GENUS TWO CURVES WITH MANY ELLIPTIC SUBCOVERS.

TONY SHASKA

To my father on the occasion of his 80th birthday.

Abstract. We determine all genus 2 curves, defined over $\mathbb{C}$, which have simultaneously degree 2 and 3 elliptic subcovers. The locus of such curves has three irreducible 1-dimensional genus zero components in $\mathcal{M}_2$. For each component we find a rational parametrization and construct the equation of the corresponding genus 2 curve and its elliptic subcovers in terms of the parameterization. Such families of genus 2 curves are determined for the first time. Furthermore, we prove that there are only finitely many genus 2 curves (up to $\mathbb{C}$-isomorphism) defined over $\mathbb{Q}$, which have degree 2 and 3 elliptic subcovers also defined over $\mathbb{Q}$.

1. Introduction

If there is a degree d covering from a genus 2 curve C to an elliptic curve E then the space $\mathcal{L}_d$ of such genus 2 curves is an algebraic 2-dimensional locus in $\mathcal{M}_2$ when $d \cong 1 \mod 2$. Genus 2 curves with this property have been studied extensively in the XIX century. In the last decade of the XX century there was renewed interests on the topic coming from interests from number theory, cryptography, mathematical physics, solitons, differential equations, etc. These spaces for $d = 3, 5$ were explicitly computed by this author and his co-authors. For a more general setting and recent results on such spaces see [12] and [11].

Due to some of the interesting properties of such genus 2 curves they have found applications in cryptography, factoring of large numbers, etc. There is always an interest in having genus 2 curves defined over $\mathbb{Q}$ with many elliptic subcovers. In [6] such genus two curves were used for factorization of large numbers. Although the arithmetic of C is more complicated than on an elliptic curve, the author shows that this is balanced by the fact that each computation on C essentially corresponds to a pair of computations carried out on the two elliptic curves E_1 and E_2.

In this paper we give a family of genus 2 curves which have 4 elliptic subcovers such that two of them are of degree 2 and the other two of degree 3. We determine such elliptic subcovers and the corresponding covers explicitly. Let $\mathfrak{p} = [C]$ denote the isomorphism class of a genus 2 curve, over $\mathbb{C}$, such that $\mathfrak{p} \in \mathcal{L}_2 \cap \mathcal{L}_3$. We denote its degree 2 (resp. 3) elliptic subcovers by E_1, E_2 (resp. E_3, E_4). Their j-invariants

2010 *Mathematics Subject Classification.* 14H10, 14H37, 14H45, 14K12, 14Q05, 14H70, 14D20, 14D22.

Key words and phrases. genus two, decomposable Jacobians, elliptic subcovers.

are denoted by j_1, j_2, j_3, j_4 respectively.

$$\begin{tikzcd}
 & & & C \arrow[dlll] \arrow[dll] \arrow[dr] \arrow[drr] & & \\
E_1 \arrow[r, squiggly, dash] & E_2 & & & E_3 \arrow[r, squiggly, dash] & E_4
\end{tikzcd}$$

The locus $\mathcal{L}_2 \cap \mathcal{L}_3$ has three irreducible 1-dimensional components in $\mathcal{M}_2$. Each component is a genus 0 curve and can therefore be parametrized. Using these parametrizations we are able construct 3 rational families of genus 2 curves and determine their 4 elliptic subcovers. Our main result can be summarized as below:

Theorem 1 (Main Theorem). *a) The locus $\mathcal{L}_2 \cap \mathcal{L}_3$ of genus 2 curves which have four elliptic subcovers, two of which are degree 2 and two of degree 3, has three irreducible, 1-dimensional, genus zero components in $\mathcal{M}_2$.*

b) For all $t \in \mathbb{C} \setminus \{\Delta_t = 0\}$ there is a genus 2 curve C_t where the j-invariants j_1, j_2 (resp. j_3, j_4) of degree 2 (resp. degree 3) of elliptic subcovers are the roots of the quadratic $j^2 + c_1 j + c_0 = 0$ (resp. given below):

i) The equation of C_t is

$$\begin{aligned}
y^2 =& 2\,x^6 + \left(2\,t + 12 - 2\,t^3 + 9\,t^2\right) x^5 - (t+2)\left(t^2 - 2\,t - 14\right)\left(t^2+1\right) x^4 - \\
&\left(t^2+1\right)\left(2\,t^4 - 6\,t^3 - 31\,t^2 - 28\,t - 37\right) x^3 - \left(t^3 - 10\,t^2 - 23\,t - 28\right)\left(t^2+1\right)^2 x^2 \\
&+ 6\,\left(t+2\right)\left(t^2+1\right)^3 x + 2\,\left(t^2+1\right)^4,
\end{aligned}$$

where $\Delta_t = (t+2)(2t-11)(t^2+1)(t-1)$. The j-invariants of elliptic subcovers are as follows,

$$\begin{aligned}
c_0 &= \frac{1}{16}\,\frac{\left(t^2 - 6\,t + 4\right)\left(t^2 + 114\,t + 124\right)\left(2\,t - 11\right)^2}{\left(t^2+1\right)^4} \\
c_1 &= \frac{-128}{\left(2\,t-11\right)^5} \cdot \left(8\,t^{10} - 320\,t^9 + 5580\,t^8 - 55460\,t^7 + 344593\,t^6 - 1379982\,t^5\right. \\
&\quad \left. + 3562940\,t^4 - 4837160\,t^3 + 7580400\,t^2 + 180256\,t + 1421824\right)
\end{aligned}$$

$$j_3 = 64\,\frac{\left(t^2 + 114\,t + 124\right)^3}{\left(2\,t - 11\right)^5}, \qquad j_4 = 64\,\frac{\left(t^2 - 6\,t + 4\right)^3}{2\,t - 11}$$

ii) The equation of C_t is

$$\begin{aligned}
y^2 =& \left(2916\,x^3 t - 2916\,x^3 - 486\,x^2 t^2 + 1944\,x^2 t - 54\,xt^4 + 216\,xt^3 - 162\,xt^2 + t^7\right. \\
&\left. -7\,t^6 + 15\,t^5 - 9\,t^4\right)\left(11664\,x^3 + 2916\,x^2 - 108\,xt^3 + 324\,xt^2 + t^6 - 6\,t^5 + 9\,t^4\right)
\end{aligned}$$

where $\Delta_t = t(t-1)(t^2-2t-2)(t-3)$. The j-invariants of elliptic subcovers are as follows,

$$\begin{aligned}
c_0 &= -\frac{1}{16}\,\frac{\left(-225 + 540\,t - 396\,t^2 + 80\,t^3\right)\left(t-3\right)^6}{t^8\left(t-1\right)^2} \\
c_1 &= \frac{384}{\left(t-1\right)\left(t-3\right)^9} \cdot \left(-820125 + 4045950\,t + 3221840\,t^8 - 5562270\,t^2 - 33869934\,t^5\right. \\
&\quad \left. + 24265899\,t^4 - 4786128\,t^3 + 25696944\,t^6 - 11732952\,t^7 - 491200\,t^9 + 32000\,t^{10}\right)
\end{aligned}$$

This family has isomorphic degree 3 elliptic subcover with j-invariants

$$j_3 = j_4 = -1728 \, \frac{(2\,t-5)^3}{(t-1)^3\,(t-3)^3}$$

iii) The equation of C_t is

$$y^2 = \left(4\,\frac{\left(2\,t^2+7\,t+2\right)^6 x^3}{t^2\,(2+3\,t+2\,t^2)^4} + \frac{\left(2\,t^2+7\,t+2\right)^6 x^2}{t^2\,(2+3\,t+2\,t^2)^4} + 2\,\frac{\left(2\,t^2+7\,t+2\right)^3 x}{t\,(2+3\,t+2\,t^2)^2} + 1\right)$$
$$\left(\frac{\left(2\,t^2+7\,t+2\right)^6 x^3}{t^2\,(2+3\,t+2\,t^2)^4} - \frac{\left(2\,t^2+7\,t+2\right)^4\left(2\,t^4+t^3-5\,t^2-2\,t-1\right)x^2}{t^2\,(2+3\,t+2\,t^2)^3} + \frac{\left(2\,t^2+7\,t+2\right)^3 x}{t\,(2+3\,t+2\,t^2)^2} + 1\right)$$

where $\Delta_t = t(2t^2+7t+2)(t-2)(t+2)(2t-1)(t+1)(2+3t+2t^2)$. *The j-invariants of elliptic subcovers are as follows,*

$$c_0 = 1024\,\frac{(t+2)^6\,t^6\,\left(t^4+56\,t^2+16\right)\left(t^4-4\,t^2+16\right)}{(t-2)^2\,(2+3\,t+2\,t^2)^8}$$
$$c_1 = -\frac{4}{t^4\,(t-2)^4\,(t+2)^4}\cdot\left(4\,t^{16}-79\,t^{14}+1000\,t^{12}+3824\,t^{10}+207616\,t^8\right.$$
$$\left.+61184\,t^6+256000\,t^4-323584\,t^2+262144\right)$$

$$j_3 := 2\,\frac{\left(t^4+120\,t^3+536\,t^2+480\,t+16\right)^3}{t\,(t-2)^8\,(t+2)^2}, \qquad j_4 := 256\,\frac{\left(t^4-4\,t^2+1\right)^3}{t^2\,(t-2)\,(t+2)}$$

c) Every curve $[C] \in \mathcal{L}_2 \cap \mathcal{L}_3$ is isomorphic, over $\mathbb{C}$, to one of the curves in i), ii), or iii) for some value of $t \in \mathbb{C} \setminus \Delta_t$.

The rest of this paper will be proving this theorem. We will use the explicit equation of $\mathcal{L}_2$ and $\mathcal{L}_3$. The idea of this paper is based on the following result where the explicit equation of $\mathcal{L}_3$ is computed.

Theorem 2 (Shaska 2001)**.** *Let K be a genus 2 field and $e_3(K)$ the number of Aut (K/k)-classes of elliptic subfields of K of degree 3. Then;*

i) $e_3(K) = 0, 1, 2,$ or 4

ii) $e_3(K) \geq 1$ if and only if the classical invariants of K satisfy the irreducible equation $F(J_2, J_4, J_6, J_{10}) = 0$ displayed in Appendix A in [16].

The equation of the second part of the theorem is called the $\mathcal{L}_3$ equation throughout this paper. Its singularities were studied in [2]. The equation of $\mathcal{L}_2$ has been known in different forms since the XIX century. We will use the equation of $\mathcal{L}_2$ as in [17]

We use parametrizations of $\mathcal{L}_2$ by the $\mathfrak{s}$-invariants which were introduced in [17] and have been used by many authors since. For computations in $\mathcal{L}_3$ we make use of the invariants among two cubics which were introduced in [16] and seem to have been unknown to classical invariant theorists. For a different approach of computing $\mathcal{L}_3$ see [12].

After determining the locus $\mathcal{L}_2 \cap \mathcal{L}_3$ in terms of absolute invariants i_1, i_2, i_3 of genus 2 curves we parametrize each component of this locus. The constructing the genus 2 curves starting from the moduli point in these loci makes use of the Prop. 1 where the equation of the curve is given in terms of the $\mathfrak{s}_1$, $\mathfrak{s}_2$ invariants as in (14). Such equations, known to the author since 2003, are being published for the first time. For a method of how to determine a minimal equation of hyperelliptic curves over its field of definition check [3, 5]. For related topics on the arithmetic of genus 2 curves check [8–10].

2. Preliminaries on genus 2 curves with split Jacobians

Curves with split Jacobians have been studied extensively before by many authors. In this section we briefly set some of the notation and describe some results that we will need in the next section.

2.1. The space $\mathcal{L}_2$.

All our computations in this paper are based on the $\mathfrak{s}$-invariants of genus 2 curves with extra involutions. Hence we will define them here and describe some basic results.

Let C be a genus 2 curve and z_1 is an elliptic involution of C. Denote by $\Gamma = PGL(2, \mathbb{C})$. Let $z_2 = z_1 z_0$, where z_0 is the hyperelliptic involution. Let E_i be the fixed field of z_i for $i = 1, 2$.

We need to determine to what extent the normalization in the above proof determines the coordinate X. The condition $z_1(X) = -X$ determines the coordinate X up to a coordinate change by some $\gamma \in \Gamma$ centralizing z_1. Such γ satisfies $\gamma(X) = mX$ or $\gamma(X) = \frac{m}{X}$, $m \in k \setminus \{0\}$. Hence we can assume that the Weierstrass points are $\{\pm\alpha_1, \pm\alpha_2, \pm\alpha_3\}$. If we denote the symmetric polynomials of $\alpha_1^2, \alpha_2^2, \alpha_3^2$ by a, b, c then C has equation $Y^2 = X^6 - aX^4 + bX^4 - c$. The additional condition $abc = 1$ forces $1 = -\gamma(\alpha_1) \dots \gamma(a_6)$, hence $m^6 = 1$. Then C is isomorphic to a curve with equation

$$Y^2 = X^6 - aX^4 + bX^2 - 1, \tag{1}$$

where $27 - 18ab - a^2b^2 + 4a^3 + 4b^3 \neq 0$.

So X is determined up to a coordinate change by the subgroup $H \cong D_6$ of Γ generated by $\tau_1 : X \to \varepsilon_6 X$, $\tau_2 : X \to \frac{1}{X}$, where ε_6 is a primitive 6-th root of unity. Let $\varepsilon_3 := \varepsilon_6^2$. The coordinate change by τ_1 replaces a by $\varepsilon_3 b$ and b by $\varepsilon_3^2 b$. The coordinate change by τ_2 switches a and b. Invariants of this action are:

$$\mathfrak{s}_1 := ab, \quad \mathfrak{s}_2 := a^3 + b^3$$

The mapping

$$A : (\mathfrak{s}_1, \mathfrak{s}_2) \to (i_1, i_2, i_3)$$

gives a birational parametrization of $\mathcal{L}_2$.

The ordered pair $\mathfrak{s}_1, \mathfrak{s}_2$ uniquely determines the isomorphism classes of curves in $\mathcal{L}_2$.

Lemma 1. *$k(\mathcal{L}_2) = k(\mathfrak{s}_1, \mathfrak{s}_2)$.*

The fibers of A of cardinality > 1 correspond to those curves C with $|\mathrm{Aut}\ (C)| > 4$. The rational expressions of $\mathfrak{s}_1, \mathfrak{s}_2$ can be found in [15]

2.2. Elliptic subcovers.

Let j_1 and j_2 denote the j-invariants of the elliptic curves E_1 and E_2. The invariants j_1 and j_2 and are roots of the quadratic

$$j^2 + 256 \frac{(2\mathfrak{s}_1^3 - 54\mathfrak{s}_1^2 + 9\mathfrak{s}_1\mathfrak{s}_2 - \mathfrak{s}_2^2 + 27\mathfrak{s}_2)}{(\mathfrak{s}_1^2 + 18\mathfrak{s}_1 - 4\mathfrak{s}_2 - 27)} j + 65536 \frac{(\mathfrak{s}_1^2 + 9\mathfrak{s}_1 - 3\mathfrak{s}_2)}{(\mathfrak{s}_1^2 + 18\mathfrak{s}_1 - 4\mathfrak{s}_2 - 27)^2} = 0, \tag{2}$$

see [17] for details.

Theorem 3. *Let $\mathfrak{p} = (\bar{\mathfrak{s}}_1, \bar{\mathfrak{s}}_2) \in \mathcal{L}_2$ there exists a genus 2 curve $C_{\bar{\mathfrak{s}}_1, \bar{\mathfrak{s}}_2}$ with equation*

$$Y^2 = a_0 X^6 + a_1 X^5 + a_2 X^4 + a_3\, X^3 + t\, a_2 X^2 + t^2 a_1\, X + t^3 a_0, \tag{3}$$

where the coefficients are given by

$$\begin{aligned}
t &= \bar{\mathfrak{s}}_2^2 - 4\bar{\mathfrak{s}}_1^3\\
a_0 &= \bar{\mathfrak{s}}_2^2 + \bar{\mathfrak{s}}_1^2\bar{\mathfrak{s}}_2 - 2\bar{\mathfrak{s}}_1^3\\
a_1 &= 2(\bar{\mathfrak{s}}_1^2 + 3\bar{\mathfrak{s}}_2)\cdot(\bar{\mathfrak{s}}_2^2 - 4\bar{\mathfrak{s}}_1^3)\\
a_2 &= (15\bar{\mathfrak{s}}_2^2 - \bar{\mathfrak{s}}_1^2\bar{\mathfrak{s}}_2 - 30\bar{\mathfrak{s}}_1^3)(\bar{\mathfrak{s}}_2^2 - 4\bar{\mathfrak{s}}_1^3)\\
a_3 &= 4(5\bar{\mathfrak{s}}_2 - \bar{\mathfrak{s}}_1^2)\cdot(\bar{\mathfrak{s}}_2^2 - 4\bar{\mathfrak{s}}_1^3)^2.
\end{aligned} \tag{4}$$

Proof. The proof can be computational. Computing the absolute invariants i_1, i_2, i_3 we have

$$\begin{aligned}
i_1 &= \frac{9}{4}\,\frac{\bar{\mathfrak{s}}_1^2 - 126\,\bar{\mathfrak{s}}_1 + 405 + 12\,\bar{\mathfrak{s}}_2}{(15 + \bar{\mathfrak{s}}_1)^2}\\
i_2 &= \frac{27}{8}\,\frac{729\,\bar{\mathfrak{s}}_1^2 + \bar{\mathfrak{s}}_1^3 + 4131\,\bar{\mathfrak{s}}_1 - 3645 - 1404\,\bar{\mathfrak{s}}_2 - 36\,\bar{\mathfrak{s}}_1\bar{\mathfrak{s}}_2}{(15 + \bar{\mathfrak{s}}_1)^3}\\
i_3 &= \frac{243}{8192}\,\frac{\left(-27 - 4\,\bar{\mathfrak{s}}_2 + 18\,\bar{\mathfrak{s}}_1 + \bar{\mathfrak{s}}_1^2\right)^2}{(15 + \bar{\mathfrak{s}}_1)^5}
\end{aligned}$$

Using the expressions of $\mathfrak{s}_1, \mathfrak{s}_2$ in [17] in terms of i_1, i_2, i_3 we get

$$(\mathfrak{s}_1, \mathfrak{s}_2) = (\bar{\mathfrak{s}}_1, \bar{\mathfrak{s}}_2).$$

This completes the proof.

□

That every genus 2 curve with automorphism group of order > 2 is defined over its field of moduli was proved before by Cardona/Quer and independently by this author in [15]. This expression of the curve in terms of the $\mathfrak{s}$-invariants is the first one and it is beneficial because it uses the rational parametrization of the surface $\mathcal{L}_2$.

We illustrate some of the ideas above with the following example.

Example 1. *Let C be a genus 2 curve with equation*

$$\begin{aligned}
y^2 = 3\,x^6 &+ \left(10\sqrt{3} - 8\right)x^5 + \left(63 - 16\sqrt{3}\right)x^4 + \left(60\sqrt{3} - 72\right)x^3\\
&+ \left(125 - 40\sqrt{3}\right)x^2 + \left(46\sqrt{3} - 36\right)x + 29
\end{aligned}$$

Below we display some of the information about this curve from the Maple package "genus 2" written by the author.

```
Info(C,x);


    "The moduli point for this curve is p=(i_1, i_2, i_3) "
                                 [31   -125    361   ]
           (i[1], i[2], i[3]) = [--, ----, -------]
                                 [12    8    3981312]
 "The Automorphism group is isomorphic to the group with GapId"
                              [4, 2]
```

```
                         "Sh-invariants are "
                        (s[1], s[2]) = [3, 28]
                      "The  field of moduli is:"
                                M = Q
                "The minimal field of definition is:"
                                F = Q
                   "The  degree of obstruction is:"
                            "[F : M]" = 1
  "Rational model is over its minimal field of definition is:"
         2         6           5             4              3
        y  = 491 x  + 62868 x  + 3615924 x  + 119727712 x

                                 2
           + 2444364624 x  + 28729167168 x + 151677646016

   "This curve has extra involutions.  Its degree 2 elliptic  subcovers

   have j-invariants"
                     23584461610752  6750000
                     --------------, -------
                         312481       3913
        "This curve has NO degree 3 elliptic subcovers"
```

The rational model refereed above is computed using the Eq. (14). *By an appropriate Möbius transformation one can show that it is isomorphic over* $\mathbb{C}$ *with the curve*

$$y^2 = 491\,x^6 + 2418\,x^5 + 5349\,x^4 + 6812\,x^3 + 5349\,x^2 + 2418\,x + 491$$

It can be checked that it has the same i_1, i_2, i_3 *invariants as the previous curve. In* [3] *we can show that we can do better and a more "minimal" equation.*

Hence, the equation provided in (14) is not necessary a "minimal" equation of the curve. For a "minimal" equation of genus 2 curves see [3].

2.3. **The space $\mathcal{L}_3$.** In [16] it was shown that every curve C in $\mathcal{L}_3$ can be written as

$$Y^2 = (X^3 + aX^2 + bX + 1)\,(4X^3 + b^2X^2 + 2bX + 1) \tag{5}$$

and the following

$$\mathfrak{u} = ab, \quad \mathfrak{v} = b^3 \tag{6}$$

are invariants of C under any change of coordinates.

The mapping $k^2 \setminus \{\Delta = 0\} \to \mathcal{L}_3$ such that

$$(\mathfrak{u}, \mathfrak{v}) \to (i_1, i_2, i_3)$$

has degree 2. Instead the invariants of two cubics as defined in [16]

$$\mathfrak{r}_1 = 27\frac{\mathfrak{v}(\mathfrak{v} - 9 - 2\mathfrak{u})^3}{4\mathfrak{v}^2 - 18\mathfrak{u}\mathfrak{v} + 27\mathfrak{v} - \mathfrak{u}^2\mathfrak{v} + 4\mathfrak{u}^3}$$

$$\mathfrak{r}_2 = -1296\frac{\mathfrak{v}(\mathfrak{v} - 9 - 2\mathfrak{u})^4}{(\mathfrak{v} - 27)(4\mathfrak{v}^2 - 18\mathfrak{u}\mathfrak{v} + 27\mathfrak{v} - \mathfrak{u}^2\mathfrak{v} + 4\mathfrak{u}^3)}$$

uniquely determine the isomorphism class of curves in $\mathcal{L}_3$. However, for the curves in $\mathcal{L}_3$ the field of moduli is not necessary a field of definition. One can show that the degree of the obstruction is ≤ 2 as proved below.

Theorem 4. *$k(\mathfrak{r}_1, \mathfrak{r}_2) = k(\mathcal{L}_3)$. Moreover, for every $\mathfrak{p} = (\mathfrak{r}_1, \mathfrak{r}_2) \in \mathcal{L}_3$ there is a genus two curve C with equation*

$$Y^2 = (\mathfrak{v}^2 X^3 + \mathfrak{u}\mathfrak{v} X^2 + \mathfrak{v} X + 1)\,(4\mathfrak{v}^2 X^3 + \mathfrak{v}^2 X^2 + 2\mathfrak{v} X + 1), \tag{7}$$

Proof. We compute absolute invariants i_1, i_2, i_3 in terms of $\mathfrak{u}, \mathfrak{v}$. Substituting them in the equation of $\mathcal{L}_3$ we check that they satisfy this equation.

□

We further discuss $\mathcal{L}_3$. We let

$$R := (27\mathfrak{v} + 4\mathfrak{v}^2 - \mathfrak{u}^2\mathfrak{v} + 4\mathfrak{u}^3 - 18\mathfrak{u}\mathfrak{v}) \neq 0.$$

For $4\mathfrak{u} - \mathfrak{v} - 9 \neq 0$ the degree 3 coverings are given by $\phi_1(X, Y) \to (U_1, V_1)$ and $\phi_2(X, Y) \to (U_2, V_2)$ where

$$\begin{aligned}
U_1 &= \frac{\mathfrak{v} X^2}{\mathfrak{v}^2 X^3 + \mathfrak{u}\mathfrak{v} X^2 + \mathfrak{v} X + 1}, \quad U_2 = \frac{(\mathfrak{v} X + 3)^2\ (\mathfrak{v}(4\mathfrak{u} - \mathfrak{v} - 9)X + 3\mathfrak{u} - \mathfrak{v})}{\mathfrak{v}\,(4\mathfrak{u} - \mathfrak{v} - 9)(4\mathfrak{v}^2 X^3 + \mathfrak{v}^2 X^2 + 2\mathfrak{v} X + 1)}, \\
V_1 &= Y\,\frac{\mathfrak{v}^2 X^3 - \mathfrak{v} X - 2}{\mathfrak{v}^2 X^3 + \mathfrak{u}\mathfrak{v} X^2 + \mathfrak{v} X + 1}, \\
V_2 &= (27 - \mathfrak{v})^{\frac{3}{2}}\, Y\, \frac{\mathfrak{v}^2(\mathfrak{v} - 4\mathfrak{u} + 8)X^3 + \mathfrak{v}(\mathfrak{v} - 4\mathfrak{u})X^2 - \mathfrak{v} X + 1}{(4\mathfrak{v}^2 X^3 + \mathfrak{v}^2 X^2 + 2\mathfrak{v} X + 1)^2}
\end{aligned} \tag{8}$$

and the elliptic curves have equations:

$$\begin{aligned}
\mathfrak{E}: \quad V_1^2 &= R\,U_1^3 - (12\mathfrak{u}^2 - 2\mathfrak{u}\mathfrak{v} - 18\mathfrak{v})U_1^2 + (12\mathfrak{u} - \mathfrak{v})U_1 - 4 \\
\mathfrak{E}': \quad V_2^2 &= c_3 U_2^3 + c_2 U_2^2 + c_1 U_2 + c_0
\end{aligned} \tag{9}$$

where

$$\begin{aligned}
c_0 &= -(9\mathfrak{u} - 2\mathfrak{v} - 27)^3 \\
c_1 &= (4\mathfrak{u} - \mathfrak{v} - 9)\,(729\mathfrak{u}^2 + 54\mathfrak{u}^2\mathfrak{v} - 972\mathfrak{u}\mathfrak{v} - 18\mathfrak{u}\mathfrak{v}^2 + 189\mathfrak{v}^2 + 729\mathfrak{v} + \mathfrak{v}^3) \\
c_2 &= -\mathfrak{v}\,(4\mathfrak{u} - \mathfrak{v} - 9)^2\,(54\mathfrak{u} + \mathfrak{u}\mathfrak{v} - 27\mathfrak{v}) \\
c_3 &= \mathfrak{v}^2\,(4\mathfrak{u} - \mathfrak{v} - 9)^3
\end{aligned} \tag{10}$$

The above facts can be deduced from Lemma 1 of [16]. The case $4\mathfrak{u} - \mathfrak{v} - 9 = 0$ is treated separately in [16].

There is an automorphism $\beta \in Gal_{k(\mathfrak{u},\mathfrak{v})/k(i_1,i_2,i_3)}$ given by

$$\begin{aligned}
\beta(\mathfrak{u}) &= \frac{(\mathfrak{v} - 3\mathfrak{u})(324\mathfrak{u}^2 + 15\mathfrak{u}^2\mathfrak{v} - 378\mathfrak{u}\mathfrak{v} - 4\mathfrak{u}\mathfrak{v}^2 + 243\mathfrak{v} + 72\mathfrak{v}^2)}{(\mathfrak{v} - 27)(4\mathfrak{u}^3 + 27\mathfrak{v} - 18\mathfrak{u}\mathfrak{v} - \mathfrak{u}^2\mathfrak{v} + 4\mathfrak{v}^2)} \\
\beta(\mathfrak{v}) &= -\frac{4(\mathfrak{v} - 3\mathfrak{u})^3}{4\mathfrak{u}^3 + 27\mathfrak{v} - 18\mathfrak{u}\mathfrak{v} - \mathfrak{u}^2\mathfrak{v} + 4\mathfrak{v}^2}
\end{aligned} \tag{11}$$

which permutes the j-invariants of $\mathfrak{E}$ and $\mathfrak{E}'$. These j invariants are given explicitly in terms of $\mathfrak{u}$ and $\mathfrak{v}$ as below:

$$\begin{aligned}
j_3 &= 16\,\frac{\mathfrak{v}\left(216\,\mathfrak{u}^2 + \mathfrak{v}\mathfrak{u}^2 - 126\,\mathfrak{u}\mathfrak{v} + 405\,\mathfrak{v} + 12\,\mathfrak{v}^2 - 972\,\mathfrak{u}\right)^3}{\left(4\,\mathfrak{u}^3 - \mathfrak{v}\mathfrak{u}^2 - 18\,\mathfrak{u}\mathfrak{v} + 4\,\mathfrak{v}^2 + 27\,\mathfrak{v}\right)^2(\mathfrak{v} - 27)^3} \\
j_4 &= -256\,\frac{\left(\mathfrak{u}^2 - 3\,\mathfrak{v}\right)^3}{\mathfrak{v}\,(4\,\mathfrak{u}^3 - \mathfrak{v}\mathfrak{u}^2 - 18\,\mathfrak{u}\mathfrak{v} + 4\,\mathfrak{v}^2 + 27\,\mathfrak{v})}
\end{aligned} \tag{12}$$

Remark 1. *There are exactly two genus 2 curves (up to isomorphism) with $e_3(K) = 4$, see 4.2 in* [16]. *The case $e_3(K) = 1$ (resp., 2) occurs for a 1-dimensional (resp., 2-dimensional) family of genus 2 curves.*

The theorem below shows that if we want to search for a family of curves with many elliptic subcovers we have to look at the curves with automorphism group V_4.

Theorem 5 (Shaska 2003)**.** *Let C be a genus two curve which has a degree 3 elliptic subcover. Then the automorphism group of C is one of the following: $\mathbb{Z}_2, V_4$, D_8, or D_{12}. Moreover, there are exactly six curves $C \in \mathcal{L}_3$ with automorphism group D_8 and six curves $C \in \mathcal{L}_3$ with automorphism group D_{12}.*

The list of all curves in $\mathcal{L}_3$ with automorphism group > 4 is given in [15], where their rational points are determined also.

2.4. **Constructing curves from their moduli points.** In our computations we will find the intersection $\mathcal{L}_2 \cap \mathcal{L}_3$ as a sublocus in $\mathcal{M}_2$. Hence, we need a constructive way to determine the equation of the curve once we know the moduli point. We summarize all the results in the following.

Proposition 1. *The following are true:*

i): *Let $j \in \mathbb{Q}$. Then there exists an elliptic curve $\mathfrak{E}$ defined over $\mathbb{Q}$ such that $j(\mathfrak{E}) = j$. Moreover the equation of $\mathfrak{E}$ is given by*

a) If $j \neq 0, 1728$ then Aut $(\mathfrak{E}) = \mathbb{Z}_2$ and

$$y^2 = x^3 - \frac{j}{48}(j-1728)^3 x - \frac{j}{864}(j-1728)^5$$

b) If $j = 0$ then Aut $(\mathfrak{E}) = \mathbb{Z}_2 \times \mathbb{Z}_3$ and $y^2 = x^3 - \frac{1}{4}$.
c) If $j = 1728$ then Aut $(\mathfrak{E}) = V_4$ and $y^2 = x^3 + x$.

ii): *The space $\mathcal{L}_2$ is parametrized by the $\mathfrak{s}$-invariants $(\mathfrak{s}_1, \mathfrak{s}_2)$, $k(\mathcal{L}_2) = k(\mathfrak{s}_1, \mathfrak{s}_2)$. Let $\mathfrak{p} \in \mathcal{M}_2$ such that $\mathfrak{p} = (i_1, i_2, i_3) \in \mathbb{Q}^3$ and Aut $(\mathfrak{p}) \cong V_4$. Then there exists a genus 2 curve C defined over $\mathbb{Q}$ such that $\mathfrak{p} = [C]$. Moreover, its equation is*

$$Y^2 = a_0 X^6 + a_1 X^5 + a_2 X^4 + a_3 X^3 + t\, a_2 X^2 + t^2 a_1 X + t^3 a_0 \tag{13}$$

where the coefficients are given by

$$\begin{aligned} t &= \mathfrak{s}_2^2 - 4\mathfrak{s}_1^3 \\ a_0 &= \mathfrak{s}_2^2 + \mathfrak{s}_1^2\mathfrak{s}_2 - 2\mathfrak{s}_1^3 \\ a_1 &= 2(\mathfrak{s}_1^2 + 3\mathfrak{s}_2) \cdot (\mathfrak{s}_2^2 - 4\mathfrak{s}_1^3) \\ a_2 &= (15\mathfrak{s}_2^2 - \mathfrak{s}_1^2\mathfrak{s}_2 - 30\mathfrak{s}_1^3)(\mathfrak{s}_2^2 - 4\mathfrak{s}_1^3) \\ a_3 &= 4(5\mathfrak{s}_2 - \mathfrak{s}_1^2) \cdot (\mathfrak{s}_2^2 - 4\mathfrak{s}_1^3)^2 \end{aligned} \tag{14}$$

and the expressions of $\mathfrak{s}_1$ and $\mathfrak{s}_2$ are given in terms of i_1, i_2, i_3 as in [15].

iii): *The space $\mathcal{L}_3$ is parametrized by the $\mathfrak{r}_1, \mathfrak{r}_2$-invariants as in [16], hence $k(\mathcal{L}_3) = k(\mathfrak{r}_1, \mathfrak{r}_1)$. Let $\mathfrak{p} \in \mathcal{L}_3$. Then there exists a genus 2 curve $C_{\mathbb{Q}}$ such that $p = [C]$ with equation*

$$Y^2 = (\mathfrak{v}^2 X^3 + \mathfrak{u}\mathfrak{v} X^2 + \mathfrak{v} X + 1)\,(4\mathfrak{v}^2 X^3 + \mathfrak{v}^2 X^2 + 2\mathfrak{v} X + 1). \tag{15}$$

Proof. The first part is elementary. The proof of the part ii) can be found on [17]. The equation of the curve C given in Eq.(13) can be verified by computing the absolute invariants of the curve and checking that they verify the equation of $\mathcal{L}_2$. Since these computations are straight forward we do not display them here. For a rational moduli point $\mathfrak{p} \in \mathcal{M}_2(\mathbb{Q})$, the curve C is defined over $\mathbb{Q}$ since $\mathfrak{s}_1$ and $\mathfrak{s}_2$ are given as rational functions in terms of i_1, i_2, i_3. A constructive proof of ii) and a discussion of a minimal polynomial of C is intended in [3].

The proof of the third part iii) can be found in [16].

□

Remark 2. *Invariants $(\mathfrak{s}_1, \mathfrak{s}_2)$ were also called u, v in [15]. We will call them $\mathfrak{s}$-invariants not to confuse them with $\mathfrak{u}, \mathfrak{v}$ for degree 3 covers.*

3. The locus $\mathcal{L}_2 \cap \mathcal{L}_3$.

In order to construct genus 2 curves which have degree 2 and degree 3 elliptic subcovers we need to determine the locus $\mathcal{L}_2 \cap \mathcal{L}_3$. This locus has three components in $\mathcal{M}_2$, say

$$G_1(i_1, i_2, i_3) \cdot G_2(i_1, i_2, i_3) \cdot G_3(i_1, i_2, i_3) = 0.$$

We will show computational that each one of these components has genus zero. Parametrizing such components we are able to express the absolute invariants i_1, i_2, i_3 in terms of two variables s and t for all points $\mathfrak{p} = (i_1, i_2, i_3) \in \mathcal{L}_2 \cap \mathcal{L}_3$.

Since for every point $\mathfrak{p} \in \mathcal{L}_2$ the field of moduli is a field of definition then there is a curve C with equations given as rational functions of s and t as in Prop. 1, part ii).

$$\begin{gathered} k^2 \setminus \{\Delta \neq 0\} \to \mathcal{L}_3 \cap \mathcal{L}_2 \to k^2 \setminus \{\Delta \neq 0\} \\ (\mathfrak{u}, \mathfrak{v}) \to (i_1, i_2, i_3) \to (\mathfrak{s}_1, \mathfrak{s}_2) \end{gathered}$$

The challenge here is to check the results of [16] in order to see which ones are valid for curves and covers over $\mathbb{Q}$. We know that for any rational point $\mathfrak{p} \in \mathcal{L}_2 \cap \mathcal{L}_3$ the field of moduli is a field of definition. In other words, there is a curve C defined over $\mathbb{Q}$.

3.1. (u, v)**–space.** As it can be seen from above, it is a challenge computationally to lift from the point of moduli to the equation of the curve. Instead we start with the curve given at Eq. (15). Such curves are in $\mathcal{L}_2$ if and only if $\mathfrak{u}$ and $\mathfrak{v}$ satisfy the following

(16)

$$
\begin{aligned}
&(-18\,\mathfrak{u}\,\mathfrak{v}^2 + \mathfrak{v}^2\,\mathfrak{u}^2 + 85\,\mathfrak{v}^2 - 2160\,\mathfrak{v} + 468\,\mathfrak{u}\,\mathfrak{v} - 28\,\mathfrak{v}\,\mathfrak{u}^2 + 4\,\mathfrak{u}^3)\\
&(8\,\mathfrak{v}^3 + 27\,\mathfrak{v}^2 - 54\,\mathfrak{u}\,\mathfrak{v}^2 - \mathfrak{v}^2\,\mathfrak{u}^2 + 108\,\mathfrak{v}\,\mathfrak{u}^2 + 4\,\mathfrak{v}\,\mathfrak{u}^3 - 108\,\mathfrak{u}^3)\\
&(3459375\,\mathfrak{v}^3 - 11390625\,\mathfrak{v}^2 - 333187\,\mathfrak{v}^4 + 274410\,\mathfrak{u}\,\mathfrak{v}^3 - 1215000\,\mathfrak{u}\,\mathfrak{v}^2 - 324\,\mathfrak{v}^6\\
&+ 2092500\,\mathfrak{v}\,\mathfrak{u}^3 - 1503225\,\mathfrak{v}^2\,\mathfrak{u}^2 + 374040\,\mathfrak{v}\,\mathfrak{u}^4 - 781106\,\mathfrak{v}^2\,\mathfrak{u}^3 + 443087\,\mathfrak{v}^3\,\mathfrak{u}^2\\
&- 69300\,\mathfrak{u}\,\mathfrak{v}^4 + 11168\,\mathfrak{v}\,\mathfrak{u}^5 - 10864\,\mathfrak{v}^2\,\mathfrak{u}^4 + 24624\,\mathfrak{v}^3\,\mathfrak{u}^3 - 16535\,\mathfrak{u}^2\,\mathfrak{v}^4 + 2250\,\mathfrak{u}\,\mathfrak{v}^5\\
&+ 16929\,\mathfrak{v}^5 + 128\,\mathfrak{u}^6 + 81\,\mathfrak{v}^5\,\mathfrak{u}^2 + 54\,\mathfrak{v}^4\,\mathfrak{u}^3 - 16\,\mathfrak{v}^4\,\mathfrak{u}^4 + 320\,\mathfrak{v}^3\,\mathfrak{u}^4 + 32\,\mathfrak{v}^3\,\mathfrak{u}^5 - 1280\,\mathfrak{v}^2\,\mathfrak{u}^5) = 0
\end{aligned}
$$

We can easily check that each component has genus 0. Hence, we can parametrize each component. This parametrization will give the equation of the curve C and its degree 3 elliptic subcovers $\mathfrak{E}$ and $\mathfrak{E}'$. Computing such equations in each case will occupy the rest of this paper.

First we settle some notation. For a polynomial $F(x) = c_n x^n + \cdots + c_1 + c_0$ the **coefficient vector** we call the vector $(c_0, c_1, \dots c_n)^t$.

The parametrization methods used in some computational algebra packages as Maple, Mathematica etc might not produce the same results. Indeed, in the third component their parametrizations were extremely long and we were not able to compute the equation of the genus 2 curve with such parametrizations. All our computations can be confirmed by substituting these parametrizations in each locus and verifying that the equation is satisfied.

3.2. First component.

We start first with the component of the locus in Eq. (16), namely

$$-18\mathfrak{u}\mathfrak{v}^2 + \mathfrak{v}^2\mathfrak{u}^2 + 85\mathfrak{v}^2 - 2160\mathfrak{v} + 468\mathfrak{u}\mathfrak{v} - 28\mathfrak{v}\mathfrak{u}^2 + 4\mathfrak{u}^3 = 0.$$

This is a genus zero curve which has a parametrization as follows

$$\mathfrak{u} = -(t+2)(t-4), \qquad \mathfrak{v} = 2\,\frac{(t+2)^3}{(t^2+1)}$$

Substituting these invariants in the expressions for $\mathfrak{s}_1, \mathfrak{s}_2$ in [15] we get

$$
\begin{aligned}
\mathfrak{s}_1 &= \frac{\left(4\,t^2 - 12\,t - 5\right)\left(8\,t^2 + 72\,t - 13\right)}{\left(2\,t - 11\right)^2}\\
\mathfrak{s}_2 &= \frac{2}{\left(2\,t - 11\right)^4} \cdot \big(128\,t^8 - 2560\,t^7 + 19776\,t^6 - 61248\,t^5 + 153600\,t^4\\
&\quad +185856\,t^3 - 192040\,t^2 - 33448\,t - 8661\big)
\end{aligned}
$$

The elliptic subcovers of degree 2 are determined by Eq. (2). The j-invariants of degree 3 elliptic subcovers are obtained by replacing for $\mathfrak{u}$ and $\mathfrak{v}$ in Eq. (12).

$$j_3 = 64\,\frac{\left(t^2 + 114\,t + 124\right)^3}{\left(2\,t - 11\right)^5}, \quad j_4 = 64\,\frac{\left(t^2 - 6\,t + 4\right)^3}{2\,t - 11}$$

It is easy now to compute the equation of C, which has equation $Y^2 = F(X)$ where $F(X)$ has coefficient vector

$$\begin{bmatrix} 1 \\ 6\,\frac{(t+2)^3}{t^2+1} \\ 12\,\frac{(t+2)^6}{(t^2+1)^2} - 2\,\frac{(t+2)^4(t-4)}{t^2+1} \\ 20\,\frac{(t+2)^6}{(t^2+1)^2} + 8\,\frac{(t+2)^9}{(t^2+1)^3} - 8\,\frac{(t+2)^7(t-4)}{(t^2+1)^2} \\ 48\,\frac{(t+2)^9}{(t^2+1)^3} - 8\,\frac{(t+2)^{10}(t-4)}{(t^2+1)^3} \\ -32\,\frac{(t+2)^{10}(t-4)}{(t^2+1)^3} + 16\,\frac{(t+2)^{12}}{(t^2+1)^4} \\ 64\,\frac{(t+2)^{12}}{(t^2+1)^4} \end{bmatrix}$$

The coefficients of $F(X)$ are obtained by simply replacing s_1, s_2 in Eq. (14).

This completes the proof of the Main Theorem, part b), i).

3.3. Second component.

The second component

$$8\,\mathfrak{v}^3 + 27\,\mathfrak{v}^2 - 54\,\mathfrak{u}\,\mathfrak{v}^2 - \mathfrak{v}^2\,\mathfrak{u}^2 + 108\,\mathfrak{v}\,\mathfrak{u}^2 + 4\,\mathfrak{v}\,\mathfrak{u}^3 - 108\,\mathfrak{u}^3 = 0,$$

of Eq. (16) is a genus zero curve. We find a parametrization of this curve as follows

$$\mathfrak{u} = 9\,\frac{t-4}{t\,(t-3)\,(t-1)}, \qquad \mathfrak{v} = -54\,\frac{1}{t^2\,(t-3)}$$

Substituting these expressions into $\mathfrak{s}_1, \mathfrak{s}_2$ we get

$$\begin{aligned} \mathfrak{s}_1 &= -3\,\frac{-243 + 324\,t + 318\,t^2 - 540\,t^3 + 125\,t^4}{(t-3)^4} \\ \mathfrak{s}_2 &= \frac{6}{(t-3)^8}\big(59049 - 157464\,t + 8748\,t^2 + 320760\,t^3 - 305802\,t^4 \\ &\quad +7128\,t^5 + 114540\,t^6 - 54200\,t^7 + 7625\,t^8\big) \end{aligned}$$

The elliptic subcovers of degree 2 are determined by Eq. (2). The j-invariants of degree 3 elliptic subcovers are obtained by replacing for $\mathfrak{u}$ and $\mathfrak{v}$ in Eq. (12). Then $\mathfrak{E}$ and $\mathfrak{E}'$ are isomorphic to each other and that is not very interesting to us, since we are looking for families with as many as possible elliptic subcovers. The j-invariant of such curves are

$$j_1 = j_2 = -1728\,\frac{(2\,t-5)^3}{(t-1)^3\,(t-3)^3}$$

The genus 2 curve has equation

$$\begin{aligned} y^2 = {}&(2916\,tx^3 - 2916\,x^3 - 486\,t^2x^2 + 1944\,tx^2 - 54\,t^4x + 216\,t^3x - 162\,t^2x \\ &+ t^7 - 7\,t^6 + 15\,t^5 - 9\,t^4)\,(11664\,x^3 + 2916\,x^2 - 108\,t^3x + 324\,t^2x + t^6 \\ &- 6\,t^5 + 9\,t^4) \end{aligned}$$

This completes the proof of the Main Theorem, part b), ii).

3.4. **Third component.** Next we consider the third component of the locus in Eq. (16). We get a parametrization

$$\begin{aligned}
\mathfrak{u} &= -\frac{\left(2\,t^2+7\,t+2\right)\left(2\,t^4+t^3-5\,t^2-2\,t-1\right)}{t\,(2+3\,t+2\,t^2)} \\
\mathfrak{v} &= \frac{\left(2\,t^2+7\,t+2\right)^3}{t\,(2+3\,t+2\,t^2)^2}
\end{aligned}$$

which can be verified by substituting these expressions for $\mathfrak{u}$ and $\mathfrak{v}$ in the corresponding locus.

Then $\mathfrak{s}_1, \mathfrak{s}_2$ in terms of the parameter t are as follows

$$\begin{aligned}
\mathfrak{s}_1 &= \frac{\left(t^4+3\,t^3+2\,t^2+6\,t+4\right)\left(4\,t^4+9\,t^3+26\,t^2+12\,t-8\right)}{t^3\,(t-2)\,(t+2)^3} \\
\mathfrak{s}_2 &= \frac{1}{4\,t^5\,(t-2)^2\,(t+2)^5}\cdot(16\,t^{14}+208\,t^{13}+896\,t^{12}+2940\,t^{11}+7785\,t^{10} \\
&\quad +16926\,t^9+22832\,t^8+18272\,t^7-4640\,t^6-42816\,t^5-50688\,t^4-35328\,t^3 \\
&\quad -30464\,t^2-18944\,t-4096)
\end{aligned}$$

The j-invariants of the degree 3 elliptic subcovers are

$$\begin{aligned}
\mathfrak{E}: \quad & j_1 = 2\,\frac{\left(t^4+120\,t^3+536\,t^2+480\,t+16\right)^3}{t\,(t-2)^8\,(t+2)^2} \\
\mathfrak{E}': \quad & j_2 = 256\,\frac{\left(t^4-4\,t^2+1\right)^3}{t^2\,(t-2)\,(t+2)}
\end{aligned}$$

Now we can compute the equation of C via Eq. (14) and we get $Y^2 = F(X)$ where $F(X)$ has coefficient vector

$$\begin{bmatrix}
1 \\
3\,\frac{\left(2\,t^2+7\,t+2\right)^3}{t(2+3\,t+2\,t^2)^2} \\
3\,\frac{\left(2\,t^2+7\,t+2\right)^6}{t^2(2+3\,t+2\,t^2)^4}-\frac{\left(2\,t^2+7\,t+2\right)^4\left(2\,t^4+t^3-5\,t^2-2\,t-1\right)}{t^2(2+3\,t+2\,t^2)^3} \\
5\,\frac{\left(2\,t^2+7\,t+2\right)^6}{t^2(2+3\,t+2\,t^2)^4}+\frac{\left(2\,t^2+7\,t+2\right)^9}{t^3(2+3\,t+2\,t^2)^6}-2\,\frac{\left(2\,t^2+7\,t+2\right)^7\left(2\,t^4+t^3-5\,t^2-2\,t-1\right)}{t^3(2+3\,t+2\,t^2)^5} \\
6\,\frac{\left(2\,t^2+7\,t+2\right)^9}{t^3(2+3\,t+2\,t^2)^6}-\frac{\left(2\,t^2+7\,t+2\right)^{10}\left(2\,t^4+t^3-5\,t^2-2\,t-1\right)}{t^4(2+3\,t+2\,t^2)^7} \\
-4\,\frac{\left(2\,t^2+7\,t+2\right)^{10}\left(2\,t^4+t^3-5\,t^2-2\,t-1\right)}{t^4(2+3\,t+2\,t^2)^7}+\frac{\left(2\,t^2+7\,t+2\right)^{12}}{t^4(2+3\,t+2\,t^2)^8} \\
4\,\frac{\left(2\,t^2+7\,t+2\right)^{12}}{t^4(2+3\,t+2\,t^2)^8}
\end{bmatrix}$$

The reader can easily verify that this equation of the genus 2 curve is the same with that claimed in the Main Theorem. This completes the proof of the Main Theorem, part b), i).

Proof of the Main theorem: Combining computations for each component we have the results of Thm. 1.

□

Given any genus 2 curve C over the complex numbers, we can check if it has degree 2 and degree 3 elliptic subcovers. Computationally this is possible from our **genus2** Maple package. Below we illustrate with an example.

Example 2. *Let C be a genus 2 curve with equation*

$$y^2 = 8\,x^6 + 187\,x^4 - 1355\,x^2 - 1088\,x^3 + 3993\,x - 3\,x^5 + 2730$$

In the ***genus2*** *package we enter only the polynomial $f(x)$, The output from the package is:*

```
Info( f, x);
                "Initial equation of the curve"
  2      6       4         2         3               5
 y  = 8 x  + 187 x  - 1355 x  - 1088 x  + 3993 x - 3 x  + 2730
"Igusa invariants are [J_2, J_4, J_6, J_10]"
[5435864, 11848141844056, -15448925968029277668, -954225510546747438407778509664]
"Clebcsh invariants are [A, B, C, D]"
[-679483  11104643929484  -1875304637846687089  3694376275475287252631213749681232]
[-------, --------------, --------------------, ----------------------------------]
[  15          5625              15625                       7119140625           ]

"The moduli point for this curve is p=(i_1, i_2, i_3) "
                      [4624326  -54010420569  -90812685325761]
 (i[1], i[2], i[3]) = [-------, ------------, ---------------]
                      [ 80089     45330374    929398866761216]
"The Automorphism group is isomorphic to the group with GapId"
                             [4, 2]
"Sh-invariants are "
                                [-688  -117101]
                 (s[1], s[2]) = [----, -------]
                                [ 27     972  ]
"The degree 2 j-invariants are roots of the quadratic"

"The  field of moduli is:"
                             M = Q
"The minimal field of definition is:"
                             F = Q
"The  degree of obstruction is:"
                         "[F : M]" = 1
"Rational model is over its minimal field of definition is:"

"A minimal rational model is over its minimal field of definition is:"
y^2 = -73190944927004215253422952448x^6+11105674732355827003234484748800x^5
+152821713034110852986785299725241600x^4-77928924518649965576021241379266720000x^3
+12331972128546830355070565201074691490000x^2
+723169150606597090269353486513192776125000x
-38459157573904353552637009599366812535828125
"with moduli point"
          [4624326  -54010420569  -90812685325761]
          [-------, ------------, ---------------]
          [ 80089     45330374    929398866761216]
"This curve has degree 3 elliptic subcovers."
```

The equation obtained above is obviously not the 'best' equation possible. Since the algorithms computes the corresponding moduli point, then it losses any information about the initial equation of the curve. How can the package get the best possible equation? This is studied in detail in [3, 4] for all algebraic curves. Notice that from methods of [3] we get that the above curve is isomorphic (over $\mathbb{C}$) to the curve

$$y^2 = 2x^6 + 15x^5 + 19x^4 + 19x^2 + 15x + 2$$

Such equation has minimal height in the sense of [4] and therefore it is the 'best' possible equation that we can get.

Remark 3. *Most of the tasks performed from the genus2 package can be generalized to higher genus curves using results in* [1] *and assuming that some equation of the curve is known. For a discussion of how to get equations of superelliptic curves see* [13, 14] *and for non-superelliptic curves see* [7].

Theorem 6. *There are only finitely many genus 2 curves (up to isomorphism) defined over $\mathbb{Q}$ such that they have degree 2 and degree 3 elliptic subcovers also defined over $\mathbb{Q}$.*

Proof. Given a genus two curve C in the locus $\mathcal{L}_2 \cap \mathcal{L}_3$, it is defined over $\mathbb{Q}$ is and only if the moduli point $\mathfrak{p} = (i_1, i_2, i_3)$ is a rational point.

Let $\mathfrak{p} = (i_1, i_2, i_3) \in \mathcal{L}_2 \cap \mathcal{L}_3$. Then, this $\mathfrak{p}$ is in one of the components from Thm. 1. Since the corresponding $\mathfrak{s}$-invariants are defined as rational functions in terms of i_1, i_2, i_3, then $\mathfrak{s}_1, \mathfrak{s}_2 \in \mathbb{Q}$. Moreover, C is defined over $\mathbb{Q}$ if and only if $\mathfrak{s}_1, \mathfrak{s}_2 \in \mathbb{Q}$.

The invariants j_1, j_2 are rational numbers if

$$\begin{aligned} g(\mathfrak{s}_1, \mathfrak{s}_2) := & -2916\, {s_1}^2 s_2 - 864\, {s_1}^3 s_2 + 486\, s_1 {s_2}^2 + 189\, {s_2}^2 {s_1}^2 + 2916\, {s_1}^4 - 216\, {s_1}^5 \\ & - 54\, {s_2}^3 + 729\, {s_2}^2 + 36\, {s_1}^4 s_2 - 4\, {s_1}^3 {s_2}^2 - 18\, s_1 {s_2}^3 + 4\, {s_1}^6 + {s_2}^4 - 4\, {s_1}^2 \\ & - 36\, s_1 + 12\, s_2 \end{aligned}$$

is a complete square in $\mathbb{Q}$, where $g(\mathfrak{s}_1, \mathfrak{s}_2)$ is the discriminant of the quadratic in 1. This expression is a complete square in $\mathbb{Q}$ if and only if the the curve

$$z^2 = g(\mathfrak{s}_1, \mathfrak{s}_2)$$

has rational points. The curve $z^2 = g(\mathfrak{s}_1, \mathfrak{s}_2)$ has genus 13, 13, 23 when $\mathfrak{p}$ is in the locus G_1, G_2, G_3 respectively. From Falting's theorem, it has only finitely many rational points. This completes the proof.

□

References

[1] L. Bedratyuk, *A note about invariants of algebraic curves*, Albanian J. Math. **6** (2012), no. 1, 3–8. MR2965665

[2] L. Beshaj, *Singular locus on the space of genus 2 curves with decomposable Jacobians*, Albanian J. Math. **4** (2010), no. 4, 147–160. MR2755393 (2012b:14054)

[3] ———, *Reduction of binary forms* (L. Beshaj, T. Shaska, and E. Zhupa, eds.), NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., IOS Press, Amsterdam, 2015.

[4] L. Beshaj and T. Shaska, *Heights on algebraic curves* (L. Beshaj, T. Shaska, and E. Zhupa, eds.), NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., IOS, Amsterdam, 2015.

[5] L. Beshaj and F. Thompson, *Equations for superelliptic curves over their minimal field of definition*, Albanian J. Math. **8** (2014), no. 1, 3–8. MR3253208

[6] R. Cosset, *Factorization with genus 2 curves*, Math. Comp. **79** (2010), no. 270, 1191–1208. MR2600562 (2011d:11289)

[7] A. Deopurkar, M. Fedorchuk, and D. Swinarski, *Gröbner techniques and ribbons,* Albanian J. Math. **8** (2014), no. 2, 55–70.

[8] Francesc Fité, Kiran S. Kedlaya, Víctor Rotger, and Andrew V. Sutherland, *Sato-Tate distributions and Galois endomorphism modules in genus 2*, Compos. Math. **148** (2012), no. 5, 1390–1442. MR2982436

[9] Kiran S. Kedlaya and Andrew V. Sutherland, *Computing L-series of hyperelliptic curves*, Algorithmic number theory, 2008, pp. 312–326. MR2467855 (2010d:11070)

[10] ______, *Hyperelliptic curves, L-polynomials, and random matrices*, Arithmetic, geometry, cryptography and coding theory, 2009, pp. 119–162. MR2555991 (2011d:11154)

[11] A. Kumar, *$K3$ surfaces associated with curves of genus two*, Int. Math. Res. Not. IMRN **6** (2008), Art. ID rnm165, 26. MR2427457 (2009d:14044)

[12] ______, *Hilbert modular surfaces for square discriminants and elliptic subfields of genus 2 function fields* (201412), available at 1412.2849.

[13] R. Sanjeewa, *Automorphism groups of cyclic curves defined over finite fields of any characteristics*, Albanian J. Math. **3** (2009), no. 4, 131–160. MR2578064 (2011a:14045)

[14] R. Sanjeewa and T. Shaska, *Determining equations of families of cyclic curves*, Albanian J. Math. **2** (2008), no. 3, 199–213. MR2492096 (2010d:14043)

[15] T. Shaska, *Genus 2 curves with $(3, 3)$-split Jacobian and large automorphism group*, Algorithmic number theory (Sydney, 2002), 2002, pp. 205–218. MR2041085 (2005e:14048)

[16] ______, *Genus 2 fields with degree 3 elliptic subfields*, Forum Math. **16** (2004), no. 2, 263–280. MR2039100 (2004m:11097)

[17] T. Shaska and H. Völklein, *Elliptic subfields and automorphisms of genus 2 function fields*, Algebra, arithmetic and geometry with applications (West Lafayette, IN, 2000), 2004, pp. 703–723. MR2037120 (2004m:14047)

Department of Mathematics, Oakland University, Rochester, MI, 48309.
E-mail address: shaska@oakland.edu