Constructing ray class fields of a real quadratic field using elliptic curves

Takashi Fukuda (Nihon University, fukuda.takashi@nihon-u.ac.jp)
Kiichiro Hashimoto (Waseda University, khasimot@waseda.jp)
Keiichi Komatsu (Waseda University, kkomatsu@waseda.jp)

How to construct ray class fields ?

- It is well known that ray class fields of an imaginary quadratic field are generated by special values of j-function, Weber function, Weierstrass σ-function or Siegel function.
- It is difficult to construct ray class fields of a real quadratic field. We have no definite methods. We know two trials.

Stark Units

- still conjectual
- often gives correct ray class field

Torsion Points of Abelian Varieties

- Few examles
- Potential ability

Ray Class Field

$k = \mathbb{Q}(\sqrt{p})$, p:prime number $\equiv 1 (\mathrm{mod}\ 12)$

Assumption: $h(k) = 1$

ε : fundamental unit of k, $G(k/\mathbb{Q}) = \langle\, \delta\, \rangle$

$\mathfrak{p}_\infty, \mathfrak{p}'_\infty$: infinite places of k

$(3) = (\pi)(\pi') \quad \pi\pi' = -3$

$\pi = a + b\sqrt{p} \quad (2a, 2b \in \mathbb{Z})$

$\mathfrak{a}_n = (3)^n \mathfrak{p}_\infty \mathfrak{p}'_\infty$

$k(\mathfrak{a}_n)$: ray class field

Is there a systematic construction of $k(\mathfrak{a}_n)$?

Known Results and Questions

Known : $k(\mathfrak{a}_1) \subset k(E_3)$

Question : $k(\mathfrak{a}_n) \subset k(E_{3^n})$?

Elliptic Curve

$\psi : (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \{\pm 1\}$: even char.

$f \in S_2(\Gamma_0(p), \psi)$: wt 2, level p, nebentype ψ

normalized common eign form of all Hecke op.

$$f(z) = \sum_{n=1}^{\infty} a_n \exp(2\pi i n z)$$

Assumption : $\mathbb{Q}(\{a_n \mid n \geq 1\}) = \mathbb{Q}(\sqrt{-3}\,)$

A: abelian variety attached to f by Shimura

$\exists\, \theta : \mathbb{Q}(\sqrt{-3}\,) \longrightarrow \mathrm{End}_{\mathbb{Q}}(A)$: isom.

$\exists\, \mu \in \mathrm{Aut}(A)$: rational over k s.t.

$$\mu^2 = 1,\ \mu\theta(a) = \theta(\overline{a})\mu,\ \ \mu^\delta = -\mu\,.$$

$E = (1+\mu)A$: Shimura's elliptic curve

$E_n = \{P \in E \mid nP = 0\}$

Theorem

Assume that $\varepsilon^2 \equiv 1 \pmod 9$, $a \not\equiv \pm 1 \pmod 9$ *and there exists a prime number* ℓ *which splits in* $k(E_3)$ *and satisfies one of the following conditions:*

(1) $\ell \equiv 1 \pmod{27}$ *and* $a_\ell \equiv 11 \pmod{27}$,

(2) $\ell \equiv 10 \pmod{27}$ *and* $a_\ell \equiv -7 \pmod{27}$,

(3) $\ell \equiv 19 \pmod{27}$ *and* $a_\ell \equiv 2 \pmod{27}$.

Then we have $k(\mathfrak{a}_2) \subset k(E_9)$.

Example ($\omega = (1+\sqrt{p}\,)/2$)

When $p = 109$ and 997, we have $k(\mathfrak{a}_2) \subset k(E_9)$ with

$p = 109,\ \ E : y^2 + \omega x y = x^3 - (1+\omega)x^2 - (245 + 58\omega)x - (2944 + 630\omega)$

$p = 997,\ \ E : y^2 + y = x^3 + x^2 - (125389 + 8202\omega)x - (24602589 + 1609311\omega)$

ANTS-XII Poster Session 2016.8.30 (Kaiserslautern, Germany)