Applications of class groups of CM-fields

Marco Streng
Universiteit Leiden

joint work with
Florian Bouyer (Warwick),
Gaetan Bisson (French Polynesia),
Pınar Kılıçer (Leiden)

Elliptic Curve Cryptography
16 September 2013

One simple equation over many fields

Consider

$$E : y^2 + xy = x^3 + 2x^2 - 18x + 27$$

over a finite field $\mathbf{F}_q$ of q elements.

If $q = 2^{256} + 9541 \cdot 2^{127} + 6328903$, then

- $P = [4](1, 3)$ has prime order $r = 2^{251} + 9544 \cdot 2^{122} + 197857$.
- The quadratic twist E' of E has order 16 times a prime.
- Starting from E or E' and using $\mathbf{F}_q$-isogenies of degree $< 2^{126}$, can reach only 4 curves.

By varying q, can construct

- many more such examples,
- pairing-friendly curves,
- supersingular curves.

One simple equation over many fields

Consider

$$E : y^2 + xy = x^3 + 2x^2 - 18x + 27$$

over a finite field $\mathbf{F}_q$ of q elements.

By varying q, can construct

- many more such examples,
- pairing-friendly curves,
- supersingular curves.

If $q = 2^{233}$, then E is the NIST standardized ECC curve "K-233". Same with 233 replaced with 283, 409, or 571.

If $q \neq 7$ is prime with $4q = u^2 + 7v^2$ $(u, v \in \mathbf{Z})$, then E and its twist are ordinary and have $q + 1 - u$ and $q + 1 + u$ points.

Why did all of this work?

- Endomorphism ring $\mathrm{End}(E) := \{\phi : E \to E\} \supset \mathbf{Z}$.
- Over $\mathbf{F}_q$, have Frobenius $Frob_q \in \mathrm{End}(E)$

$$Frob_q : (x, y) \mapsto (x^q, y^q),$$

  and $\#E(\mathbf{F}_q) = p + 1 - \mathrm{tr}(Frob_q)$.
- The curve on the previous slide has $\mathrm{End}(E) \supset \mathbf{Z}[\frac{\sqrt{-7}+1}{2}]$.
- "lack of space" often forces $Frob_q \in \mathbf{Z}[\frac{\sqrt{-7}+1}{2}]$, hence

$$Frob_q = \frac{1}{2}(u + v\sqrt{-7}) \quad \text{for some } u, v \in \mathbf{Z}.$$

- Then $u^2 + 7v^2 = 4q$ and $\#E(\mathbf{F}_q) = q + 1 - u$.

Which curves allow us to repeat this trick?

Requirements:

- $E/\mathbf{Q}$ (for coefficients in $\mathbf{Z}$)
- $\mathrm{End}(E) \supsetneq \mathbf{Z}$ (to force a "lack of space")

2nd requirement is called Complex Multiplication (CM), and the trick is well-known (CM method, Atkin-Morain)

Theorem (Heegner, 1952).
There are exactly 13 CM elliptic curves over $\mathbf{Q}$.
They have $\mathrm{End}(E) \cong \mathbf{Z}[\frac{\sqrt{D}+D}{2}]$ with $D \in \{-3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163\}$.

Hyperelliptic curves

- A (hyperelliptic) curve of genus 2 over $\mathbf{Q}$ (or $\mathbf{F}_q$ for odd q) is

$$C : y^2 = f(x),$$

  where f has degree $2g+1$ or $2g+2$ and no multiple roots.
- The Jacobian J_C of C is the group of pairs of points of C (up to some equivalence).
- More precisely $J_C(\mathbf{F}_q) = \mathrm{Pic}^0(C) = \mathrm{Div}^0(C)/\mathrm{Prin}(C)$.
- $J_C(\mathbf{F}_q)$ can replace EC in ECC $\rightsquigarrow$ hyperelliptic crypto.

Can we repeat this trick in genus two?

Def. A hyperelliptic curve C has CM iff $K := \mathrm{End}(J_{C,\overline{\mathbf{Q}}}) \otimes \mathbf{Q}$ is a number field of degree 4.

- Then K is a quartic CM-field,
  i.e., $K = K_0(\sqrt{\alpha})$, were $K_0 = \mathbf{Q}(\sqrt{d})$, $d > 0$ and
  $\alpha = -a + b\sqrt{d} \in K_0$ is totally negative.
- Compare to elliptic curve case:
  $K_0 = \mathbf{Q}$, $K = \mathbf{Q}(\sqrt{\alpha})$, $\alpha \in \mathbf{Q}$ negative.
- CM gives control over $Frob_q \rightsquigarrow$ genus-two CM method

Question:
Can we find all CM curves of genus two over $\mathbf{Q}$?

CM curves of genus two defined over the rationals

Van Wamelen (1997) gave a list of 19 curves of genus two over $\mathbf{Q}$ with CM. (At least numerically to high precision.)

Theorem (Murabayashi-Umegaki, 2001).
Van Wamelen's list is complete.

Claim. Van Wamelen's list is incomplete

CM curves of genus two defined over the rationals

Van Wamelen (1997) gave a list of 19 curves of genus two over $\mathbf{Q}$ with CM. (At least numerically to high precision.)

Theorem (Murabayashi-Umegaki, 2001).
Van Wamelen's list contains all curves of genus two over $\mathbf{Q}$ with CM by the maximal order of a quartic CM-field.

Claim. Van Wamelen's list is incomplete :

- restricting to $\mathbf{Q}$ eliminates the most interesting cases,
- the only reason to restrict to the maximal order is that it is easier.

Restricting to $\mathbf{Q}$ eliminates the most interesting cases

Van Wamelen observed that for $C/\mathbf{Q}$ with CM, the quartic CM-field K always has 4 automorphisms over $\mathbf{Q}$ (Galois), while generically it only has $\sqrt{\alpha} \mapsto \pm\sqrt{\alpha}$ (non-Galois).

- In other words, the most natural CM-fields do not appear on his list.
- Some types of curves are excluded by this (e.g., p-rank 1).

More precisely, if $K = \mathbf{Q}(\sqrt{-a + b\sqrt{d}})$ is non-Galois, and C is defined over L, then $\sqrt{a^2 - b^2 d} \in L$.

- So the smallest "generic" CM curves are defined over $K_0^r := \mathbf{Q}(\sqrt{a^2 - b^2 d})$.

Examples of CM curves of genus 2 defined over K_0^r

(joint work with Florian Bouyer, arXiv:1307.0486)

- The Echidna database (Kohel et al) contains many CM-fields K and Igusa invariants of CM curves. (At least numerically to high precision).

- Mestre's algorithm: Igusa invariants $\rightsquigarrow$ curves.
- Problem: 1000's of digits in their coefficients
- Can make coefficients smaller using an algorithm based on Stoll-Cremona (2003).

Theorem (Bouyer-S.) All of the ~ 100 curves in our preprint have CM by the maximal order of a quartic CM-field and are defined over K_0^r.

Examples of CM curves of genus 2 defined over K_0^r

(joint work with Florian Bouyer, arXiv:1307.0486)

Theorem (Bouyer-S.) All of the ~ 100 curves in our preprint have CM by the maximal order of a quartic CM-field and are defined over K_0^r.

Examples

Let $a = \sqrt{2}$, $b = \frac{\sqrt{89}-1}{2}$, $K = \mathbf{Q}(\sqrt{-5+b})$, $K^r = \mathbf{Q}(\sqrt{-11+4a})$.
Then

$$y^2 = x^5 + (4a-2)\,x^4 - 21x^3 + (16a-64)\,x^2 + 160x + (-142a+190)$$

has CM by $\mathcal{O}_K$, and

$$y^2 = (b-4)\,x^6 + (8b-36)\,x^5 + (16b-62)\,x^4 + (-13b+57)\,x^3 + (-17b+73)\,x^2 + (13b-57)\,x + (-b+5)$$

has CM by $\mathcal{O}_{K^r}$.

Examples of CM curves of genus 2 defined over K_0^r

(joint work with Florian Bouyer, arXiv:1307.0486)

Theorem (Bouyer-S.) All of the ~ 100 curves in our preprint have CM by the maximal order of a quartic CM-field and are defined over K_0^r.

Proof. Implementation of denominator bounds of Lauter-Viray + interval arithmetic. $\square$

First bounds that are general, sharp, and fast enough for our list.

Open problems relating to Lauter-Viray:

- make bounds on "$\mathcal{J}$" sharper,
- work directly with $\mathcal{O}_K$ rather than with $\mathcal{O}_{K_0}[\eta] \subset \mathcal{O}_K$,
- generalize to arbitrary orders.

Cryptographic application?

Genus-two CM method as it has been for 20 years (Spallek 1994):

$$\begin{array}{c} \text{CM Igusa invariants over } \overline{\mathbf{Q}} \\ \text{(i.e., Igusa class polynomials)} \\ \Big\downarrow \text{reduction} \\ \text{CM Igusa invariants over } \mathbf{F}_q \\ \Big\downarrow \text{Mestre} \\ \text{CM curve over } \mathbf{F}_q \\ \text{(huge random-looking} \\ \text{coefficients)} \end{array}$$

Cryptographic application?

Genus-two CM method as it has been for 20 years (Spallek 1994):

CM Igusa invariants over $\overline{\mathbf{Q}}$
(i.e., Igusa class polynomials)

$\Big\downarrow$ reduction

CM Igusa invariants over $\mathbf{F}_q$

$\Big\downarrow$ Mestre

CM curve over $\mathbf{F}_q$
(huge random-looking coefficients)

Alternative:

Our list

$\Big\downarrow$ reduction

CM curve over $\mathbf{F}_q$
(small coefficients)

Cryptographic application? Example

$$K = \mathbf{Q}(\sqrt{-26+\sqrt{20}}),\ K_0^r = \mathbf{Q}(\sqrt{41}) = \mathbf{Q}(a),\ a^2 + a - 10 = 0.$$

$p =$142003856595807482747635387048977088071520136032341569014612056864049709760143646636956724980664377491196079730519617723521029855649462172148699393958968638652107696147277436345811056227385195781997362304851932650270514293705125991379

$\exists$ curve C of genus two over $\mathbf{F}_{p^2}$ with CM by $\mathcal{O}_K$ and a subgroup of order $2^{192} + 18513$ suitable for pairing-based cryptography.

Write $C : y^2 = a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$. Scale $a_6 \approx 1$, translate $a_5 = 0$. Still have $a_4, a_3, a_2, a_1, a_0 \in \mathbf{F}_{p^2}$, each with twice as many digits as p.

These coefficients seem "random", and there is no efficient way to make them smaller.

However, this CM curve can be defined over K_0^r, where "size" makes more sense.

Cryptographic application? Example

$$K = \mathbf{Q}(\sqrt{-26+\sqrt{20}}),\ K_0^r = \mathbf{Q}(\sqrt{41}) = \mathbf{Q}(a),\ a^2 + a - 10 = 0.$$

$p =$ 142003856595807482747635387048977088071520136032341569014612056864049709760143646636956724980664377491196079730519617723521029855649462172148699393958968638652107696147277436345811056227385195781997362304851932650270514293705125991379

However, this CM curve can be defined over K_0^r, where "size" makes more sense.

Get equation

$$y^2 = (-a+3)\,x^6 + (4a-8)\,x^5 + 10x^4 + (-a+20)\,x^3 + (4a+5)\,x^2 + (a+4)\,x + 1.$$

Work in ring $\mathbf{F}_p[A]/(A^2 + A - 10) = \mathbf{F}_{p^2}$, all coefficients are small.

- Save bandwidth, carries, and reductions mod p.
- Make it possible to print examples in a journal or on slides.

Is this list complete? First: what is K_0^r?

$$\begin{tikzcd}
\mathrm{End}(J_C)\otimes\mathbf{Q} \arrow[r, equal] & K \arrow[d, dash] \arrow[rr, dashed, bend right, "N_\Phi"'] & & K^{\mathrm{r}} \subset \mathbf{C} \arrow[d, dash] \arrow[ll, dashed, bend right, "N_{\Phi^{\mathrm{r}}}"'] \\
& K_0 & & K_0^{\mathrm{r}}
\end{tikzcd}$$

Geometrically

- $N_\Phi(x)$ is the determinant of the action of the endomorphism x on tangent spaces.
- K^r, K_0^r, $N_{\Phi^{\mathrm{r}}}$ appear naturally too.

Explicitly

- For elliptic curves, $K^r = K$, $K_0 = K_0^r = \mathbf{Q}$, $N_\Phi = N_{\Phi^{\mathrm{r}}} = \mathrm{id}_K$.
- if $K = \mathbf{Q}(\sqrt{-a + b\sqrt{d}})$, then $K^r = \mathbf{Q}(\sqrt{-2a + \sqrt{a^2 - b^2 d}})$, $K_0 = \mathbf{Q}(\sqrt{d})$, and $K_0^r = \mathbf{Q}(\sqrt{a^2 - b^2 d})$.

The class group from the title

$$\mathrm{End}(J_C) \otimes \mathbf{Q} = K \overset{N_{\Phi^{\mathrm{r}}}}{\dashleftarrow} K^{\mathrm{r}} \subset \mathbf{C}$$

- if $K = \mathbf{Q}(\sqrt{-a + b\sqrt{d}})$, then $K^r = \mathbf{Q}(\sqrt{-2a + \sqrt{a^2 - b^2 d}})$

Fact: $N_{\Phi^{\mathrm{r}}}$ is a "half norm", i.e., $N_{\Phi}(x)\overline{N_{\Phi}(x)} = N(x)$.

Let

$$C_{\Phi^{\mathrm{r}}} = \frac{\{\text{ideals } \mathfrak{a} \text{ of } \mathcal{O}_{K^r}\}}{\{\mathfrak{a} : N_{\Phi^r}(\mathfrak{a}) = (\mu) \text{ for some } \mu \in K^* \text{ with } \mu\overline{\mu} \in \mathbf{Q}\}}.$$

- This is a group of ℓ-isogenies up to endomorphisms.
- For elliptic curves, $K^r = K$, N_{Φ^r} is the identity map, $C_{\Phi^{\mathrm{r}}}$ is the class group of K.
- For principal ideals $\mathfrak{a} = x\mathcal{O}_{K^r}$, can take $\mu = N_{\Phi^r}(x)$ with $\mu\overline{\mu} = N(x) \in \mathbf{Q}$.
  So $C_{\Phi^{\mathrm{r}}}$ is a quotient of the class group of K^r.

The class group from the title

Let

$$C_{\Phi^r} = \frac{\{\text{ideals } \mathfrak{a} \text{ of } \mathcal{O}_{K^r}\}}{\{\mathfrak{a} : N_{\Phi^r}(\mathfrak{a}) = (\mu) \text{ for some } \mu \in K^* \text{ with } \mu\overline{\mu} \in \mathbf{Q}\}}.$$

- This is a group of ℓ-isogenies up to endomorphisms.
- For principal ideals $\mathfrak{a} = x\mathcal{O}_{K^r}$, can take $\mu = N_{\Phi^r}(x)$ with $\mu\overline{\mu} = N(x) \in \mathbf{Q}$.
  So C_{Φ^r} is a quotient of the class group of K^r.

Main Theorem 1 of Complex Multiplication (Shimura-Taniyama)
The subfield of $\mathbf{C}$ generated over K^r by the Igusa invariants of C has Galois group C_{Φ^r}.

Corollary: If C is defined over K^r, then C_{Φ^r} is trivial.

CM class number one problem: find all K with $C_{\Phi^r} = 1$.

CM class number one problem

(work in progress of Pınar Kılıçer)

The list is complete: all genus-two curves with CM by a maximal order that are defined over K_0^r.

Ingredients:

- Bounds from analytic number theory devised for solving "easier" class number one problems (Louboutin).
- Genus theory and explicit manipulations with CM-types and ideals (to relate the class groups).
- Many hours of CPU time.

Next stops:

- CM hyperelliptic curves of genus 3
- CM Picard curves $y^3 =$ quartic
- arbitrary CM curves genus 3

Arbitrary orders

(joint work with Gaetan Bisson, arXiv:1302.3756)

- $\mathcal{O} := \mathrm{End}(J_C)$ is an order in K stable under complex conjugation.
- Take F such that $F\mathcal{O}_K \subset \mathcal{O}$ (e.g., $F = [\mathcal{O}_K : \mathcal{O}]$).

Let

$$C_{\Phi^{\mathrm{r}},\mathcal{O}} = \frac{\{\text{ideals } \mathfrak{a} \text{ of } \mathcal{O}_{K^r} \text{ coprime to } F\}}{\{\mathfrak{a} : N_{\Phi^r}(\mathfrak{a}) = (\mu),\ \mu\overline{\mu} \in \mathbf{Q},\ \mu\mathcal{O} \text{ coprime to } F\mathcal{O} \text{ as } \mathcal{O}\text{-ideal}\}}.$$

In case of elliptic curves, $C_{\Phi^{\mathrm{r}},\mathcal{O}} = \mathrm{Pic}(\mathcal{O})$.

Main Theorem 3 of Complex Multiplication (Shimura-Taniyama)
The subfield of $\mathbf{C}$ generated over K^r by the Igusa invariants of C has Galois group $C_{\Phi^{\mathrm{r}},\mathcal{O}}$ over K^{r}.

Arbitrary orders

(joint work with Gaetan Bisson, arXiv:1302.3756)

- $\mathcal{O} := \mathrm{End}(J_C)$ is an order in K stable under complex conjugation.
- Take F such that $F\mathcal{O}_K \subset \mathcal{O}$ (e.g., $F = [\mathcal{O}_K : \mathcal{O}]$).

Let

$$C_{\Phi^r,\mathcal{O}} = \frac{\{\text{ideals } \mathfrak{a} \text{ of } \mathcal{O}_{K^r} \text{ coprime to } F\}}{\{\mathfrak{a} : N_{\Phi^r}(\mathfrak{a}) = (\mu),\ \mu\overline{\mu} \in \mathbf{Q},\ \mu\mathcal{O} \text{ coprime to } F\mathcal{O} \text{ as } \mathcal{O}\text{-ideal}\}}.$$

Main Theorem 3 of Complex Multiplication (Shimura-Taniyama)
The subfield of $\mathbf{C}$ generated over K^r by the Igusa invariants of C has Galois group $C_{\Phi^r,\mathcal{O}}$ over K^r.

Corollary: If C is defined over K^r, then $C_{\Phi^r,\mathcal{O}} = 1$.
Goal: Find all $\mathcal{O}$ with $C_{\Phi^r,\mathcal{O}} = 1$.

Relating the orders

Given two orders $\mathcal{O} \subset \mathcal{O}' \subset K$ stable under complex conjugation.

Recall

$$C_{\Phi^r,\mathcal{O}} = \frac{\{\text{ideals } \mathfrak{a} \text{ of } \mathcal{O}_{K^r} \text{ coprime to } F\}}{\{\mathfrak{a} : N_{\Phi^r}(\mathfrak{a}) = (\mu),\ \mu\overline{\mu} \in \mathbf{Q},\ \mu\mathcal{O} \text{ coprime to } F\mathcal{O}\}}.$$

So $C_{\Phi^r,\mathcal{O}} \twoheadrightarrow C_{\Phi^r,\mathcal{O}'}$ with kernel

$$A = \frac{\{\mathfrak{a} : N_{\Phi^r}(\mathfrak{a}) = (\mu),\ \mu\overline{\mu} \in \mathbf{Q},\ \mu\mathcal{O}' \text{ coprime to } F\mathcal{O}'\}}{\{\mathfrak{a} : N_{\Phi^r}(\mathfrak{a}) = (\mu),\ \mu\overline{\mu} \in \mathbf{Q},\ \mu\mathcal{O} \text{ coprime to } F\mathcal{O}\}}.$$

Conclusion:
$\#C_{\Phi^r,\mathcal{O}} = \#A \cdot \#C_{\Phi^r,\mathcal{O}'}$,
so If $C_{\Phi^r,\mathcal{O}} = 1$, then both $C_{\Phi^r,\mathcal{O}'}$ and A are trivial.

Relating the orders

$$A = \frac{\{\mathfrak{a} : N_{\Phi^r}(\mathfrak{a}) = (\mu),\ \mu\overline{\mu} \in \mathbf{Q},\ \mu\mathcal{O}' \text{ coprime to } F\mathcal{O}'\}}{\{\mathfrak{a} : N_{\Phi^r}(\mathfrak{a}) = (\mu),\ \mu\overline{\mu} \in \mathbf{Q},\ \mu\mathcal{O} \text{ coprime to } F\mathcal{O}\}}.$$

Conclusion:

$\#C_{\Phi^r,\mathcal{O}} = \#A \cdot \#C_{\Phi^r,\mathcal{O}'}$,

Let $\mathcal{O}'_0 = \mathcal{O}' \cap K_0$, $\mathcal{O}_0 = \mathcal{O} \cap K_0$, and

$$\psi \ : \ \frac{(\mathcal{O}'/f\mathcal{O}_K)^\times}{(\mathcal{O}/f\mathcal{O}_K)^\times \mu_{\mathcal{O}'}} \longrightarrow \frac{(\mathcal{O}'_0/f\mathcal{O}_{K_0})^\times}{(\mathcal{O}_0/f\mathcal{O}_{K_0})^\times} \ : \ x \mapsto x\overline{x}.$$

We get $A \hookrightarrow \ker(\psi) : \mathfrak{a} \mapsto \mu$.

Can prove:

If $\ker(\psi) = 1$, then $A = 1$, so $C_{\Phi^r,\mathcal{O}} = C_{\Phi^r,\mathcal{O}'}$.

If $\ker(\psi)$ has an element of order > 2, then $A \neq 1$, so $\#C_{\Phi^r,\mathcal{O}} > \#C_{\Phi^r,\mathcal{O}'}$.

Example

$$\psi \;:\; \frac{(\mathcal{O}'/f\mathcal{O}_K)^\times}{(\mathcal{O}/f\mathcal{O}_K)^\times \mu_{\mathcal{O}'}} \longrightarrow \frac{(\mathcal{O}_0'/f\mathcal{O}_{K_0})^\times}{(\mathcal{O}_0/f\mathcal{O}_{K_0})^\times} \;:\; x \mapsto x\overline{x}.$$

Example:

If $\mathcal{O}_K = \mathbf{Z}[\beta]$, where $\beta = \sqrt{\alpha} = \sqrt{-a + b\sqrt{d}}$ take $F \in \mathbf{Z}_{>0}$ odd,

$$\begin{aligned} \text{let} \quad \mathcal{O} &= \mathbf{Z} + F^2\beta\mathbf{Z} + F^2\beta^2\mathbf{Z} + F^2\beta^3\mathbf{Z} \subset \\ \mathcal{O}' &= \mathbf{Z} + F^2\beta\mathbf{Z} + F\ \beta^2\mathbf{Z} + F^2\beta^3\mathbf{Z}, \\ \text{so} \quad \mathcal{O}_0 &= \mathbf{Z} + F^2\alpha^2\mathbf{Z}, \\ \mathcal{O}_0' &= \mathbf{Z} + F\ \alpha^2\mathbf{Z}, \end{aligned}$$

Example

$$\psi \ : \ \frac{(\mathcal{O}'/F^2\mathcal{O}_K)^\times}{(\mathcal{O}/F^2\mathcal{O}_K)^\times \mu_{\mathcal{O}'}} \longrightarrow \frac{(\mathcal{O}_0'/F^2\mathcal{O}_{K_0})^\times}{(\mathcal{O}_0/F^2\mathcal{O}_{K_0})^\times} \ : \ x \mapsto x\overline{x}.$$

Example:

If $\mathcal{O}_K = \mathbf{Z}[\beta]$, where $\beta = \sqrt{\alpha} = \sqrt{-a + b\sqrt{d}}$ take $F \in \mathbf{Z}_{>0}$ odd,

$$\begin{aligned} \text{let} \quad \mathcal{O} &= \mathbf{Z} + F^2\beta\mathbf{Z} + F^2\beta^2\mathbf{Z} + F^2\beta^3\mathbf{Z} \subset \\ \mathcal{O}' &= \mathbf{Z} + F^2\beta\mathbf{Z} + F\ \beta^2\mathbf{Z} + F^2\beta^3\mathbf{Z}, \\ \text{so} \quad \mathcal{O}_0 &= \mathbf{Z} + F^2\alpha^2\mathbf{Z}, \qquad (\mathcal{O}/F^2\mathcal{O}_K) = (\mathcal{O}_0/F^2\mathcal{O}_{K_0}), \\ \mathcal{O}_0' &= \mathbf{Z} + F\ \alpha^2\mathbf{Z}, \qquad (\mathcal{O}'/F^2\mathcal{O}_K) = (\mathcal{O}_0'/F^2\mathcal{O}_{K_0}). \end{aligned}$$

- Unit groups have order $(F-1)F^3$ and $(F-1)F$.
- So ψ is $x \mapsto x\overline{x} = x^2$ on a group of odd order F^2.
- So $\ker(\psi) = 1$, hence $C_{\Phi^r,\mathcal{O}} = C_{\Phi^r,\mathcal{O}'}$.

Relating the orders

Theorem (Bisson-S.)
If $C_{\Phi^r,\mathcal{O}} \cong C_{\Phi^r,\mathcal{O}'}$ and $\mathcal{O}' \ncong \mathbf{Z}[\zeta_5]$, then $[\mathcal{O}' : \mathcal{O}]/[\mathcal{O}'_0 : \mathcal{O}_0]$ divides $2^{10}3^4$.

Example shows division by $[\mathcal{O}'_0 : \mathcal{O}_0]$ is necessary.

Theorem (Bisson-S.)
If $C_{\Phi^r,\mathcal{O}} \cong C_{\Phi^r,\mathcal{O}_K}$ and $\mathcal{O}_K \ncong \mathbf{Z}[\zeta_5]$, then $[\mathcal{O}_K : \mathcal{O}]^2$ divides $2^{40}3^{16}N_{K_0/\mathbf{Q}}(\Delta_{K/K_0})$.

Corollary
For each K, only finitely many orders $\mathcal{O}$ with $C_{\Phi^r,\mathcal{O}} = 1$, and it is possible to enumerate them.

Open question
Is the factor $N_{K_0/\mathbf{Q}}(\Delta_{K/K_0})$ necessary?

More CM curves over $\mathbf{Q}$

Theorem (Bisson-S.)

- The curve

$$C : y^2 = x^6 - 4x^5 + 10x^3 - 6x - 1$$

  has endomorphism ring $\mathbf{Z} + 2\zeta_5\mathbf{Z} + (\zeta_5^2 + \zeta_5^3)\mathbf{Z} + 2\zeta_5^3\mathbf{Z}$,
- There exists a unique genus-two curve D with endomorphism ring $\mathbf{Z} + (\zeta_5 + 3\zeta_5^3)\mathbf{Z} + (\zeta_5^2 + \zeta_5^3)\mathbf{Z} + 5\zeta_5^3\mathbf{Z}$.
- Assuming Kılıçer's work in progress, this completes the list of curves over $\mathbf{Q}$.

Conjecture:

$$D : y^2 = 4x^5 + 40x^4 - 40x^3 + 20x^2 + 20x + 3.$$

Computing endomorphism rings

Gaetan Bisson at ECC 2011:
Compute endomorphism rings in heuristic subexponential time.

Application:
p-adic and CRT methods for computing Igusa class polynomials.

Method:

- Test whether $\mathfrak{a}$ is in the trivial class of $C_{\Phi^r,\mathrm{End}(J_C)}$ by computing the corresponding ℓ-isogenies for $\ell \mid N(\mathfrak{a})$.
- This allows one to test whether $C_{\Phi^r,\mathrm{End}(J_C)} = C_{\Phi^r,\mathcal{O}}$.
- Finitely many possibilities for $\mathcal{O}$.

One of his assumptions:
If $C_{\Phi^r,\mathcal{O}} = C_{\Phi^r,\mathcal{O}'}$, then 'almost' $\mathcal{O} = \mathcal{O}'$
(in the sense that $[\mathcal{O} + \mathcal{O}' : \mathcal{O} \cap \mathcal{O}'] < cst$).

Our example shows this is false, index can be any F.

Computing endomorphism rings

Gaetan Bisson at ECC 2011:
Compute endomorphism rings in heuristic subexponential time.

One of his assumptions:
If $C_{\Phi^r,\mathcal{O}} = C_{\Phi^r,\mathcal{O}'}$, then 'almost' $\mathcal{O} = \mathcal{O}'$
(in the sense that $[\mathcal{O} + \mathcal{O}' : \mathcal{O} \cap \mathcal{O}'] < cst$).

Our example shows this is false, index can be any F.

But our theorems show that it does not fail by much.

Conclusion (Bisson-S.):
If $[\mathcal{O}_K : \mathbf{Z}[\pi, \overline{\pi}]]$ behaves as a random integer, then can compute endomorphism rings in heuristic subexponential average time.