modular

$E(\mathbb{Q})$ is hard to understand. Easier to study $E(\mathbb{F}_p)$

$$a_p = p+1 - \#E(\mathbb{F}_p)$$

Basic idea: $\{a_p\}$ gives you a lot of information about $E(\mathbb{Q})$.

Use these to produce an L-function

$$L(E,s) = \prod_{p \text{ good}} (1 - a_p p^{-s} + p^{1-2s})^{-1} \times \underset{\text{from bad primes}}{*}$$

Abs conv. for $Re(s) > 3/2$.

Thm (Wiles & BCDT): $L(E,s)$ has analytic continuation to the whole complex plane and

$$L(E,s) = W(E) * L(E, 2-s)$$

($*$: Γ-factors; $W(E)$: root # of E, $= \pm 1$)

$s=1 \Rightarrow \quad L(E,1) = W(E)\, L(E,1)$ $\quad W(E)=1$ doesn't say much

$W(E)=-1 \Rightarrow L(E,1) = 0$

BSD conj: ① $\operatorname{ord}_{s=1} L(E,s) = \operatorname{rk} E(\mathbb{Q})$

② Leading coefficients of $L(E,s)$ at $s=1$ gives more about $E(\mathbb{Q})$.

Cor: (BSD) $W(E)=-1 \Rightarrow E(\mathbb{Q})$ is infinite

Thm (Gross-Zagier, Kolyvagin, Waldspurger): If $\operatorname{ord}_{s=1} L(E,s) = 0, 1$ then BSD ① holds. Moreover, in the case $L'(E,1) \neq 0$, we can construct a pt in $E(\mathbb{Q})$ of infinite order.

(This pt is called a **Heegner pt**.)

Modular Curves and Heegner Pts:

$\mathfrak{H} = \{ z \in \mathbb{C} : \operatorname{Im}(z) > 0 \}$ $\circlearrowleft SL_2(\mathbb{R})$

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

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : N \mid c \right\}$$

$\Gamma_0(N) \backslash \mathfrak{H} = Y_0(N) =$ open Riemann surface / $\mathbb{C}$.

This is actually defined over $\mathbb{Q}$ since it is a moduli space of $(E \xrightarrow{\varphi} E')$ where E, E' are elliptic curves, φ is an isogeny s.t. $\ker\varphi$ is a cyclic group of order N. (It is actually even defined over $\mathbb{Z}$!)

Heegner pts: $\tau \in \mathfrak{h}$ is an algebraic number.

$$[\tau] \in \mathfrak{h}/\Gamma_0(N) = Y_0(N)$$

Thm: $[\tau]$ is algebraic iff τ is a quadratic

Heegner pt: $\tau = \frac{b+\sqrt{D}}{2a} \in \mathfrak{h}$ is a Heegner pt of disc D in $Y_0(N)$ if every $p \mid N$ splits / ramifies in $\mathbb{Q}(\sqrt{D})$.

There are finitely many Heegner pt of disc. D.

$$Z(D) = \sum_{\mathrm{disc}(\tau)=D} [\tau] \in Z^1(Y_0(N)) \cap 1 \qquad \text{Heegner cycle defined over } \mathbb{Q}.$$

$$X_0(N) =$$

$$y(D) = Z(D) - \deg Z(D) \frac{(0)+(\infty)}{2} \in J_0(N)(\mathbb{Q}) \text{ an abelian variety.}$$

Neron-Tate: $J_0(N)(\mathbb{Q})$ = f.g. abelian group

There is a canonical positive definite quadratic form (Neron-Tate height)

$$\langle , \rangle_{NT} : J_0(N)(\mathbb{Q})/_{\text{tors}} \times J_0(N)(\mathbb{Q})/_{\text{tors}} \longrightarrow \mathbb{R}_{\geq 0}.$$

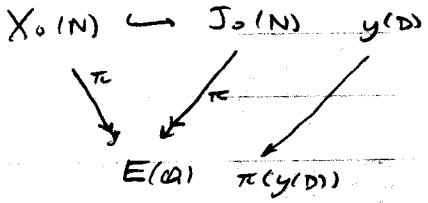
$\langle y, y \rangle_{NT} = 0 \iff y$ is of finite order.

Basically, we have used a nice field to produce a rational pt on an abelian

variety. Neron-Tate tells you whether the pt you produced is trivial or not!

Wiles + BCDT: E is modular

① $\exists$ a non-zero map



② $L(E,s) = L(f_E, s)$ for some newform f_E of wt 2 level $\Gamma_0(N)$.

Gross-Zagier Formula: (1980's) (Special case) $w(E) = -1$, $p \mid N$ is split in $\mathbb{Q}(\sqrt{D})$.

$$L'(E,1)\, L(E^D, 1) = * \langle y(D), y(D) \rangle_{NT}$$

where

E_D: $Dy^2 = x^3 + ax + b$ is the quadratic twist of E.

One can always find D s.t. $L(E^D, 1) \neq 0 \Rightarrow L'(E,1) \neq 0 \iff$ $y(D)$ is of infinite order.

$\overset{\text{Kolyvagin}}{\Rightarrow}$ $\operatorname{rk} E(\mathbb{Q}) = 1$ (all other pts are mult. of $y(D)$).

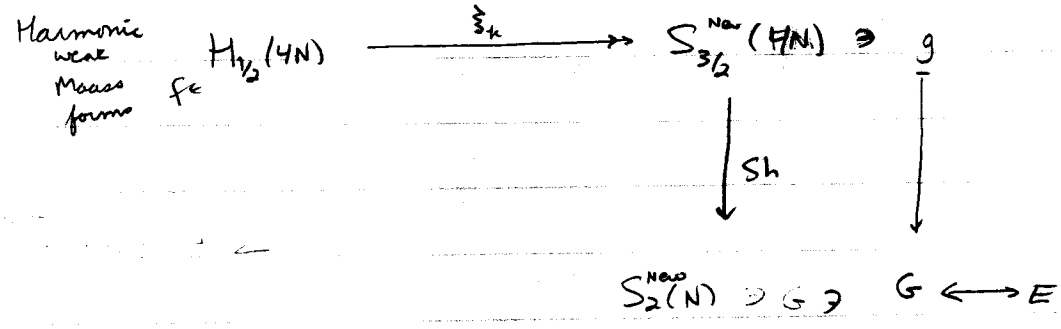
Question: Can we construct "y_E" s.t. $L'(E,1) = * \langle y_E, y_E \rangle_{NT}$?

Thm (Brunier & Y. to appear in Invent.): We can construct y_E systematically s.t. $L'(E,1) = * \langle y_E, y_E \rangle_{NT}$ when $w(E) = -1$.

The proof is very different from the standard proof of G-Z. using mostly modularity.

This theorem is part of a more general form on Shimura variety of orthogonal type.

(Actually for general modular forms, not just at 2 & 4)



$$f = \underbrace{\sum_{n \geq n_0} c^+(n) q^n}_{f^+(\tau)} + \underbrace{\sum_{n<0} c^-(n)\, \Gamma(1/2, 4\pi|n|v)\, q^n}_{f^-(\tau)}$$

$$y(f) \longrightarrow y_E$$

$$y(f) = \sum_{n>0} c^+(-n)\, y(-n) \in J_0(N) \longrightarrow E$$

Thm: $* \quad L'(G, 1) = \langle y(f), y(f) \rangle_{NT}$