Explicit class field theory over quadratic fields

From CM to RM theory

Óscar Rivero

Study group organizational meeting

10/08/2021

Caveat: most of the materials of this talk have been extracted from different surveys of Henri Darmon and Jan Vonk.

Class field theory

- K number field, C_K idèle class group.
- Global Artin map

$$\varphi : C_K \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

  Surjective, and injective after passing to profinite completion

$$\hat{\varphi} : \hat{C}_K \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

- Does not give an easy way to find explicit generators for abelian extensions of K.

Theorem (Kronecker-Weber)

All finite abelian extensions of $\mathbb{Q}$ are generated by combinations of

$$\exp(2\pi i z), \quad z \in \mathbb{Q}.$$

Class field theory

Let K be an imaginary quadratic field.

Theorem (Kronecker-Weber)

All finite abelian extensions of K are generated by combinations of values at $z \in K$ of the j-function and the Weber function

$$j(q) = q^{-1} + 744 + 196844q + 21493670q^2 + \dots, \quad q = \exp(2\pi i z).$$

- The j-function generates the Hilbert class field (or ring class fields).
- For $K = \mathbb{Q}(\sqrt{-14})$,

$$j(\sqrt{-14}) = 2^3\left(323 + 228\sqrt{2} + (231 + 161\sqrt{2})\sqrt{2\sqrt{2} - 1}\right).$$

- When K has class number one, $j(z)$ takes integer values:

$$j(i) = 1728, \quad j\left(\frac{1+\sqrt{-3}}{2}\right) = 0, \quad j\left(\frac{1+\sqrt{-7}}{2}\right) = -3375.$$

Class field theory

- The role of the Weber function is to produce abelian extensions beyond the Hilbert class field.
- Assume for simplicity that K has class number one.
- Take E an elliptic curve with $\mathrm{End}(E) = \mathcal{O}_K$.
- Example. For $K = \mathbb{Q}(i)$, take

$$E : y^2 = x^3 - x.$$

- $E[n]$ n-torsion points. Defined over algebraic extensions, abstractly isomorphic (as a group) to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.
- Adjoining the x-coordinates of all the torsion points generates all the abelian extensions of K.
- Analogy with the case of $\mathbb{Q}$.
- When the class number is > 1 must be more careful.

Singular moduli

Let d_1, d_2 be two fundamental discriminants with $(d_1, d_2) = 1$. Define

$$J(d_1, d_2) = \prod_{[\tau_1],[\tau_2]} \left(j(\tau_1) - j(\tau_2)\right)^{\frac{4}{w_1 w_2}},$$

where the product runs over $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of quadratic imaginary numbers τ_1 and τ_2 of discriminant d_1 and d_2, and w_i is the number of roots of unity in the quadratic field of discriminant d_i.

Theorem

If ℓ is a prime dividing $J(d_1, d_2)^2$, then

$$\left(\frac{d_1}{\ell}\right), \left(\frac{d_2}{\ell}\right) \neq 1, \quad \ell \mid \frac{d_1 d_2 - b^2}{4},$$

for some $b < \sqrt{d_1 d_2}$.

Singular moduli

An explicit example of differences of singular moduli.

$$j\left(\frac{1+\sqrt{-67}}{2}\right) - j\left(\frac{1+\sqrt{-163}}{2}\right) = 2^{15}\cdot 3^7\cdot 5^3\cdot 7^2\cdot 13\cdot 139\cdot 331.$$

(Taken from the original paper of Gross–Zagier.)

- **Singular moduli:** begin with a quadratic number $\tau \in \mathbb{H} \cap K$ and evaluate on it the function j.
- Differences of singular moduli $j(\tau_1) - j(\tau_2)$ encode relevant arithmetic information.
- **Heegner points:** images of quadratic numbers under *modular parametrizations* to obtain rational points over elliptic curves.
- **Elliptic units:** precursor of the theory of Heegner points. Units over abelian extensions of imaginary quadratic fields.

Heeger points

E elliptic curve over $\mathbb{Q}$ of conductor N. Modular parametrization

$$\Phi_N : \mathbb{H}/\Gamma_0(N) \longrightarrow E(\mathbb{C}).$$

- K imaginary quadratic field, $\tau \in \mathbb{H} \cap K$.
- Two orders attached to τ in $\mathcal{O}_K$:

$$\mathcal{O}_\tau := \{\gamma \in M_2(\mathbb{Z}) \text{ with } \det\gamma \neq 0 \text{ and } \gamma\tau = \tau\} \cup 0_2,$$

$$\mathcal{O}_\tau^{(N)} := \{\gamma \in M_0(N) \text{ with } \det\gamma \neq 0 \text{ and } \gamma\tau = \tau\} \cup 0_2.$$

- Given an order $\mathcal{O} \subset \mathcal{O}_K$, $\mathrm{CM}(\mathcal{O})$ is the set of quadratic numbers τ with $\mathcal{O}_\tau^{(N)} = \mathcal{O}$. Nice action of the class group.

Theorem

1. *$j(\tau)$ belongs to H, the ring class field attached to $\mathcal{O}_\tau$.*
2. *$\Phi_N(\tau)$ belongs to $E(H')$, the ring class field attahced to $\mathcal{O}_\tau^{(N)}$.*

Heegner points

Elliptic curve E of conductor 11

$$E : y^2 + y = x^3 - x^2 - 10x - 20.$$

$K = \mathbb{Q}(\sqrt{-7})$, since the order $\mathcal{O}_K = \mathbb{Z}\left(\frac{1+\sqrt{-7}}{2}\right)$ embeds in $M_0(11)$.

We can find a point τ such that $\mathcal{O}_\tau^{(11)} \simeq \mathcal{O}_K$:

$$\tau = \frac{-9 + \sqrt{-7}}{22}.$$

Then, we can compute its image, which agrees (to 35 decimal digits of accuracy) with

$$\Phi_{11}(\tau) = \left(\frac{1 - \sqrt{-7}}{2}, -2 - 2\sqrt{-7}\right) \in E(K).$$

Towards the quadratic case

What about K real quadratic field?

- We cannot evaluate j at real quadratic values.
- **Main idea.** Replace ∞ by p and consider $\mathbb{H}_p$ instead of $\mathbb{H}$.
- j is a function invariant by $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, hence an element in $H^0(\Gamma, \mathcal{M})$, where $\mathcal{M}$ are the meromorphic functions of $\mathbb{H}$.
- The corresponding H^0 is not interesting in our case. Consider instead $\Gamma = \mathrm{SL}_2(\mathbb{Z}[1/p])$, $\mathcal{M}$ ring of meromorphic functions of $\mathbb{H}_p$ and

$$H^1(\Gamma, \mathcal{M}).$$

- Produce interesting elements there?

Rigid meromorphic cocycles

- An element $J \in H^1(\Gamma, \mathcal{M})$ is called a rigid meromorphic cocycle.
- Can define its evaluation at RM points in $\mathbb{H}_p$.
- For $\tau \in \mathbb{H}_p \cap K$,

$$\mathrm{Stab}_\Gamma \tau \simeq \langle \pm\gamma_\tau \rangle.$$

- RM value:

$$J[\tau] := J(\gamma_\tau)(\tau).$$

- Independent of choice of choice of cocycle J in the class and τ in its Γ-orbit.
- Analogue for the difference of singular moduli:

$$J(\tau_1, \tau_2) := J(\gamma_{\tau_1})(\tau_2).$$

- Algebraicity conjectures?

Stark–Heegner points

E elliptic curve over $\mathbb{Q}$ of conductor N. Modular parametrization

$$\Phi_N : \mathbb{H}/\Gamma_0(N) \longrightarrow E(\mathbb{C}).$$

- Theory developed by Darmon and his collaborators since 2001 (Stark–Heegner points are also known as Darmon points).
- We need to consider now quotients of $\mathbb{H}_p \times \mathbb{H}$ by *interesting* groups: $(\mathbb{H}_p \times \mathbb{H})/\Gamma$.
- Analogues for the modular parametrization?
- Need to develop a p-adic integration theory.

This study group

CM theory

- CM elliptic curves (Kat).
- Explicit class field theory for imaginary quadratic fields (James).
- Heegner points (Arshay).
- Singular moduli and the class number one problem (David).

RM theory

- Tate uniformisation of elliptic curves (Xenia).
- The Bruhat–Tits tree (Elvira).
- Stark–Heegner points I (Muhammad).
- Stark–Heegner points II (Oscar).
- Real quadratic singular moduli (Chris).