On Polarized Class Groups of Orders in Quartic CM-Fields

Gaetan Bisson
(joint work with Marco Streng)

Rennes, 10 June 2014

1 Cryptographic Motivation

Consider **Jacobian varieties of genus-one and two curves**, the effective groups for which DLP seems hardest.

Isogenies are efficiently computable for elliptic curves (Vélu, 1971), more recently abelian varieties (Lubicz–Robert, 2009). Have found many applications beyond mere DLP transport.

To best exploit isogenies, we need to understand their structure.

2 Complex Multiplication

Assume $\mathscr{A} = \mathrm{Jac}(\mathscr{C})$ is ordinary, absolutely simple. **The field $K = \mathbb{Q} \otimes \mathrm{End}(\mathscr{A})$ is:**

- over $\mathbb{F}_q$, a CM-field: imaginary quadratic extension of a degree-g real field K_0.
- over $\mathbb{Q}$, a subfield of a CM-field, often $\mathbb{Q}$.

The endomorphism ring is an order in K stable under complex conjugation.

Definition. *The polarized class group of such an order $\mathcal{O}$ is*

$$\mathfrak{C}(\mathcal{O}) = \frac{I_{\mathcal{O}}}{P_{\mathcal{O}}} = \frac{\left\{(\mathfrak{a}, \alpha) : \mathfrak{a}\overline{\mathfrak{a}} = \alpha\mathcal{O}, \alpha \in K_0^{++}\right\}}{\{(x\mathcal{O}, x\overline{x}) : x \in K^\times\}}.$$

It acts faithfully and transitively as isogenies on $\{\mathscr{A}/\overline{k} : \mathrm{End}(\mathscr{A}) = \mathcal{O}\}/\sim$.

3 Two Problems

Heegner classifies elliptic curves with CM over $\mathbb{Q}$ into 13 isomorphism classes. Van Wamelen conjectures an exhaustive list of 19 dimension-two Jacobians with CM by a maximal order. He proves CM, not the order.

Problem. *What are their endomorphism rings? Are there other abelian surfaces with CM?*

Computing endomorphism rings over finite fields can be done very efficiently deriving $\mathrm{End}(\mathscr{A})$ from its class group (seen acting as isogenies).

Problem. *To what extent is $\mathcal{O}$ characterized by $\mathfrak{C}(\mathcal{O})$ in quartic CM-fields?*

Both problems really depend on $\ker(N_{\Phi^r} : I_{K^r} \to \mathfrak{C}(\mathcal{O}))$; this talk uses $\mathfrak{C}(\mathcal{O})$ for simplicity.

4 Classical Case

Assume for simplicity $\mathcal{O} \subset \mathcal{O}'$. We want a necessary condition for the natural map $\mathfrak{C}(\mathcal{O}) \to \mathfrak{C}(\mathcal{O}')$ to be an isomorphism.

In dimension one $K_0 = \mathbb{Q}$ and $\mathfrak{C}$ collapses to the classical class group. We have

$$1 \to \mathcal{O}^\times \to \mathcal{O}_K^\times \to \frac{(\mathcal{O}_K/\mathfrak{f})^\times}{(\mathcal{O}/\mathfrak{f})^\times} \to \mathrm{cl}(\mathcal{O}) \to \mathrm{cl}(\mathcal{O}_K) \to 1$$

and thus

$$h(\mathcal{O}) = \frac{h(\mathcal{O}_K)}{[\mathcal{O}_K^\times : \mathcal{O}^\times]} f \prod_{p \mid f} \left(1 - \left(\frac{\Delta_K}{p}\right)\frac{1}{p}\right)$$

Whence $\mathfrak{C}(\mathcal{O}) \xrightarrow{\sim} \mathfrak{C}(\mathcal{O}')$ implies $[\mathcal{O} : \mathcal{O}'] \mid 6$.

5 Our Contribution

Using the structure of $\mathfrak{C}$ and some algebra, the condition becomes

$$\ker\left(\frac{(\mathcal{O}/f\,\mathcal{O}_K)^\times}{(\mathcal{O}^\circ/f\,\mathcal{O}_K)^\times \mu_{\mathcal{O}}} \to \frac{(\mathcal{O} \cap K_0/f\,\mathcal{O}_{K_0})^\times}{(\mathcal{O}^\circ \cap K_0/f\,\mathcal{O}_{K_0})^\times}\right) \quad \text{of exponent at most two.}$$

Bounding everything, we obtain:

Theorem. *If $\mathfrak{C}(\mathcal{O}) \xrightarrow{\sim} \mathfrak{C}(\mathcal{O}')$ with $\mathcal{O} \ncong \mathbb{Z}[\zeta_5]$, then $\dfrac{[\mathcal{O}' : \mathcal{O}]}{[\mathcal{O}' \cap \mathcal{O}_{K_0} : \mathcal{O} \cap \mathcal{O}_{K_0}]}$ divides $2^{10}3^4$.*

We can furthermore bound the denominator when $\mathcal{O}' = \mathcal{O}_K$, which gives:

Theorem. *If $K \ncong \mathbb{Q}(\zeta_5)$ is a quartic non-biquadratic CM-field of which $\mathcal{O}$ is an order stable under complex conjugation satisfying $\mathfrak{C}(\mathcal{O}) \xrightarrow{\sim} \mathfrak{C}(\mathcal{O}_K)$, then $[\mathcal{O}_K : \mathcal{O}] \,\Big|\, 2^{20}3^8\sqrt{N_{K_0/\mathbb{Q}}(\Delta_{K/K_0})}$.*

6 Applications

Theorem. *The* 19 *Jacobians of Van Wamelen have maximal endomorphism rings.*

Theorem. *The Jacobians of*

$$y^2 = x^6 - 4x^5 + 10x^3 - 6x - 1,$$
$$y^2 = 4x^5 + 40x^4 - 40x^3 + 20x^2 + 20x + 3$$

are up to $\overline{\mathbb{Q}}$-isomorphism the only abelian surfaces over $\mathbb{Q}$ with CM by a non-maximal order in a Van Wamelen or Bouyer–Streng field.

Kılıçer recently proved no other CM-field possible.

To compute the endomorphism ring of an abelian surface, compare $\mathfrak{C}(\mathrm{End})$ with $\mathfrak{C}(\mathcal{O})$ for candidate orders $\mathcal{O}$ through their action as isogenies.

Theorem. *Under GRH and heuristics (such as random Frobeniuses), the endomorphism rings of almost all abelian surfaces over $\mathbb{F}_q$ can be computed in time* $\exp\left(\sqrt{12\log(q)\log(\log(q))}\right)$.