$\mathbb{Q}$-rational CM points on $\mathcal{A}_4$

Laurens Wiersema
Master student, Rijksuniversiteit Groningen
Supervisor: Pınar Kılıçer

Motivation

Let E be an elliptic curve. Then the endomorphism ring $\mathrm{End}(E)$ is either $\mathbb{Z}$ or an *order* $\mathcal{O}$ in an imaginary quadratic number field $K = \mathbb{Q}(\sqrt{-d})$ where $d \in \mathbb{Z}_{>0}$.

If $\mathrm{End}(E) \cong \mathcal{O} \neq \mathbb{Z}$, then we say that E has complex multiplication by $\mathcal{O}$.

Main Theorem of CM for Elliptic Curves

Let E be an elliptic curve with CM by $\mathcal{O}_K$. Then

$$[K(j(E)) : K] = \#\mathrm{Cl}(\mathcal{O}_K),$$

where $\mathrm{Cl}(\mathcal{O}_K) = I_K/P_K$, and where I_K is the group of fractional ideals and P_K is the group of principal fractional ideals of $\mathcal{O}_K$.

Theorem (Heegner 1952, Baker 1966, Stark 1967)

Let K be an imaginary quadratic field with the maximal order $\mathcal{O}_K$. Then $h_K = 1$ if and only if $K \cong \mathbb{Q}(\sqrt{d})$ where $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$.

Corollary

If E has field of moduli $\mathbb{Q}$, then $h_K = 1$ hence K is one of the nine fields in the theorem.

- What is the analogue for abelian varieties of dimension g?

CM fields and CM types

- A CM field is a totally imaginary number field K that is a degree 2 extension of a totally real number field K_+. We fix an automorphism ρ of K of order 2 which commutes with all other automorphisms of K, and identify it with *complex conjugation*.
- A CM type Φ of a CM field K of degree $2n$ is a set consisting of n many automorphisms of K such that exactly one of each conjugate pair is in Φ. We also call (K, Φ) a CM type.
- If K_0 is a CM subfield of K with CM type Φ_0, then it *induces* a unique CM type Φ of K such that $\Phi = \{\varphi \in \mathrm{Gal}(K/\mathbb{Q}) \mid \varphi|_{K_0} \in \Phi_0\}$. If a CM type Φ is not induced by any other CM type, it is called *primitive*.
- The reflex CM type (K^r, Φ^r) of a CM type (K, Φ) is the unique primitive CM type that induces $\Phi^{-1} = \{\varphi^{-1} \mid \varphi \in \Phi\}$. If $K/\mathbb{Q}$ is an abelian extension and (K, Φ) is primitive, then $K = K^r$ and $\Phi^r = \Phi^{-1}$.
- The *type norm* of a CM type (K, Φ) is the multiplicative map $N_\Phi : K \to K^r$ defined by $N_\Phi(x) = \prod_{\varphi \in \Phi} \varphi(x)$.

CM abelian varieties

An abelian variety A over a field k of characteristic 0 has *CM by the maximal order of a CM field* if there exists an embedding $\theta : K \to \mathrm{End}(A_{\bar{k}}) \otimes \mathbb{Q}$ for a CM field K of dimension $2 \cdot \dim(A)$ such that $\theta^{-1}(\mathrm{End}(A_{\bar{k}})) = \mathcal{O}_K \subset K$.

Given an abelian variety A with CM by $\mathcal{O}_K$ via an embedding θ, we obtain a CM-type Φ of K with values in k as follows: let $\mathrm{Tgt}_0(A)$ be the tangent space of A over k at 0. Let Φ be the set of homomorphisms $K \to k$ occurring in the diagonalisation of the representation $K \to \mathrm{End}_k(\mathrm{Tgt}_0(A_k)) : \alpha \mapsto D(\theta(\alpha))$. Then Φ is a CM-type of K, and we say that (A, θ) is of type (K, Φ). The variety (A, θ) is *simple* if the CM type (K, Φ) is primitive.

Let (A, φ) be defined over a field k of characteristic 0. Then there exists a unique field $k_0 \subset k$, called the field of moduli of (A, φ), with the following property: for all $\sigma : k \to \bar{k}$, it holds that (A, φ) and $(\sigma A, \sigma\varphi)$ are isomorphic over k if and only if $\sigma_{k_0} = \mathrm{id}_{k_0}$.

Main Theorem of CM [Shimura-Taniyama]

Let A be a principally polarized abelian variety with CM by the maximal order $\mathcal{O}_K$ and of a primitive CM type (K, Φ). Let θ denote the embedding $\theta : K \hookrightarrow \mathrm{End}(A) \otimes \mathbb{Q}$ and φ the principal polarization.

Let k_0 be the field of moduli of (A, φ). Then $K^r \cdot k_0$ is the unramified class field over K^r corresponding to the ideal group

$$I_0(\Phi^r) = \{\mathfrak{p} \in I_{K^r} \mid N_{\Phi^r}(\mathfrak{p}) = \alpha\mathcal{O}_K, \alpha\bar{\alpha} \in \mathbb{Q} \text{ for some } \alpha \in K^\times\}.$$

Corollary

Let A be a principally polarized abelian variety with CM by the maximal order $\mathcal{O}_K$ and of a primitive CM type (K, Φ). If (A, φ) has field of moduli $\mathbb{Q}$ then $[I_{K^r} : I_0(\Phi^r)] = 1$.

We say that a CM type (K, Φ) has CM class number one if $[I_{K^r} : I_0(\Phi^r)] = 1$.

What is known?

- Murabayashi-Umegaki determined all simple, maximal $\mathbb{Q}$-rational CM points on the moduli space $\mathcal{A}_2$ of principally polarized abelian surfaces.
- Kilicer-Streng determined all simple, maximal $\mathbb{Q}$-rational CM points on the moduli space $\mathcal{A}_3$ of principally polarized abelian threefolds.

Octic cyclic CM fields

Let K be a Galois extension of $\mathbb{Q}$ of degree 8 with a cyclic Galois group $G = \mathrm{Gal}(K/\mathbb{Q}) = \langle\sigma\rangle$.

- There are 16 CM types: up to equivalence represented by $\Phi_1 = \{\mathrm{id}, \sigma, \sigma^2, \sigma^3\}$ and $\Phi_2 = \{\mathrm{id}, \sigma^5, \sigma^2, \sigma^3\}$. (All CM-types are primitive.)
- The reflex (K^r, Φ^r) of any CM type (K, Φ) satisfies $K^r = K$ and $\Phi^r = \{\tau^{-1} \mid \tau \in \Phi\}$.

Proposition

Let K be a cyclic octic CM field with maximal totally real subfield K_+. Suppose Φ is a CM type of K such that (K, Φ) has CM class number one. Then the relative class number of K is given by $h_K^* = 2^{t_K - 1}$, where t_K is the number of prime ideals of K_+ that ramify in K.

Proposition

For a field K as above, the conductor f_K is bounded above by

$$f_K \leq \begin{cases} 655856 & \text{if 2 is totally ramified in } K, \\ 1866221 & \text{otherwise.} \end{cases}$$

We compute the exact list of CM class number one fields by the following algorithm.

Algorithm

Output: The defining polynomials and conductors of all cyclic octic CM fields K for which there exists a CM type Φ such that (K, Φ) has CM class number one.

1. Construct all possible conductors below the bounds given above, using the restrictions and relations given by Kwon-Park.
2. For each conductor, construct the associated odd Dirichlet characters χ of degree 8. Determine the ramification type of rational primes for each character. Discard any character that yields a bad ramification type.
3. For each surviving character, compute the discriminants d_K and d_{K_+}. Discard the character if there is a totally split rational prime q that satisfies $q < \frac{1}{4}\sqrt[4]{d_K/d_{K_+}^2}$.
4. For each remaining candidate, compute the number of ramified primes t_K and the target class number $2^{t_K - 1} h_{K_+}$ (assuming GRH). Compute the size of the subgroup of the class group of K generated by prime ideals with norm ≤ 100. If this size does not divide the target class number, discard the candidate. Otherwise, unconditionally compute the full class number h_K to verify it matches the target.
5. For the exact fields surviving Step 4, explicitly compute the CM class group $I_K/I_0(\Phi^r)$ for each CM type Φ. Keep only the pairs (K, Φ) where the quotient is trivial.

Implementing the Algorithm in Magma returns the fields in the following table. For these fields, every CM type has CM class number one.

h_K^*	f_K	h_{K_+}	f_{K_+}	Quartic subfield
Polynomial defining K				
1	32	1	16	$\mathbb{Q}(\sqrt{2+\sqrt{2}})$
$x^8 + 8x^6 + 20x^4 + 16x^2 + 2$				
1	41	1	41	$\mathbb{Q}(\sqrt{41+4\sqrt{41}})$
$x^8 + x^7 + 3x^6 + 11x^5 + 44x^4 - 53x^3 + 153x^2 - 160x + 59$				
2	51	1	17	$\mathbb{Q}(\sqrt{17+4\sqrt{17}})$
$x^8 + x^7 + 10x^6 + 11x^5 + 15x^4 + 61x^3 + 58x^2 + 47x + 103$				
2	85	2	85	$\mathbb{Q}(\sqrt{85+20\sqrt{17}})$
$x^8 - x^7 + 10x^6 - 79x^5 + 134x^4 + 41x^3 + 245x^2 - 846x + 596$				
4	68	1	17	$\mathbb{Q}(\sqrt{17+4\sqrt{17}})$
$x^8 + 17x^6 + 68x^4 + 85x^2 + 17$				

$\mathbb{Q}$-rational CM points on $\mathcal{A}_4$

Main Theorem

Let $\mathcal{A}_4$ be the moduli space of principally polarized abelian varieties of dimension 4. Then in $\mathcal{A}_4$ there exist precisely **sixteen** $\mathbb{Q}$-rational points corresponding to the abelian fourfolds whose endomorphism rings are isomorphic to the ring of integers of cyclic octic CM-fields.

A genus 4 CM curve over $\mathbb{Q}$

A genus-4 curve with CM by the maximal order of the field of conductor 32:

$$y^2 = x^9 - 2x^8 - 8x^7 + 16x^6 + 20x^5 - 40x^4 - 16x^3 + 32x^2 + 2x - 4$$

(Hanselman - Pieper - Schiavone)