② Complex Multiplication (CM)

27/10/2023

Warmup: Calculate $e^{\pi\sqrt{163}} - (640320)^3$.

SAGE: 256
Google: 0
Phone: −288
Wolfram: 743.999999999999

→ What's going on?

Today: 2 parts I. EC with CM & the main thm of CM
II. Heegner constructions

I. Towards the Main Thm of CM

Def. An *elliptic curve* E/k is a smooth projective algebraic curve of genus 1 together with a given point $O \in E(k)$.

↳ can define a group law on E with O = identity.

If $\mathrm{char}(k) \neq 2,3$, then $\exists A, B \in k$ s.t. (E, O) is isomorphic to a Weierstraß equation

$$y^2 = x^3 + Ax + B \quad \subseteq \mathbb{P}^2, \quad [0:1:0]$$

or to an eq. of the form

$$y^2 = 4x^3 - g_2 x - g_3, \quad g_2, g_3 \in k$$

s.t. $\Delta := g_2^3 - 27 g_3^2 \neq 0$.

Its *j-invariant* is

$$j(E) := 1728 \frac{g_2^3}{\Delta}.$$

Uniformization Theorem: If E is an EC/$\mathbb{C}$, $\exists$ lattice $\Lambda \subset \mathbb{C}$ s.t.

$$\mathbb{C}/\Lambda \xrightarrow{\sim} E(\mathbb{C}) \qquad \text{(iso. of complex Lie groups)}$$

$$z \longmapsto [\wp_\Lambda(z) : \wp_\Lambda'(z) : 1]$$

Idea of proof: We learned last week that $\exists$ function

$$j : SL_2(\mathbb{Z}) \backslash \mathbb{H} \xrightarrow{\sim} \mathbb{C}.$$

More precisely: For $\tau \in \mathbb{H}$, let $\Lambda_\tau := \mathbb{Z}\tau \oplus \mathbb{Z} \subset \mathbb{C}$ and

$$g_2(\tau) := g_2(\Lambda_\tau) := 60 \sum_{\lambda \in \Lambda_\tau \setminus \{0\}} \lambda^{-4}$$

$$g_3(\tau) := g_3(\Lambda_\tau) := 140 \sum_{\lambda \in \Lambda_\tau \setminus \{0\}} \lambda^{-6}$$

$$\Delta(\tau) := g_2(\tau)^3 - 27\, g_3(\tau)^2$$

$$j(\tau) := 1728 \frac{g_2(\tau)^3}{\Delta(\tau)}$$

So pick τ s.t. $j(\tau) = \tau$. A few steps of algebra then show that for $\Lambda = \alpha \Lambda_\tau$ with

$$\alpha = \sqrt{\frac{g_2 \cdot g_3(\tau)}{g_3 \cdot g_2(\tau)}}$$

we have

$$g_2(\Lambda) = g_2 \,, \quad g_3(\Lambda) = g_3.$$

Once we have such a Λ, the isom. is given by $/$, where $\wp_\Lambda$ is the Weierstraß $\wp$-function of Λ. $\square$

Note: Eq. of E $\rightsquigarrow$ Diff. eq. for $\wp_\Lambda$

Remark: The isom. is "very transcendental":

"$\mapsto$" involves $\wp_\Lambda$, so complex analysis.

"$\leftarrow$" can be given by integrating the invariant differential $\frac{dx}{y}$

& Λ is also called the period lattice of E.

Example: Take $\tau = i$. Then $i \cdot \Lambda_\tau = \Lambda_\tau$, so $g_3(\Lambda_\tau) = -g_3(\Lambda_\tau) = 0$

$\rightsquigarrow$ EC $y^2 = 4x^3 - g_2(\Lambda_\tau)x$ ← some transcendental number

which is isomorphic (over $\mathbb{C}$) to the EC

$$E: y^2 = x^3 + x$$

from before. **Note:** E is defined over $\mathbb{Q}$! (& $j(\tau) = 1728 = j(E)$.)

With a little bit more of complex analysis, it's not difficult to show

$$\mathrm{Hom}\left(\mathbb{C}/\Lambda, \mathbb{C}/\Lambda'\right) \cong \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subset \Lambda'\}$$
$$[z \mapsto \alpha z] \longleftarrow \alpha$$

↑ isogenies (either analytic or algebraic)

In particular, $\mathbb{C}/\Lambda \cong \mathbb{C}/\Lambda_\tau$ for some $\tau \in \mathbb{H}$.

We get a category equivalence

$$\left\{\begin{array}{c}\text{EC}/\mathbb{C} \\ \text{isogenies}\end{array}\right\} \xrightarrow{\sim} \left\{\begin{array}{c}\text{lattices} \subset \mathbb{C} \\ \alpha\Lambda \subset \Lambda'\end{array}\right\}$$

On iso. classes, this gives

$$\{\text{EC}/\mathbb{C}\}/_{\text{iso}} \cong \{\text{lattices} \subset \mathbb{C}\}/_{\text{homothety}} \cong \mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{H}.$$

$[\mathbb{C}/\Lambda_\tau] \longleftrightarrow [\Lambda_\tau] \longleftrightarrow [\tau]$

This connects EC to the picture drawn last week.

PAUSE FOR QUESTIONS

Lemma: Let $E = \mathbb{C}/\Lambda_\tau$. Then

either $\mathrm{End}(E) = \mathbb{Z}$

or τ is imag. quads., $\mathrm{End}(E) = \mathcal{O} \subset K = \mathbb{Q}(\tau)$ is an order (subring of $\mathcal{O}_K$ containing a $\mathbb{Q}$-basis of K.) ("WLOG" $\mathcal{O} = \mathcal{O}_K$.)

and $\Lambda_\tau \subset K$ is a proper fractional $\mathcal{O}$-ideal. (f.g. $\mathcal{O}$-submodule of K)

i.e. $\{\beta \in K \mid \beta\Lambda_\tau \subset \Lambda_\tau\} = \mathcal{O}$ (not just "$\supseteq$".)

Proof: Let $\alpha \in \mathrm{End}(E) = R$, i.e. $\alpha \in \mathbb{C}$ with $\alpha\Lambda_\tau \subset \Lambda_\tau$, i.e. $\exists a,b,c,d \in \mathbb{Z}$:

(1) $\alpha\tau = a + b\tau$

(2) $\alpha = c + d\tau$ $(\Rightarrow R \subset K)$

Plug one eq. into the other $\rightsquigarrow$ α integral over $\mathbb{Z}$, hence so is R. $\Rightarrow R \subset \mathcal{O}_K$.

- If $R \neq \mathbb{Z}$, take $\alpha \in R - \mathbb{Z}$ (i.e. $d \neq 0$). Plug (2) in (1) $\Rightarrow$ $K/\mathbb{Q}$ imag. quads. (as $\tau \notin \mathbb{R}$)

By def., $\mathcal{O}$ acts on $\Lambda_\tau \subset K$

& Λ_τ is a proper fractional $\mathcal{O}$-ideal. ∎

Def. If $\mathrm{End}(E) = \mathcal{O} \neq \mathbb{Z}$, say E has CM by $\mathcal{O}$. ("multiplication" as endos act by numbers; complex es imag. quads etc.)

In our example: Must have $\mathrm{End}(E) = \mathbb{Z}[i]$.

- $(x,y) \mapsto (x,-y)$: $-1 \in \mathrm{End}(E)$
- $\phi : (x,y) \mapsto (-x, iy)$ $\rightsquigarrow$ $\phi^2 = -1$, so $\phi = i$.

Digression: Orders in IQNFs

← can ignore this if you prefer $\mathcal{O} = \mathcal{O}_K$

- If $\mathcal{O} = \mathbb{Z}\alpha \oplus \mathbb{Z}\beta$ is an order of K, define its **discriminant** by

$$D := \det\begin{pmatrix} \alpha & \beta \\ \bar{\alpha} & \bar{\beta} \end{pmatrix}^2 = \underbrace{[\mathcal{O}_K : \mathcal{O}]^2}_{=: f} \cdot d_K$$

(f: conductor; d_K: "fundamental discriminant")

Then $D < 0$ and $D \equiv 0, 1 \pmod 4$.

Conversely, for any such $D \in \mathbb{Z}$ $\exists!$ order $\mathcal{O}$ in some IQNF K with $\operatorname{disc} = D$.

- For a fractional ideal $\mathfrak{a}$ of an order $\mathcal{O}$ in an IQNF, have:

$$\mathfrak{a} \text{ proper} \iff \mathfrak{a} \text{ invertible}.$$

Why? "$\Leftarrow$" holds in general.

"$\Rightarrow$" Check that $\mathfrak{a}\bar{\mathfrak{a}} = N\mathcal{O}$ for some (explicit) $N \in \mathbb{Z}$.

- The **class group** of $\mathcal{O}$ is

$$\mathcal{Cl}(\mathcal{O}) := \frac{\{\text{invertible fr. } \mathcal{O}\text{-ideals}\}}{\{\text{principal fr. } \mathcal{O}\text{-ideals}\}}$$

Cayley!

= class gp of pos def primitive binary quadr. forms of disc $= D$

← For $\mathcal{O} = \mathcal{O}_K$: usual ideal class group

$\mathcal{Cl}(\mathcal{O})$ is **finite**.

PAUSE FOR QUESTIONS

Back to EC:

careful: better to talk about $\{(E, \iota : \mathcal{O} \xrightarrow{\sim} \operatorname{End}(E)) \mid E \in EC\}/\cong$.

Observation: $\{E \in EC : \mathbb{C}/\mathbb{C} \text{ with } \operatorname{End}(E) = \mathcal{O}\}/\cong \;\xleftarrow{\sim}\; \mathcal{Cl}(\mathcal{O})$

$$[\mathbb{C}/\mathfrak{a}] \longleftarrow [\mathfrak{a}]$$

Why? Lemma ⇒ well-defined & surjective

injective also easy.

Picture:

$$\{EC/\mathbb{C}\text{ + cyclic } N\text{-sg.}\}/_{\text{iso.}} = Y_0(N) \xrightarrow{\sim} \Gamma_0(N)\backslash\mathcal{H}$$

$$[\mathbb{C}/\Lambda_\tau, \mathbb{C}/\Lambda_\tau \to \mathbb{C}/\tau\mathbb{Z}\oplus\mathbb{Z}] \longmapsto [\tau]$$

Also have CM points here: they are defined over H & can describe Galois-action.

$$\{EC/\mathbb{C}\}/_{\text{iso.}} = Y_0(1) \xrightarrow{\sim} SL_2(\mathbb{Z})\backslash\mathcal{H} \xrightarrow{j}_{\sim} \mathbb{C}$$

$$\cup \qquad\qquad \cup \qquad\qquad \cup$$

$$\{EC/\mathbb{C} \text{ with CM by } \mathcal{O}\}/_{\text{iso}} \subseteq \{EC/\mathbb{C} \text{ with CM}\}/_{\text{iso}} \xrightarrow{\sim} SL_2(\mathbb{Z})\backslash\mathcal{H}^{CM} \xrightarrow{j} \overline{\mathbb{Q}}$$

$$\| \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \cup$$

$$\mathrm{Cl}(\mathcal{O}) \ni [\mathfrak{b}] \longmapsto j(\mathfrak{b}) \in H$$

+ know Gal-action

Corollary: If E has CM by $\mathcal{O}$, then $j(E) \in \overline{\mathbb{Q}}$ of degree $\leq \#\mathrm{Cl}(\mathcal{O})$

MIRACLE!

Proof: For $\sigma \in \mathrm{Aut}(\mathbb{C})$, ${}^\sigma E : y^2 = 4x^3 - {}^\sigma g_2 x - {}^\sigma g_3$ also has CM by $\mathcal{O}$ (just act by σ on the coeff. of the rat'l fct describing an isogeny of $E : y^2 = 4x^3 - g_2 x - g_3$).

so there are only $\#\mathrm{Cl}(\mathcal{O})$ many possibilities for the iso.cl. of ${}^\sigma E$ & hence also ——— " ——— ${}^\sigma j(E) = j({}^\sigma E)$.

↑ as j is a rational fct in coeff. g_2, g_3

In fact, more is true:

Theorem: If E has CM, then $j(E)$ is an algebraic integer.

Sketch: (3 proofs: this is the "ℓ-adic one")

Idea: $j(E)$ integral $\Leftrightarrow$ E has potentially good reduction.

("$\Leftarrow$": E good red. means $\Delta \in \mathcal{O}_{L_v}^\times$, hence $j = \frac{g_2^3}{\Delta} \in \mathcal{O}_{L_v}$)

By Néron-Ogg-Shafarevich criterion, pot. good red at v

$\Leftrightarrow$ I_v acts by a finite quotient on $T_\ell E$ (any $v \nmid \ell$)

So assume E & all endos of E are def. over a local field L of residue char. $p \neq \ell$.

$\mathrm{Gal}_L \curvearrowright E[\ell^n]$ & action commutes with action of $\mathcal{O} = \mathrm{End}(E)$

$$\Rightarrow \quad \mathrm{Gal}_L \longrightarrow \underbrace{\mathrm{Aut}_{\mathcal{O}} E[\ell^n]}_{\cong (\mathcal{O}/\ell^n)^\times} \hookrightarrow \mathrm{Aut}\, E[\ell^n]$$

as $E[\ell^n]$ is free $\mathcal{O}/\ell^n$-module of rk 1

Thus $\mathrm{Gal}_L \curvearrowright T_\ell E$ factors through Gal_L^{ab}. By CFT:

$$\begin{array}{ccccccccc}
 & & & & I & & & & \\
 & & & & \downarrow & & & & \\
 & & \text{pro-}p & & I^{ab} & & & & \\
 & & \downarrow & & \| & & & & \\
1 & \longrightarrow & \mathcal{O}_L^{\times,(1)} & \longrightarrow & \mathcal{O}_L^\times & \longrightarrow & (\mathcal{O}_L/\mathfrak{p}_L)^\times & \longrightarrow & 1 \\
 & & & & \downarrow & & & & \\
1 & \longrightarrow & GL_2(\mathbb{Z}_\ell)_1 & \longrightarrow & \mathrm{Aut}\, T_\ell E & \longrightarrow & GL_2(\mathbb{Z}/\ell) & \longrightarrow & 1 \\
 & & \uparrow & & & & & & \\
 & & \text{pro-}\ell & & & & & &
\end{array}$$

$$\Rightarrow \quad \mathrm{Im}\Big(\underbrace{\mathcal{O}_L^{\times,(1)}}_{\text{finite index in } \mathcal{O}_L^\times} \longrightarrow \mathrm{Aut}\, T_\ell E \Big) \hookrightarrow GL_2(\mathbb{Z}/\ell) \quad \text{finite}$$

$\Rightarrow$ done. ▨

PAUSE FOR QUESTION

Can do even better, namely determine the field in which $j(E)$ lives.

Digression: Ring class fields

set of going up & down in $\mathcal{O}_K/\mathcal{O}$

Let $\mathcal{O}$ be an order in an IQNF K of conductor $f=[\mathcal{O}_K:\mathcal{O}]$. One can show:

$$Cl(\mathcal{O}) \cong \frac{\{\text{fr. } \mathcal{O}_K\text{-ideals prime to } f\}}{\langle \alpha\mathcal{O}_K \mid \alpha\in\mathcal{O}_K \text{ s.t. } \exists a\in\mathbb{Z} \text{ coprime to } f:\ \alpha\equiv a \bmod f\mathcal{O}_K\rangle}$$

$$\uparrow$$

$$Cl_{(f)}(\mathcal{O}_K) := \frac{\{\text{fr. } \mathcal{O}_K\text{-ideals prime to } f\}}{\langle \alpha\mathcal{O}_K \mid \alpha\equiv 1 \bmod f\mathcal{O}_K\rangle}$$

ray class group

By class field theory (in the ideal-theoretic formulation):

$$Cl_{(f)}(\mathcal{O}_K)\left[\begin{array}{c} K_{(f)} \\ | \\ H \\ | \\ K \end{array}\right) Cl(\mathcal{O})$$

H is called the ring class field assoc. to $\mathcal{O}$

Note: $\mathcal{O}=\mathcal{O}_K \Rightarrow Cl(\mathcal{O}) = Cl_{(1)}(\mathcal{O}_K) = Cl_K$

& H = Hilbert class field of K.

Reminder:

$$\left(\frac{H/K}{\cdot}\right) : Cl(\mathcal{O}) \xrightarrow{\sim} Gal(H/K)$$

Artin map

$$[\mathfrak{p}] \longmapsto \text{arithmetic Frobenius of } \mathfrak{p}$$

for $\mathfrak{p}$ an $\mathcal{O}_K$-prime ideal, prime to f & unram. in H/K.

PAUSE

Main Theorem of CM (MIRACLE) Let E be an EC with CM by $\mathcal{O}$, say $E = \mathbb{C}/\mathfrak{b}$ for a proper fr. $\mathcal{O}$-ideal $\mathfrak{b}$.

Then $K(j(E))$ is the ring class field H of $\mathcal{O}$ ← & $[\mathbb{Q}(j(E)):\mathbb{Q}] = [K(j(E)):K]$

& $\left(\frac{H/K}{\sigma}\right) j(\mathfrak{b}) = j(\sigma^{-1}\mathfrak{b})$.

↑ algebraic action (via Galois & CFT) ↑ analytic action

Later: Moreover, can also describe Gal_K-"action" on torsion points of E.

Idea of proof:

(1) "analytic": study the "modular equation" to know enough about the minpo of $j(E)$.

(2) "algebraic": Note: $\mathcal{Cl}(\mathcal{O}) \curvearrowright \{\text{EC with CM by } \mathcal{O}\}/\cong$ simply transitively

$\mathfrak{a} * (\mathbb{C}/\Lambda) := \mathbb{C}/\mathfrak{a}^{-1}\Lambda$

$\Rightarrow$ get hom. $F: \mathrm{Gal}_K^{ab} \longrightarrow \mathcal{Cl}(\mathcal{O})$ given by

could do this with $\mathrm{Gal}_{\mathbb{Q}}$, but then would depend on choice of E

$${}^{\sigma}E = F(\sigma) * E \qquad \forall E \ \forall \sigma.$$

Of course, F factors through a finite quotient $\mathrm{Gal}(L/K)$.

For simplicity: $\mathcal{O} = \mathcal{O}_K$.

Remains to show: For almost all p split in K, say $p = \mathfrak{p}\bar{\mathfrak{p}}$:

$$F\left(\frac{L/K}{\mathfrak{p}}\right) = [\mathfrak{p}]$$

($\Rightarrow F$ = inverse of the Artin map $\Rightarrow K(j(E)) \overset{\text{def. of } F}{=} \overline{K}^{\ker F} = H$)

To show this, look at E (etc.) over some very large field of def. M & use reduction modulo a good prime $\mathfrak{P} \mid \mathfrak{p}$ of M.

The CM reduces, too!

For simplicity, assume $\mathfrak{p}$ is principal, $\mathfrak{p} = (\alpha)$. Then:

$$\begin{array}{ccccc} \mathbb{C}/\Lambda & \xrightarrow{z \mapsto z} & \mathbb{C}/\mathfrak{p}^{-1}\Lambda & \xrightarrow[\sim]{z \mapsto \alpha z} & \mathbb{C}/\Lambda \\ \| & & \| & & \| \\ E & \xrightarrow{\phi} & \mathfrak{p} \times E & \xrightarrow[\sim]{\lambda} & E \end{array}$$

via differential

Modulo $\mathfrak{P}$, one checks that $\widetilde{\lambda} \circ \widetilde{\phi}$ is inseparable, of deg $= p$.

As λ iso $\Rightarrow$ $\widetilde{\phi}$ is insep. of deg p

$\Rightarrow$ $\widetilde{\phi}$ "$=$" p-power Frobenius

($\&$ ϕ is a lift of it)

This translates to what we wanted! ▨

Corollary: Let E be an EC with CM by $\mathcal{O}_K$. Then $K(j(E))$ is the Hilbert class field of K.

Example: a) $E: y^2 = x^3 + x$, $\mathcal{O} = \mathbb{Z}[i]$, $j = 1728 \in \mathbb{Z}$.

b) $\mathcal{O} = \mathbb{Z}\left[\frac{1+\sqrt{-163}}{2}\right] \rightsquigarrow Cl_K = 1$ (the smallest/largest IQNF with $Cl_K = 1$)

$j(\tau) = \frac{1}{q} + 744 + 196884q + \dots$

Thm $\Rightarrow$

$$\mathbb{Z} \ni j\left(\frac{1+\sqrt{-163}}{2}\right) = -e^{\pi\sqrt{163}} + 744 + (-)e^{-\pi\sqrt{163}} + \dots$$

$= -(640\,320)^3$ $\Rightarrow$ almost an integer; (tiny)

in fact: $= 262537412640768743.999999999999925$,

so within 10^{-12} of the integer $640\,320^3 + 744$.

Digression: Hilbert's 12th problem, Kronecker's Jugendtraum

i.e. explicit CFT:

We saw: • $j(E)$ gives abelian ext. of K

Interesting history (see Schappacher): Hilbert "wanted"

$$K^{ab} = K(j(E) \mid \text{all } E \text{ with CM by some } \mathcal{O}_K)\, \mathbb{Q}^{ab},$$
$$= K(j(\tau) \mid \tau \in K) \quad : \text{ very similar to } \mathbb{Q}^{ab} = \mathbb{Q}(e^{2\pi i r} \mid r \in \mathbb{Q})$$

but: not true.

Instead, also need values of other "elliptic functions", namely $\wp$:

Fix one EC E with CM by some order $\mathcal{O}_K$. Then:

$$K^{ab} = K(j(E), x(P) : P \in E_{tors}) \qquad \text{unless } j = 0, 1728$$

↑ see beginning: adjoin values of $\wp_\Lambda(\tau)$ at $\tau \in K$.

To prove this, need extension of Main Thm of CM that also determines the Gal_K-action on torsion points. ✓
(but ideas very similar)

To sum up: back to picture ✓

& can actually extend to CM points of $Y_0(N)$.

PAUSE FOR QUESTIONS

II. Heegner constructions

Have a supply of rational points (over explicitly given abelian ext. of K) on $Y_0(1)$ & $Y_0(N)$. Often called "Heegner points".

Idea: If $\phi: X_0(N) \to X$ is def. $/\mathbb{Q}$,

also get rational (over those fields) points of X.

3 examples:

	X	ϕ
singular moduli	$\mathbb{A}^1$	j
elliptic units	$\mathbb{G}_m$	modular unit
Heegner points	EC $E/\mathbb{Q}$	modular param. $\pi: X_0(N) \to E$ (by modularity)

↑ doesn't matter if CM or not