On the invariants of the quotients of the Jacobian of a curve of genus 2

P. Gaudry
LIX, École polytechnique
91128 Palaiseau Cedex, France
gaudry@lix.polytechnique.fr

É. Schost
Laboratoire GAGE, UMS MEDICIS, École polytechnique
91128 Palaiseau Cedex, France
schost@gage.polytechnique.fr
(corresponding author)

January 31, 2001

Abstract

Let $\mathcal{C}$ be a curve of genus 2 that admits a non-hyperelliptic involution. We show that there are at most 2 isomorphism classes of elliptic curves that are quotients of degree 2 of the Jacobian of $\mathcal{C}$.

Our proof is constructive, and we present explicit formulae, classified according to the involutions of $\mathcal{C}$, that give the minimal polynomial of the j-invariant of these curves in terms of the moduli of $\mathcal{C}$. The coefficients of these minimal polynomials are given as rational functions of the moduli.

keywords: curve of genus 2, group of involutions, Igusa invariants, reducible Jacobian

Introduction

Among the curves of genus 2, those with reducible Jacobian have a particular interest. For instance, the present records for rank or torsion are obtained on such curves [3]. Also, it is in this particular setting that Dem'janenko-Manin's method yields all the rational points of a curve [7].

The aim of this paper is to give a constructive proof of the following theorem.

Theorem 1 *Let $\mathcal{C}$ be a curve of genus 2 with (2,2)-reducible Jacobian. Then there are at most 2 elliptic curves that are quotients of degree 2 of its Jacobian, up to isomorphism.*

If this is the case, we present rational formulae that give the j-invariant of these elliptic curves in terms of the moduli of $\mathcal{C}$.

The moduli of the curves of genus 2 form a 3-dimensional variety that was first described by Igusa in [4]. His construction relies on 4 covariants of the associated sextic, denoted by (A, B, C, D); the formulae for these covariants are given again in [11]. We use the moduli (j_1, j_2, j_3) proposed in [5], which are ratios of these covariants. If we suppose that A is not zero, they are given by

$$\begin{aligned} j_1 &= 144\frac{B}{A^2}, \\ j_2 &= -1728\frac{AB - 3C}{A^3}, \\ j_3 &= 486\frac{D}{A^5}. \end{aligned}$$

The special case $A = 0$ is dealt with in appendix 5.3. All along the paper, the characteristic of the basefield will be supposed different from 2, 3 and 5. We will regularly feel free to work over an algebraic closure of the initial field of definition of the curves.

Acknowledgements

The computations necessary to obtain the formulae given here were done on the computers of UMS MEDICIS 658 (CNRS – École polytechnique, `http://medicis.polytechnique.fr`). We thank Philippe Satgé for his careful reading of this paper, and François Morain for his numerous comments and suggestions.

1 Preliminaries

Definition 2 *The Jacobian of a curve $\mathcal{C}$ of genus 2 is (2,2)-reducible if there exists a (2,2)-isogeny between $Jac(\mathcal{C})$ and a product $\mathcal{E}_1 \times \mathcal{E}_2$ of elliptic curves. The curve $\mathcal{E}_1$ is then called a quotient of $Jac(\mathcal{C})$ of degree 2.*

As usual, the prefix $(2, 2)$ means that the kernel of the isogeny is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. A curve of genus 2 always admits the hyperelliptic involution, denoted ι, which commutes with all other automorphisms. The following lemma, in substance in [4], relates the reducibility to the existence of other involutions.

Lemma 3 *Let $\mathcal{C}$ be of genus 2 curve. The set of the non-hyperelliptic involutions of $\mathcal{C}$ is mapped onto the isomorphisms classes of elliptic curves which are quotient of degree 2 of the Jacobian of $\mathcal{C}$, via $\tau \mapsto \mathcal{C}/\tau$. As a consequence the Jacobian of $\mathcal{C}$ is (2,2)-reducible if and only if $\mathcal{C}$ admits a non-hyperelliptic involution.*

Proof. Let τ be a non-hyperelliptic involution of $\mathcal{C}$. The quotient of $\mathcal{C}$ by τ is a curve $\mathcal{E}$ of genus 1 [4]; this curve is a also quotient of the Jacobian of $\mathcal{C}$. The Jacobian projects onto $\mathcal{E}$, and the kernel of this map is another elliptic curve $\mathcal{E}'$. Consequently, the Jacobian of $\mathcal{C}$ splits as $\mathcal{E} \times \mathcal{E}'$.

On the other hand, let $\mathcal{E}$ be an elliptic quotient of degree 2 of $\mathrm{Jac}(\mathcal{C})$. There exists a morphism φ of degree 2 from $\mathcal{C}$ onto $\mathcal{E}$. For a generic point p on $\mathcal{C}$, the fiber $\varphi^{-1}(\varphi(p))$ can be written $\{p, q(p)\}$, where q is a rational function of p. We define τ as the map $p \mapsto q(p)$. Since the curve $\mathcal{E}$ has genus one, τ is not the hyperelliptic involution. □

Bolza [1], Igusa [4] and Lange [8] have classified the curves with automorphisms, and in particular the curves with involutions. The moduli of such curves describe a 2-dimensional subvariety of the moduli space; we will denote this set by $\mathcal{H}_2$. In our local coordinates, this hypersurface is described by the following equation R, whose construction is done in [11].

$$
\begin{aligned}
R: \quad & 8393900389396594682757 12 j_3^2 + 92114133216972232458240000 0 j_3^3 \\
& + 32983576347223130112000 j_1^2 j_3^2 + 18220094257462272 0 j_3 j_1 j_2^2 \\
& - 37481336758208102 4 j_3 j_1^2 j_2 + 99950231355221606400 00 j_3^2 j_1 j_2 \\
& + 94143178827 j_2^4 - 562220513731215360 j_3 j_2^2 - 562220051373121536 j_3 j_1^3 \\
& + 43381176803481600 j_3 j_2^3 - 71964166575759556608000 j_3^2 j_2 \\
& - 38860649950910160568320 0 j_3^2 j_1 - 1156831381426176 j_1^5 j_3 \\
& - 31381059609 j_1^7 + 627621192 18 j_1^4 j_2^2 + 13947137604 j_1^3 j_2^3 \\
& - 31381059609 j_1 j_2^4 - 188286357654 j_1^3 j_2^2 - 6973568802 j_1^6 j_2 \\
& + 19261242500745830 4 j_1^4 j_3 + 94143178827 j_1^6 - 6973568802 j_2^5 \\
& + 28920784535654400 j_1^2 j_3 j_2^2 + 164848471853230080 j_1^3 j_3 j_2 = 0.
\end{aligned}
$$

We will call *reduced group of automorphisms* of a curve the quotient of its group of automorphisms by $\{1, \iota\}$. The points on $\mathcal{H}_2$ can be classified according to their reduced group of automorphisms $\mathcal{G}$.

- $\mathcal{G}$ is the dihedral group D_6; this is the case for the point on $\mathcal{H}_2$ associated to the curve $y^2 = x^6 + 1$.
- $\mathcal{G}$ is the symmetric group $\mathfrak{S}_4$; this is the case for the point associated to the curve $y^2 = x^5 - x$.
- $\mathcal{G}$ is the dihedral group D_3; the corresponding points describe a curve $\mathcal{D}$ on $\mathcal{H}_2$, excluding the two previous points.
- $\mathcal{G}$ is Klein's group V_4. The corresponding points describe a curve $\mathcal{V}$ on $\mathcal{H}_2$, excluding the two previous points; these 2 points form the intersection of $\mathcal{D}$ and $\mathcal{V}$.
- $\mathcal{G}$ is the group $\mathbb{Z}/2\mathbb{Z}$. This corresponds to the open subset $\mathcal{U} = \mathcal{H}_2 - \mathcal{D} - \mathcal{V}$; this situation will be called the *generic case*.

In the sequel, we characterize all these cases, except the two isolated points, in terms of the moduli of $\mathcal{C}$, describe the involutions of $\mathcal{C}$ and compute the corresponding j-invariants.

In the "generic case", we introduce two characteristic invariants of the isomorphism classes. Our explicit formuae then give an easy proof of the fact that the curves whose moduli lie on $\mathcal{D}$ admit a real multiplication by $\sqrt{3}$. Finally, the involutions are naturally paired as $(\tau, \tau\iota)$, and these involutions correspond in general to distinct elliptic curves; we show that on the curve $\mathcal{V}$, each pair $(\tau, \tau\iota)$ yields a single elliptic curve.

The proof of Theorem 1 could be achieved through the exhaustive study of all possible automorphism groups, which would require to consider groups of order up to 48. We follow another approach, which relies on the computer algebra of polynomials systems.

This method brings to treat many polynomial systems. While most of them can be easily treated by the Gröbner bases package of the Magma Computer Algebra System [10], the more difficult one in section 2 requires another approach, which we will briefly describe. The systems we solved cannot given here, for lack of space; they are available upon request. The study of the group action in section 2 was partly conducted using the facilities of Magma for computing in finite groups.

2 The generic case

In the open set $\mathcal{U}$, the reduced group of automorphisms is $\mathbb{Z}/2\mathbb{Z}$. Consequently, the whole group of automorphisms has the form $\{1, \iota, \tau, \tau\iota\}$, and lemma 3 implies that there are at most two elliptic quotients. Our goal is then to compute a polynomial of degree 2 giving their j-invariants in terms of the moduli (j_1, j_2, j_3).

2.1 The minimal polynomial from a Rosenhain form

As a first step, we obtain the j-invariants from a Rosenhain form. The following result is based on [4], which gives the Rosenhain form of a $(2,2)$-reducible curve.

Theorem 4 *Let $\mathcal{C}$ be a curve of genus 2 whose moduli belong to $\mathcal{H}_2$. On an algebraic closure of its definition field, $\mathcal{C}$ is isomorphic to a curve of equation*

$$y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu), \text{ where } \mu = \nu\frac{1-\lambda}{1-\nu},$$

and λ, ν, μ are pairwise distinct, different from 0 and 1. The Jacobian of $\mathcal{C}$ is $(2,2)$-isogeneous to the product of the elliptic curves of equation $y^2 = x(x-1)(x-\Lambda)$, where Λ is a solution of

$$\nu^2\lambda^2\Lambda^2 + 2\nu\mu(-2\nu+\lambda)\Lambda + \mu^2 = 0. \tag{1}$$

Proof. The curve $\mathcal{C}$ has 6 Weierstraß points, and an isomorphism from $\mathcal{C}$ to another curve is determined by the images of 3 of these points. Let τ be a non-hyperelliptic involution of $\mathcal{C}$, and P_1, P_2, P_3 be Weierstraß points on $\mathcal{C}$ that represent the orbits of τ. The curve $\mathcal{C}'$ defined by sending $\{P_1, P_2, P_3\}$ to $\{0, 1, \infty\}$ admits the equation

$$y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu).$$

This curve is not singular, so λ, ν, μ are pairwise distinct, and different from 0 and 1.

The image of the involution of $\mathcal{C}$ on $\mathcal{C}'$ is still denoted by τ. This involution permutes the Weierstraß points of $\mathcal{C}'$; up to a change of names, we have $\tau(0) = \lambda$, $\tau(1) = \mu$ and $\tau(\infty) = \nu$. On another hand, τ can be written

$$\tau(x, y) = \left(\frac{ax + b}{cx + d}, \frac{wy}{(cx + d)^3} \right),$$

and since it has order 2, we have $a = -d$ and $w = \pm(ad - bc)^{3/2}$. The involution τ is determined by $\tau(0) = \lambda$ and $\tau(\infty) = \nu$, which gives

$$\tau(x, y) = \left(\nu \frac{x - \lambda}{x - \nu}, \frac{u^3 y}{(x - \nu)^3} \right),$$

where

$$u = \pm\sqrt{\nu(\nu - \lambda)}.$$

Changing the sign of u is equivalent to composing τ with ι. The relation $\tau(1) = \mu$ then yields the first assertion

$$\mu = \nu \frac{1 - \lambda}{1 - \nu}.$$

We now look for a curve isomorphic to $\mathcal{C}'$, where the involution can be written $(x, y) \mapsto (-x, y)$. This means that we are interested in a transformation

$$\varphi \ : \ x \mapsto \frac{ax + b}{cx + d}$$

such that $\varphi(0) = -\varphi(\lambda)$, $\varphi(1) = -\varphi(\mu)$, $\varphi(\infty) = -\varphi(\nu)$. It is straightforward to check that

$$\varphi(x) = \frac{x - \nu - u}{x - \nu + u},$$

is such a transformation. As a result, the curve $\mathcal{C}$ is isomorphic to the curve $\mathcal{C}''$ of equation $y^2 = (x^2 - x_1^2)(x^2 - x_2^2)(x^2 - x_3^2)$, where

$$x_1 = \varphi(\infty) = 1, \quad x_2 = \varphi(0) = \frac{\nu - u}{\nu + u}, \quad x_3 = \varphi(1) = \frac{1 - (\nu - u)}{1 - (\nu + u)}.$$

The morphism $(x, y) \mapsto (x^2, y)$ maps $\mathcal{C}''$ onto the elliptic curve $\mathcal{E}$ of equation

$$y^2 = (x - 1)(x - x_2^2)(x - x_3^2).$$

The curve $\mathcal{E}$ has Legendre form $y^2 = x(x - 1)(x - \Lambda)$, where

$$\Lambda = \frac{x_2^2 - x_3^2}{1 - x_3^2} = \frac{\mu}{\left(\nu \pm \sqrt{\nu(\nu - \lambda)}\right)^2}.$$

Computing the minimal polynomial of Λ proves the theorem. The conditions on λ, μ, ν show that none of the denominators vanishes, and that $\mathcal{E}$ is not singular. □

Corollary 5 *Let $\mathcal{C}$ be a curve whose moduli belong to $\mathcal{U}$, and (λ, μ, ν) defined as above. The j-invariants of the quotients of degree 2 of the Jacobian of $\mathcal{C}$ are the solutions of the equation*

$$j^2 + c_1(\lambda, \nu)j + c_0(\lambda, \nu) = 0, \tag{2}$$

where (c_0, c_1) are rational functions.

Proof. The j-invariant of an elliptic curve under Legendre form is given by the relation

$$\Lambda^2(\Lambda - 1)^2 j - 2^8(\Lambda^2 - \Lambda + 1)^3 = 0. \tag{3}$$

The previous theorem yields 2 elliptic curves that are quotients of the Jacobian of $\mathcal{C}$, and on the open set $\mathcal{U}$, they are the only ones. The polynomial equation giving j is obtained as the resultant of equations 3 and 1, using the relation $\mu = \nu\frac{1-\lambda}{1-\nu}$. □

We do not print the values of $c_0(\lambda, \nu)$ and $c_1(\lambda, \nu)$ for lack of space. Since the moduli (j_1, j_2, j_3) can be written in terms of λ and ν, an elimination procedure could give the coefficients c_0 and c_1 in terms of the moduli. Our approach is less direct, but yields to lighter computations.

2.2 The group acting on Rosenhain forms

In this section, we introduce two invariants that characterize the isomorphism classes of (2,2)-reducible curves.

Theorem 6 *Let $\mathcal{C}$ be a curve of genus 2 whose moduli belong to $\mathcal{H}_2$. There are 24 triples $(\lambda, \mu = \nu\frac{1-\lambda}{1-\nu}, \nu)$ for which the curve of equation $y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$ is isomorphic to $\mathcal{C}$. The unique subgroup of order 24 of $PGL(2,5)$ acts transitively on the set of these triples.*

Proof. Theorem 4 yields a triple $(\lambda_1, \mu_1, \nu_1)$ that satisfies the condition, so from now on, we consider that $\mathcal{C}$ is the corresponding curve. Every curve isomorphic to $\mathcal{C}$ is given by a birational transformation

$$x \mapsto \frac{ax + b}{cx + d}.$$

Since this curve must be under Rosenhain form, the transformation must map 3 of the 6 Weierstraß points $(0, 1, \infty, \lambda_1, \mu_1, \nu_1)$ on the points $(0, 1, \infty)$. The corresponding homographic transformations form a group of order $6.5.4 = 120$, and an exhaustive search shows that only 24 of them satisfy the relation on the new values (λ, μ, ν),

$$\mu = \nu\frac{1 - \lambda}{1 - \nu}.$$

Let us denote by $(\lambda_i, \mu_i, \nu_i)_{i=1,\dots,24}$ the corresponding triples. The exhaustive study shows that the curve of Rosenhain form $\{0, 1, \infty, \lambda_i, \mu_i, \nu_i\}$ is sent to the curve of Rosenhain form $\{0, 1, \infty, \lambda_j, \mu_j, \nu_j\}$ by successive applications on these 6 points of the maps $\sigma_1(x) = 1/x$, $\sigma_2(x) = 1 - x$, $\sigma_3(x) = \frac{x-\lambda}{1-\lambda}$, $\sigma_4(x) = x/\mu$. These maps generate a

group isomorphic to the unique subgroup of order 24 of $PGL(2,5)$, and the action of this group on the triples (λ,μ,ν) is given by the following table.

map	σ_1	σ_2	σ_3	σ_4
λ	$\frac{1}{\nu}$	$1-\mu$	$\frac{\lambda}{\lambda-1}$	$\frac{\lambda}{\mu}$
μ	$\frac{1}{\mu}$	$1-\lambda$	$\frac{\mu-\lambda}{1-\lambda}$	$\frac{1}{\mu}$
ν	$\frac{1}{\lambda}$	$1-\nu$	$\frac{\nu-\lambda}{1-\lambda}$	$\frac{\nu}{\mu}$

□

The 24 triples (λ_i,μ_i,ν_i) are explicitely given in appendix 5.3. The symmetric functions in these triples are invariants of the isomorphism class of $\mathcal{C}$. We will now define two specific invariants that *characterize* these classes.

Definition 7 *Let $\mathcal{C}$ be a curve of genus 2 whose moduli belong to $\mathcal{H}_2$, and let $\{(\lambda_i,\mu_i,\nu_i)\}$ be the set of triples defined above. We denote by Ω and Υ the following functions:*

$$\begin{aligned}\Omega &= \textstyle\sum_{i=1}^{24}\nu_i^2,\\ \Upsilon &= \textstyle\sum_{i=1}^{24}\lambda_i\nu_i.\end{aligned}$$

The following proposition shows that Ω and Υ characterize the isomorphism classes of such curves. It is straightforward to check all the following formulae, since (j_1,j_2,j_3), (c_0,c_1) and (Ω,Υ) can be written in terms of (λ,ν).

Proposition 8 *Let $\mathcal{C}$ be a curve of genus 2 whose moduli belong to $\mathcal{H}_2$, and (Ω,Υ) defined as above. If all terms are defined, then the following holds:*

$$\begin{aligned}j_1 &= \frac{36(\Omega-2)\Upsilon^2}{(\Omega-8)(2\Upsilon-3\Omega)^2},\\ j_2 &= -\frac{216\Upsilon^2(\Omega\Upsilon+\Upsilon-27\Omega)}{(\Omega-8)(2\Upsilon-3\Omega)^3},\\ j_3 &= -\frac{243\Omega\Upsilon^4}{64(\Omega-8)^2(2\Upsilon-3\Omega)^5}.\end{aligned}$$

The previous system can be solved for (j_1,j_2,j_3) only if the point (j_1,j_2,j_3) belongs to $\mathcal{H}_2$. In this case, Ω and Υ are given by the following proposition.

Proposition 9 *Let $\mathcal{C}$ be a curve of genus 2 whose moduli belong to $\mathcal{H}_2$, and (Ω,Υ) defined as above. If all terms are defined, then the following holds:*

$$\begin{aligned}\Omega &= (349360128j_1j_3 - 29859840j_3j_2 + 1911029760000j_3^2 + 972j_1^2j_2 - 110730240j_1^2j_3\\ &\quad - 45j_1j_2^2 - 12441600j_1j_3j_2 + 6j_2^3 + 45j_1^4 - 330j_1^3j_2 - 56j_1^2j_2^2 - 16j_1^5)\,/\\ &\quad (-26873856j_1j_3 - 14929920j_3j_2 + 955514880000j_3^2 + 3732480j_1^2j_3 - 9j_1j_2^2\\ &\quad + 4147200j_1j_3j_2 + 3j_2^3 + 9j_1^4 - 3j_1^3j_2 + 2j_1^2j_2^2 - 2j_1^5),\\ \Upsilon &= 3/4(162j_1^4 - 483729408j_1j_3 + 17199267840000j_3^2 + 67184640j_1^2j_3 - 36j_1^5\\ &\quad - 134369280j_3j_2 + 162j_1j_2^2 + 45j_2^3 + 35251200j_1j_3j_2 - 45j_1^3j_2 - 72j_1^2j_2^2\\ &\quad - 6912000j_3j_2^2 - 20j_1j_2^3 - 4j_1^4j_2)(349360128j_1j_3 - 29859840j_3j_2\\ &\quad + 1911029760000j_3^2 + 972j_1^2j_2 - 110730240j_1^2j_3 - 45j_1j_2^2 - 12441600j_1j_3j_2\\ &\quad + 6j_2^3 + 45j_1^4 - 330j_1^3j_2 - 56j_1^2j_2^2 - 16j_1^5)\,/\\ &\quad ((27j_1^4 + 161243136j_1j_3 + 1433272320000j_3^2 - 53498880j_1^2j_3 - 9j_1^5\\ &\quad + 44789760j_3j_2 + 486j_1^2j_2 + 135j_1j_2^2 - 23846400j_1j_3j_2 - 162j_1^3j_2 - 81j_1^2j_2^2\\ &\quad - 3456000j_3j_2^2 - 10j_1j_2^3 - 2j_1^4j_2)(-26873856j_1j_3 - 14929920j_3j_2\\ &\quad + 955514880000j_3^2 + 3732480j_1^2j_3 - 9j_1j_2^2 + 4147200j_1j_3j_2 + 3j_2^3 + 9j_1^4\\ &\quad - 3j_1^3j_2 + 2j_1^2j_2^2 - 2j_1^5)).\end{aligned}$$

Remark The invariants (Ω, Υ) are rational functions defined on the variety $\mathcal{H}_2$. Consequently, there may exist simpler formulae to express them.

We now give the coefficients of the minimal polynomial of the j-invariant in terms of Ω and Υ.

Proposition 10 *Let $\mathcal{C}$ be a curve of genus 2 whose moduli belong to the open set $\mathcal{U}$. The j-invariants of the elliptic quotients of degree 2 of its Jacobian are the solutions of the equation $j^2 + c_1 j + c_0$, where c_0 and c_1 are given below.*

$$\begin{aligned} c_0 &= \frac{4096\Upsilon^2(\Omega-32)^3}{\Omega^2(\Omega-8)}, \\ c_1 &= -\frac{128\Upsilon(\Omega^2-4\Omega\Upsilon+56\Omega-512)}{\Omega(\Omega-8)}. \end{aligned}$$

The two previous propositions lead to an expression of the form

$$j^2 + c_1(j_1, j_2, j_3)j + c_0(j_1, j_2, j_3) = 0,$$

where $c_1(j_1, j_2, j_3)$ and $c_0(j_1, j_2, j_3)$ are rational functions in (j_1, j_2, j_3). The denominators in these functions vanish on the two curves $\mathcal{D}$ and $\mathcal{V}$, and two additional curves. This last degeneracy is an artifact due to our choice of denominators; it is treated in appendix 5.3.

Computational considerations. To derive the previous formulae, the first step is to obtain each of the functions $(c_0, c_1, j_1, j_2, j_3)$ in terms of Ω and Υ. Let us consider the case of, say, j_1. The indeterminates $(\lambda, \nu, j_1, \Omega, \Upsilon)$ are related by the system

$$\left\{ \begin{array}{rcl} \Omega &=& \Omega(\lambda, \nu), \\ \Upsilon &=& \Upsilon(\lambda, \nu), \\ j_1 &=& j_1(\lambda, \nu), \end{array} \right.$$

where the right-hand side is a rational function. The relation between (Ω, Υ, j_1) is the equation of the image of the corresponding rational function. Determining this relation is often called *implicitization*.

A well-known approach to solve this question relies on a Gröbner basis computation. The system can be rewritten as a polynomial system F_{j_1} in $(\lambda, \nu, j_1, \Omega, \Upsilon)$. The relation we seek is the intersection of the ideal generated by F_{j_1} and the additional equation $1 - ZD(\lambda, \nu)$ with $\mathbb{Q}[j_1, \Omega, \Upsilon]$, where Z is a new indeterminate, and D the lcm of the denominators [2, chapter 3.3]. The intersection can be computed by a Gröbner basis for an eliminating order. In our case, such computations take several hours, using Magma on a DEC EV6 500 Mhz machine.

We followed another approach to treat this question. The system we consider defines a finite extension of the field $\mathbb{Q}(\Omega, \Upsilon)$, and the relation we seek is the minimal polynomial of j_1 in this extension. In [12], the second author proposes a probabilistic polynomial-time algorithm to compute this minimal polynomial; its Magma implantation solves the present question in a matter of minutes.

Finally, once j_1, j_2 and j_3 are obtained in terms of (Ω, Υ), we have to solve the system in Proposition 8 for (Ω, Υ). This system defines a finite extension of $\mathbb{Q}(j_1, j_2)$. Since Ω and Υ are know to be functions of (j_1, j_2, j_3), j_3 is a primitive element for this extension, and our question is reduced to compute Ω and Υ using this primitive element. The methods in [12] apply as well in this case, and give the formulae in Proposition 9.

3 The curve $\mathcal{D}$

We now turn to the first special case, the curve $\mathcal{D}$ defined in the preliminaries, and prove Theorem 1 in this case. The computations turn out to be quite simpler, mainly because this variety has dimension only one. Our formulation also leads to additional results concerning the endomorphism ring of the Jacobian in question.

Theorem 11 *Let $\mathcal{C}$ be a curve of genus 2 whose moduli belong to $\mathcal{D}$. There are two elliptic curves that are quotients of degree 2 of $Jac(\mathcal{C})$.*

Proof. As in the generic case, we start form a characterization of those curves due to Igusa [4].

Lemma 12 *Let $\mathcal{C}$ be a curve of genus 2. The reduced group of automorphisms of $\mathcal{C}$ is D_3 if and only if $\mathcal{C}$ is isomorphic to a curve of equation*

$$y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu), \text{ where } \mu = \frac{1}{1-\lambda}, \text{ and } \nu = 1 - \frac{1}{\lambda}, \qquad (4)$$

with λ different from 0, 1 and $(1 \pm \sqrt{3})/2$.

If $\mathcal{C}$ is under the form 4, its reduced group of automorphisms can be explicitely written. In the following table, u denotes $\pm\sqrt{\lambda^2 - \lambda + 1}$.

	map	order
Id	$(x,y) \mapsto (x,y)$	1
τ_1	$(x,y) \mapsto \left(\frac{\lambda-x}{(\lambda-1)x+1}, \frac{u^3 y}{((\lambda-1)x+1)^3}\right)$	2
τ_2	$(x,y) \mapsto \left(\frac{(\lambda-1)x+1}{\lambda x+1-\lambda}, \frac{u^3 y}{(\lambda x+1-\lambda)^3}\right)$	2
τ_3	$(x,y) \mapsto \left(\frac{\lambda x+1-\lambda}{x-\lambda}, \frac{u^3 y}{(x-\lambda)^3}\right)$	2
ρ_1	$(x,y) \mapsto \left(1-\frac{1}{x}, \frac{y}{x^3}\right)$	3
ρ_2	$(x,y) \mapsto \left(\frac{1}{1-x}, \frac{y}{(1-x)^3}\right)$	3

For each of the involutions τ_1, τ_2, τ_3, we repeat the construction done in the proof of theorem 4: we associate to each τ_i a pair of elliptic curves.

To this effect, we determine an isomorphism φ from $\mathcal{C}$ to a curve where τ_i becomes $(x,y) \mapsto (-x,y)$, and denote by $x_1 = 1$, x_2 and x_3 the values taken by φ at $\{0, 1, \infty\}$. The means that the curve $\mathcal{C}$ is isomorphic to the curve $y^2 = (x^2-1)(x^2-x_2^2)(x^2-x_3^2)$, and the elliptic curves we look for are $y^2 = (x-1)(x-x_2^2)(x-x_3^2)$, whose Legendre forms is $y^2 = x(x-1)(x-\Lambda)$, where $\Lambda = (x_2^2 - x_3^2)/(1-x_3^2)$. These computations are summarized in the following table.

involution	φ	x_2	x_3	Λ
τ_1	$x \mapsto \frac{(-1-u)x+\lambda}{(-1+u)x+\lambda}$	$\frac{-1-u+\lambda}{-1+u+\lambda}$	$\frac{u+1}{u-1}$	$\Lambda_1 = \lambda(\lambda-1-u)^2$
τ_2	$x \mapsto \frac{(\lambda-1-u)x+1}{(\lambda-1+u)x+1}$	$\frac{-1-u+\lambda}{-1+u+\lambda}$	$\frac{\lambda-u}{\lambda+u}$	$\Lambda_2 = \frac{1}{\lambda(\lambda-1+u)^2}$
τ_3	$x \mapsto \frac{x-\lambda+u}{x-\lambda-u}$	$\frac{-1-u+\lambda}{-1+u+\lambda}$	$\frac{\lambda-u}{\lambda+u}$	$\Lambda_3 = \frac{1}{\lambda(\lambda-1+u)^2}$

Let Λ_i' be the conjugate of Λ_i, obtained when u is replaced by $-u$. The elliptic curves corresponding to τ_i and $\tau_i\iota$ have Legendre parameters Λ_i and Λ_i', and we have $\Lambda_2 =$

$\Lambda_3 = 1/\Lambda_1'$, $\Lambda_2' = \Lambda_3' = 1/\Lambda_1$. Since changing Λ_i to its inverse $1/\Lambda_i$ leaves the j-invariant unchanged, there are only 2 isomorphism classes of elliptic quotients. □

We now give generators of the ideals defining the curves in $\mathcal{D}$, in terms of their moduli. We follow the Gröbner basis approach we already mentioned; Magma's Gröbner package takes about a minute to treat these simpler problems.

Equation 4 gives the moduli in terms of λ, and these relations can be expressed by a polynomial system $F_{\mathcal{D}}$ in $\mathbb{Q}[j_1, j_2, j_3, \lambda]$. The ideal defining the curve $\mathcal{D}$ is obtained as the intersection of the ideal generated by $F_{\mathcal{D}}$ and $1 - ZD(\lambda)$ with $\mathbb{Q}[j_1, j_2, j_3]$, where Z is a new indeterminate, and $D(\lambda)$ the lcm of the denominators of (j_1, j_2, j_3) expressed in terms of λ:

$$\begin{aligned} j_1 j_2^2 - 297 j_1 j_2 - 90 j_2^2 - 725760 j_1 j_3 + 172800 j_2 j_3 & \\ -2187 j_1 - 243 j_2 + 169641216 j_3 &= 0, \\ 7 j_2^3 - 57600 j_3 j_1 j_2 + 8991 j_1 j_2 + 2646 j_2^2 - 34774272 j_3 j_1 - 22394880 j_3 j_2 & \\ -9953280000 j_3^2 + 65610 j_1 + 7290 j_2 - 4901119488 j_3 &= 0, \\ -81 j_1 + 21 j_1^2 - 9 j_2 + 5 j_1 j_2 + 864000 j_3 &= 0. \end{aligned}$$

As in section 2, the previous proof yields the minimal polynomial of the Legenbre parameters Λ, and then of j-invariants in terms of λ, under the form $j^2 + c_1(\lambda) j + c_0(\lambda)$. Eliminating λ is a simple task, which gives the formulae:

$$\begin{aligned} c_1 &= \frac{3}{8} \frac{-85221 j_1 j_2 - 69228 j_1^2 - 6621 j_2^2 + 6054374400 j_3 j_1 + 692576000 j_3 j_2 - 5952061440 j_3}{j_3 (4705 j_2 + 21492 j_1 - 129816)}, \\ c_0 &= -81 \frac{2373 j_1^2 + 1412 j_1 j_2 + 210 j_2^2 + 33696000 j_3 j_1 + 4320000 j_3 j_2 - 246067200 j_3}{j_3 (5 j_2 + 27 j_1 - 108)}. \end{aligned}$$

The points were a denominator vanishes must be treated separately. This is done in appendix 5.3.

Finally, the previous results make the proof of the following corollaries quite easy.

Theorem 13 *Let $\mathcal{C}$ be curve of genus 2 whose moduli belong to $\mathcal{D}$. Its two elliptic quotients are 3-isogeneous.*

Proof. We use the same notation as in the previous proof. Let $\mathcal{E}_1$ be the elliptic curve associated to the involution τ_1, under the form $y^2 = x(x-1)(x-\Lambda_1)$. Its 3-division polynomial is

$$\psi_3(x) = 3x^4 + (-4\Lambda_1 - 4)x^3 + 6\Lambda_1 x^2 - \Lambda_1^2.$$

The following linear form divides $\psi_3(x)$:

$$S_3(x) = 3x + \lambda - 2(u+1),$$

and corresponds to a subgroup of $\mathcal{E}_1$ of order 3. Using Vélu's formulae [13], we can explicitely determine a curve 3-isogeneous to $\mathcal{E}_1$, of the form

$$y^2 = x^3 + a_2 x^2 + a_4 x + a_6,$$

where a_2, a_4, a_6 are defined by

$$\begin{aligned} x_0 &= (2(u+1)-\lambda)/3, \\ t &= 6x_0^2 - 4(\Lambda_1+1)x_0 + 2\Lambda_1, \\ u &= 4x_0^3 - 4(\Lambda_1+1)x_0^2 + 4\Lambda_1 x_0, \\ a_2 &= -(\Lambda_1+1), \\ a_4 &= \Lambda_1 - 5t, \\ a_6 &= 4(\Lambda_1+1)t - 7(u+x_0 t). \end{aligned}$$

It is a straightforward computation to check that the j-invariant of this curve is Λ_1'. □

Corollary 14 *Let $\mathcal{C}$ be curve of genus 2 whose moduli are on $\mathcal{D}$. The endomorphism ring of the Jacobian of $\mathcal{C}$ contains an order in the quaternion algebra $(\frac{3,1}{\mathbb{Q}})$. In particular, it admits a real multiplication by $\sqrt{3}$.*

Proof. The Jacobian of $\mathcal{C}$ is isogeneous to $\mathcal{E}_1 \times \mathcal{E}_2$, where $\mathcal{E}_1$ and $\mathcal{E}_2$ are 3-isogeneous elliptic curves. Let us denote by $\mathcal{I} : \mathcal{E}_1 \to \mathcal{E}_2$ a degree-3 isogeny, and $\hat{\mathcal{I}}$ its dual isogeny. Let $\mathcal{O}$ be the ring

$$\mathcal{O} = \left\{ \begin{pmatrix} a & \sqrt{3}b \\ \sqrt{3}c & d \end{pmatrix}, \text{ where } a,b,c,d \in \mathbb{Z} \right\}.$$

The map sending $\begin{pmatrix} a & \sqrt{3}b \\ \sqrt{3}c & d \end{pmatrix}$ to the endomorphism

$$\begin{aligned} \mathcal{E}_1 \times \mathcal{E}_2 &\to \mathcal{E}_1 \times \mathcal{E}_2 \\ (P,Q) &\mapsto ([a]P + [b]\hat{\mathcal{I}}Q, [c]\mathcal{I}P + [d]Q) \end{aligned}$$

is an injective ring homomorphism. Multiplication by $\sqrt{3}$ is for instance represented by the endomorphism $(P,Q) \mapsto (\hat{\mathcal{I}}Q, \mathcal{I}P)$. □

4 The curve $\mathcal{V}$

This is the second special case; as previously, the study is based on a result due to Igusa.

Theorem 15 *Let $\mathcal{C}$ be a curve of genus 2 whose moduli belong to $\mathcal{V}$. There exist two elliptic curves $\mathcal{E}_1$ and $\mathcal{E}_2$ such that $\mathcal{V}$ is (2,2)-isogeneous to $\mathcal{E}_1 \times \mathcal{E}_1$ and $\mathcal{E}_2 \times \mathcal{E}_2$. These elliptic curves are 2-isogeneous.*

Proof. The following result is taken from [4].

Lemma 16 *Let $\mathcal{C}$ be a curve of genus 2. The reduced groups of automorphisms of $\mathcal{C}$ is V_4 if and only if $\mathcal{C}$ is isomorphic to the curve of equation*

$$y^2 = x(x-1)(x+1)(x-\lambda)(x-1/\lambda), \tag{5}$$

where λ is different from 0, -1 and 1.

If $\mathcal{C}$ is under the form 5, its reduced automorphisms can be explicitely determined; in the following table, u denotes $\pm\sqrt{1-\lambda^2}$ and $\overline{u}$ denotes $\pm\sqrt{\lambda^2-1}$.

	map	order
Id	$(x,y) \mapsto (x,y)$	1
τ_1	$(x,y) \mapsto \left(\frac{x-\lambda}{\lambda x-1}, \frac{u^3 y}{(\lambda x-1)^3}\right)$	2
τ_2	$(x,y) \mapsto \left(\frac{\lambda x-1}{x-\lambda}, \frac{\overline{u}^3 y}{(x-\lambda)^3}\right)$	2
ρ	$(x,y) \mapsto \left(\frac{1}{x}, \frac{iy}{x^3}\right)$	4

We follow the same method as in the proof of theorem 11: for each τ_i, we make up an isomorphism φ from $\mathcal{C}$ to a curve where τ_i becomes $(x,y) \mapsto (-x,y)$. This curve is then isogeneous to the elliptic curve $y^2 = (x-1)(x-x_2^2)(x-x_3^2)$, whose Legendre forms are $y^2 = x(x-1)(x-\Lambda)$. This leads to the following table.

involution	φ	x_2	x_3	Λ	j
τ_1	$x \mapsto \frac{(1-u)x-\lambda}{(1+u)x-\lambda}$	$\frac{\lambda+u-1}{\lambda-u-1}$	$\frac{1-u}{1+u}$	$\Lambda_1 = \frac{\lambda^2(1-\lambda)}{(\lambda-1-u)^2}$	$J_1 = 64\frac{(4-l^2)^3}{l^4}$
τ_2	$x \mapsto \frac{(-\lambda-\bar{u})x+1}{(-\lambda+\bar{u})x+1}$	$\frac{\lambda+\bar{u}-1}{\lambda-\bar{u}-1}$	$\frac{\lambda+\bar{u}}{\lambda-\bar{u}}$	$\Lambda_2 = \frac{\lambda-1}{\lambda(\lambda-1-\bar{u})^2}$	$J_2 = 64\frac{(4l^2-1)^3}{l^2}$

The invariants J_1 and J_2 do not depend on u. This implies that the Jacobian of $\mathcal{C}$ is (2,2)-isogeneous to the products $\mathcal{E}_1 \times \mathcal{E}_1$ and $\mathcal{E}_2 \times \mathcal{E}_2$, and consequently, also to $\mathcal{E}_1 \times \mathcal{E}_2$.

Finally, the curves $\mathcal{E}_1$ and $\mathcal{E}_2$ are 2-isogeneous, since (J_1, J_2) cancels the modular equation of degree 2. □

Following the same method as in the previous section, we obtain an ideal defining the moduli of such curves:

$$\begin{aligned} 32j_1j_2^2 - 27j_1j_2 - 54j_2^2 + 4423680j_1j_3 + 14745600j_2j_3 - 13436928j_3 &= 0, \\ 64j_2^3 - 78643200j_1j_2j_3 + 243j_1j_2 - 378j_2^2 + 31850496j_1j_3 - 8847360j_2j_3 & \\ -36238786560000j_3^2 + 120932352j_3 &= 0, \\ 3j_1^2 - 10j_1j_2 + 18j_2 - 4608000j_3 &= 0. \end{aligned}$$

Their j-invariant are solution of the equation $j^2 + c_1 j + c_0$, where c_0 and c_1 are given by the following formulae, again obtained through a Gröbner basis computation for an eliminating order.

$$\begin{aligned} c_1 &= \frac{9}{4}\frac{3j_1j_2 - 2j_2^2 + 1866240j_3 + 211200j_3j_1 + 64000j_3j_2}{j_3(-243 + 78j_1 + 20j_2)}, \\ c_0 &= 108\frac{2560000j_3j_2 + 51j_1j_2 + 30j_2^2 + 768000j_3j_1 + 18662400j_3}{j_3(-243 + 78j_1 + 20j_2)}. \end{aligned}$$

5 Examples

In this section, we present examples, mostly taken from the literature, that show the use of our results.

5.1 The generic case

Let $\mathcal{C}$ be the curve defined over $\mathbb{Q}$ by the equation

$$y^2 = x^6 - x^5 + x^4 - x^2 - x - 1.$$

Its moduli are

$$j_1 = \frac{2^3 \times 3^2 \times 5 \times 13}{37^2},\ j_2 = -\frac{2^3 \times 3^3 \times 11 \times 13}{37^3},\ j_3 = \frac{3^5 \times 53^2}{2^8 \times 37^5}.$$

They belong to the open set $\mathcal{U} \subset \mathcal{H}_2$, so $\mathrm{Jac}(\mathcal{C})$ is isogeneous to a product of two elliptic curves. On this example, finding these curves through a Rosenhain form requires to work in an extension of $\mathbb{Q}$ of degree 24. Propositions 9 and 10 directly give:

$$c_0 = \frac{2^{14} \times 5^6 \times 37^3}{53^2},\ c_1 = \frac{2^8 \times 3^4 \times 47}{53},$$

and the j-invariants of the elliptic curves are defined on $\mathbb{Q}(i)$ by

$$j = -\frac{2^7 \times 3^4 \times 47}{53} \pm \frac{2^8 \times 7 \times 11 \times 181}{53} i.$$

Notice that 53 divides the discriminant of the curve, it is no surprise to see it appear in the denominator of j.

5.2 The curve $\mathcal{D}$

The following example is taken from [6], where Kulesz builds a curve admitting many rational points. Let $\mathcal{C}$ be the curve defined on $\mathbb{Q}$ by the equation

$$y^2 = 1412964(x^2 - x + 1)^3 - 8033507x^2(x - 1)^2.$$

Its moduli are

$$\begin{aligned}
j_1 &= \frac{3^2 \times 149 \times 167 \times 239^2 \times 3618470803 \times 33613^2}{757^2 \times 76832154757^2}, \\
j_2 &= -\frac{3^3 \times 239^2 \times 33613^2 \times 195593 \times 31422316507485410373257}{757^3 \times 76832154757^3}, \\
j_3 &= -\frac{2^{22} \times 3^17 \times 5^9 \times 7^6 \times 47^3 \times 89^3 \times 239^4 \times 33613^4}{757^5 \times 76832154757^5}.
\end{aligned}$$

We check that they belong to the curve $\mathcal{D}$, so the reduced group of automorphisms of $\mathcal{C}$ is D_3 — the construction of this curve in [6] already implies this result. Again, writing down a Rosenhain form for this curve requires to work in an algebraic extension of $\mathbb{Q}$. Our formulae readily give the j-invariants of the quotient elliptic curves:

$$-\frac{239 \times 33613 \times 84333563^3}{2^{24} \times 3^4 \times 5^9 \times 7^2 \times 47^3 \times 89}, \quad \text{and} \quad \frac{19^3 \times 67^3 \times 239 \times 349^3 \times 33613}{2^8 \times 3^{12} \times 5^3 \times 7^6 \times 47 \times 89^3}.$$

5.3 The curve $\mathcal{V}$

In the paper [9], Leprévost and Morain study the curve $\mathcal{C}_\theta$ defined on $\mathbb{Q}(\theta)$ by the equation

$$y^2 = x(x^4 - \theta x^2 + 1),$$

with the purpose to study sums of caracters. Its moduli are

$$j_1 = 144\frac{9\theta^2 - 20}{(3\theta^2+20)^2}, \quad j_2 = -3456\frac{27\theta^2 - 140}{(3\theta^2+20)^3}, \quad j_3 = 243\frac{\theta^2 - 4}{(3\theta^2+20)^5}.$$

We check that they belong to the curve $\mathcal{V}$, so the reduced group of automorphisms of $\mathcal{C}$ is V_4. This yields the j-invariants of the quotient elliptic curves:

$$j = 64\frac{(3\theta-10)^3}{(\theta-2)(\theta+2)^2} \quad \text{and} \quad j' = 64\frac{(3\theta+10)^3}{(\theta+2)(\theta-2)^2}.$$

Notice that the curves E_θ and E'_θ given in [9]

$$y^2 = x(x^2 \pm 4x + 2 - \theta),$$

have the same invariants j'. The other quotient curves, with invariant j, admit the equation

$$y^2 = x(x^2 \pm 4x + 2 + \theta).$$

Appendix: formulary

To complete the previous study, we give formulae describing the following cases:

- The reduced group of automorphisms $\mathcal{G}$ is neither D_3 nor V_4, nor $\mathbb{Z}/2\mathbb{Z}$: this is the case for the two points 2.(a) and 2.(b) below.
- A denominator vanishes. On the curve $\mathcal{D}$, this happens at a single point, treated in 2.(c); in the generic case, two curves must be studied in 2.(f) and 2.(g).
- The covariant A vanishes, so the moduli (j_1, j_2, j_3) are not adapted. We choose two other invariants, and go through the same exhaustive process.

All these formulae are gathered as an algorithm, taking as input a curve of genus 2, with (2,2)-reducible Jacobian, that outputs the minimal polynomial of the j-invariants of the elliptic quotients.

1. Compute the covariants A, B, C, D, R of $\mathcal{C}$ given in [4], and check that $R = 0$.
2. If $A \neq 0$: compute j_1, j_2, j_3.
   (a) If $(j_1, j_2, j_3) = (\frac{81}{20}, -\frac{729}{200}, \frac{729}{25600000})$, then the reduced group of automorphisms is D_6; return $j(j - 54000)$.
   (b) If $(j_1, j_2, j_3) = (-\frac{36}{5}, \frac{1512}{25}, \frac{243}{200000})$, then the reduced group of automorphisms is $\mathfrak{S}_4$; return $j - 8000$.
   (c) If $(j_1, j_2, j_3) = (\frac{24297228}{885481}, -\frac{81449284536}{833237621}, -\frac{57798021931029}{47220229240364864})$, then the reduced group of automorphisms is D_3; return

$$j^2 + \frac{471690263168}{658503}j - \frac{8094076887461888}{57289761}.$$

(d) If (j_1, j_2, j_3) cancel the polynomials defining $\mathcal{D}$, then the reduced group of automorphisms is D_3; return j as computed in section 3.

(e) If (j_1, j_2, j_3) cancel the polynomial defining $\mathcal{V}$, then the reduced group of automorphisms is V_4; return j as computed in section 4.

(f) If (j_1, j_2, j_3) satisfy

$$\begin{aligned} 331776j_3 - j_2^2 - 24j_1j_2 - 144j_1^2 &= 0, \\ 9j_1 + j_2 &= 0, \end{aligned}$$

then the reduced group of automorphisms is $\mathbb{Z}/2\mathbb{Z}$; return

$$j^2 + \frac{150994944j_3}{j_2 + 12j_1}j - \frac{260919263232j_3}{j_2 + 12j_1}.$$

(g) If (j_1, j_2, j_3) satisfy

$$\begin{aligned} j_2^5 + 54j_2^4 - 322486272j_2^2j_3 + 481469424205824j_3^2 &= 0, \\ 18j_1 + 5j_2 &= 0, \end{aligned}$$

then the reduced group of automorphisms is $\mathbb{Z}/2\mathbb{Z}$; return $j^2 + c_1j + c_0$, where

$$\begin{aligned} c_0 &= -\frac{125}{9559130112}\frac{(-j_2^2 - 24j_1j_2 - 144j_1^2 + 16257024j_3)^2}{j_3^2} \\ c_1 &= \frac{(-j_2^2 - 24j_1j_2 - 144j_1^2 + 16257024j_3)(2723051520j_3 - 289j_2^2 - 6936j_1j_2 - 41616j_1^2)}{2064772104192j_3^2}, \end{aligned}$$

(h) Else, we are in the generic case, and no denominator vanishes; return j as computed in section 2.

3. The case $A = 0$

(a) If $B = 0$ and $C^5 = 4050000D^3$, the reduced group of automorphisms is $\mathbb{Z}/2\mathbb{Z}$; return $(j - 4800)(j - 8640)$.

(b) If $C = 0$ and $B^5 = 3037500D^2$, the reduced group of automorphisms is $\mathbb{Z}/2\mathbb{Z}$; return $(j - 160)(j + 21600)$.

Compute the invariants

$$t_1 = \frac{3}{512}\frac{CD}{B^4} \quad \text{and} \quad t_2 = 1536\frac{BC}{D}.$$

(c) If $(t_1, t_2) = (1/576000, -460800)$, the reduced group of automorphisms is V_4; return $j^2 + 7200j + 13824000$.

(d) If $(t_1, t_2) = (-1/864000, -172800)$, the reduced group of automorphisms is D_3; return $j^2 + 55200j - 69984000$.

(e) The reduced group of automorphisms is $\mathbb{Z}/2\mathbb{Z}$. Compute

$$\Omega = -4\frac{-238878720000t_1 + 1555200t_2t_1 + 7t_2^2t_1 + 2t_2}{477757440000t_1 + 2073600t_2t_1 + t_2^2t_1 - t_2} \quad \text{and} \quad \Upsilon = \frac{3}{2}\Omega,$$

then c_0 and c_1 given in section 2; return $j^2 + c_1j + c_0$.

Appendix: the 24 triples

The following table gives the full list of the triples defined in theorem 6.

$\left(\lambda, \frac{\lambda\nu-\nu}{\nu-1}, \nu\right)$	$\left(\frac{-1}{\nu-1}, \frac{-\lambda+\nu}{\lambda\nu-\lambda-\nu+1}, \frac{-\lambda+\nu}{\lambda\nu-\lambda}\right)$	$\left(\frac{-\lambda\nu+2\nu-1}{\nu-1}, \frac{-\lambda+\nu}{\nu-1}, \frac{(-\lambda+\nu}{\lambda\nu-\lambda}\right)$
$\left(\frac{\lambda\nu-\lambda}{\lambda\nu-\nu}, \frac{\nu-1}{\lambda\nu-\nu}, \frac{\nu-1}{\lambda-1}\right)$	$\left(\lambda, \frac{-\lambda+\nu}{\nu-1}, \frac{\lambda-\nu}{\lambda\nu-2\nu+1}\right)$	$\left(\frac{-\lambda\nu+2\nu-1}{\nu-1}, -\lambda+1, -\nu+1\right)$
$\left(\frac{\lambda\nu-\lambda}{\lambda\nu-\nu}, \frac{\nu-1}{\nu}, \frac{\lambda\nu-\lambda-\nu+1}{\lambda\nu-2\nu+1}\right)$	$\left(\frac{\lambda}{\lambda-1}, \frac{-\lambda+\nu}{\lambda\nu-\lambda-\nu+1}, \frac{\lambda-\nu}{\lambda-1}\right)$	$\left(\frac{\lambda-1}{\nu-1}, \frac{\lambda\nu-\nu}{\nu-1}, \frac{\lambda\nu-\nu}{\lambda\nu-\lambda}\right)$
$\left(\frac{\lambda}{\lambda-1}, \frac{\nu}{\nu-1}, \frac{\lambda\nu-\nu}{\lambda\nu-2\nu+1}\right)$	$\left(\frac{\lambda-1}{\lambda-\nu}, \frac{\lambda\nu-\nu}{\lambda-\nu}, \frac{\lambda\nu-\nu}{\lambda\nu-2\nu+1}\right)$	$\left(\frac{\lambda\nu-2\nu+1}{\lambda\nu-\nu}, \frac{\nu-1}{\nu}, \frac{\lambda-1}{\lambda}\right)$
$\left(\frac{\lambda\nu-2\nu+1}{\lambda\nu-\lambda-\nu+1}, \frac{-1}{\lambda-1}, \frac{\nu-1}{\lambda-1}\right)$	$\left(\frac{1}{\nu}, \frac{\lambda-\nu}{\lambda\nu-\nu}, \frac{\lambda-\nu}{\lambda\nu-2\nu+1}\right)$	$\left(\frac{\lambda\nu-2\nu+1}{\lambda\nu-\lambda-\nu+1}, \frac{\nu}{\nu-1}, \frac{\lambda\nu-\nu}{\lambda\nu-\lambda}\right)$
$\left(\frac{-1}{\nu-1}, \frac{-1}{\lambda-1}, \frac{-\nu+1}{\lambda\nu-2\nu+1}\right)$	$\left(\frac{\lambda\nu-2\nu+1}{\lambda\nu-\nu}, \frac{\lambda-\nu}{\lambda\nu-\nu}, \frac{\lambda-\nu}{\lambda-1}\right)$	$\left(\frac{\lambda\nu-2\nu+1}{\lambda-\nu}, \frac{-\nu+1}{\lambda-\nu}, \frac{1}{\lambda}\right)$
$\left(\frac{\lambda-1}{\lambda-\nu}, \frac{-\lambda\nu+\lambda+\nu-1}{\lambda-\nu}, \frac{\lambda-1}{\lambda}\right)$	$\left(\frac{\lambda\nu-2\nu+1}{\lambda-\nu}, \frac{\lambda\nu-\nu}{\lambda-\nu}, \nu\right)$	$\left(\frac{1}{\nu}, \frac{\nu-1}{\lambda\nu-\nu}, \frac{1}{\lambda}\right)$
$\left(\frac{\lambda-1}{\nu-1}, -\lambda+1, \frac{\lambda\nu-\lambda-\nu+1}{\lambda\nu-2\nu+1}\right)$	$\left(\frac{-\lambda\nu+\lambda}{\lambda-\nu}, \frac{-\lambda\nu+\lambda+\nu-1}{\lambda-\nu}, -\nu+1\right)$	$\left(\frac{-\lambda\nu+\lambda}{\lambda-\nu}, \frac{-\nu+1}{\lambda-\nu}, \frac{-\nu+1}{\lambda\nu-2\nu+1}\right)$

References

[1] O. Bolza. On binary sextics with linear transformations onto themselves. *Amer. J. Math.*, 10:47–70, 1888.

[2] D. Cox, J. Little, .D. O'Shea Ideals, Varieties and Algorithms Springer-Verlag, 1992.

[3] E. Howe, F. Leprevost, and B. Poonen. Large torsion subgroups of split Jacobians of curves of genus 2 or three. *Forum Math.*, 12:315–364, 2000.

[4] J. Igusa. Arithmetic variety of moduli for genus 2. *Ann. of Math. (2)*, 72:612–649, 1960.

[5] J. Igusa. On Siegel modular forms of genus 2. *Amer. J. Math.*, 84:175–200, 1962.

[6] L. Kulesz. Courbes algébriques de genre 2 possédant de nombreux points rationnels. *C. R. Acad. Sci. Paris Sér. I Math.*, 321:91–94, 1995.

[7] L. Kulesz. Application de la méthode de Dem'janenko-Manin à certaines familles de courbes de genre 2 et 3. *J. Number Theory*, 76:130–146, 1999.

[8] H. Lange. Über die Modulvarietät der Kurven vom Geschlecht 2. *J. Reine Angew. Math.*, 281:80–96, 1976.

[9] F. Leprévost and F. Morain. Revêtements de courbes elliptiques à multiplication complexe par des courbes hyperelliptiques et sommes de caractères. *J. Number Theory*, 64:165–182, 1997.

[10] Magma. `http://www.maths.usyd.edu.au:8000/u/magma/`

[11] J.-F. Mestre. Construction de courbes de genre 2 à partir de leurs modules. In T. Mora and C. Traverso, editors, *Effective methods in algebraic geometry*, volume 94 of *Progr. Math.*, pages 313–334. Birkhäuser, 1991. Proc. Congress in Livorno, Italy, April 17–21, 1990.

[12] É. Schost Sur la résolution des systèmes polynomiaux à paramètres. PhD Thesis, École polytechnique, 2000.

[13] J. Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. I Math.*, 273:238–241, July 1971. Série A.