Construction of CM moduli by p-adic lifting

David R. Kohel
The University of Sydney

29 September 2006

Theory of canonical lifts

Let $A/\mathbb{F}_q$ be an *ordinary* abelian variety over a finite field,

Theory of canonical lifts

Let $A/\mathbb{F}_q$ be an *ordinary* abelian variety over a finite field, and let R be the *Witt ring* of $\mathbb{F}_q$.

Theory of canonical lifts

Let $A/\mathbb{F}_q$ be an *ordinary* abelian variety over a finite field, and let R be the *Witt ring* of $\mathbb{F}_q$. Up to isomorphism, R is the unique unramified extension of $\mathbb{Z}_p$ with $[R : \mathbb{Z}_p] = [\mathbb{F}_q : \mathbb{F}_p]$, and equipped with a surjection $R \to \mathbb{F}_q$.

Theory of canonical lifts

Let $A/\mathbb{F}_q$ be an *ordinary* abelian variety over a finite field, and let R be the *Witt ring* of $\mathbb{F}_q$. Up to isomorphism, R is the unique unramified extension of $\mathbb{Z}_p$ with $[R : \mathbb{Z}_p] = [\mathbb{F}_q : \mathbb{F}_p]$, and equipped with a surjection $R \to \mathbb{F}_q$. A *canonical lift* of A is an abelian variety $\tilde{A}/R$ such that

$$\text{(i) } \tilde{A}/R \longleftarrow A/\mathbb{F}_q \text{ and } \text{(ii) } \mathrm{End}_R(\tilde{A}) = \mathrm{End}_{\mathbb{F}_q}(A).$$

Theory of canonical lifts

Let $A/\mathbb{F}_q$ be an *ordinary* abelian variety over a finite field, and let R be the *Witt ring* of $\mathbb{F}_q$. Up to isomorphism, R is the unique unramified extension of $\mathbb{Z}_p$ with $[R:\mathbb{Z}_p] = [\mathbb{F}_q:\mathbb{F}_p]$, and equipped with a surjection $R \to \mathbb{F}_q$. A *canonical lift* of A is an abelian variety $\tilde{A}/R$ such that

$$\text{(i) } \tilde{A}/R \longleftarrow A/\mathbb{F}_q \text{ and } \text{ (ii) } \mathrm{End}_R(\tilde{A}) = \mathrm{End}_{\mathbb{F}_q}(A).$$

The existence of canonical lifts of ordinary abelian varieties was proved by Serre and Tate.

Theory of canonical lifts

Let $A/\mathbb{F}_q$ be an *ordinary* abelian variety over a finite field, and let R be the *Witt ring* of $\mathbb{F}_q$. Up to isomorphism, R is the unique unramified extension of $\mathbb{Z}_p$ with $[R : \mathbb{Z}_p] = [\mathbb{F}_q : \mathbb{F}_p]$, and equipped with a surjection $R \to \mathbb{F}_q$. A *canonical lift* of A is an abelian variety $\tilde{A}/R$ such that

$$\text{(i) } \tilde{A}/R \longleftarrow A/\mathbb{F}_q \text{ and (ii) } \mathrm{End}_R(\tilde{A}) = \mathrm{End}_{\mathbb{F}_q}(A).$$

The existence of canonical lifts of ordinary abelian varieties was proved by Serre and Tate. Here we take a constructive approach to the theory of canonical lifts.

Canonical lifts of elliptic curves

First we must have some effective way of representing an abelian variety.

Canonical lifts of elliptic curves

First we must have some effective way of representing an abelian variety. The simplest example of an abelian variety is an elliptic curve, which may be given by an equation

$$E : y^2 + (a_1 x + a_3)y = x^3 + a_2 x^2 + a_4 x + a_6.$$

Canonical lifts of elliptic curves

First we must have some effective way of representing an abelian variety. The simplest example of an abelian variety is an elliptic curve, which may be given by an equation

$$E : y^2 + (a_1 x + a_3)y = x^3 + a_2 x^2 + a_4 x + a_6.$$

The projective closure of this curve admits a group law, with a point at infinity $O = (0 : 1 : 0)$ as identity.

Canonical lifts of elliptic curves

First we must have some effective way of representing an abelian variety. The simplest example of an abelian variety is an elliptic curve, which may be given by an equation

$$E : y^2 + (a_1 x + a_3)y = x^3 + a_2 x^2 + a_4 x + a_6.$$

The projective closure of this curve admits a group law, with a point at infinity $O = (0 : 1 : 0)$ as identity.

In order to understand canonical lifts, we need also to understand the endomorphism rings of such curves.

Canonical lifts of elliptic curves

First we must have some effective way of representing an abelian variety. The simplest example of an abelian variety is an elliptic curve, which may be given by an equation

$$E : y^2 + (a_1 x + a_3)y = x^3 + a_2 x^2 + a_4 x + a_6.$$

The projective closure of this curve admits a group law, with a point at infinity $O = (0 : 1 : 0)$ as identity.

In order to understand canonical lifts, we need also to understand the endomorphism rings of such curves. In this one-dimensional case, the only CM endomorphism rings are orders in an imaginary quadratic field K.

Example of a canonical lift

Example. The simplest example of such a curve is

$$E/\mathbb{F}_p : y^2 = x^3 - x,$$

where $p = 1 \bmod 4$, which has canonical lift $\tilde{E}/\mathbb{Z}_p : y^2 = x^3 - x$.

Example of a canonical lift

Example. The simplest example of such a curve is

$$E/\mathbb{F}_p : y^2 = x^3 - x,$$

where $p = 1 \bmod 4$, which has canonical lift $\tilde{E}/\mathbb{Z}_p : y^2 = x^3 - x$. Here the endomorphism ring $\mathrm{End}(E) = \mathrm{End}(\tilde{E}) \cong \mathbb{Z}[\sqrt{-1}]$.

Example of a canonical lift

Example. The simplest example of such a curve is

$$E/\mathbb{F}_p : y^2 = x^3 - x,$$

where $p = 1 \bmod 4$, which has canonical lift $\tilde{E}/\mathbb{Z}_p : y^2 = x^3 - x$. Here the endomorphism ring $\mathrm{End}(E) = \mathrm{End}(\tilde{E}) \cong \mathbb{Z}[\sqrt{-1}]$.

The objective of our investigation, however, is to recover the *invariants* or *moduli* of $\tilde{E}$, which in the elliptic curve case is the j-invariant.

Example of a canonical lift

Example. The simplest example of such a curve is

$$E/\mathbb{F}_p : y^2 = x^3 - x,$$

where $p = 1 \bmod 4$, which has canonical lift $\tilde{E}/\mathbb{Z}_p : y^2 = x^3 - x$. Here the endomorphism ring $\mathrm{End}(E) = \mathrm{End}(\tilde{E}) \cong \mathbb{Z}[\sqrt{-1}]$.

The objective of our investigation, however, is to recover the *invariants* or *moduli* of $\tilde{E}$, which in the elliptic curve case is the j-invariant. For $p = 17$ we compute $j(E) = 18 \in \mathbb{F}_{19}$,

Example of a canonical lift

Example. The simplest example of such a curve is

$$E/\mathbb{F}_p : y^2 = x^3 - x,$$

where $p = 1 \bmod 4$, which has canonical lift $\tilde{E}/\mathbb{Z}_p : y^2 = x^3 - x$. Here the endomorphism ring $\mathrm{End}(E) = \mathrm{End}(\tilde{E}) \cong \mathbb{Z}[\sqrt{-1}]$.

The objective of our investigation, however, is to recover the *invariants* or *moduli* of $\tilde{E}$, which in the elliptic curve case is the j-invariant. For $p = 17$ we compute $j(E) = 18 \in \mathbb{F}_{19}$, however the canonical lift has invariant $j(\tilde{E}) = 12^3 \in \mathbb{Z}$.

Example of a canonical lift

N.B. The j-invariant of the canonical lift of $E/\mathbb{F}_p$ lies in $\mathbb{Z}_p$, but is algebraic over $\mathbb{Z}$,

Example of a canonical lift

N.B. The j-invariant of the canonical lift of $E/\mathbb{F}_p$ 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

N.B. The j-invariant of the canonical lift of $E/\mathbb{F}_p$ 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

$$E/\mathbb{F}_{19} : y^2 = x^3 + x + 8$$

has j-invariant 5,

Example of a canonical lift

N.B. The j-invariant of the canonical lift of $E/\mathbb{F}_p$ 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

$$E/\mathbb{F}_{19} : y^2 = x^3 + x + 8$$

has j-invariant 5, but its canonical lift in $\mathbb{Z}_{19}$ is

$$5 + 9 \cdot 19 + 8 \cdot 19^2 + 3 \cdot 19^3 + 3 \cdot 19^4 + 7 \cdot 19^5 + 7 \cdot 19^6 + 15 \cdot 19^7 + \cdots$$

Example of a canonical lift

N.B. The j-invariant of the canonical lift of $E/\mathbb{F}_p$ 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

$$E/\mathbb{F}_{19} : y^2 = x^3 + x + 8$$

has j-invariant 5, but its canonical lift in $\mathbb{Z}_{19}$ is

$$5 + 9 \cdot 19 + 8 \cdot 19^2 + 3 \cdot 19^3 + 3 \cdot 19^4 + 7 \cdot 19^5 + 7 \cdot 19^6 + 15 \cdot 19^7 + \cdots$$

By lifting to sufficient precision we verify that $j = j(\tilde{E})$ satisfies the quadratic relation:

$$j^2 + 191025j - 121287375.$$

Canonical lifting algorithm

A p-adic algorithm for constructive CM must

Canonical lifting algorithm

A p-adic algorithm for constructive CM must

- construct the lifted invariant (to some finite precision), and

Canonical lifting algorithm

A p-adic algorithm for constructive CM must

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

Canonical lifting algorithm

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.

Canonical lifting algorithm

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.

Canonical lifting algorithm

The j-invariant of an elliptic curve is a point on the modular curve $X(1)$.

Canonical lifting algorithm

The j-invariant of an elliptic curve is a point on the modular curve $X(1)$. Its canonical lift is determined by means of a correspondence

$$X_0(p) \longrightarrow X(1) \times X(1),$$

describing j-invariants of p-isogenous elliptic curves,

Canonical lifting algorithm

The j-invariant of an elliptic curve is a point on the modular curve $X(1)$. Its canonical lift is determined by means of a correspondence

$$X_0(p) \longrightarrow X(1) \times X(1),$$

describing j-invariants of p-isogenous elliptic curves, together with the Galois theoretic properties of this lift.

Canonical lifting algorithm

The j-invariant of an elliptic curve is a point on the modular curve $X(1)$. Its canonical lift is determined by means of a correspondence

$$X_0(p) \longrightarrow X(1) \times X(1),$$

describing j-invariants of p-isogenous elliptic curves, together with the Galois theoretic properties of this lift. An explicit algorithm for this construction was described by Couveignes and Henocq.

Canonical lifting algorithm

The j-invariant of an elliptic curve is a point on the modular curve $X(1)$. Its canonical lift is determined by means of a correspondence

$$X_0(p) \longrightarrow X(1) \times X(1),$$

describing j-invariants of p-isogenous elliptic curves, together with the Galois theoretic properties of this lift. An explicit algorithm for this construction was described by Couveignes and Henocq.

A prior algorithm for constructing canonical lifts for point counting was developed by Satoh. Efficient versions were introduced by Mestre, which generalise to higher dimension.

Canonical lifts of abelian surfaces

In higher dimension, we first need explicit models for abelian varieties, secondly, and explicit descriptions of their invariants or moduli.

Canonical lifts of abelian surfaces

In higher dimension, we first need explicit models for abelian varieties, secondly, and explicit descriptions of their invariants or moduli. For genus 2 curves "most" abelian surfaces are Jacobians of genus 2 curves,

Canonical lifts of abelian surfaces

In higher dimension, we first need explicit models for abelian varieties, secondly, and explicit descriptions of their invariants or moduli. For genus 2 curves "most" abelian surfaces are Jacobians of genus 2 curves, and we have an explicit algebraic description of their invariants by Igusa (following analytic invariants of Clebsch in the 19th century).

Canonical lifts of abelian surfaces

In higher dimension, we first need explicit models for abelian varieties, secondly, and explicit descriptions of their invariants or moduli. For genus 2 curves "most" abelian surfaces are Jacobians of genus 2 curves, and we have an explicit algebraic description of their invariants by Igusa (following analytic invariants of Clebsch in the 19th century). In the above construction we replace j with a triple of Igusa invariants (j_1, j_2, j_3) on $\mathcal{M}_2$, and find suitable correspondences relating the invariants of (p, p)-isogenous abelian varieties.

Constructive CM algorithms for genus 2

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

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).

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),

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 $p \neq \ell$).

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 $p \neq \ell$).

The first uses Richelot isogenies between Jacobians of curves in Rosenhain form:

$$y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3),$$

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

Example of genus 2 CM construction

Example. Let C be defined over $\mathbb{F}_2$ with model

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

Example of genus 2 CM construction

Example. Let C be defined over $\mathbb{F}_2$ with model

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

Its Jacobian is an abelian surface with complex multiplication by the maximal order of the number field

$$K = \mathbb{Q}[x]/(x^4 + 10x^2 + 17) \cong \mathbb{Q}\left(i\sqrt{5 + 2\sqrt{2}}\right).$$

Example of genus 2 CM construction

Example. Let C be defined over $\mathbb{F}_2$ with model

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

Its Jacobian is an abelian surface with complex multiplication by the maximal order of the number field

$$K = \mathbb{Q}[x]/(x^4+10x^2+17) \cong \mathbb{Q}\left(i\sqrt{5+2\sqrt{2}}\right).$$

Then canonically lifted Igusa invariants (j_1, j_2, j_3) satisfy:

$$\begin{array}{ll} j_1^2 - 531441j_1 + 55788550416, & 34j_2 - 36864j_3 + 10206, \\ 8j_2^2 - 4374j_2 - 9565938, & j_1 + 176j_2 - 73728j_3 - 27483. \\ 8192j_3^2 - 8667j_3 - 6561, & \end{array}$$

Effective Class Field Theory

Finding suitable modular equations describing moduli of abelian varieties and their isogenies is a one-time effort.

Effective Class Field Theory

Finding suitable modular equations describing moduli of abelian varieties and their isogenies is a one-time effort. Subsequently, the runtime of the algorithm is dominated by the time to compute the ideal of relations between the Igusa invariants.

Effective Class Field Theory

Finding suitable modular equations describing moduli of abelian varieties and their isogenies is a one-time effort. Subsequently, the runtime of the algorithm is dominated by the time to compute the ideal of relations between the Igusa invariants. The main difficulty is the large height of the algebraic numbers (j_1, j_2, j_3) for which we have p-adic approximations.

Effective Class Field Theory

Finding suitable modular equations describing moduli of abelian varieties and their isogenies is a one-time effort. Subsequently, the runtime of the algorithm is dominated by the time to compute the ideal of relations between the Igusa invariants. The main difficulty is the large height of the algebraic numbers (j_1, j_2, j_3) for which we have p-adic approximations. It is known, however, that the Igusa invariants lie in the Hilbert class field H of the reflex field K^r of K.

Effective Class Field Theory

Finding suitable modular equations describing moduli of abelian varieties and their isogenies is a one-time effort. Subsequently, the runtime of the algorithm is dominated by the time to compute the ideal of relations between the Igusa invariants. The main difficulty is the large height of the algebraic numbers (j_1, j_2, j_3) for which we have p-adic approximations. It is known, however, that the Igusa invariants lie in the Hilbert class field H of the reflex field K^r of K.

We want to make use of this knowledge...

Effective Class Field Theory

Returning to the previous example, we find that the reflex field is

$$K^r = \mathbb{Q}[x]/(x^4 + 5x^2 + 2) \cong \mathbb{Q}\left(i\sqrt{(5+\sqrt{17})/2}\right).$$

Effective Class Field Theory

Returning to the previous example, we find that the reflex field is

$$K^r = \mathbb{Q}[x]/(x^4 + 5x^2 + 2) \cong \mathbb{Q}\left(i\sqrt{(5+\sqrt{17})/2}\right).$$

Since K^r has class number 1 we know that in fact the Igusa invariants (j_1, j_2, j_3) lie in $H = K^r$.

Effective Class Field Theory

Returning to the previous example, we find that the reflex field is

$$K^r = \mathbb{Q}[x]/(x^4 + 5x^2 + 2) \cong \mathbb{Q}\left(i\sqrt{(5+\sqrt{17})/2}\right).$$

Since K^r has class number 1 we know that in fact the Igusa invariants (j_1, j_2, j_3) lie in $H = K^r$. In fact they generate its real quadratic subfield $\mathbb{Q}(\sqrt{17})$.

Effective Class Field Theory

Returning to the previous example, we find that the reflex field is

$$K^r = \mathbb{Q}[x]/(x^4 + 5x^2 + 2) \cong \mathbb{Q}\left(i\sqrt{(5+\sqrt{17})/2}\right).$$

Since K^r has class number 1 we know that in fact the Igusa invariants (j_1, j_2, j_3) lie in $H = K^r$. In fact they generate its real quadratic subfield $\mathbb{Q}(\sqrt{17})$. In less trivial examples, the Igusa invariants generate a nontrivial extension H/K^r.

Effective Class Field Theory

Returning to the previous example, we find that the reflex field is

$$K^r = \mathbb{Q}[x]/(x^4 + 5x^2 + 2) \cong \mathbb{Q}\left(i\sqrt{(5+\sqrt{17})/2}\right).$$

Since K^r has class number 1 we know that in fact the Igusa invariants (j_1, j_2, j_3) lie in $H = K^r$. In fact they generate its real quadratic subfield $\mathbb{Q}(\sqrt{17})$. In less trivial examples, the Igusa invariants generate a nontrivial extension H/K^r.

With Claus Fieker, we are combining algorithms for effective class field theory, to determine H, with the algebraic reconstruction of (j_1, j_2, j_3), to determine them as elements of the known field H.

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

The curve is ordinary and has complex multiplication by the maximal order of $K = \mathbb{Q}(i\sqrt{23 + 4\sqrt{5}})$.

The field K has class number is 3, and there exist 6 isomorphism classes of principally polarized abelian varieties.

Cryptographic applications

We can construct the defining ideal of relations in Igusa invariants (j_1, j_2, j_3) from the canonical lift of (the Jacobian of) C.

Cryptographic applications

We can construct the defining 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

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

Cryptographic applications

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

Cryptographic applications

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

$$\begin{aligned} C : y^2 = x^6 &+ 82786472892612927893758462218876965\,0\,x^4 \\ &+ 102877610579816483342116736180407060\,x^3 \\ &+ 335099510136640078379392471445640199\,x^2 \\ &+ 351831044709132324687022261714141411\,x \\ &+ 274535330436225557527308493450553085. \end{aligned}$$

Cryptographic applications

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

$$\begin{aligned} C : y^2 = x^6 &+ 82786472892612927893758462218876965 0\, x^4 \\ &+ 102877610579816483342116736180407060\, x^3 \\ &+ 335099510136640078379392471445640199\, x^2 \\ &+ 351831044709132324687022261714141411\, x \\ &+ 274535330436225557527308493450553085. \end{aligned}$$

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

Database of CM moduli

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

`http://www.maths.usyd.edu.au/u/kohel/dbs/index.html`,

Database of CM moduli

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

`http://www.maths.usyd.edu.au/u/kohel/dbs/index.html`,

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