A gallimaufry of Heegner points

Alex

"The fun of the subject seems to be in the examples." - Gross ①

Fix an elliptic curve $E/\mathbb{Q}$ conductor N

$$\begin{tikzcd}
\phi_N: X_0(N) \arrow[r, hook] \arrow[d, phantom, sloped, "\cong"] & J_0(N) \arrow[r, two heads] & E \arrow[d, phantom, sloped, "\cong"] & \text{modularity} \\
\mathbb{H}/\Gamma_0(N) & & \mathbb{C}/\Lambda \ \leftarrow \text{period lattice}
\end{tikzcd}$$

$$\overset{\Psi}{\tau} \longmapsto \int_{\infty}^{\tau} 2\pi i f(z)\,dz = \sum_{n=1}^{\infty} \frac{a_n}{n} q^n, \quad q = e^{2\pi i \tau}$$

where f modular form corr. to E ie $f = \sum a_n q^n$

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

Approximate image of map at CM i.e. Heegner pts by computing "enough" Fourier coeffs.

Defn $\tau \in \mathbb{H}$ is a CM point if it satisfies $A\tau^2 + B\tau + C = 0$ where $\Delta(\tau) = B^2 - 4AC < 0$ assuming ~~assuming~~ $(A,B,C) = 1$, $A > 0$. Associated quadratic form is $Ax^2 + Bxy + Cy^2$.

A Heegner point of level N is such a τ where $\Delta(N\tau) = \Delta(\tau)$.

Part I: generators of rank 1 elliptic curves

Prop: With the notation above, τ is a Heegner point iff $N \mid A$, and one of the following hold:

(i) $\gcd(A/N, B, CN) = 1$

(ii) $\gcd(N, B, AC/N) = 1$

(iii) $\exists F \in \mathbb{Z}$ st $B^2 - 4NF = D$ w/ $\gcd(B, N, F) = 1$.
$\quad\quad\uparrow$ discriminant

cor If τ Heegner level N then so is $\frac{-1}{N\tau} =: W(\tau)$. "Fricke involution"

prop There is a one-to-one correspondence between the sets

$$\left\{ \begin{matrix} \text{Heegner pts of} \\ \text{level } N, \text{ disc } D \end{matrix} \right\} \Big/ \Gamma_0(N) \longleftrightarrow \left\{ (\beta, [\mathfrak{a}]) \mid \beta \in \mathbb{Z}/2N, [\mathfrak{a}] \in Cl(K), \ \beta^2 \equiv D \bmod 4N, \ K = \mathbb{Q}(\sqrt{D}) \right\}$$

Idea: $(\beta, [\mathfrak{a}]) \to$ quad form $Ax^2 + Bxy + Cy^2$ ~~and~~ ~~$B \equiv B$ mod $2N$~~
~~for~~ $\Leftrightarrow$ square disc mod $4N$ $\quad \Rightarrow$ ~~[illegible]~~ $\beta \equiv B$ mod $2N$
$N \mid A$,

$$\tau = \frac{-B + \sqrt{D}}{2A}.$$

$\textcircled{?}$ $\square$

---

① Reference: Henri Cohen: Number Theory: Part I (tools...)

Fix τ a Heegner point level N disc D corresponding to $(\beta, [\alpha])$

Then the "main theorem to CM" implies $\phi_N(\tau)$ lands in $E(H)$ where H is the Hilbert class field of K.

To turn the image into K-pts, take traces; in the following way:

$P \in E(K)$ can be written as

$$P = \sum_{\sigma \in Gal(H/K)} \phi_N((\beta, [\mathfrak{a}]))^{\sigma} = \sum_{\cancel{\mathfrak{b}} \in Cl(K)} \phi_N((\beta, [\cancel{\mathfrak{a}}\mathfrak{a}\mathfrak{b}^{-1}]))$$

RHS faster to compute (as an approx. first add in $E(\mathbb{C})$, then recognize as $E(K)$ pt rather than LHS acting by Gal in $E(H)$.)

<u>Lemma</u>: If $\varepsilon = -1$ ← root number = sign in functional eqn for $L(E,s)$ then $P \in E(\mathbb{Q})$.

<u>Pf</u> $\varepsilon = -1 \Leftrightarrow \phi_N \circ W = \phi$ then $\overline{P} = P$. $\square$

If $\varepsilon = +1$ then $P + \overline{P}$ torsion.

<u>Gross-Zagier</u>

$$\hat{h}(P) = \frac{\sqrt{D}}{4\,Vol(E)} L'(E,1)\, L(E_D,1)$$

$Vol(E)$ ← $Vol(\Lambda)$

where E_D is the Dth quadratic twist

<u>Example</u> If $L(E_D,1) = 0$ for some D then $RHS = 0 \Rightarrow P$ is torsion.

If $rk\ E = 1$ and G generates $E(\mathbb{Q})$ $P = \ell \cdot G$ for some $\ell \in \mathbb{Z}$

combine $GZ + BSD$:

$c(E)$ ← product of Tamagawa #s

$$\frac{\ell^2}{|Ш(E)|} = \omega_1(E) \cdot \frac{c(E)\sqrt{|D|}}{4\,Vol(E)\,|E_{tors}(\mathbb{Q})|^2} L(E_D,1)$$

$\omega_1(E)$ ↑ real period

RHS is quite computable in practice!

So: want to compute evaluations $\phi_N\left(\frac{-B+\sqrt{D}}{2A}\right)$ for (A,B,C) representing all classes in $Cl(K)$.

Question How does ϕ_N converge?

A: "like a geometric series w/ ratio $e^{-2\pi\, im\, \tau} = e^{-2\pi\sqrt{|D|}/2A}$ "

(apply Hasse bd + some composite/power ... $\frac{a_n}{n} \leftarrow$ dominates)

can also use

$$\phi_N((B,[A])) = \phi_N(B,[\mathfrak{a}^{-1}\mathfrak{n}])$$

↑ ideal norm N need all primes of norm N to split

to halve the # of classes to consider

Algorithm input E rank 1

1. Use BSD to find

$$|Ш(E)|\cdot R(E) = \frac{|E_{tors}(\mathbb{Q})|^2 \cdot L'(E,1)}{c(E)\,\omega_1(E)}$$

2. Find height bound

$$HB = \frac{h(j(E))}{12} + \underset{???}{\mu(E)} + 1.946$$

3. Let $d = 2(|Ш(E)|\,R(E) + HB)$

$dd = \lceil d/\log(10)\rceil + 10$

bad var name

4. Run through D until we find one st ① $D \equiv \square^2 \mod 4N$

② $L(E_D,1)$ is not too close to zero.
{has formula, rapidly converging}

③ all primes dividing N split in $K = \mathbb{Q}(\sqrt{D})$ ← for simplicity $[D \neq -3,-4]$

otherwise: try next D.

5. Fix $\beta \in \mathbb{Z}/2N$ such that $D = \beta^2 \mod 4N$, compute

$$m^2 = \omega_1(E)\,\frac{c(E)\sqrt{|D|}}{|E_{tors}(\mathbb{Q})|^2\, 4\, Vol(E)}\, L(E_D,1)$$

m "should be close to an integer or at least small denominator" [ie $m^2 = \frac{l^2}{|\text{Ш}(E)|}$ should be a small # on denom ~~fraction~~ which is square ie $\frac{l^2}{b^2}$ $\overset{\uparrow}{}$ small --]

6. Find a list $\mathcal{L}$ of forms (A, B, C) corr. to $Cl(K)$ such that $N \mid A$, $\beta \equiv B \bmod 2N$ minimal

7. $$z = \sum_{\substack{(A,B,C) \\ \in \mathcal{L}}} \phi_N\left(\frac{-B+\sqrt{D}}{2A}\right) \in \mathbb{C} \longrightarrow \mathbb{C}/\Lambda \xrightarrow[(\wp, \wp')]{} E(\mathbb{C})$$

Note: Want element in $\mathbb{C}/\Lambda$ to be as close to zero as possible

8. Normalize further using torsion points to get point closer to 0. $z \mapsto z'$. Compute $\wp(z')$

Recognize this as $x = \frac{a}{d^2}$ (continued fractions).

Output Generator for finite index subgrp $y = \frac{b}{d^3}$.

E.g. Recall congruent number problem : what #s are areas of rational right Δs ?

$$E_n : y^2 = x^3 - n^2 x$$

for instance is $n = 157$ a congruent number? BSD says yes!

But what Δ? Need genuine rational pt.

$N = 788768$. $\omega_1 = 0, 2092...$ $|E(\mathbb{Q})_{\text{tors}}| = 4$

$c(E) = 8$, $|\text{Ш}| R(E) \approx 54.6...$ $HB = 10.6$

$d \approx 130.4 \ldots$ $\leadsto$ use 67 decimal digits

What D?

Up to -4, -31 and -34 work ie they are squares mod 4N

but $L(E_{-31}, 1) \approx 0$

$\Rightarrow$ use $D = -39$ $\frac{l^2}{|\text{Ш}|} \approx 16$ so $m = 4$

$\beta = 1275547$ ($\overset{\text{mod}}{4N}$). $Cl(\mathbb{Q}(\sqrt{-39})) = \mathbb{Z}/4\mathbb{Z}$

$z = 2\,\text{Re}\,(\phi_N(x_1) + \phi_N(x_2))$, $x_1 = \frac{-\beta + \sqrt{-39}}{2_1 N}$. largest $A = 2N$, need 10.5 million coeffs. of ϕ_N

so $z = -5.639\ldots \bmod \Lambda$ $\leftarrow$ ω_1 generates Λ so reduce $\leadsto z = 0.0111\ldots + 27\omega_1$ then compute $\wp$(this complex + tors) $= \frac{20 \text{digits}}{18 \text{digits}}$ = x-coord