Complex multiplication and canonical lifts
SAGA 2007

David R. Kohel
The University of Sydney

7 mai 2007

Complex Multiplication in Genus 1

The Main Theorem of Complex Multiplication gives the relation between ideal classes and abelian varieties.

Complex Multiplication in Genus 1

The Main Theorem of Complex Multiplication gives the relation between ideal classes and abelian varieties. For example, in genus 1, the j-variant of an elliptic curve with CM by a maximal order $\mathcal{O}_K$ in K, generates the Hilbert class field $H = K(j)/K$.

Complex Multiplication in Genus 1

The Main Theorem of Complex Multiplication gives the relation between ideal classes and abelian varieties. For example, in genus 1, the j-variant of an elliptic curve with CM by a maximal order $\mathcal{O}_K$ in K, generates the Hilbert class field $H = K(j)/K$.

More precisely, an embedding $K \to \mathbb{C}$ gives the relation between ideals of $\mathcal{O}_K$ and isomorphism classes of elliptic curves over $\mathbb{C}$:

$$\mathfrak{a} \longmapsto E_{\mathfrak{a}} = \mathbb{C}/\mathfrak{a}^{-1}.$$

Complex Multiplication in Genus 1

The Main Theorem of Complex Multiplication gives the relation between ideal classes and abelian varieties. For example, in genus 1, the j-variant of an elliptic curve with CM by a maximal order $\mathcal{O}_K$ in K, generates the Hilbert class field $H = K(j)/K$.

More precisely, an embedding $K \to \mathbb{C}$ gives the relation between ideals of $\mathcal{O}_K$ and isomorphism classes of elliptic curves over $\mathbb{C}$:

$$\mathfrak{a} \longmapsto E_{\mathfrak{a}} = \mathbb{C}/\mathfrak{a}^{-1}.$$

The Artin isomorphism $\sigma : \mathrm{Gal}(H/K) \cong \mathrm{Cl}(\mathcal{O}_K)$, determines an action on $\{E_{\mathfrak{a}}\}$ compatible induced isogenies

$$E_{\mathfrak{a}} \to E_{\mathfrak{a}\mathfrak{p}} \cong_{\mathbb{C}} E_{\mathfrak{a}}^{\sigma(\mathfrak{p})}$$

N.B. The Galois action on $\{E_{\mathfrak{a}}\}$ is determined on any model $E_{\mathfrak{a}}/H$.

Complex Multiplication in Genus 1

A CM construction is an algorithm for the construction of invariants of an abelian variety with complex multiplication.

Complex Multiplication in Genus 1

A CM construction is an algorithm for the construction of invariants of an abelian variety with complex multiplication.

In genus 1, the traditional method is to evaluate the j-function at points τ in the upper half Poincaré plane, which correspond to lattices with complex multiplication.

Complex Multiplication in Genus 1

A CM construction is an algorithm for the construction of invariants of an abelian variety with complex multiplication.

In genus 1, the traditional method is to evaluate the j-function at points τ in the upper half Poincaré plane, which correspond to lattices with complex multiplication.

The objective of this algorithm is to determine the minimal polynomial $H_D(x)$ for $j(\tau)$ over $\mathbb{Q}$.

Complex Multiplication in Genus 1

A CM construction is an algorithm for the construction of invariants of an abelian variety with complex multiplication.

In genus 1, the traditional method is to evaluate the j-function at points τ in the upper half Poincaré plane, which correspond to lattices with complex multiplication.

The objective of this algorithm is to determine the minimal polynomial $H_D(x)$ for $j(\tau)$ over $\mathbb{Q}$. This polynomial defines a zero dimensional subscheme of $\mathbb{A}^1 \subset \mathbb{P}^1 \cong X(1)$.

Complex Multiplication in Genus 1

A CM construction is an algorithm for the construction of invariants of an abelian variety with complex multiplication.

In genus 1, the traditional method is to evaluate the j-function at points τ in the upper half Poincaré plane, which correspond to lattices with complex multiplication.

The objective of this algorithm is to determine the minimal polynomial $H_D(x)$ for $j(\tau)$ over $\mathbb{Q}$. This polynomial defines a zero dimensional subscheme of $\mathbb{A}^1 \subset \mathbb{P}^1 \cong X(1)$.

We may choose, instead, a function f on a modular curve $X = X(N)$ or $X = X_0(N)$ such that

$$X \xrightarrow{f} \mathbb{P}^1 \xrightarrow{j} X(1),$$

Complex Multiplication in Genus 1

A CM construction is an algorithm for the construction of invariants of an abelian variety with complex multiplication.

In genus 1, the traditional method is to evaluate the j-function at points τ in the upper half Poincaré plane, which correspond to lattices with complex multiplication.

The objective of this algorithm is to determine the minimal polynomial $H_D(x)$ for $j(\tau)$ over $\mathbb{Q}$. This polynomial defines a zero dimensional subscheme of $\mathbb{A}^1 \subset \mathbb{P}^1 \cong X(1)$.

We may choose, instead, a function f on a modular curve $X = X(N)$ or $X = X_0(N)$ such that

$$X \xrightarrow{f} \mathbb{P}^1 \xrightarrow{j} X(1),$$

in order to determine a *class polynomial* $F_D(x)$, as the minimal polynomial of $f(\tau)$.

Complex Multiplication in Genus 1

For example, the class polynomial $F_{-23}(x) = x^3 - x^2 + 1$, is defined in terms of the Weber function $f : X(48) \to X = \mathbb{P}^1$, where

$$j = \frac{(f^{24} - 16)^3}{f^{24}}.$$

Complex Multiplication in Genus 1

For example, the class polynomial $F_{-23}(x) = x^3 - x^2 + 1$, is defined in terms of the Weber function $f : X(48) \to X = \mathbb{P}^1$, where

$$j = \frac{(f^{24} - 16)^3}{f^{24}}.$$

This polynomial generates the same class field as the Hilbert class polynomial : $x^3 + 3491750x^2 - 5151296875x + 12771880859375$.

Complex Multiplication in Genus 1

For example, the class polynomial $F_{-23}(x) = x^3 - x^2 + 1$, is defined in terms of the Weber function $f : X(48) \to X = \mathbb{P}^1$, where

$$j = \frac{(f^{24} - 16)^3}{f^{24}}.$$

This polynomial generates the same class field as the Hilbert class polynomial : $x^3 + 3491750x^2 - 5151296875x + 12771880859375$.

The complete decomposition of $H_{-23}(j)$ in $\mathbb{Z}[f, f^{-1}]$ is given by the factoration :

$$\begin{aligned} & H_{-23}\left((f^{24} - 16)^3/f^{24}\right) f^{72} \\ & \quad = (f^3 - f^2 + 1) \cdot (f^3 + f^2 - 1) \cdot (f^6 + f^4 + 2f^2 + 1) \cdot \\ & \qquad (f^6 - f^5 + f^4 - 2f^3 + f^2 + 1) \cdot (f^6 + f^5 + f^4 + 2f^3 + f^2 + 1) \cdot \\ & \qquad (f^{12} - f^{10} - f^8 + 3f^4 - 2f^2 + 1) \cdot (f^{12} - 3f^8 + 2f^4 + 1) \cdot \\ & \qquad G_{24}(f) \cdot G_{48}(f) \cdot G_{96}(f). \end{aligned}$$

Thus there are multiple components over $H_{-23}(j)$ on X.

Complex Multiplication in Genus 2

In genus 2 (i.e. Jacobian surfaces), a generic CM field K is non-Galois over $\mathbb{Q}$, and its normal closure is a degree 2 extension L/K with Galois group D_4 over $\mathbb{Q}$.

Complex Multiplication in Genus 2

In genus 2 (i.e. Jacobian surfaces), a generic CM field K is non-Galois over $\mathbb{Q}$, and its normal closure is a degree 2 extension L/K with Galois group D_4 over $\mathbb{Q}$. There exist a triple of invariants (j_1, j_2, j_3) of any maximal order $\mathcal{O}_K$ (with associated CM type Φ), contained in the Hilbert class field H^r of the reflex field K^r :

Complex Multiplication in Genus 2

In genus 2 (i.e. Jacobian surfaces), a generic CM field K is non-Galois over $\mathbb{Q}$, and its normal closure is a degree 2 extension L/K with Galois group D_4 over $\mathbb{Q}$. There exist a triple of invariants (j_1, j_2, j_3) of any maximal order $\mathcal{O}_K$ (with associated CM type Φ), contained in the Hilbert class field H^r of the reflex field K^r :

$$\begin{tikzcd}
 & L & & H^r \supseteq K^r(j_1, j_2, j_3) \\
K \arrow[ur] & & K^r \arrow[ul] \arrow[ur] & \\
F \arrow[u] & & F^r \arrow[u] & \\
 & \mathbb{Q} \arrow[ul] \arrow[ur] & &
\end{tikzcd}$$

The field K^r is constructed in terms of the CM type Φ.

Complex Multiplication in Genus 2

The abelian surfaces (with fixed polarization type) correspond to pairs $(\mathfrak{a}, \alpha)$ such that $\mathfrak{a}\bar{\mathfrak{a}} = (\alpha)$ for $(\alpha) \equiv (1)$ in $\mathrm{Cl}^+(\mathcal{O}_F)$.

Complex Multiplication in Genus 2

The abelian surfaces (with fixed polarization type) correspond to pairs $(\mathfrak{a}, \alpha)$ such that $\mathfrak{a}\bar{\mathfrak{a}} = (\alpha)$ for $(\alpha) \equiv (1)$ in $\mathrm{Cl}^+(\mathcal{O}_F)$. The set of pairs $(\mathfrak{a}, \alpha)$ forms a groupe $\mathfrak{C}(\mathcal{O}_K)$ with identity $(\mathcal{O}_K, 1)$.

Complex Multiplication in Genus 2

The abelian surfaces (with fixed polarization type) correspond to pairs $(\mathfrak{a}, \alpha)$ such that $\mathfrak{a}\bar{\mathfrak{a}} = (\alpha)$ for $(\alpha) \equiv (1)$ in $\mathrm{Cl}^+(\mathcal{O}_F)$. The set of pairs $(\mathfrak{a}, \alpha)$ forms a groupe $\mathfrak{C}(\mathcal{O}_K)$ with identity $(\mathcal{O}_K, 1)$.

The class group $\mathrm{Cl}(\mathcal{O}_{K^r})$ acts on the group $\mathfrak{C}(\mathcal{O}_K)$ by means of the homomorphism :

$$\begin{aligned} \mathrm{Gal}(H^r/K^r) \cong \mathrm{Cl}(\mathcal{O}_{K^r}) &\longrightarrow \mathfrak{C}(\mathcal{O}_K) \\ \mathfrak{c} &\longmapsto \left(\mathrm{N}_\Phi(\mathfrak{c}), \mathrm{N}_{\mathbb{Q}}^{K^r}(\mathfrak{c})\right) \end{aligned}$$

where $\mathrm{N}_\Phi(\mathfrak{c}) = \mathrm{N}_K^L(\mathfrak{c}\mathcal{O}_L)$.

Complex Multiplication in Genus 2

The abelian surfaces (with fixed polarization type) correspond to pairs $(\mathfrak{a}, \alpha)$ such that $\mathfrak{a}\bar{\mathfrak{a}} = (\alpha)$ for $(\alpha) \equiv (1)$ in $\mathrm{Cl}^+(\mathcal{O}_F)$. The set of pairs $(\mathfrak{a}, \alpha)$ forms a groupe $\mathfrak{C}(\mathcal{O}_K)$ with identity $(\mathcal{O}_K, 1)$.

The class group $\mathrm{Cl}(\mathcal{O}_{K^r})$ acts on the group $\mathfrak{C}(\mathcal{O}_K)$ by means of the homomorphism :

$$\begin{aligned} \mathrm{Gal}(H^r/K^r) \cong \mathrm{Cl}(\mathcal{O}_{K^r}) &\longrightarrow \mathfrak{C}(\mathcal{O}_K) \\ \mathfrak{c} &\longmapsto \left(\mathrm{N}_\Phi(\mathfrak{c}), \mathrm{N}_{\mathbb{Q}}^{K^r}(\mathfrak{c})\right) \end{aligned}$$

where $\mathrm{N}_\Phi(\mathfrak{c}) = \mathrm{N}_K^L(\mathfrak{c}\mathcal{O}_L)$. Composing with multiplication in $\mathfrak{C}(\mathcal{O}_K)$, we obtain the Galois action :

$$\mathrm{Gal}(H^r/K^r) \times \mathfrak{C}(\mathcal{O}_K) \to \mathfrak{C}(\mathcal{O}_K).$$

Complex Multiplication in Genus 2

The abelian surfaces (with fixed polarization type) correspond to pairs $(\mathfrak{a}, \alpha)$ such that $\mathfrak{a}\bar{\mathfrak{a}} = (\alpha)$ for $(\alpha) \equiv (1)$ in $\mathrm{Cl}^+(\mathcal{O}_F)$. The set of pairs $(\mathfrak{a}, \alpha)$ forms a groupe $\mathfrak{C}(\mathcal{O}_K)$ with identity $(\mathcal{O}_K, 1)$.

The class group $\mathrm{Cl}(\mathcal{O}_{K^r})$ acts on the group $\mathfrak{C}(\mathcal{O}_K)$ by means of the homomorphism :

$$\begin{aligned} \mathrm{Gal}(H^r/K^r) \cong \mathrm{Cl}(\mathcal{O}_{K^r}) &\longrightarrow \mathfrak{C}(\mathcal{O}_K) \\ \mathfrak{c} &\longmapsto \left(\mathrm{N}_\Phi(\mathfrak{c}), \mathrm{N}^{K^r}_{\mathbb{Q}}(\mathfrak{c})\right) \end{aligned}$$

where $\mathrm{N}_\Phi(\mathfrak{c}) = \mathrm{N}^L_K(\mathfrak{c}\mathcal{O}_L)$. Composing with multiplication in $\mathfrak{C}(\mathcal{O}_K)$, we obtain the Galois action :

$$\mathrm{Gal}(H^r/K^r) \times \mathfrak{C}(\mathcal{O}_K) \to \mathfrak{C}(\mathcal{O}_K).$$

N.B. The above homomorphism can fail to be injective (hence $\{j_1, j_2, j_3\}$ does not generate H^r) or fail to be surjective (in which case there are multiple Galois orbits of invariants).

Complex Multiplication in Genus 2

An analytic construction for dimension 2 uses theta functions on Siegel to determine points (j_1, j_2, j_3) in $\mathcal{M}_2(\mathbb{C})$, the moduli space of curves of genus 2

Complex Multiplication in Genus 2

An analytic construction for dimension 2 uses theta functions on Siegel to determine points (j_1, j_2, j_3) in $\mathcal{M}_2(\mathbb{C})$, the moduli space of curves of genus 2 (which we identify with its image in the moduli space $\mathcal{A}_2(\mathbb{C})$ of principally polarized abelian surfaces).

Complex Multiplication in Genus 2

An analytic construction for dimension 2 uses theta functions on Siegel to determine points (j_1, j_2, j_3) in $\mathcal{M}_2(\mathbb{C})$, the moduli space of curves of genus 2 (which we identify with its image in the moduli space $\mathcal{A}_2(\mathbb{C})$ of principally polarized abelian surfaces).

The result of a CM construction is an ideal in $\mathbb{Q}[x_1, x_2, x_3]$ defining the zero dimensional scheme over $\mathbb{Q}$ of the Galois orbit of the point (j_1, j_2, j_3).

Complex Multiplication in Genus 2

An analytic construction for dimension 2 uses theta functions on Siegel to determine points (j_1, j_2, j_3) in $\mathcal{M}_2(\mathbb{C})$, the moduli space of curves of genus 2 (which we identify with its image in the moduli space $\mathcal{A}_2(\mathbb{C})$ of principally polarized abelian surfaces).

The result of a CM construction is an ideal in $\mathbb{Q}[x_1, x_2, x_3]$ defining the zero dimensional scheme over $\mathbb{Q}$ of the Galois orbit of the point (j_1, j_2, j_3).

Examples. The curves $y^2 = x^5 + 1$ and $y^2 = x^6 + 1$ have Igusa invariants

$$(0, 0, 0) \text{ and } (6400000/3, 440000/9, -32000/81).$$

Complex Multiplication in Genus 2

An analytic construction for dimension 2 uses theta functions on Siegel to determine points (j_1, j_2, j_3) in $\mathcal{M}_2(\mathbb{C})$, the moduli space of curves of genus 2 (which we identify with its image in the moduli space $\mathcal{A}_2(\mathbb{C})$ of principally polarized abelian surfaces).

The result of a CM construction is an ideal in $\mathbb{Q}[x_1, x_2, x_3]$ defining the zero dimensional scheme over $\mathbb{Q}$ of the Galois orbit of the point (j_1, j_2, j_3).

Examples. The curves $y^2 = x^5 + 1$ and $y^2 = x^6 + 1$ have Igusa invariants

$$(0, 0, 0) \text{ and } (6400000/3, 440000/9, -32000/81).$$

Thus their respective defining ideals are

$$(x_1, x_2, x_3) \text{ and } (3x_1 - 6400000, 9x_2 - 440000, 81x_3 + 32000).$$

Complex Multiplication in Genus 2

An analytic construction for dimension 2 uses theta functions on Siegel to determine points (j_1, j_2, j_3) in $\mathcal{M}_2(\mathbb{C})$, the moduli space of curves of genus 2 (which we identify with its image in the moduli space $\mathcal{A}_2(\mathbb{C})$ of principally polarized abelian surfaces).

The result of a CM construction is an ideal in $\mathbb{Q}[x_1, x_2, x_3]$ defining the zero dimensional scheme over $\mathbb{Q}$ of the Galois orbit of the point (j_1, j_2, j_3).

Examples. The curves $y^2 = x^5 + 1$ and $y^2 = x^6 + 1$ have Igusa invariants

$$(0, 0, 0) \text{ and } (6400000/3, 440000/9, -32000/81).$$

Thus their respective defining ideals are

$$(x_1, x_2, x_3) \text{ and } (3x_1 - 6400000, 9x_2 - 440000, 81x_3 + 32000).$$

We now describe a p-adic algorithm for the construction of ideals.

Canonical Lifts

Suppose that A/k is an ordinary, simple abelian variety over a finite field of characteristic p, and let R be its Witt ring, i.e. an extension of $\mathbb{Z}_p$ such that $[R : \mathbb{Z}_p] = [k : \mathbb{F}_p]$ and $\pi : R \to k$.

Canonical Lifts

Suppose that A/k is an ordinary, simple abelian variety over a finite field of characteristic p, and let R be its Witt ring, i.e. an extension of $\mathbb{Z}_p$ such that $[R : \mathbb{Z}_p] = [k : \mathbb{F}_p]$ and $\pi : R \to k$. A canonical lift is an abelian variety $\tilde{A}/R$ such that

$$\tilde{A}/R \times_R k = A/k \text{ and } \mathrm{End}(\tilde{A}) = \mathrm{End}(A).$$

Canonical Lifts

Suppose that A/k is an ordinary, simple abelian variety over a finite field of characteristic p, and let R be its Witt ring, i.e. an extension of $\mathbb{Z}_p$ such that $[R : \mathbb{Z}_p] = [k : \mathbb{F}_p]$ and $\pi : R \to k$. A canonical lift is an abelian variety $\tilde{A}/R$ such that

$$\tilde{A}/R \times_R k = A/k \text{ and } \mathrm{End}(\tilde{A}) = \mathrm{End}(A).$$

An abelian variety $\tilde{A}_1/R$ is a canonical lift if there exists an isogeny $\varphi : \tilde{A}_1 \to \tilde{A}_2$ for $\tilde{A}_1^\sigma = \tilde{A}_2$ such that $\tilde{A}_1 \times_R k = A$ and for some ℓ

$$\tilde{A}_2[\ell] = \ker(\varphi)^\sigma \oplus \varphi(\tilde{A}_1[\ell]).$$

Canonical Lifts

Suppose that A/k is an ordinary, simple abelian variety over a finite field of characteristic p, and let R be its Witt ring, i.e. an extension of $\mathbb{Z}_p$ such that $[R:\mathbb{Z}_p] = [k:\mathbb{F}_p]$ and $\pi : R \to k$. A canonical lift is an abelian variety $\tilde{A}/R$ such that

$$\tilde{A}/R \times_R k = A/k \text{ and } \mathrm{End}(\tilde{A}) = \mathrm{End}(A).$$

An abelian variety $\tilde{A}_1/R$ is a canonical lift if there exists an isogeny $\varphi : \tilde{A}_1 \to \tilde{A}_2$ for $\tilde{A}_1^\sigma = \tilde{A}_2$ such that $\tilde{A}_1 \times_R k = A$ and for some ℓ

$$\tilde{A}_2[\ell] = \ker(\varphi)^\sigma \oplus \varphi(\tilde{A}_1[\ell]).$$

We construct the canonical lifted invariants, given x in $\mathcal{A}_g(k)$, by solving for $\tilde{x}$ in $\mathcal{A}_g(R)$ such that $(\tilde{x}, \tilde{x}^\sigma)$ lies on a subscheme of $\mathcal{A}_g \times \mathcal{A}_g$ defined by isogenies with kernel of type $(\mathbb{Z}/\ell\mathbb{Z})^g$.

Canonical Lifts

An algorithm pour the construction of the p-adic canonical lift of an elliptic curve was introduced by Satoh in 1999, to determine the number of points on a given $E/\mathbb{F}_q$ (in small characteristic p).

Canonical Lifts

An algorithm pour the construction of the p-adic canonical lift of an elliptic curve was introduced by Satoh in 1999, to determine the number of points on a given $E/\mathbb{F}_q$ (in small characteristic p). The algorithm constructs the canonically lifted $\tilde{\jmath}$ of an given ordinary j-invariant j in $\mathbb{F}_q$, as the unique point $(\tilde{\jmath}, \tilde{\jmath}^\sigma)$ on

$$X_0(p) \to X(1) \times X(1).$$

Canonical Lifts

An algorithm pour the construction of the p-adic canonical lift of an elliptic curve was introduced by Satoh in 1999, to determine the number of points on a given $E/\mathbb{F}_q$ (in small characteristic p). The algorithm constructs the canonically lifted $\tilde{\jmath}$ of an given ordinary j-invariant j in $\mathbb{F}_q$, as the unique point $(\tilde{\jmath}, \tilde{\jmath}^\sigma)$ on

$$X_0(p) \to X(1) \times X(1).$$

An algorithm of Mestre, in 2000, introduced the use of theta functions and the AGM. This algorithm determines canonically lifted invariants $(\tilde{x}, \tilde{x}^\sigma)$ on $X_0(8)$ (in residue characteristic 2).

Canonical Lifts

An algorithm pour the construction of the p-adic canonical lift of an elliptic curve was introduced by Satoh in 1999, to determine the number of points on a given $E/\mathbb{F}_q$ (in small characteristic p). The algorithm constructs the canonically lifted $\tilde{\jmath}$ of an given ordinary j-invariant j in $\mathbb{F}_q$, as the unique point $(\tilde{\jmath}, \tilde{\jmath}^\sigma)$ on

$$X_0(p) \to X(1) \times X(1).$$

An algorithm of Mestre, in 2000, introduced the use of theta functions and the AGM. This algorithm determines canonically lifted invariants $(\tilde{x}, \tilde{x}^\sigma)$ on $X_0(8)$ (in residue characteristic 2).

Couveignes and Henocq in 2002 introduced the idea of p-adic lifting as a CM construction, to determine a high precision approximation to the Hilbert class polynomial on $X(1)$.

Example of a Canonical Lift

Note that the j-invariant $\tilde{\jmath}$ of the canonical lift of any $E/\mathbb{F}_p$ lies in $\mathbb{Z}_p$, but is algebraic over $\mathbb{Z}$,

Example of a Canonical Lift

Note that the j-invariant $\tilde{\jmath}$ of the canonical lift of any $E/\mathbb{F}_p$ lies in $\mathbb{Z}_p$, but is algebraic over $\mathbb{Z}$, and moreover generates the Hilbert class field over $K = \mathrm{End}(E) \otimes \mathbb{Q}$.

Example of a Canonical Lift

Note that the j-invariant $\tilde{\jmath}$ of the canonical lift of any $E/\mathbb{F}_p$ lies in $\mathbb{Z}_p$, but is algebraic over $\mathbb{Z}$, and moreover generates the Hilbert class field over $K = \mathrm{End}(E) \otimes \mathbb{Q}$. For instance

$$E/\mathbb{F}_{59} : y^2 = x^3 + 31x + 54$$

has j-invariant 20,

Example of a Canonical Lift

Note that the j-invariant $\tilde{\jmath}$ of the canonical lift of any $E/\mathbb{F}_p$ lies in $\mathbb{Z}_p$, but is algebraic over $\mathbb{Z}$, and moreover generates the Hilbert class field over $K = \mathrm{End}(E) \otimes \mathbb{Q}$. For instance

$$E/\mathbb{F}_{59} : y^2 = x^3 + 31x + 54$$

has j-invariant 20, but its canonical lift in $\mathbb{Z}_{59}$ is

$$\tilde{\jmath} = 20 + 53 \cdot 59 + 0 \cdot 59^2 + 57 \cdot 59^3 + 9 \cdot 59^4 + 3 \cdot 59^5 + 5 \cdot 59^6 + \cdots$$

Example of a Canonical Lift

Note that the j-invariant $\tilde{\jmath}$ of the canonical lift of any $E/\mathbb{F}_p$ lies in $\mathbb{Z}_p$, but is algebraic over $\mathbb{Z}$, and moreover generates the Hilbert class field over $K = \mathrm{End}(E) \otimes \mathbb{Q}$. For instance

$$E/\mathbb{F}_{59} : y^2 = x^3 + 31x + 54$$

has j-invariant 20, but its canonical lift in $\mathbb{Z}_{59}$ is

$$\tilde{\jmath} = 20 + 53 \cdot 59 + 0 \cdot 59^2 + 57 \cdot 59^3 + 9 \cdot 59^4 + 3 \cdot 59^5 + 5 \cdot 59^6 + \cdots$$

By lifting to sufficient precision we verify that $\tilde{\jmath}$ is a root of

$$x^3 + 3491750x^2 - 5151296875x + 12771880859375.$$

Example of a Canonical Lift

Note that the j-invariant $\tilde{\jmath}$ of the canonical lift of any $E/\mathbb{F}_p$ lies in $\mathbb{Z}_p$, but is algebraic over $\mathbb{Z}$, and moreover generates the Hilbert class field over $K = \mathrm{End}(E) \otimes \mathbb{Q}$. For instance

$$E/\mathbb{F}_{59} : y^2 = x^3 + 31x + 54$$

has j-invariant 20, but its canonical lift in $\mathbb{Z}_{59}$ is

$$\tilde{\jmath} = 20 + 53 \cdot 59 + 0 \cdot 59^2 + 57 \cdot 59^3 + 9 \cdot 59^4 + 3 \cdot 59^5 + 5 \cdot 59^6 + \cdots$$

By lifting to sufficient precision we verify that $\tilde{\jmath}$ is a root of

$$x^3 + 3491750x^2 - 5151296875x + 12771880859375.$$

In general, a p-adic algorithm for constructive CM must

- construct the lifted invariant (to some finite precision), and
- recognize an algebraic number from its approximation.

Relèvements canoniques

In general, a p-adic algorithm for constructive CM must

- construct the lifted invariant (to some finite precision), and
- recognize an algebraic number from its approximation.

Relèvements canoniques

In general, a p-adic algorithm for constructive CM must

- construct the lifted invariant (to some finite precision), and
- recognize an algebraic number from its approximation.

The first step replaces the p-adic numbers with complex numbers in analogous analytic constructions. Rather than a period lattice, the input is a suitable curve which we lift p-adically.

Relèvements canoniques

In general, a p-adic algorithm for constructive CM must

- construct the lifted invariant (to some finite precision), and
- recognize an algebraic number from its approximation.

The first step replaces the p-adic numbers with complex numbers in analogous analytic constructions. Rather than a period lattice, the input is a suitable curve which we lift p-adically.

The second step uses an LLL reconstruction, from one or multiple points on the CM subscheme.

Relèvements canoniques

In general, a p-adic algorithm for constructive CM must

- construct the lifted invariant (to some finite precision), and
- recognize an algebraic number from its approximation.

The first step replaces the p-adic numbers with complex numbers in analogous analytic constructions. Rather than a period lattice, the input is a suitable curve which we lift p-adically.

The second step uses an LLL reconstruction, from one or multiple points on the CM subscheme.

Currently several constructive CM algorithms for genus 2 CM moduli exist :

Relèvements canoniques

In general, a p-adic algorithm for constructive CM must

- construct the lifted invariant (to some finite precision), and
- recognize an algebraic number from its approximation.

The first step replaces the p-adic numbers with complex numbers in analogous analytic constructions. Rather than a period lattice, the input is a suitable curve which we lift p-adically.

The second step uses an LLL reconstruction, from one or multiple points on the CM subscheme.

Currently several constructive CM algorithms for genus 2 CM moduli exist :

- 2-adic lifting of $(2, 2)$-isogenies (Gaudry, Houtmann, K., Ritzenthaler, Weng).

Relèvements canoniques

In general, a p-adic algorithm for constructive CM must

- construct the lifted invariant (to some finite precision), and
- recognize an algebraic number from its approximation.

The first step replaces the p-adic numbers with complex numbers in analogous analytic constructions. Rather than a period lattice, the input is a suitable curve which we lift p-adically.

The second step uses an LLL reconstruction, from one or multiple points on the CM subscheme.

Currently several constructive CM algorithms for genus 2 CM moduli exist :

- 2-adic lifting of $(2, 2)$-isogenies (Gaudry, Houtmann, K., Ritzenthaler, Weng).
- 3-adic lifting of $(3, 3)$-isogenies (Carls, K., Lubicz),

Relèvements canoniques

In general, a p-adic algorithm for constructive CM must

- construct the lifted invariant (to some finite precision), and
- recognize an algebraic number from its approximation.

The first step replaces the p-adic numbers with complex numbers in analogous analytic constructions. Rather than a period lattice, the input is a suitable curve which we lift p-adically.

The second step uses an LLL reconstruction, from one or multiple points on the CM subscheme.

Currently several constructive CM algorithms for genus 2 CM moduli exist :

- 2-adic lifting of $(2, 2)$-isogenies (Gaudry, Houtmann, K., Ritzenthaler, Weng).
- 3-adic lifting of $(3, 3)$-isogenies (Carls, K., Lubicz),
- p-adic lifting of (ℓ, ℓ)-isogenies (K., adapting above to $p \neq \ell$).

Constructive CM algorithms for genus 2

Currently several constructive CM algorithms for genus 2 CM moduli exist :

- 2-adic lifting of $(2, 2)$-isogenies (Gaudry, Houtmann, K., Ritzenthaler, Weng).
- 3-adic lifting of $(3, 3)$-isogenies (Carls, K., Lubicz),
- p-adic lifting of (ℓ, ℓ)-isogenies (K., adapting above to $\ell \neq p$).

Constructive CM algorithms for genus 2

Currently several constructive CM algorithms for genus 2 CM moduli exist :

- 2-adic lifting of $(2, 2)$-isogenies (Gaudry, Houtmann, K., Ritzenthaler, Weng).
- 3-adic lifting of $(3, 3)$-isogenies (Carls, K., Lubicz),
- p-adic lifting of (ℓ, ℓ)-isogenies (K., adapting above to $\ell \neq p$).

The first uses Richelot isogenies between Jacobians of curves in Rosenhain form : $y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$.

Constructive CM algorithms for genus 2

Currently several constructive CM algorithms for genus 2 CM moduli exist :

- 2-adic lifting of $(2, 2)$-isogenies (Gaudry, Houtmann, K., Ritzenthaler, Weng).
- 3-adic lifting of $(3, 3)$-isogenies (Carls, K., Lubicz),
- p-adic lifting of (ℓ, ℓ)-isogenies (K., adapting above to $\ell \neq p$).

The first uses Richelot isogenies between Jacobians of curves in Rosenhain form : $y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$.

The 3-adic algorithm makes use of correspondence equations of algebraic theta functions.

Constructive CM algorithms for genus 2

Currently several constructive CM algorithms for genus 2 CM moduli exist :

- 2-adic lifting of $(2, 2)$-isogenies (Gaudry, Houtmann, K., Ritzenthaler, Weng).
- 3-adic lifting of $(3, 3)$-isogenies (Carls, K., Lubicz),
- p-adic lifting of (ℓ, ℓ)-isogenies (K., adapting above to $\ell \neq p$).

The first uses Richelot isogenies between Jacobians of curves in Rosenhain form : $y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$.

The 3-adic algorithm makes use of correspondence equations of algebraic theta functions.

Finding suitable input curves, whose Jacobian has endomorphism ring which is a maximal order of low class number, is the primary difficulty in the first step.

Constructive CM algorithms for genus 2

Currently several constructive CM algorithms for genus 2 CM moduli exist :

- 2-adic lifting of $(2, 2)$-isogenies (Gaudry, Houtmann, K., Ritzenthaler, Weng).
- 3-adic lifting of $(3, 3)$-isogenies (Carls, K., Lubicz),
- p-adic lifting of (ℓ, ℓ)-isogenies (K., adapting above to $\ell \neq p$).

The first uses Richelot isogenies between Jacobians of curves in Rosenhain form : $y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$.

The 3-adic algorithm makes use of correspondence equations of algebraic theta functions.

Finding suitable input curves, whose Jacobian has endomorphism ring which is a maximal order of low class number, is the primary difficulty in the first step. The height of the moduli points (hence the resulting output size) presents the major challenge to the LLL phase.

Algorithmic Problems

As the size of the input field grows, the following problems present themselves :

- The determination of the exact endomorphism ring $\mathcal{O} = End(J)$, where $\mathbb{Z}[\pi, \bar{\pi}] \subseteq \mathcal{O} \subseteq \mathcal{O}_K$.

Algorithmic Problems

As the size of the input field grows, the following problems present themselves :

- The determination of the exact endomorphism ring $\mathcal{O} = End(J)$, where $\mathbb{Z}[\pi, \bar{\pi}] \subseteq \mathcal{O} \subseteq \mathcal{O}_K$.

  Idea : determine and use (ℓ, ℓ)-modular correspondences in $\mathcal{A}_g \times \mathcal{A}_g$ in order to determine $\mathrm{Cl}(\mathcal{O}_K)$, or rather $\mathfrak{C}(\mathcal{O}_K)$.

Algorithmic Problems

As the size of the input field grows, the following problems present themselves :

- The determination of the exact endomorphism ring $\mathcal{O} = End(J)$, where $\mathbb{Z}[\pi, \bar{\pi}] \subseteq \mathcal{O} \subseteq \mathcal{O}_K$.

  Idea : determine and use (ℓ, ℓ)-modular correspondences in $\mathcal{A}_g \times \mathcal{A}_g$ in order to determine $\mathrm{Cl}(\mathcal{O}_K)$, or rather $\mathfrak{C}(\mathcal{O}_K)$.
- The reconstruction of the ideal of relations for (j_1, j_2, j_3).

Algorithmic Problems

As the size of the input field grows, the following problems present themselves :

- The determination of the exact endomorphism ring $\mathcal{O} = End(J)$, where $\mathbb{Z}[\pi, \bar{\pi}] \subseteq \mathcal{O} \subseteq \mathcal{O}_K$.

  Idea : determine and use (ℓ, ℓ)-modular correspondences in $\mathcal{A}_g \times \mathcal{A}_g$ in order to determine $\mathrm{Cl}(\mathcal{O}_K)$, or rather $\mathfrak{C}(\mathcal{O}_K)$.
- The reconstruction of the ideal of relations for (j_1, j_2, j_3).

  Idea : Determine H_r by algebraic algorithms, then identify each j_k as an integral element of in terms of a basis for $\mathcal{O}_{H^r}$.

  This avoids reconstructing relations between powers of the elements j_k of large height.

Algorithmic Problems

As the size of the input field grows, the following problems present themselves :

- The determination of the exact endomorphism ring $\mathcal{O} = End(J)$, where $\mathbb{Z}[\pi, \bar{\pi}] \subseteq \mathcal{O} \subseteq \mathcal{O}_K$.

  Idea : determine and use (ℓ, ℓ)-modular correspondences in $\mathcal{A}_g \times \mathcal{A}_g$ in order to determine $\mathrm{Cl}(\mathcal{O}_K)$, or rather $\mathfrak{C}(\mathcal{O}_K)$.
- The reconstruction of the ideal of relations for (j_1, j_2, j_3).

  Idea : Determine H_r by algebraic algorithms, then identify each j_k as an integral element of in terms of a basis for $\mathcal{O}_{H^r}$.

  This avoids reconstructing relations between powers of the elements j_k of large height.

The combined algebraic and analytic methods has potential to improve both algorithms when the exponent of $\mathrm{Cl}(\mathcal{O}_{K^r})$ contains large a prime power divisor.

Cryptographic applications

Example. Let C be the curve $y^2 + h(x)y = f(x)$ over

$$\mathbb{F}_8 = \mathbb{F}_2[t]/(t^3 + t + 1),$$

with $h(x) = x(x+1)$ and $f(x) = x(x+1)(x^3 + x^2 + t^2x + t^3)$.

Cryptographic applications

Example. Let C be the curve $y^2 + h(x)y = f(x)$ over

$$\mathbb{F}_8 = \mathbb{F}_2[t]/(t^3 + t + 1),$$

with $h(x) = x(x+1)$ and $f(x) = x(x+1)(x^3 + x^2 + t^2x + t^3)$. The curve is ordinary and has complex multiplication by the maximal order of $K = \mathbb{Q}(i\sqrt{23 + 4\sqrt{5}})$.

Cryptographic applications

Example. Let C be the curve $y^2 + h(x)y = f(x)$ over

$$\mathbb{F}_8 = \mathbb{F}_2[t]/(t^3 + t + 1),$$

with $h(x) = x(x+1)$ and $f(x) = x(x+1)(x^3 + x^2 + t^2x + t^3)$. The curve is ordinary and has complex multiplication by the maximal order of $K = \mathbb{Q}(i\sqrt{23 + 4\sqrt{5}})$. The maximal order has class number is 3, and there exist 6 isomorphism classes of principally polarized abelian varieties.

Cryptographic applications

Example. Let C be the curve $y^2 + h(x)y = f(x)$ over

$$\mathbb{F}_8 = \mathbb{F}_2[t]/(t^3 + t + 1),$$

with $h(x) = x(x+1)$ and $f(x) = x(x+1)(x^3 + x^2 + t^2 x + t^3)$. The curve is ordinary and has complex multiplication by the maximal order of $K = \mathbb{Q}(i\sqrt{23 + 4\sqrt{5}})$. The maximal order has class number is 3, and there exist 6 isomorphism classes of principally polarized abelian varieties.

We construct the ideal of relations in Igusa invariants (j_1, j_2, j_3) from the canonical lift of the Jacobian of C. For example, the invariant j_1 satisfies a minimal polynomial :

$$\begin{aligned}
H_1(x) = {} & 2^{18} 5^{36} 7^{24}\, x^6 \\
& - 11187730399273689774009740470140169672902905436515808105468750000\, x^5 \\
& + 501512527690591679504420832767471421512684501403834547644662988263671875000\, x^4 \\
& - 10112409242787391786676284633730575047614543135572025667468221432704263857808262923\, x^3 \\
& + 118287000250588667564540744739406154398135978447792771928535541240797386992091828213521875\, x^2 \\
& - 2^1 3^{50} 5^{10} 11^1 13^1 53^1 701^1 16319^1 69938793494948953569198870004032131926868578084899317\, x \\
& + 3^{60} 5^{15} 23^5 409^5 179364113^5
\end{aligned}$$

Cryptographic applications

Choosing the 120-bit prime

$$p = 954090659715830612807582649452910809,$$

and solving a norm equation in the endomorphism ring $\mathcal{O}_K$,

Cryptographic applications

Choosing the 120-bit prime

$$p = 954090659715830612807582649452910809,$$

and solving a norm equation in the endomorphism ring $\mathcal{O}_K$, we determine that the Jacobian of some curve over $\mathbb{F}_p$ with CM by $\mathcal{O}_K$ will have prime order

$$\begin{gathered}910288986956988885753118558284481029\backslash\\ 311411128276048027584310525408884449.\end{gathered}$$

Solving for a solution to the system of equations over $\mathbb{F}_p$, we find a corresponding curve

Cryptographic applications

Choosing the 120-bit prime

$$p = 954090659715830612807582649452910809,$$

and solving a norm equation in the endomorphism ring $\mathcal{O}_K$, we determine that the Jacobian of some curve over $\mathbb{F}_p$ with CM by $\mathcal{O}_K$ will have prime order

$$\begin{array}{l} 910288986956988885753118558284481029\backslash \\ 311411128276048027584310525408884449. \end{array}$$

Solving for a solution to the system of equations over $\mathbb{F}_p$, we find a corresponding curve

$$\begin{aligned} C : y^2 = x^6 &+ 827864728926129278937584622188769650\,x^4 \\ &+ 102877610579816483342116736180407060\,x^3 \\ &+ 335099510136640078379392471445640199\,x^2 \\ &+ 351831044709132324687022261714141411\,x \\ &+ 274535330436225557527308493450553085. \end{aligned}$$

Cryptographic applications

We solve for the curve

Cryptographic applications

We solve for the curve

$$\begin{aligned} C : y^2 = x^6 &+ 827864728926129278937584622188769650\, x^4 \\ &+ 102877610579816483342116736180407060\, x^3 \\ &+ 335099510136640078379392471445640199\, x^2 \\ &+ 351831044709132324687022261714141411\, x \\ &+ 274535330436225557527308493450553085. \end{aligned}$$

Cryptographic applications

We solve for the curve

$$\begin{aligned} C : y^2 = x^6 &+ 827864728926129278937584622188769650\, x^4 \\ &+ 1028776105798164833421167361804070\,60\, x^3 \\ &+ 335099510136640078379392471445640199\, x^2 \\ &+ 351831044709132324687022261714141411\, x \\ &+ 274535330436225557527308493450553085. \end{aligned}$$

A test of a random point on the Jacobian verifies the group order.

Cryptographic applications

We solve for the curve

$$\begin{aligned} C : y^2 = x^6 &+ 827864728926129278937584622188769650\, x^4 \\ &+ 1028776105798164833421167361804070600\, x^3 \\ &+ 335099510136640078379392471445640199\, x^2 \\ &+ 351831044709132324687022261714141411\, x \\ &+ 274535330436225557527308493450553085. \end{aligned}$$

A test of a random point on the Jacobian verifies the group order.

A comprehensive database for CM invariants in genera 1 and 2 is being developed :

`http://echidna.maths.usyd.edu.au/~kohel/dbs/`

providing an interface for the interrelated invariants of CM fields K, their Hilbert class fields, and CM moduli of abelian varieties.

FIN

Un relèvement canonique 2-adique

Soit $C/\mathbb{F}_2$ la courbe :

$$y^2 + (x^3 + x^2 + 1)y = (x^2 + 1)(x^3 + x^2 + 1),$$

Un relèvement canonique 2-adique

Soit $C/\mathbb{F}_2$ la courbe :

$$y^2 + (x^3 + x^2 + 1)y = (x^2 + 1)(x^3 + x^2 + 1),$$

alors le relèvement arbitraire

$$Y^2 = (2y + (x^3 + x^2 + 1))^2 = (x^3 + x^2 + 1)^2 + 4(x^2 + 1)(x^3 + x^2 + 1)$$

vers $\mathbb{Z}_2$ nous donne une courbe initiale pour la relèvement canonique (sur une extension de degré 3 qui nous donne tous les points de Weierstrass).

Un relèvement canonique 2-adique

Soit $C/\mathbb{F}_2$ la courbe :

$$y^2 + (x^3 + x^2 + 1)y = (x^2 + 1)(x^3 + x^2 + 1),$$

alors le relèvement arbitraire

$$Y^2 = (2y + (x^3 + x^2 + 1))^2 = (x^3 + x^2 + 1)^2 + 4(x^2 + 1)(x^3 + x^2 + 1)$$

vers $\mathbb{Z}_2$ nous donne une courbe initiale pour la relèvement canonique (sur une extension de degré 3 qui nous donne tous les points de Weierstrass).

Un comptage de points naïf nous donne le polynôme de Frobenius,

$$T^4 + T^3 + T^2 + 2T + 4.$$

Un relèvement canonique 2-adique

Soit $C/\mathbb{F}_2$ la courbe :

$$y^2 + (x^3 + x^2 + 1)y = (x^2 + 1)(x^3 + x^2 + 1),$$

alors le relèvement arbitraire

$$Y^2 = (2y + (x^3 + x^2 + 1))^2 = (x^3 + x^2 + 1)^2 + 4(x^2 + 1)(x^3 + x^2 + 1)$$

vers $\mathbb{Z}_2$ nous donne une courbe initiale pour la relèvement canonique (sur une extension de degré 3 qui nous donne tous les points de Weierstrass).

Un comptage de points naïf nous donne le polynôme de Frobenius,

$$T^4 + T^3 + T^2 + 2T + 4.$$

Le corps CM engendré par le Frobenius π,

$$K = \mathbb{Q}(\pi) \cong \mathbb{Q}[T]/(T^4 + T^3 + T^2 + 2T + 4).$$

Un relèvement canonique 2-adique

Le corps CM engendré par le Frobenius π,

$$K = \mathbb{Q}(\pi) \cong \mathbb{Q}[T]/(T^4 + T^3 + T^2 + 2T + 4),$$

est une extension de degré 2 de $\mathbb{Q}(\sqrt{13})$ avec discriminant $13^2\,17$.

Un relèvement canonique 2-adique

Le corps CM engendré par le Frobenius π,

$$K = \mathbb{Q}(\pi) \cong \mathbb{Q}[T]/(T^4 + T^3 + T^2 + 2T + 4),$$

est une extension de degré 2 de $\mathbb{Q}(\sqrt{13})$ avec discriminant $13^2\,17$. L'ordre maximal $\mathcal{O}_K$ est égal à $\mathbb{Z}[\pi, \bar{\pi}]$, où $\bar{\pi} \in \mathrm{End}(J)$ est le Verschiebung $\pi\bar{\pi} = q$.

Un relèvement canonique 2-adique

Le corps CM engendré par le Frobenius π,

$$K = \mathbb{Q}(\pi) \cong \mathbb{Q}[T]/(T^4 + T^3 + T^2 + 2T + 4),$$

est une extension de degré 2 de $\mathbb{Q}(\sqrt{13})$ avec discriminant $13^2\,17$. L'ordre maximal $\mathcal{O}_K$ est égal à $\mathbb{Z}[\pi, \bar{\pi}]$, où $\bar{\pi} \in \mathrm{End}(J)$ est le Verschiebung $\pi\bar{\pi} = q$. Le nombre des classes de K est 1, et le relèvement 2-adique des invariants de C nous donne des invariants d'Igusa (j_1, j_2, j_3), qui sont des racines de l'idéal engendré par les polynômes :

$$\begin{aligned}
&4j_1^2 + 8218017j_1 + 146211169851,\\
&j_2^2 + 1008855j_2 - 342014432400,\\
&j_3^2 + 1368387j_3 - 240090131376,\\
&4480j_1 + 7499j_2 - 12255j_3,\\
&716j_1 + 1212j_2 - 1971j_3 - 1666737
\end{aligned}$$

Un relèvement canonique 2-adique

Le corps CM engendré par le Frobenius π,

$$K = \mathbb{Q}(\pi) \cong \mathbb{Q}[T]/(T^4 + T^3 + T^2 + 2T + 4),$$

est une extension de degré 2 de $\mathbb{Q}(\sqrt{13})$ avec discriminant $13^2\,17$. L'ordre maximal $\mathcal{O}_K$ est égal à $\mathbb{Z}[\pi, \bar{\pi}]$, où $\bar{\pi} \in \mathrm{End}(J)$ est le Verschiebung $\pi\bar{\pi} = q$. Le nombre des classes de K est 1, et le relèvement 2-adique des invariants de C nous donne des invariants d'Igusa (j_1, j_2, j_3), qui sont des racines de l'idéal engendré par les polynômes :

$$\begin{array}{l} 4j_1^2 + 8218017j_1 + 146211169851, \\ j_2^2 + 1008855j_2 - 342014432400, \\ j_3^2 + 1368387j_3 - 240090131376, \\ 4480j_1 + 7499j_2 - 12255j_3, \\ 716j_1 + 1212j_2 - 1971j_3 - 1666737 \end{array}$$

qui definissent un sous-schéma de $\mathcal{M}_2$ de dimension 0 et degré 2.

Un relèvement canonique 3-adique

Soit $\mathbb{F}_{27} = \mathbb{F}_3[w]/(w^3 - w + 1)$, et soit C le courbe

$$y^2 = x(x-1)(x-t_1)(x-t_2)(x-t_3),$$

où

$$(t_1, t_2, t_3) = (w^{14}, w^8, 2).$$

Le point

$$(u_1, u_2, u_3) = (w^{16}, w^{24}, 2)$$

est l'image de (t_1, t_2, t_3) par le Frobenius et définit une seconde courbe

$$y^2 = x(x-1)(x-u_1)(x-u_2)(x-u_3),$$

reliée à la première par une correspondance de Richelot.

Un relèvement canonique 3-adique

Soit $\mathbb{F}_{27} = \mathbb{F}_3[w]/(w^3 - w + 1)$, et soit C le courbe

$$y^2 = x(x-1)(x-t_1)(x-t_2)(x-t_3),$$

où

$$(t_1, t_2, t_3) = (w^{14}, w^8, 2).$$

Le point

$$(u_1, u_2, u_3) = (w^{16}, w^{24}, 2)$$

est l'image de (t_1, t_2, t_3) par le Frobenius et définit une seconde courbe

$$y^2 = x(x-1)(x-u_1)(x-u_2)(x-u_3),$$

reliée à la première par une correspondance de Richelot. Alors les relèvements 3-adiques de ces invariants s'envoient sur un triplet d'invariants d'Igusa absolus (j_1, j_2, j_3), qui satisfont :

Un relèvement canonique 3-adique

$$
\begin{aligned}
&10460353203 j_1^6 - 2064460619497231368 0 j_1^5 + \\
&\quad 15847979034447250690001811 84 j_1^4 - \\
&\quad 5793420366997177472966359429986 8672 j_1^3 - \\
&\quad 4757210399363959986030325710967261851156 48 j_1^2 - \\
&\quad 2319410019701066580457483440392962776928771637248 j_1 - \\
&\quad 16336107525394146516376676933186699100640370289729 86368,
\end{aligned}
$$

$$
\begin{aligned}
&19683 j_2^6 - 3154427913690 j_2^5 + 1301845828470564217 5 j_2^4 - \\
&\quad 9011847196705020909893875 j_2^3 - \\
&\quad 469129225123381529988370573200 00 j_2^2 + \\
&\quad 1371934434680672253419375717574400000 0 j_2 - \\
&\quad 4251723415703581159078958066726110412800 0000,
\end{aligned}
$$

$$
\begin{aligned}
&531441 j_3^6 - 800798197608 54 j_3^5 + 6816522313564588247 13 j_3^4 - \\
&\quad 1621537231026449336569333993 j_3^3 - \\
&\quad 1566137192004297839675972173376896 j_3^2 - \\
&\quad 1479377322341359891148215922582439772160 j_3 - \\
&\quad 9399370213706557076073840873302176987265 10592.
\end{aligned}
$$