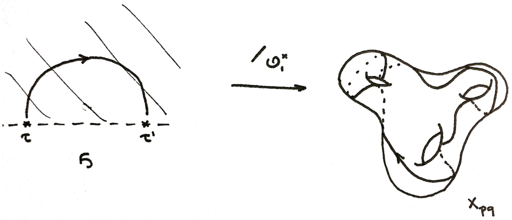
Singular moduli for real quadratic fields

Jan Vonk

CTNT at UConn, 14 June 2020



Joint work with Henri Darmon, Alice Pozzi, Yingkun Li

Outline

Outline

Let us begin with the observation, often attributed to Ramanujan, that

$$e^{\pi\sqrt{163}} = 262537412640768743.99999999999925\ldots$$

Why is this so close to an integer? Answer comes from the theory of *complex multiplication*, by looking at the j-function

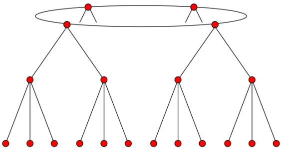
$$j(q) = q^{-1} + 744 + 196884q + 21493760q^2 + \ldots \qquad q = e^{2\pi iz}$$

This function satisfies

$$j\left(\frac{az+b}{cz+d}\right) = j(z), \qquad \text{for all } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}).$$

The values of this function at $z \in K$ quadratic imaginary are called *singular moduli*. They are always algebraic integers, e.g

$$\begin{aligned} j(\sqrt{-1}) &= 1728 \\ j(\sqrt{-5}) &= 2^6 \cdot 5 \cdot (884\sqrt{5} + 1975) \\ j(\sqrt{-14}) &= 2^3\left(323 + 228\sqrt{2} + (231 + 161\sqrt{2})\sqrt{2\sqrt{2} - 1}\right)^3 \end{aligned}$$



Let us explore the isogeny volcano (Cfr. Pete Clark/Drew Sutherland)

- $j(\sqrt{-5})$ generates $\mathbf{Q}(\sqrt{5})$,
- $j(2\sqrt{-5})$ generates $\mathbf{Q}(\sqrt{\frac{1+\sqrt{5}}{2}})$,
- ...

Theorem (Complex multiplication)

All finite abelian extensions of K are (essentially) generated by

$$j(z) \;\; z \in K, \qquad \exp(\pi i z) \;\; z \in \mathbf{Q}\,.$$

Understand the $K(j(\tau))$ (= ring class fields) and the Galois action on the set of $j(\tau)$. Has many applications, e.g. proof of Euler's conjecture:

$$p = x^2 + 27y^2 \iff \begin{cases} p \equiv 1 \pmod 3 \text{ and} \\ t^3 - 2 \in \mathbf{F}_p[t] \text{ has a root.} \end{cases}$$

A singular modulus is an integer if and only if argument generates an order of class number one. There is a finite list! The maximal ones are:

Field	$E_{\mathbf{Q}}$ with CM by maximal order	$j(E)$
$\mathbf{Q}(\sqrt{-1})$	$y^2 = x^3 + x$	$2^6 \cdot 3^3$
$\mathbf{Q}(\sqrt{-2})$	$y^2 = x^3 + x$	$2^6 \cdot 5^3$
$\mathbf{Q}(\sqrt{-3})$	$y^2 + xy = x^3 - x^2 - 2x - 1$	0
$\mathbf{Q}(\sqrt{-7})$	$y^2 = x^3 + 4x^2 + 2x$	$-3^3 \cdot 5^3$
$\mathbf{Q}(\sqrt{-11})$	$y^2 + y = x^3 - x^2 - 7x + 10$	-2^{15}
$\mathbf{Q}(\sqrt{-19})$	$y^2 + y = x^3 - 38x + 90$	$-2^{15} \cdot 3^3$
$\mathbf{Q}(\sqrt{-43})$	$y^2 + y = x^3 - 860x + 9707$	$-2^{18} \cdot 3^3 \cdot 5^3$
$\mathbf{Q}(\sqrt{-67})$	$y^2 + y = x^3 - 7370x + 243528$	$-2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$
$\mathbf{Q}(\sqrt{-163})$	$y^2 + y = x^3 - 2174420x + 1234136692$	$-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$

This explains the observation on our first slide!

$$-262537412640768000 = j\left(\frac{1+\sqrt{-163}}{2}\right) = -e^{\pi\sqrt{163}} + 744 + (\text{very small}).$$

CM theory was believed to have reached satisfactory conclusion in early 20th century. Until Gross–Zagier got their hands on it! Observe

$$\begin{aligned} j\left(\frac{1+\sqrt{-67}}{2}\right) - j\left(\frac{1+\sqrt{-163}}{2}\right) &= -2^{15}\cdot 3^3\cdot 5^3\cdot 11^3 + 2^{18}\cdot 3^3\cdot 5^3\cdot 23^3\cdot 29^3 \\ &= 2^{15}\cdot 3^7\cdot 5^3\cdot 7^2\cdot 13\cdot 139\cdot 331 \end{aligned}$$

Differences are very smooth! But wait... doesn't ABC say this must be rare? Luckily, there are only finitely many class number one orders!

Remark 1. This is the *class number one* problem, solved by Heegner by finding all integral points on $X_{\mathrm{ns}}^+(24)$. Amusing: Can also use $X_{\mathrm{ns}}^+(13)$, solved in Balakrishnan–Dogra–Müller–Tuitman–V. using p-adic heights.

Remark 2. Note that according to Gauß, *real* quadratic fields $K/\mathbf{Q}$ should have class number one very often! Keep that in mind in what follows.

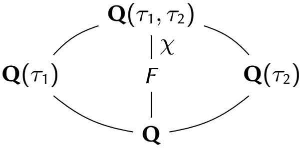
Let τ_1, τ_2 be two CM points in $\mathcal{H}_\infty = \{z \in \mathbf{C} : \mathrm{Im}(z) > 0\}$.
Gross and Zagier (1985) find explicit formula for

$$\mathrm{Nm}\left(j(\tau_1) - j(\tau_2)\right) \quad \in \mathbf{Z}$$

- **Algebraic proof:** Uses CM elliptic curves! Its q-adic valuation is given in terms of arithmetic intersection of embeddings

$$\mathbf{Q}(\tau_1), \mathbf{Q}(\tau_2) \ \hookrightarrow \ B_{\infty q} = \text{Quat alg conductor } \infty q$$

- **Analytic proof:** Fourier coefficients of Hecke's real analytic Eisenstein series over F, attached to the character χ:



Real analytic Hilbert Eisenstein series $E_s(z_1, z_2)$ defined by Hecke:

$$\sum_{[\mathfrak{a}]\in \mathrm{Cl}(\Delta_1\Delta_2)} \chi(\mathfrak{a})\,\mathrm{Nm}(\mathfrak{a})^{1+2s} \sideset{}{'}\sum_{(m,n)\in\mathfrak{a}^2/U} \frac{y_1^s y_2^s}{(mz_1+n)(m'z_2+n')|mz_1+n|^{2s}|m'z_2+n'|^{2s}}$$

Gross–Zagier consider its diagonal restriction $E_s(z, z)$ and show

- When $s = 0$, have $E_s(z, z) = 0$,
- The holomorphic projection of the first derivative

$$\left(\frac{\partial}{\partial s} E_s(z, z)\right)\Bigg|_{s=0}^{\mathrm{hol}}$$

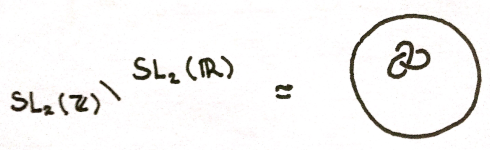
  has Fourier coefficients related to $\log \mathrm{Nm}\left(j(\tau_1) - j(\tau_2)\right)$.
- The holomorphic projection must vanish!
  $\Rightarrow$ formula for $\mathrm{Nm}\left(j(\tau_1) - j(\tau_2)\right)$.

Remark: Does not use CM elliptic curves!

Outline

The work of Duke–Imamoḡlu–Tóth

Inspiration comes from work of Duke–Imamoḡlu–Tóth on linking numbers of modular geodesics.



If $\gamma \in \mathrm{SL}_2(\mathbf{Z})$ is hyperbolic, get associated knot

$$\begin{aligned} \mathrm{Kn}(\gamma) &\hookrightarrow \mathrm{SL}_2(\mathbf{Z})\backslash \mathrm{SL}_2(\mathbf{R}) \\ t &\mapsto \mathrm{SL}_2(\mathbf{Z}) g \begin{pmatrix} e^t & \\ & e^{-t} \end{pmatrix}, \quad \text{where } g^{-1}\gamma g = \text{diagonal} \end{aligned}$$

- Linking $\mathrm{Kn}(\gamma)$ and trefoil $\leftrightarrow$ Dedekind–Rademacher cocycle (Ghys)
- Linking $\mathrm{Kn}(\gamma_1)$ and $\mathrm{Kn}(\gamma_2)$ $\leftrightarrow$ Knopp cocycle (DIT)

I. The Dedekind–Rademacher cocycle

Consider E_2, the Eisenstein series of weight 2, defined by

$$\frac{\pi i}{6} E_2(z) = \sum_{m \in \mathbf{Z}} \sum_{n \in \mathbf{Z}}{}' \frac{1}{(mz+n)^2}.$$

It is *nearly* invariant under $\mathrm{SL}_2(\mathbf{Z})$, in the sense that

$$(cz+d)^{-2} E_2\left(\frac{az+b}{cz+d}\right) = E_2(z) - \frac{12c}{cz+d}$$

The abstract map $\gamma \mapsto 12c/(cz+d)$ is a weight 2 *cocycle* for $\mathrm{SL}_2(\mathbf{Z})$:

$$f : \mathrm{SL}_2(\mathbf{Z}) \to \mathcal{O}_2, \qquad f(\gamma_1\gamma_2) = f(\gamma_1)^{\gamma_2} f(\gamma_2)$$

These are classified up to equivalence by $\mathrm{H}^1(\mathrm{SL}_2(\mathbf{Z}), \mathcal{O}_2)$.

I. The Dedekind–Rademacher cocycle

It lifts uniquely to a weight 0 cocycle:

$$0 \longrightarrow \mathrm{H}^1(\mathrm{SL}_2(\mathbf{Z}), \mathcal{O}) \xrightarrow{d} \mathrm{H}^1(\mathrm{SL}_2(\mathbf{Z}), \mathcal{O}_2) \longrightarrow 0$$

The Dedekind–Rademacher symbol $\Phi(\gamma) \in \mathbf{Z}$ is defined by

$$\log \Delta(\gamma z) - \log \Delta(z) = 6 \log(-(cz+d)^2) + 2\pi i \Phi(\gamma).$$

since $\operatorname{dlog} \Delta(z) = E_2(z)$, the unique lift is given by the right hand side!
When applied to a hyperbolic matrix γ with fixed point τ, we get

$$6 \log(-(cz+d)^2) \qquad + \quad 2\pi i \Phi(\gamma)$$

$$\Big\downarrow z=\tau \qquad\qquad \Big\downarrow z = i\infty \quad \text{(+ homog.)}$$

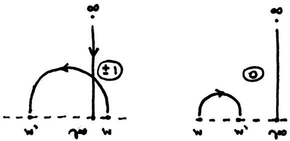
$$12 \log(\text{fundamental unit}) \qquad \mathit{Link}(\mathrm{Kn}(\gamma), \text{trefoil})$$

II. The Knopp cocycle

The *Knopp cocycle* in $Z^1(\mathrm{SL}_2(\mathbf{Z}), \mathcal{O}_2)$ attached to an RM point τ is

$$\gamma \longmapsto \sum_{w \in \mathrm{SL}_2(\mathbf{Z})\tau} \frac{\{\infty \to \gamma\infty\} \cap \{w \to w'\}}{z - w}$$

where the exponent is the intersection number of the geodesic from w' to w with the geodesic from ∞ to $\gamma\infty$, and hence ± 1 or 0.



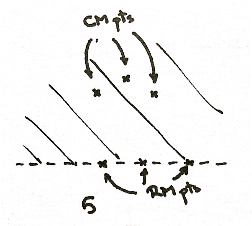
In similar way, Duke–Imamoḡlu–Tóth extract linking $\mathrm{Kn}(\gamma_1)$ and $\mathrm{Kn}(\gamma_2)$.

Remark. An analogue of $E_2(z)$ for the Knopp cocycle was constructed in a different article of Duke–Imamoglu–Toth (2011). It's a deep object.

Outline

∞ versus p

Cannot evaluate $j(z)$ at arguments in a real quadratic field K.



Naive issue: ∞ is split in K.
Naive solution: Plenty of finite primes p are not split in K.

points?	$\mathcal{H}_\infty$	$\mathcal{H}_2$	$\mathcal{H}_3$	$\mathcal{H}_5$	$\mathcal{H}_7$	$\mathcal{H}_{11}$
$\mathbf{Q}(i)$	yes	yes	yes	no	yes	yes
$\mathbf{Q}(\sqrt{5})$	no	yes	yes	yes	yes	no

Work over p-adic numbers (cfr. Liang Xiao's course), where p is inert in K.

With Henri Darmon, we upgrade linking number ideas to setting

$$\begin{aligned} \Gamma &= \mathrm{SL}_2(\mathbf{Z}[1/p]) \\ \mathcal{M} &= \text{Meromorphic functions on } \mathcal{H}_p = \mathbf{P}^1(\mathbf{C}_p) \setminus \mathbf{P}^1(\mathbf{Q}_p) \end{aligned}$$

The dichotomy Dedekind–Rademacher / Knopp cocycle becomes:

(Darmon–Dasgupta 2006) Constructed p-adic invariants

$$J_{\mathrm{DR}}(\tau) \in \mathbf{C}_p \, .$$

Give p-units in ring class field of τ. *E.g.* $p = 7$ and $\tau = \frac{-17+\sqrt{321}}{4}$ gives

$$7^4x^6 - 20976x^5 - 270624x^4 + 526859689x^3 - 649768224x^2 - 120922465776x + 7^{16}$$

Independent proofs by Darmon–Pozzi–V. /Dasgupta–Kakde (forthcoming).
Also purely archimedean variant by Charollois–Darmon, no proof.

(Darmon–V. 2020) Constructed p-adic invariants

$$J_p(\tau_1, \tau_2) \in \mathbf{C}_p$$

for pair of RM points τ_1, τ_2 which appear to be good analogues of the quantity $J_\infty(\tau_1, \tau_2) = j(\tau_1) - j(\tau_2)$ appearing in Gross–Zagier.

Let $\Delta_1 = 13$, then for below choices of p and τ consider the quantity

$$J_p\left(\frac{1+\sqrt{13}}{2},\ \tau\right).$$

Can compute these numerically (this is not a proof!) and seem to get:

τ	$p = 11$	$p = 19$	$p = 59$
$2\sqrt{2}$	$\frac{3-4\sqrt{-1}}{5}$	$\frac{3-4\sqrt{-1}}{5}$	1
$3\sqrt{2}$	$\frac{11+21\sqrt{-3}}{2\cdot 19}$	$\frac{5-4\sqrt{-6}}{11}$	1
$4\sqrt{2}$	$\frac{57-176\sqrt{-1}}{5\cdot 37}$	$\frac{5-12\sqrt{-1}}{13}$	$\frac{3+4\sqrt{-1}}{5}$
$7\sqrt{2}$	$\frac{118393-8328\sqrt{-14}}{5^2\cdot 59\cdot 83}$	$\frac{93+95\sqrt{-7}}{2^2\cdot 67}$	$\frac{37+9\sqrt{-7}}{2^2\cdot 11}$
$8\sqrt{2}$	$\frac{1312-1425\sqrt{-1}}{13\cdot 149}$	$\frac{43+924\sqrt{-1}}{5^2\cdot 37}$	$\frac{3+4\sqrt{-1}}{5}$
$9\sqrt{2}$	$\frac{11387+12320\sqrt{-3}}{19^2\cdot 67}$	$\frac{43+4100\sqrt{-6}}{11^2\cdot 83}$	1

Observe that for any pair of primes p, q there seems to be some relation

$$\text{“ord}_p\text{”}(q\text{-adic invariant}) = \text{“ord}_q\text{”}(p\text{-adic invariant}).$$

(Gross–Zagier) Let τ_1, τ_2 be CM points, consider

$$J_\infty(\tau_1, \tau_2) = j(\tau_1) - j(\tau_2) \;\in\; \overline{\mathbf{Q}}$$

- Related to real analytic Eisenstein family.
- $\mathrm{ord}_q\, J_\infty(\tau_1, \tau_2) =$ Intersection multiplicities

$$\mathbf{Q}(\tau_1), \mathbf{Q}(\tau_2) \;\hookrightarrow\; B_{\infty q}.$$

(Darmon–V.) Let τ_1, τ_2 be RM points, construct

$$J_p(\tau_1, \tau_2) \;\overset{?}{\in}\; \overline{\mathbf{Q}}$$

- Related to p-adic analytic families.
- $\mathrm{ord}_q\, J_p(\tau_1, \tau_2) \overset{?}{=}$ Intersection multiplicities

$$\mathbf{Q}(\tau_1), \mathbf{Q}(\tau_2) \;\hookrightarrow\; B_{pq}.$$

Towards a proof?

Can relate real quadratic singular moduli to derivatives of p-adic families of modular forms. Then have big (and exclusively p-adic) advantage:

p-Adic families of modular forms

$\updownarrow$

Deformations of Galois representations

(Cfr. Jeremy Booher / David Savitt)

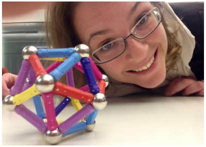
- **(With Darmon and Pozzi)** Proof that $\Theta_{\mathrm{DR}}[\tau] \in \mathcal{O}_H[1/p]^\times$. Use deformation of Eisenstein series in weight $(1, 1)$.
- **(With Darmon and Li)** Proof that p-adic family through a certain modular form of weight $3/2$ is closely related to

$$J_p(\tau_1, D) = \prod_{\mathrm{disc}(\tau_2)=D} J_p(\tau_1, \tau_2)$$

Implies certain algebraicity results (in progress).

And finally...

... a **huge** thanks to the organisers: Jennifer Balakrishnan, Keith Conrad, Álvaro Lozano-Robledo, Christelle Vincent

as well as the lovely people at UConn

for a fantastic CTNT! Let us give them a huge round of applause!!