RATIONAL POINTS IN THE MODULI SPACE OF GENUS TWO

L. BESHAJ, R. HIDALGO, S. KRUK, A. MALMENDIER, S. QUISPE, AND T. SHASKA

Abstract. We build a database of genus 2 curves defined over $\mathbb{Q}$ which contains all curves with minimal absolute height $\mathrm{h} \leq 5$, all curves with moduli height $\mathfrak{h} \leq 20$, and all curves with extra automorphisms in standard form $y^2 = f(x^2)$ defined over $\mathbb{Q}$ with height $\mathrm{h} \leq 101$. For each isomorphism class in the database, an equation over its minimal field of definition is provided, the automorphism group of the curve, Clebsch and Igusa invariants. The distribution of rational points in the moduli space $\mathcal{M}_2$ for which the field of moduli is a field of definition is discussed and some open problems are presented.

1. Introduction

In [71] were introduced concepts of *minimum absolute height* of a binary form, the *moduli height*, and discussed relations between the two. Moreover, some computations were performed for binary sextics of minimum absolute height one. A natural problem in that paper was to check whether a large database of binary forms (equivalently genus 2 curves) of relatively small minimum absolute height could be constructed. Comparing the minimum absolute height with the moduli height would be the main point of this database. Moreover, such a database would shed some light to other problems related to the rational points of the moduli space $\mathcal{M}_2$. For example, not every rational point $\mathfrak{p} \in \mathcal{M}_2$ has a representative genus 2 curve $\mathcal{X}$ defined over $\mathbb{Q}$. What is the percentage of points of bounded height for which the field of moduli is not a field of definition? How does this ratio is affected when the height increases?

From another point of view, we can list genus two curves based on their moduli height. For example, traditionally there have been plenty of effort to count the curves with bounded discriminant. That is not an easy problem, but would it make more sense to have an estimate on the number of curves with bounded moduli height? After all, the moduli height is the most natural way of sorting points in $\mathcal{M}_2$.

And then, there are also the curves with automorphisms. In [5] it was shown that such curves can always be written in an equation such that the corresponding binary sextic is reduced; see [2] for details. Reduced usually means minimal absolute height for the binary form. Is this really supported computationally?

Our goal was to construct a database of genus 2 curves which addresses some of these questions.

In this paper we construct three main databases:

i) integral binary sextics of minimum absolute height ≤ 4,
ii) integral binary sextics with moduli height $\mathfrak{h} \leq 20$,
iii) integral binary sextics $f(x^2, z^2)$ of height $\mathrm{h} \leq 101$.

All combined we have over 1 million isomorphism classes of genus two curves (equivalently rational points in $\mathcal{M}_2$) without counting twists. We compute the minimal absolute height, the moduli height, the discriminant, automorphism group, field of definition, and an equation over the field of definition for all such points. We discuss all the technical details of organizing the data and some open questions on the distribution of the rational points with non-trivial obstruction in the moduli space $\mathcal{M}_2$.

Let k be an algebraically closed field of characteristic zero and $\mathcal{M}_g$ the moduli space of smooth, projective, genus $g \geq 2$ algebraic curves defined over k. The moduli space $\mathcal{M}_2$ of genus 2 curves is the most understood moduli space among all moduli spaces. This is mostly due to two main facts; first all genus two curves are hyperelliptic and therefore studying them it is easier than general curves, secondly even among hyperelliptic curves the curves of genus two have a special place since they correspond to binary sextics which, from the computational point of view, are relatively well understood compared to higher degree binary forms.

Some of the main questions related to $\mathcal{M}_2$ have been to recover a nice equation for any point $\mathfrak{p} \in \mathcal{M}_2$. Since $\mathcal{M}_2$ is a coarse moduli space, such equation is not always defined over the field of moduli of $\mathfrak{p}$. Can we find a universal equation for genus two curves over their minimal field of definition? Can such equation provide a minimal model for the curve? Does the height of this minimal model has any relation to the projective height of the corresponding moduli point $\mathfrak{p} \in \mathcal{M}_2$? What is the distribution in $\mathcal{M}_2$ of points $\mathfrak{p}$ for which the field of moduli is not a field of definition? The answers to these questions are still unknown.

In [13] we provide a computational package for computing with genus 2 curves and a database of genus 2 curves which contains all curves with height $\mathrm{h} \leq 5$, curves with moduli height $\mathfrak{h} \leq 20$, and curves with automorphism and height ≤ 101. They are organized in three Python directories $\mathcal{L}_i$, $i = 1, 2, 3$ as explained in Section 2.

The database is build with the idea of better understanding $\mathcal{M}_2$, the distribution of points in $\mathcal{M}_2$ based on the moduli height, the distribution of points for which the field of moduli is not a field of definition.

The goal of this paper is twofold: to provide the mathematical background for most of the algorithms in [13] and to discuss some of the open questions and problems raised there. Most of the material of the first part has already appeared in the vast literature on genus two curves some of which is previous work of these authors. For sake of completeness and straightening out some notational confusion we define all the basic invariants of genus two curves in this paper.

The current database and all the functions are implemented in Sage. It improves and expands a previous Maple genus 2 computational algebra package as in [70]. There is another database of genus 2 curves in [15] which collects all genus 2 curves with discriminants ≤ 1000. Some remarks on how the two databases overlap can be found in the last section.

There is a lot of confusion in the literature about the invariants of genus two curves. We go to great lengths to make sure that all the invariants are defined explicitly and there is no room for misunderstanding. We like to warn the reader that our invariants are different from the ones used by Magma and all the papers which use Magma in their computations.

2. A database of integral binary sextics

Our main goal is to create an extensive database of integral binary sextics with minimal absolute height and all the twists with minimal height. We will use the definitions of minimal absolute height, moduli height, and the basic properties of heights of polynomials from [71] and will provide details in the next coming sections. The database will be organized in a Sage/Python dictionary, where the key will be the moduli point

$$\mathfrak{p} = \begin{cases} (-1, i_1, i_2, i_3), & if\ J_2 \neq 0 \\ (0, t_1, t_2, t_3), & if\ J_2 = 0, \end{cases}$$

see Eq. (15) for definitions of such moduli point. The data is organized in three main dictionaries:

i) integral binary sextics with minimum absolute height $\mathrm{h} \leq 10$,
ii) decomposable integral binary sextics $f(x^2, z^2)$ with minimum absolute $\mathrm{h} \leq 101$ and,
iii) integral binary sextics with moduli height $\mathfrak{h} \leq 20$

Each point in the database has the following invariants

$$\begin{aligned} \mathfrak{p} = (r, i_1, i_2, i_3): \quad & \mathrm{h} && = \textit{minimal absolute height} \\ & \mathfrak{h} && = \textit{moduli height} \\ & \Delta && = \textit{minimal discriminant} \\ & \mathrm{Aut}(\mathfrak{p}) && = \textit{automorphism group} \\ & C && = \textit{Conductor} \\ & M_{\mathfrak{p}} && = \textit{field of definition of the universal curve} \\ & \mathrm{Twist} && = \textit{List of twists} \end{aligned}$$

An entry in each dictionary looks as the following:

$$(r, i_1, i_2, i_3): \Big[\mathrm{h},\ \mathfrak{h},\ \Delta,\ \mathrm{Aut}(\mathfrak{p}),\ C,\ M_{\mathfrak{p}},\ \Big[[a_0, \ldots, a_6], \ldots, [b_0, \ldots, b_6]\Big]\ \Big]$$

We illustrate with an example.

Example 1. *Let $\mathcal{X}$ be the curve with equation*

$$y^2 = x^6 - 14x^4 - 82x^2 + 1 \tag{1}$$

If we load the database in Sage and let

$$f = t^6 - 14t^4 - 82t^2 + 1$$

then the command $\mathfrak{p}$=***ModPoint (f)*** *displays*

$$\left(-1, -\frac{49281147}{5410276}, \frac{706232480445}{12584301976}, \frac{3071021069999403}{17429644021121376256}\right)$$

If we ask if $\mathfrak{p} \in \mathcal{L}$, where $\mathcal{L}$ is the second dictionary from above, the answer will be ***yes*** *and $\mathcal{L}(\mathfrak{p})$ will display*

$$[82, 2^{14} \cdot 1163^5, 17^2 \cdot 12301^2, [4, 2], C, \mathbb{Q}, [[1, 0, -14, 0, -82, 0, 1]]]$$

which means that the minimal absolute height is $\mathrm{h} = 82$*, automorphism group with GapId* $[4, 2]$ *which is the Klein group V_4, minimal field of definition $\mathbb{Q}$, and minimal*

discriminant $\Delta = 17^2 \cdot 12301^2$. *The moduli height is* $\mathfrak{h} = 2^{14} \cdot 1163^5$. *We chose not to display the conductor and all the twists.*

In the Appendix A is given a list of all the functions used for the genus 2 curves package in Sage. In the next few sections we will go over the necessary definitions and procedures to construct such databases. The details will be explained in Section 9.

3. Heights of genus two curves

In this section we define heights on algebraic curves when such curves are given by some affine equation. Throughout this paper K denotes an algebraic number field and $\mathcal{O}_K$ its ring of integers.

Let $\mathcal{X}_g$ be an irreducible algebraic curve with affine equation $F(x, y) = 0$ for $F(x, y) \in K[x, y]$. We define the **height of the curve over** K to be

$$H_K(\mathcal{X}_g) := \min \{H_K(G) \, : H_K(G) \leq H_K(F)\} .$$

where the curve $G(x, y) = 0$ is isomorphic to $\mathcal{X}_g$ over K.

If we consider the equivalence over $\bar{K}$ then we get another height which we denote it as $\overline{H}_K(\mathcal{X}_g)$ and call it **the height over the algebraic closure**. Namely,

$$\overline{H}_K(\mathcal{X}_g) = \min\{H_K(G) : H_K(G) \leq H_K(F)\},$$

where the curve $G(x, y) = 0$ is isomorphic to $\mathcal{X}_g$ over $\overline{K}$.

In the case that $K = \mathbb{Q}$ we do not write the subscript K and use $H(\mathcal{X}_g)$ or $\overline{H}(\mathcal{X}_g)$. Obviously, for any algebraic curve $\mathcal{X}_g$ we have $\overline{H}_K(\mathcal{X}_g) \leq H_K(\mathcal{X}_g)$. In [71] is proved that given K a number field such that $[K : \mathbb{Q}] = d$, the height $H_K(\mathcal{X}_g)$ and $\overline{H}_K(\mathcal{X}_g)$ are well defined.

Theorem 1 ([71])**.** *Let* K *be a number field such that* $[K : \mathbb{Q}] \leq d$. *Given a constant* $\mathrm{h}_0 \geq 1$ *there are only finitely many curves such that* $H_K(\mathcal{X}_g) \leq \mathrm{h}_0$.

As an immediate corollary we have the following

Corollary 1. *Let* $\mathrm{h}_0 \geq 1$ *be a fixed integer,* K *a number field, and* $\mathcal{O}_K$ *its ring of integers. For any genus* $g \geq 2$ *curve* $\mathcal{X}_g$ *defined over* $\mathcal{O}_K$ *with height* $\mathrm{h}(\mathcal{X}_g) = \mathrm{h}_0$ *there are only finitely many twists of* $\mathcal{X}_g$ *with height* h_0.

Given a genus two curve $\mathcal{X}_g$ the following algorithm computes a curve isomorphic over K to $\mathcal{X}_g$ of minimum height

Algorithm 1. ***Input:*** *an algebraic curve* $\mathcal{X}_g : F(x, y) = 0$, *where* F *has degree* d *and is defined over* K

Output: *an algebraic curve* $\mathcal{X}'_g : G(x, y) = 0$ *such that* $\mathcal{X}'_g \cong_K \mathcal{X}_g$ *and* $\mathcal{X}'_g$ *has minimum height.*

Step 1: *Compute* $c_0 = H_K(F)$

Step 2: *List all points* $P \in \mathbb{P}^s(K)$ *such that* $H_K(P) \leq c_0$.

Note: s *is the number of terms of* F *which is the number of monomials of degree* d *in* n *variables, and this is equal to* $\binom{d+n-1}{d}$. *From Thm. 1 there are only finitely many such points assume* $P_1, \ldots, P_r$.

Step 3: *for* $i = 1$ *to* r *do*

Let $G_i(x, y) = p_i$;

if $g(G_i(x, y)) = g(\mathcal{X}_g)$ *then*

if $G_i(x,y)=0 \cong_K F(x,y)=0$
then add G_i *to the list* L
end if;
end if;

Step 4: *Return all entries of* L *of minimum height , L has curves isomorphic over* K *to* $\mathcal{X}_g$ *of minimum height.*

Note that this algorithm is not very efficient if we start with an algebraic curve of genus two and very big height. Hence, the question that can be raised at this point is: how can we reduce the height of the curve? This is done using reduction theory, see [2, 79] and others for more details, and some elementary ways of reducing are given next. The following elementary lemma is useful.

Lemma 1. *Let* $\mathcal{X}$ *be a superelliptic curve with Weierstrass equation* $y^m=\sum_{i=0}^{d} a_i x^i$, *defined over* $\mathbb{Z}$, *and height* $\mathrm{h}(\mathcal{X})$. *Let* p *be a prime such that* $p \,|\, a_0$ *and* $\mathfrak{v}_p(a_i)=\alpha_i$, *such that* $\alpha_0 \geq \alpha_i$, *for* $i=0,\ldots,d$. *Choose* m *to be the largest nonnegative integer which satisfies*

$$m \leq \frac{\alpha_0-\alpha_i}{i}, \quad i=1,\ldots,d.$$

Then, there is a twist $\mathcal{X}'$ *of* $\mathcal{X}$ *such that*

$$\mathfrak{v}_p\left(\mathrm{h}(\mathcal{X}')\right) \leq \mathfrak{v}_p\left(\mathrm{h}(\mathcal{X})\right) - m.$$

Proof. Let p be a prime such that

$$a_i = p^{\alpha_i}\cdot b_i, \quad \textit{such that } \ (p,b_i)=1$$

In other words, $\mathfrak{v}_p(a_i)=\alpha_i$, for $i=1,\ldots,d$, as in the assumptions of the theorem. Hence, the equation of the curve is

$$y^m = \sum_{i=0}^{d} p^{\alpha_i}\, b_i \cdot x^i$$

Choose m as the largest nonnegative integer such that

$$m \leq \frac{\alpha_0-\alpha_i}{i}, \quad i=1,\ldots,d.$$

If $m=0$, then the curve can no further reduced by this method at the prime p. If $m>0$, then we let

$$(x,y) \mapsto (p^m\cdot x,\, y)$$

which gives the curve

$$y^m = \sum_{i=0}^{d} a_i'\, x^i = \sum_{i=0}^{d} p^{\alpha_i+im}\, b_i\, x^i$$

Then,

$$\mathfrak{v}_p(a_i') = \alpha_i + i\cdot m.$$

Hence, to have reduction of $\mathfrak{v}_p\left(\mathrm{h}(\mathcal{X})\right)$ we must have $\alpha_i+im\leq\alpha_0$ for $i=1,\ldots,d$. Thus, $m \leq \frac{\alpha_0-\alpha_i}{i}$, for $i=1,\ldots d$. Choosing the largest such m will result to the biggest possible reduction on p. Dividing both sides by the content of the polynomial, which has the maximum power of p as a factor, gives a twist $\mathcal{X}'$ of $\mathcal{X}$ with height which has valuation at p, $\mathfrak{v}_p\left(\mathrm{h}(\mathcal{X}')\right) \leq \mathfrak{v}_p\left(\mathrm{h}(\mathcal{X})\right) - m$. This completes the proof. □

Remark 1. *Notice that the curve $\mathcal{X}^\sigma$ could be in the same Γ-orbit of $\mathcal{X}$ or could be a twist of $\mathcal{X}$, depending on the values of m, where Γ is the modular group.*

Corollary 2. *Let $\mathcal{X}$ be a curve with $\mathrm{Aut}(\mathcal{X}) \cong D_6$ and equation*

$$y^2 = x^6 + x^3 + s$$

where $s \in \mathbb{Z}$ such that it has a prime factorization

$$s = p^\alpha \cdot s', \quad \text{where} \quad (s, s') = 1$$

Then, we can reduce the height by the transformation $x \mapsto p^m \cdot x$, where $m = \lfloor \frac{\alpha}{6} \rfloor$

Example 2. *Let us consider the curve from Ex. 4, namely*

$$y^2 = x^6 + x^3 + 2^{33}$$

This curve has height $\mathrm{h} = 2^{33}$. Then m has to be the largest nonnegative integer such that it is $\leq$ to

$$\frac{33-0}{6}, \frac{33-0}{5},$$

which makes $m = 5$.

Consider the transformation $x \mapsto 2^5 \cdot x$. Then the curve becomes

$$y^2 = 2^{15} \cdot x^6 + x^3 + 2^{18}$$

which is with height $\mathrm{h} = 2^{18}$.

Next we will define the moduli height of genus g curves.

3.1. **Moduli height of curves.** Let g be an integer $g \geq 2$ and $\mathcal{M}_g$ denote the coarse moduli space of smooth, irreducible algebraic curves of genus g. It is known that $\mathcal{M}_g$ is a quasi projective variety of dimension $3g-3$. Hence, $\mathcal{M}_g$ is embedded in $\mathbb{P}^{3g-2}$. Let $\mathfrak{p} \in \mathcal{M}_g$. We call the moduli height $\mathfrak{h}(\mathfrak{p})$ the usual height $H(P)$ in the projective space $\mathbb{P}^{3g-2}$. Obviously, $\mathfrak{h}(\mathfrak{p})$ is an invariant of the curve. In [71] is proved the following result.

Theorem 2. *For any constant $c \geq 1$, degree $d \geq 1$, and genus $g \geq 2$ there are finitely many superelliptic curves $\mathcal{X}_g$ defined over the ring of integers $\mathcal{O}_K$ of an algebraic number field K such that $[K : \mathbb{Q}] \leq d$ and $\mathfrak{h}(\mathcal{X}_g) \leq c$.*

While the above theorem shows that the number of curves with bounded moduli height is finite, determine this number seems to be a very difficult problem.

4. Genus 2 curves over $\mathbb{C}$

In this section we give a quick overview of the basic setup for genus two curves. The material is part of the folklore on the literature of genus 2 curves and we don't mention all the possible references. While the main definitions and results on what follows are valid for any $g \geq 2$ we only state them for the case $g = 2$. We mainly follow the approach of [14, 19, 32, 33, 38, 55].

4.1. **Periods and invariants.** Let $\mathcal{X}$ be a genus $g = 2$ algebraic curve. We choose a symplectic homology basis for $\mathcal{X}$, say $\{A_1, A_2, B_1, B_2\}$, such that the intersection products $A_i \cdot A_j = B_i \cdot B_j = 0$ and $A_i \cdot B_j = \delta_{ij}$, where δ_{ij} is the Kronecker delta. We choose a basis $\{w_i\}$ for the space of holomorphic 1-forms such that $\int_{A_i} w_j = \delta_{ij}$. The matrix

$$\Omega = \left[\int_{B_i} w_j\right]$$

is the *period matrix* of $\mathcal{X}$. The columns of the matrix $[I\ |\Omega]$ form a lattice Λ in $\mathbb{C}^g$ and the Jacobian of $\mathcal{X}$ is Jac $(\mathcal{X}) = \mathbb{C}^g/\Lambda$. Let $\mathbb{H}_g$ be the *Siegel upper-half space* and $Sp_4(\mathbb{Z})$ is the *symplectic group*. Then $\Omega \in \mathbb{H}_g$.

Proposition 1. *Two period matrices Ω, Ω' define isomorphic principally polarized abelian varieties if and only if they are in the same orbit under the action of $Sp_4(\mathbb{Z})$ on $\mathbb{H}_g$.*

Hence, there is an injection

$$\mathcal{M}_2 \hookrightarrow \mathbb{H}_2/Sp_4(\mathbb{Z}) =: \mathcal{A}_2$$

For any $z \in \mathbb{C}^2$ and $\tau \in \mathbb{H}_2$ *Riemann's theta function* is defined as

$$\theta(z, \tau) = \sum_{u \in \mathbb{Z}^2} e^{\pi i(u^t \tau u + 2u^t z)}$$

where u and z are $2-$dimensional column vectors and the products involved in the formula are matrix products. The fact that the imaginary part of τ is positive makes the series absolutely convergent over any compact sets. Therefore, the function is analytic. The theta function is holomorphic on $\mathbb{C}^2 \times \mathbb{H}_2$ and satisfies

$$\theta(z + \tau u) = \theta(z, \tau), \quad \theta(z + \tau, \tau u) = e^{-\pi i(u^t \tau u + 2z^t u)} \cdot \theta(z, \tau),$$

where $u \in \mathbb{Z}^2$. Any point $e \in$ Jac $(\mathcal{X})$ can be written uniquely as $e = (b, a)\begin{pmatrix} 1_2 \\ \Omega \end{pmatrix}$, where $a, b \in \mathbb{R}^2$ are row vectors. We shall use the notation $[e] = \begin{bmatrix} a \\ b \end{bmatrix}$ for the characteristic of e. For any $a, b \in \mathbb{Q}^2$, the theta function with rational characteristics is defined as

$$\theta \begin{bmatrix} a \\ b \end{bmatrix}(z, \tau) = \sum_{u \in \mathbb{Z}^2} e^{\pi i((u+a)^t \tau (u+a) + 2(u+a)^t (z+b))}.$$

When the entries of column vectors a^t and b^t are from the set $\{0, \frac{1}{2}\}$, then the characteristics $\begin{bmatrix} a \\ b \end{bmatrix}$ are called the *half-integer characteristics*. The corresponding theta functions with rational characteristics are called *theta characteristics*. A scalar obtained by evaluating a theta characteristic at $z = 0$ is called a *theta constant*. Any half-integer characteristic is given by

$$\mathfrak{m} = \frac{1}{2}m = \frac{1}{2}\begin{pmatrix} m_1 & m_2 \\ m_1' & m_2' \end{pmatrix}$$

where $m_i, m_i' \in \mathbb{Z}$. For $\gamma = \begin{bmatrix} \gamma' \\ \gamma'' \end{bmatrix} \in \frac{1}{2}\mathbb{Z}^4/\mathbb{Z}^4$ we define

$$e_*(\gamma) = (-1)^{4(\gamma')^t \gamma''}.$$

Then,

$$\theta[\gamma](-z,\tau) = e_*(\gamma)\theta[\gamma](z,\tau).$$

We say that γ is an **even** (resp. **odd**) characteristic if $e_*(\gamma) = 1$ (resp. $e_*(\gamma) = -1$).

For any genus 2 curve we have six odd theta characteristics and ten even theta characteristics. The following are the sixteen theta characteristics, where the first ten are even and the last six are odd. For simplicity, we denote them by $\theta_i \begin{bmatrix} a \\ b \end{bmatrix}$ instead of $\theta_i \begin{bmatrix} a \\ b \end{bmatrix}(z,\tau)$ where $i = 1,\ldots,10$ for the even theta functions.

$$\theta_1 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \theta_2 = \begin{bmatrix} 0 & 0 \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}, \theta_3 = \begin{bmatrix} 0 & 0 \\ \frac{1}{2} & 0 \end{bmatrix}, \theta_4 = \begin{bmatrix} 0 & 0 \\ 0 & \frac{1}{2} \end{bmatrix}, \theta_5 = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & 0 \end{bmatrix},$$
$$\theta_6 = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix}, \theta_7 = \begin{bmatrix} 0 & \frac{1}{2} \\ 0 & 0 \end{bmatrix}, \theta_8 = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ 0 & 0 \end{bmatrix}, \theta_9 = \begin{bmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{bmatrix}, \theta_{10} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix},$$

and the odd theta functions correspond to the following characteristics

$$\begin{bmatrix} 0 & \frac{1}{2} \\ 0 & \frac{1}{2} \end{bmatrix}, \begin{bmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}, \begin{bmatrix} \frac{1}{2} & 0 \\ \frac{1}{2} & 0 \end{bmatrix}, \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & 0 \end{bmatrix}, \begin{bmatrix} \frac{1}{2} & 0 \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}, \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ 0 & \frac{1}{2} \end{bmatrix}$$

The complete set of thetanulls above are not independent, their relations are given via Frobenious relations. There are four theta constants which generate all the others, namely **fundamental theta constants** θ_1, θ_2, θ_3, θ_4; see [75] for details. The following is Igusa's result, which is valid for any $g \geq 2$. We only state it for $g = 2$.

Theorem 3. *The complete set of theta constants uniquely determine the isomorphism class of a principally polarized abelian variety of dimension 2.*

For curves of genus 2 this can be made more precise. Let a genus 2 curve in Rosenheim form be given by

$$Y^2 = X(X-1)(X-\lambda)(X-\mu)(X-\nu). \tag{2}$$

By the sa called Picard's lemma λ, μ, ν can be written as follows:

$$\lambda = \frac{\theta_1^2\theta_3^2}{\theta_2^2\theta_4^2}, \quad \mu = \frac{\theta_3^2\theta_8^2}{\theta_4^2\theta_{10}^2}, \quad \nu = \frac{\theta_1^2\theta_8^2}{\theta_2^2\theta_{10}^2}. \tag{3}$$

We can determine an equation of the curve in terms of the fundamental thetas as follows:

Proposition 2 ([75]). *Every genus two curve can be written in the form:*

$$y^2 = x\,(x-1)\left(x - \frac{\theta_1^2\theta_3^2}{\theta_2^2\theta_4^2}\right)\left(x^2 - \frac{\theta_2^2\,\theta_3^2 + \theta_1^2\,\theta_4^2}{\theta_2^2\,\theta_4^2}\cdot\alpha\,x + \frac{\theta_1^2\theta_3^2}{\theta_2^2\theta_4^2}\,\alpha^2\right), \tag{4}$$

where $\alpha = \frac{\theta_8^2}{\theta_{10}^2}$ *and in terms of* $\theta_1,\ldots,\theta_4$ *is given by*

$$\alpha^2 + \frac{\theta_1^4 + \theta_2^4 - \theta_3^4 - \theta_4^4}{\theta_1^2\theta_2^2 - \theta_3^2\theta_4^2}\,\alpha + 1 = 0$$

Furthermore, if $\alpha = \pm 1$ *then* $\mathcal{X}$ *has an extra involution.*

From the above we have that $\theta_8^4 = \theta_{10}^4$ implies that $\mathcal{X}$ has an extra involution. Hence, the Klein viergrouppe $V_4 \hookrightarrow Aut(\mathcal{X})$. The last part of the lemma above shows that if $\theta_8^4 = \theta_{10}^4$ then all coefficients of the genus 2 curve are given as rational functions of the 4 fundamental theta functions. Such fundamental theta functions

determine the field of moduli of the given curve. Hence, the curve is defined over its field of moduli.

Corollary 3. *Let $\mathcal{X}$ be a genus 2 curve which has an extra involution. Then $\mathcal{X}$ is defined over its field of moduli.*

We will revisit the curves defined over their field of moduli again in the coming sections.

4.2. **Siegel modular forms.** Here we define Siegel modular forms ψ_4, ψ_6, χ_{10}, χ_{12}, of degree 4, 6, 10, and 12, as in [38, pg. 848].

$$
\begin{aligned}
2^2 \cdot \psi_4 &= \sum (\theta_m)^8 \\
2^2 \cdot \psi_6 &= \sum_{syzygous} \pm (\theta_{m_1}\theta_{m_2}\theta_{m_3})^4 \\
-2^{14} \cdot \chi_{10} &= \prod (\theta_m)^2 \\
2^{17} \cdot 3 \cdot \chi_{12} &= \sum (\theta_{m_1}\theta_{m_2}\cdots\theta_{m_6})^4 \\
2^{39} \cdot 5^3 \cdot \chi_{35} &= \left(\prod \theta_m\right)\left(\sum_{azygous} \pm (\theta_{m_1}\theta_{m_2}\theta_{m_3})^{20}\right).
\end{aligned} \tag{5}
$$

In definition of χ_{12} the summation is taken over all Göpel systems as explained in [75], where all the Göpel systems are displayed.

Theta constants provide a complete system of invariants for isomorphism classes of principally polarized varieties of dimension $g = 2$. But there are two main issues with this approach: First, these invariants are not independent. This can be fixed via the fundamental theta constants as in Prop. 2, however computationally things get difficult when we try to express all the results in terms of $\theta_1, \theta_2, \theta_3, \theta_4$. Secondly, and more importantly, they are defined analytically. Naturally, we would like to have algebraically defined invariants.

5. Algebraic invariants

Let $f(x, z)$ be a binary sextic defined over a field k, char $k = 0$, given by

$$
\begin{aligned}
f(x,z) &= a_0x^6 + a_1x^5z + \cdots + a_6z^6 \\
&= (z_1x - x_1z)(z_2x - x_2z)\ldots(z_6x - x_6z)
\end{aligned} \tag{6}
$$

A **covariant** I of $f(x, z)$ is a homogenous polynomial in x, z with coefficients in $k[a_0, \ldots, a_{2g+2}]$. The **order** of I is the degree of I as a polynomial in x, z and the **degree** of I is the degree of I as a polynomial in $k[a_0, \ldots, a_{2g+2}]$. An **invariant** is a covariant of order zero. The binary form $f(x, z)$ is a covariant of order $2g + 2$ and degree 1. Throughout this paper we will use as basic references [19], [14], and [32, 33, 38].

5.1. **Invariants and covariants via transvections.** For any two binary forms f and g the symbol $(f, g)_r$ denotes the r-transvection. Notice that the transvections are conveniently computed in terms of the coefficients of the binary forms.

Let $f(x, z)$ be a binary sextic as in Eq. (6) and consider the following covariants

$$
\begin{aligned}
\Delta &= ((f,f)_4,(f,f)_4)_2\,, & Y_1 &= (f,(f,f)_4)_4 \\
Y_2 &= ((f,f)_4,Y_1)_2\,, & Y_3 &= ((f,f)_4,Y_2)_2
\end{aligned} \tag{7}
$$

The **Clebsch invariants** A, B, C, D are defined as follows

$$\begin{aligned} A &= (f,f)_6, & B &= ((f,f)_4,(f,f)_4)_4\,, \\ C &= ((f,f)_4,\Delta)_4\,, & D &= (Y_3,Y_1)_2 \end{aligned} \tag{8}$$

see Clebsch [19] or Bolza [14, Eq. (7), (8), pg. 51] for details.

We display the invariants A, B, C, D in terms of the coefficients in the Appendix. The following result is elementary but very important in our computations.

5.2. **Root differences.** Let $f(x,z)$ be a binary sextic as above and set $D_{ij} := \begin{pmatrix} x_i & x_j \\ z_i & z_j \end{pmatrix}$. For $\tau \in SL_2(k)$, we have

$$\tau(f) = (z_1'x - x_1'z)\dots(z_6'x - x_6'z), \qquad \textit{with} \qquad \begin{pmatrix} x_i' \\ z_i' \end{pmatrix} = \tau^{-1}\begin{pmatrix} x_i \\ z_i \end{pmatrix}.$$

Clearly D_{ij} is invariant under this action of $SL_2(k)$ on $\mathbb{P}^1$. Let $\{i,j,k,l,m,n\} = \{1,2,3,4,5,6\}$. Treating a_i as variables, we construct the following elements in the ring of invariants $\mathcal{R}_6$

$$\mathfrak{A} = a_0^2 \prod_{fifteen} (12)^2(34)^2(56)^2 = \sum_{i<j,k<l,m<n} D_{ij}^2 D_{kl}^2 D_{mn}^2$$

$$\mathfrak{B} = a_0^4 \prod_{ten} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2 = \sum_{\substack{i<j,j<k,\\ l<m,m<n}} D_{ij}^2 D_{jk}^2 D_{ki}^2 D_{lm}^2 D_{mn}^2 D_{nl}^2$$

$$\begin{aligned} \mathfrak{C} &= a_0^6 \prod_{sixty} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2(14)^2(25)^2(36)^2 \\ &= \sum_{\substack{i<j,j<k,l<m,m<n \\ i<l',j<m',k<n' \\ l',m',n' \in \{l,m,n\}}} D_{ij}^2 D_{jk}^2 D_{ki}^2 D_{lm}^2 D_{mn}^2 D_{nl}^2 D_{il'}^2 D_{jm'}^2 D_{kn'}^2 \end{aligned} \tag{9}$$

$$\mathfrak{D} = a_0^{10} \prod_{i<j} (ij)^2$$

These invariants, sometimes called **integral invariants**, are defined in [32, pg. 620] where they are denoted by A, B, C, D. Incidentally even Clebsch invariants which are defined next are also denoted by A, B, C, D by many authors.

To quote Igusa *"if we restrict to integral invariants, the discussion will break down in characteristic 2 simply because Weierstrass points behave badly under reduction modulo 2"*; see [32, pg. 621]. Next we define invarints which will work in every characteristic.

5.3. **Igusa invariants.** In [32, pg. 622] Igusa defined what he called **basic arithmetic invariants**, which are now commonly known as **Igusa invariants**

$$\begin{aligned} J_2 &= \frac{1}{2^3}\mathfrak{A}, & J_4 &= \frac{1}{2^5\cdot 3}(4J_2^2 - \mathfrak{B}), \\ J_6 &= \frac{1}{2^6\cdot 3^2}(8J_2^3 - 160J_2J_4 - \mathfrak{C}), & J_{10} &= \frac{1}{2^{12}}\mathfrak{D} \end{aligned}$$

While most of the current literature on genus 2 curves uses invariants $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}$, which are now most commonly labeled as I_2, I_4, I_6, I_{10}, Igusa went to great lengths in [32] to define J_2, J_4, J_6, J_{10} and to show that they also work in characteristic 2.

Lemma 2. *J_{2i} are homogeneous elements in $\mathcal{R}_6$ of degree $2i$, for i = 1,2,3,5.*

A degree $d \geq 2$ binary form $f(x, z)$ is called **semistable** if it has no root of multiplicity $> \frac{d}{2}$.

Lemma 3. *A sextic has a root of multiplicity at least four if and only if the basic invariants vanish simultaneously.*

So a sextic for which all the basic invariants vanish simultaneously is not semistable.

Throughout this paper, we will use these invariants J_2, J_4, J_6, J_{10}. For a binary form $f(x, z) = \sum_{i=0}^{6} a_i\, x^i z^{6-i}$ as in Eq. (6) we display these invariants in terms of the coefficients $a_0, \ldots, a_6$ in B.

Invariants $\{J_{2i}\}$ are homogeneous polynomials of degree $2i$ in $k[a_0, \ldots, a_6]$, for $i = 1, 2, 3, 5$. These J_{2i} are invariant under the natural symmetries of the roots, namely the action of S_6 on the set of the roots. They are also natural on the action of $SL_2(k)$ on the sextic.

Lemma 4. [32, Cor. pg. 632] *Two genus 2 curves C and C' are isomorphic if and only if there exists an $r \neq 0$ such that*

$$J_{2i}(C) = r^{2i} \cdot J_{2i}(C'), \qquad \text{for} \quad i = 1, 2, 3, 5.$$

Remark 2. *There is a lot of confusion in the literature about the definitions of the generators of $\mathcal{R}_6$. Many authors have used different names and different notations for generators of $\mathcal{R}_6$. Moreover, many times the symbols $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}$ are defined by scaling with different constants by many authors. Hence, sometimes equations in terms of these invariants might not be the same. To avoid any confusion, we display the expressions of j_2, J_4, J_6, j_{10} in terms of the coefficients of the binary sextic in Eq. (B).*

Igusa invariants are expressed in terms of the Clebsch invariants as follows:

$$\begin{aligned} J_2 &= -2^3 \cdot 3 \cdot 5\, A\,, \\ J_4 &= 2^3 \cdot 2^5\, (75B - 8A^2) \\ J_6 &= 2^2 \cdot 3^3 \cdot 5\, \left(16\, A^3 - 200\, A\, B + 375\, C\right) \\ J_{10} &= 2^3 \cdot 4\, \big(-384\, A^5 + 6000\, A^3\, B + 10000\, A^2\, C - 18750\, A\, B^2 \\ &\qquad -37500\, B\, C - 28125\, D\big) \end{aligned} \tag{10}$$

Conversely, the invariants (A, B, C, D) are polynomial expressions in the Igusa invariants (J_2, J_4, J_6, J_{10}) with rational coefficients are displayed in Eq. B in the Appendix.

Thus, the invariants of a sextic define a point in a weighted projective space $[J_2 : J_4 : J_6 : J_{10}] \in \mathbb{WP}^3_{(2,4,6,10)}$. It was shown in [40] that points in the projective variety Proj $\mathbb{C}[J_2, J_4, J_6, J_{10}]$ which are not on $J_2 = 0$ form the variety $\mathcal{U}_6$ of moduli of sextics. Equivalently, points in the weighted projective space $\{[J_2 : J_4 : J_6 : J_{10}] \in \mathbb{WP}^3_{(2,4,6,10)} : J_{10} \neq 0\}$ are in one-to-one correspondence with isomorphism classes of sextics.

5.4. **Absolute invariants.** Dividing any $SL_2(k)$ invariant by another one of the same degree gives an invariant under $GL_2(k)$ action.

We follow [33, pg. 181] and define the following absolute invariants

$$i_1 := 144\frac{J_4}{J_2^2}, \quad i_2 := -1728\frac{J_2J_4 - 3J_6}{J_2^3}, \quad i_3 := 486\frac{J_{10}}{J_2^5} \tag{11}$$

for $J_2 \neq 0$. Notice that Igusa denotes them by x_1, x_2, x_3.

Theorem 4. [33, Theorem 3] *The three absolute invariants can be expressed by the four modular forms in the form*

$$i_1 = \frac{\psi_4\chi_{10}^2}{\chi_{12}^2}, \quad i_2 = \frac{\psi_6\,\chi_{10}^3}{\chi_{12}^3}, \quad i_3 = \frac{\chi_{10}^6}{\chi_{12}^5} \tag{12}$$

Hence, the theorem says that every modular form, in the degree 2 case, is expressed in the Eisenstein series of weight four, six, ten, and twelve. It is the main result of [33].

There is another set of absolute invariants

$$j_1 := \frac{\mathfrak{A}^5}{\mathfrak{D}}, \quad j_2 := \frac{\mathfrak{B}\mathfrak{A}^3}{\mathfrak{D}}, \quad j_3 := \frac{\mathfrak{C}\mathfrak{A}^2}{\mathfrak{D}}, \tag{13}$$

The popularity of invariants j_1, j_2, j_3 is due to P. Van Wamelen who used them in [81] and later implemented them in Magma. They have no advantages over the invariants i_1, i_2, i_3 since both sets of invariants are not defined for $J_2 = 0$ or equivalently $\mathfrak{A} = 0$. Indeed, we could not find a direct proof that such invariants generate the field of invariants for $\mathcal{R}_6$, even though it is probably true. The results of other authors who have worked with j_1, j_2, j_3 can be converted into our results and vice-versa using the formulas

$$i_1 = 144\,\frac{j_2}{j_1}, \quad i_2 = -1728\,\frac{j_2 - 3j_3}{j_1}, \quad i_3 = 486\frac{1}{j_1}$$

and conversely

$$j_1 = 486\,\frac{1}{i_3}, \quad j_2 = \frac{27}{8}\,\frac{i_1}{i_3}, \quad j_3 = \frac{3}{32}\,\frac{i_2 + 12i_1}{i_3}$$

Remark 3. *It is to be noted that for computational purposes i_1, i_2, i_3 are much better than j_1, j_2, j_3 since they are of lower degrees. Especially, for our purposes it is very important that the moduli point $\mathfrak{p} = (r, i_1, i_2, i_3)$ (cf. next section) it is expressed in as small numbers as possible.*

There is another set of invariants defined by Igusa in [32],

$$t_1 = \frac{J_2^5}{J_{10}}, \quad t_2 = \frac{J_4^5}{J_{10}^2}, \quad t_3 = \frac{J_6^5}{J_{10}^3}$$

which are defined everywhere in the moduli space. Due to their high degrees, they become difficult to use especially when someone wants to do symbolic computations.

In the case $J_2 = 0$ we define

$$a_1 := \frac{J_4 \cdot J_6}{J_{10}}, \quad a_2 := \frac{J_6 \cdot J_{10}}{J_4^4} \tag{14}$$

to determine genus two fields with $J_2 = 0$, $J_4 \neq 0$, and $J_6 \neq 0$ up to isomorphism. They were used in [22,55,61,74] and others. Moreover, when $J_2 = 0, J_4 = 0, J_6 \neq 0$

we have $\frac{J_6^5}{J_{10}^3}$ as an invariant and when $J_2 = 0, J_6 = 0, J_4 \neq 0$ we have $\frac{J_4^5}{J_{10}^2}$ as an invariant.

All our computations are made in terms of absolute invariants i_1, i_2, i_3 or the Igusa invariants J_2, J_4, J_6, J_{10}. In the Appendix, we provide formulas how to convert back and forth among all sets of invariants. When $J_2 = 0$ we will use invariants t_1, t_2, t_3 instead, in this case $t_1 = 0$, so this locus is determined by t_2 and t_3.

5.5. **Representing a point in the moduli space.** In creating a large database of genus two curves we need a way to identify uniquely a point $\mathfrak{p} \in \mathcal{M}_2$. Such point would ideally be defined everywhere, computationally feasable, and should not involve large integers. Of course, the representation $\mathfrak{p} = (t_1, t_2, t_3)$ is unique, but these invariants are very large and extremely difficult to handle in a large database. The set of invariants (i_1, i_2, i_3) is nicer, but they are not defined for $J_2 = 0$.

To find a compromise and simplify the implementation in [13], for a given genus 2 curve $\mathcal{X}$ we define the corresponding **moduli point** $\mathfrak{p} = [\mathcal{X}]$ to be

$$\mathfrak{p} = \begin{cases} (i_1, i_2, i_3) & if\ J_2 \neq 0 \\ (t_1, t_2, t_3) & if\ J_2 = 0 \end{cases} \tag{15}$$

This moduli point $\mathfrak{p}$ together with J_2 will be the *key* in our dictionary of genus 2 curves. It will be stored as a 4-tuple $(r, \mathfrak{p})$ as explained before.

For $I_2 \neq 0$ we use the variables i_1, i_2, i_3 to write

$$\Big[J_2 : J_4 : J_6 : J_{10}\Big] = \left[1 : \frac{1}{2^4\,3^2}\, i_1 : \frac{1}{2^6\,3^4}\, i_2 + \frac{1}{2^4\,3^3}\, i_1 : \frac{1}{2\cdot 3^5}\, i_3\right] \in \mathbb{WP}^3_{(2,4,6,10)}\ ,$$

see [47] *pg. 13 for details. Notice that i_1, i_2, i_3 are denoted by $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3$ and J_2, J_4, J_6, J_{10} respectively by I_2, I_4, I_6, I_{10} in [47].

5.6. **Relations among different sets of invariants.** There are three sets of $SL_2(k)$ invariants most commonly used, namely (A, B, C, D), $(\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D})$, and (J_2, J_4, J_6, J_{10}). Many authors will use the notation (I_2, I_4, I_6, I_{10}) for $(\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D})$ due to the Magma notation (they are called *Igusa Clebsch invariants* in Magma) or some scaling of them.

Notice that

$$J_{2i} = \frac{1}{2^{4i}}\, I_{2i}, \qquad i = 1, 2, 3, 5. \tag{16}$$

For a given genus two curve $\mathcal{X}$ with equation $y^2 = f(x)$, the relations between invariants $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}$ and even Siegel modular forms $\psi_4, \psi_6, \chi_{10}, \chi_{12}, \chi_{35}$ of $\mathcal{A}_2$ are given by Igusa in [38, p. 848]:

$$\begin{aligned} \mathfrak{A}(f) &= -2^3 \cdot 3\, \frac{\chi_{12}(\tau)}{\chi_{10}(\tau)}\ , & \mathfrak{B}(f) &= \ \ 2^2\, \psi_4(\tau)\ , \\ \mathfrak{C}(f) &= -\frac{2^3}{3}\, \psi_6(\tau) - 2^5\, \frac{\psi_4(\tau)\, \chi_{12}(\tau)}{\chi_{10}(\tau)}\ , & \mathfrak{D}(f) &= -2^{14}\, \chi_{10}(\tau)\ . \end{aligned} \tag{17}$$

In the Appendix are given the relations between A, B, C, D and J_2, J_4, J_6, J_{10}. Using such relations we get the absolute invariants i_1, i_2, i_3 in terms of A, B, C, D are as follows:

$$i_1 = \frac{9}{10} \cdot \frac{75B - 8A^2}{A^2}$$

$$i_2 = \frac{27}{50} \cdot \frac{112A^3 - 900AB - 1125C}{A^3}$$

$$i_3 = \frac{81}{2^{13}\cdot 5^5}\cdot\frac{384A^5 - 6000A^3B - 10000A^2C + 18750AB^2 + 37500BC + 28125CD}{A^5}$$

Next we see how to construct the equation of a curve starting from a moduli point $\mathfrak{p} \in \mathcal{M}_2$.

5.7. **Recovering an equation of the curve from the moduli point.** Some other invariants are as follows

$$\begin{aligned} A_{ij} &= (Y_iY_j)_2, && (1 \le i,j \le 3)\\ H_{ijk} &= (fY_i)_2(fY_j)_2(fY_k)_2 && (1 \le i,j,k \le 3)\\ R &= -(Y_1Y_2)(Y_2Y_3)(Y_3Y_1) \end{aligned}$$

Note that A_{ij} and H_{ijk} can be expressed in terms of the Clebsch invariants, see [55, pg. 318]. Moreover, $R^2 = \frac{1}{2}\det M$ where M is the **Clebsch matrix** defined as follows.

$$M = \begin{bmatrix} A_{11} & A_{12} & A_{13}\\ A_{12} & A_{22} & A_{23}\\ A_{13} & A_{23} & A_{33}\end{bmatrix} \tag{18}$$

The following is an immediate consequence of classical invariant theory

Let J_{30} denote the degree 30 invariant

$$J_{30} := \det M$$

An expression of J_{30} in terms of J_2, J_4, J_6, J_{10} is given in [74, Theorem 3], where it is also expressed in terms of the roots of the sextic and its coefficients.

Let us now compute the determinant of the minor $S = \begin{pmatrix} A_{1,1} & A_{1,2}\\ A_{2,1} & A_{2,2}\end{pmatrix}$ from the matrix $M = [A_{i,j}]$.

$$\begin{aligned} \det S &= A_{1,1}A_{2,2} - A_{1,2}^2\\ &= \frac{2^{16}}{3^6\cdot 5^4 J_2^8}\left(15\,J_2^3J_4\,J_6 - 4\,J_2^4J_4^2 - 175\,J_2^2J_4^3 + 2430\,J_{10}\,J_2^3 - 9\,J_2^2J_6^2\right.\\ &\left.+1488\,J_2\,J_4^2J_6 - 64\,J_4^4 + 113400\,J_{10}\,J_2\,J_4 - 2880\,J_4\,J_6^2 - 648000\,J_{10}\,J_6\right) \end{aligned}$$

We define the new invariant

$$\begin{aligned} J_{16} :=& 15\,J_2^3J_4\,J_6 - 4\,J_2^4J_4^2 - 175\,J_2^2J_4^3 + 2430\,J_{10}\,J_2^3 - 9\,J_2^2J_6^2 + 1488\,J_2\,J_4^2J_6\\ &- 64\,J_4^4 + 113400\,J_{10}\,J_2\,J_4 - 2880\,J_4\,J_6^2 - 648000\,J_{10}\,J_6 \end{aligned}$$

which is a degree 16 invariant.

6. Automorphisms

Let $\mathcal{X}$ be a genus 2 curve defined over an algebraically closed field k. Let K be the function field of $\mathcal{X}$. Then K has exactly one genus 0 subfield of degree 2, denote it $k(x)$. Since $k(x)$ is the only genus 0 subfield of degree 2 of K, then $G = \mathrm{Aut}(K/k)$ (or equivalently $\mathrm{Aut}(\mathcal{X})$) fixes $k(x)$. It is the fixed field of the hyperelliptic involution τ in $\mathrm{Aut}(K)$. Thus τ is in the center of $\mathrm{Aut}(K)$ and $\langle\tau\rangle \lhd \mathrm{Aut}(K)$. The quotient group $\overline{\mathrm{Aut}}(K) = \mathrm{Aut}(K)/\langle\tau\rangle$ is called the **reduced automorphism group** of $\mathcal{X}$ (or equivalently of K).

The reduced automorphism group embeds as a finite subgroup of $PGL(2,\mathbb{C})$, therefore it is isomorphic to C_n, D_n, A_4, S_4, A_5. Hence, the full automorphism group $\mathrm{Aut}(\mathcal{X})$ is a degree 2 central extension of $\overline{\mathrm{Aut}}(\mathcal{X})$.

The extension $K/k(x)$ is ramified at exactly six distinct points, namely the points $P = \{\omega_1, \cdots, \omega_6\}$ in $\mathbb{P}^1$. The corresponding places of this points in K are called Weierstrass points of K. The group $\mathrm{Aut}(K)$ permutes the 6 Weierstrass points and the group $\overline{\mathrm{Aut}}(K)$ permutes accordingly $\{\omega_1, \cdots, \omega_6\}$ in its action on $\mathbb{P}^1$ as subgroup of $PLG(2,\mathbb{C})$. This yields an embedding $\overline{\mathrm{Aut}}(K) \hookrightarrow S_6$, so all elements of $\overline{\mathrm{Aut}}(K)$ have order ≤ 6.

In any characteristic different from 2, the automorphism group $\mathrm{Aut}(\mathcal{X})$ is isomorphic to one of the groups given by the following theorem from [74].

Theorem 5 ([74])**.** *The automorphism group G of a genus 2 curve $\mathcal{X}$ in characteristic $\neq 2$ is isomorphic to $\mathbb{Z}_2$, $\mathbb{Z}_{10}$, V_4, D_8, D_{12}, $SL_2(3)$, $GL_2(3)$, or 2^+S_5. The case when $G \cong 2^+S_5$ occurs only in characteristic 5. If $G \cong SL_2(3)$ (resp., $GL_2(3)$) then $\mathcal{X}$ has equation $Y^2 = X^6 - 1$ (resp., $Y^2 = X(X^4-1)$). If $G \cong \mathbb{Z}_{10}$ then $\mathcal{X}$ has equation $Y^2 = X^6 - X$.*

An **elliptic involution** of K is an involution in G which is different from z_0 (the hyperelliptic involution). Thus the elliptic involutions of G are in 1-1 correspondence with the elliptic subfields of K of degree 2 (by the Riemann-Hurwitz formula). For the number of elliptic involutions of a genus 2 curve see [74].

6.1. **Automorphisms in terms of theta functions.** The locus $\mathcal{L}_2$ of genus 2 curves $\mathcal{X}$ which have an elliptic involution is a closed subvariety of $\mathcal{M}_2$.

Lemma 5. *Let $\mathcal{X}$ be a genus 2 curve. Then $Aut(\mathcal{X}) \cong V_4$ if and only if the theta functions of $\mathcal{X}$ satisfy*

(19)
$$\begin{aligned}
&(\theta_1^4-\theta_2^4)(\theta_3^4-\theta_4^4)(\theta_8^4-\theta_{10}^4)(-\theta_1^2\theta_3^2\theta_8^2\theta_2^2-\theta_1^2\theta_2^2\theta_4^2\theta_{10}^2+\theta_1^4\theta_3^2\theta_{10}^2+\theta_3^2\theta_2^4\theta_{10}^2)\\
&(\theta_3^2\theta_8^2\theta_2^2\theta_4^2-\theta_2^2\theta_4^4\theta_{10}^2+\theta_1^2\theta_3^2\theta_4^2\theta_{10}^2-\theta_3^4\theta_2^2\theta_{10}^2)(-\theta_8^4\theta_3^2\theta_2^2+\theta_8^2\theta_2^2\theta_{10}^2\theta_4^2+\theta_1^2\theta_3^2\theta_8^2\theta_{10}^2-\theta_3^2\theta_2^2\theta_{10}^4)\\
&(-\theta_1^2\theta_8^4\theta_4^2-\theta_1^2\theta_{10}^4\theta_4^2+\theta_8^2\theta_2^2\theta_{10}^2\theta_4^2+\theta_1^2\theta_3^2\theta_8^2\theta_{10}^2)(-\theta_1^2\theta_8^2\theta_3^2\theta_4^2+\theta_1^2\theta_{10}^2\theta_4^2+\theta_1^2\theta_3^4\theta_{10}^2-\theta_3^2\theta_2^2\theta_{10}^2\theta_4^2)\\
&(-\theta_1^2\theta_8^2\theta_2^2\theta_4^2+\theta_1^4\theta_{10}^2\theta_4^2-\theta_1^2\theta_3^2\theta_2^2\theta_{10}^2+\theta_2^4\theta_4^2\theta_{10}^2)(-\theta_8^4\theta_2^2\theta_4^2+\theta_1^2\theta_8^2\theta_{10}^2\theta_4^2-\theta_2^2\theta_{10}^4\theta_4^2+\theta_3^2\theta_8^2\theta_2^2\theta_{10}^2)\\
&(\theta_1^4\theta_8^2\theta_4^2-\theta_1^2\theta_2^2\theta_4^2\theta_{10}^2-\theta_1^2\theta_3^2\theta_8^2\theta_2^2+\theta_8^2\theta_2^4\theta_4^2)(\theta_1^4\theta_3^2\theta_8^2-\theta_1^2\theta_8^2\theta_2^2\theta_4^2-\theta_1^2\theta_3^2\theta_2^2\theta_{10}^2+\theta_3^2\theta_8^2\theta_2^4)\\
&(\theta_1^2\theta_8^4\theta_3^2-\theta_1^2\theta_8^2\theta_{10}^2\theta_4^2+\theta_1^2\theta_3^2\theta_{10}^4-\theta_3^2\theta_8^2\theta_2^2\theta_{10}^2)(\theta_1^2\theta_8^2\theta_4^4-\theta_1^2\theta_3^2\theta_4^2\theta_{10}^2+\theta_1^2\theta_3^4\theta_8^2-\theta_3^2\theta_8^2\theta_2^2\theta_4^2)=0
\end{aligned}$$

This was done in [75]. We would like to express the conditions of the previous lemma in terms of the fundamental theta constants only.

Lemma 6. *Let $\mathcal{X}$ be a genus 2 curve. Then we have the following:*

i: *$V_4 \hookrightarrow Aut(\mathcal{X})$ if and only if the fundamental theta constants of $\mathcal{X}$ satisfy*

(20)
$$\begin{aligned}
&(\theta_3^4-\theta_4^4)\,(\theta_1^4-\theta_3^4)\,(\theta_2^4-\theta_4^4)\,(\theta_1^4-\theta_4^4)\,(\theta_3^4-\theta_2^4)\,(\theta_1^4-\theta_2^4)\\
&(-\theta_4^2+\theta_3^2+\theta_1^2-\theta_2^2)\,(\theta_4^2-\theta_3^2+\theta_1^2-\theta_2^2)\,(-\theta_4^2-\theta_3^2+\theta_2^2+\theta_1^2)\,(\theta_4^2+\theta_3^2+\theta_2^2+\theta_1^2)\\
&({\theta_1}^4{\theta_2}^4+{\theta_3}^4{\theta_2}^4+{\theta_1}^4{\theta_3}^4-2\,\theta_1^2\theta_2^2\theta_3^2\theta_4^2)\,(-{\theta_3}^4{\theta_2}^4-{\theta_2}^4{\theta_4}^4-{\theta_3}^4{\theta_4}^4+2\,\theta_1^2\theta_2^2\theta_3^2\theta_4^2)\\
&({\theta_2}^4{\theta_4}^4+{\theta_1}^4{\theta_2}^4+{\theta_1}^4{\theta_4}^4-2\,\theta_1^2\theta_2^2\theta_3^2\theta_4^2)\,({\theta_1}^4{\theta_4}^4+{\theta_3}^4{\theta_4}^4+{\theta_1}^4{\theta_3}^4-2\,\theta_1^2\theta_2^2\theta_3^2\theta_4^2)=0
\end{aligned}$$

ii: *$D_8 \hookrightarrow Aut(\mathcal{X})$ if and only if the fundamental theta constants of $\mathcal{X}$ satisfy Eq. (3) in [75]*

iii: *$D_6 \hookrightarrow Aut(\mathcal{X})$ if and only if the fundamental theta constants of $\mathcal{X}$ satisfy Eq. (4) in [75]*

Hence, one can determine very easily the automorphism group of the curve once its thetanulls are known. However, this is not quite easy since thetanulls are defined in terms of the complex integrals. However, since the Siegel modular forms are expressed in terms of the thetanulls as in Eq. (5), we should be able to express such loci in terms of the modular forms.

Instead, it is much easier to determine the automorphism groups in terms of the algebraic invariants which are given in terms of the coefficients of the curve, but are invariant of the equation of the curve. In the next section we will express such loci in terms of the absolute invariants i_1, i_2, i_3. Then, using formulas in Eq.(12) we can always express these equations in terms of the modular forms.

6.2. **Automorphisms in terms of algebraic invariants.** The locus of genus 2 curves with an extra involution is computed in [74, Theorem 3] in terms of J_2, J_4, J_6, J_{10}. It corresponds precisely to the locus $\det M = 0$.

Proposition 3. *Let $\mathfrak{p} \in \mathcal{M}_2$. The following hold:*

(1) *If $J_{30}(\mathfrak{p}) \neq 0$, then $|\operatorname{Aut}(\mathfrak{p})| = 2$ or $\mathfrak{p}$ correspond to the curve $y^2 = x(x^5-1)$. Moreover, $J_{30}(\mathfrak{p}) = 0$ if and only if $V_4 \hookrightarrow \operatorname{Aut}(\mathfrak{p})$.*
(2) *If $J_{30}(\mathfrak{p}) = 0$ and $J_{16}(\mathfrak{p}) = 0$, then $V_4 \hookrightarrow \overline{\operatorname{Aut}}(\mathfrak{p})$.*

Part i) was known to Clebsch and proved independently in [74, Theorem 3]. The proof of 2) can be found in [74, Lemma 3]. In the following proposition we give conditions on the absolute invariants i_1, i_2 and i_3 for each automorphism to happen.

Proposition 4. *Let $\mathfrak{p} = (i_1, i_2, i_3) \in \mathcal{M}_2 \setminus \{J_2 = 0\}$. Then the following hold:*

i) *If $\mathfrak{p} = (0, 0, 0)$ then $\operatorname{Aut}(\mathfrak{p}) \cong C_{10}$*
ii) *If $\mathfrak{p} = (\frac{81}{20}, -\frac{729}{200}, \frac{729}{25600000})$, then $\operatorname{Aut}(\mathfrak{p}) \cong SL_2(3)$*
iii) *If $\mathfrak{p} = (-\frac{36}{5}, \frac{1512}{25}, \frac{243}{200000})$, then $\operatorname{Aut}(\mathfrak{p}) \cong GL_2(3)$*
iv) *If the following conditions are satisfied*

$$
\begin{aligned}
&27i_2^4 - 9i_2^4 i_1 + 9459597312000 i_3^2 i_1^2 - 111451255603200 i_3^2 i_1 + 55240704 i_3 i_1^4 \\
&-161243136 i_3 i_1^3 + 27 i_1^6 + 2407347121029 12 i_3^2 + 264180754022400000 i_3^3 \\
&-9 i_1^7 + 18 i_2^2 i_1^4 - 54 i_1^3 i_2^2 - 161243136 i_3 i_2^2 + 12441600 i_3 i_2^3 - 107495424 i_3 i_2 i_1^2 \\
&+52254720 i_3 i_2^2 i_1 - 2 i_2 i_1^6 + 4 i_2^3 i_1^3 - 206391214080000 i_3^2 i_2 + 8294400 i_3 i_2^2 i_1^2 \\
&-331776 i_3 i_1^5 + 2866544640000 i_3^2 i_1 i_2 + 47278080 i_3 i_1^3 i_2 - 2 i_2^5 = 0 \\
&-243 i_1^2 + 80 i_1^3 - 1458 i_2 + 540 i_2 i_1 + 100 i_2^2 = 0
\end{aligned}
\tag{21}
$$

and $\mathfrak{p}$ is not one of the cases ii) and iii), then $\operatorname{Aut}(\mathfrak{p}) \cong D_4$

v) *If the following conditions are satisfied*

$$
\begin{aligned}
&3888 i_1 + 432 i_2 - 1188 i_1^2 + 5 i_1^3 - 25 i_2^2 - 360 i_2 i_1 = 0 \\
&26873856 i_3 + 5184000 i_3 i_1^2 - 9331200 i_3 i_1 - 149299200000 i_3^2 - 729 i_1^2 - \\
&27 i_1^4 + 243 i_1^3 + i_1^5 = 0
\end{aligned}
\tag{22}
$$

and $\mathfrak{p}$ is not one of the cases ii) and iii), then $\operatorname{Aut}(\mathfrak{p}) \cong D_6$

vi) *If the following is satisfied*

(23)
$$\begin{aligned}
&-27i_1^6 - 9459597312000i_3^2i_1^2 + 20639121408000i_3^2i_2 + 111451255603200i_3^2i_1\\
&-240734712102912i_3^2 - 55240704i_3i_1^4 - 18i_1^4i_2^2 - 8294400i_3i_2^2i_1^2 - 47278080i_3i_2i_1^3\\
&-264180754022400000i_3^3 - 2866544640000i_3^2i_2i_1 + 2i_1^6i_2 - 4i_1^3i_2^3 + 9i_1^7 + 331776i_3i_1^5\\
&+107495424i_3i_2i_1^2 - 27i_2^4 + 9i_1i_2^4 - 52254720i_3i_2^2i_1 + 2i_2^5 + 161243136i_3i_2^2\\
&+161243136i_3i_1^3 - 12441600i_3i_2^3 + 54i_1^3i_2^2 = 0
\end{aligned}$$

and $\mathfrak{p}$ *is not one of the above cases, then* $\mathrm{Aut}(\mathfrak{p}) \cong V_4$.

Proof. The proof is computational and straightforward. The reader can check [60] or [74] for details. □

If $\mathcal{X}$ has extra involutions (i.e. it has automorphisms other then the hyperelliptic involution), then X is isomorphic to a curve given by

$$y^2 = x^6 + ax^4 + bx^2 + 1 \tag{24}$$

for appropriate values of a, b (i.e. the discriminant is nonzero). Such form of genus 2 curves with automorphisms was know to XIX century mathematicians, but it has been used in the last decade quite often mostly due to Shaska and Völklein paper [74] which first appeared in 2000.

In [74] for curves with automorphism were defined the dihedral invariants

$$u := ab, \qquad v := a^3 + b^3 \tag{25}$$

which give a birational parametrization of this locus $\mathcal{L}_2$ which is a 2-dimensional subvariety of $\mathcal{M}_2$. It was the first time that such parametrization was discovered and since it has become the common way of computing with genus 2 curves with automorphisms. We can express u, and v in terms of the absolute invariants i_1, i_2, i_3 as in [74]. Moreover, the invariant J_{16} is expressed in terms of u, and v as follows

$$J_{16} = \left(4u^3 - v^2\right)\left(u^2 - 110\,u - 4\,v + 1125\right)^2$$

We have the following:

Proposition 5. *Let* $\mathfrak{p}$ *be a genus 2 curve such that* $G := \mathrm{Aut}(\mathfrak{p})$ *has an elliptic involution. Then,*

a) $G \cong SL_2(3)$ *if and only if* $(u, v) = (0, 0)$ *or* $(u, v) = (225, 6750)$.

b) $G \cong GL_2(3)$ *if and only if* $u = 25$ *and* $v = -250$.

c) $G \cong D_6$ *if and only if* $4v - u^2 + 110u - 1125 = 0$, *for* $u \neq 9, 70 + 30\sqrt{5}, 25$.

d) $G \cong D_4$ *if and only if* $v^2 - 4u^3 = 0$, *for* $u \neq 1, 9, 0, 25, 225$. *Cases* $u = 0, 225$ *and* $u = 25$ *are reduced to cases a),and b) respectively.*

The V_4-locus (i.e., the locus $J_{30} = 0$) is birationally parametrized by dihedral invariants u, v as in [74].

6.3. **The locus** $J_2 = 0$**.** If a point $p \in \mathcal{M}_2$ is in the locus $J_2 = 0$ then the following result holds true:

Proposition 6. *Let* $\mathfrak{p} = (0, t_1, t_2, t_3) \in \mathcal{M}_2$. *Then* $|\mathrm{Aut}(\mathfrak{p})| > 2$ *if and only if the invariants* t_2, t_3 *satisfy the Eq.* (34) *in the Appendix. Moreover,* $\mathrm{Aut}(\mathfrak{p}) \cong D_4$ *if and only if*

$$y^2 = x^5 + x^3 - \frac{3}{20}x$$

and $\mathrm{Aut}(\mathfrak{p}) \cong D_6$ *if and only if*

$$y^2 = x^6 + x^3 + -\frac{1}{40}$$

Proof. We let $\mathfrak{p}$ be a curve with extra automorphisms. Then its equation can be written as

$$y^2 = x^6 + ax^4 + bx^2 + 1$$

Compute t_2, t_3 in terms of the dihedral invariants u, v. Since $J_2 = 0$, then $u = 0$. Hence, t_2 and t_3 are expressed only in terms of v. Eliminate v and we get the equation in Eq. (34).

Assume that $\mathrm{Aut}(\mathfrak{p}) \cong D_4$. Then, the curve has equation

$$y^2 = x^5 + x^3 + sx,$$

cf. section 8.2. We then have

$$J_2 = 6 + 40s = 0$$

Hence, $s = -\frac{3}{20}$.

If $\mathrm{Aut}(\mathfrak{p}) \cong D_4$, then the equation of the curve is

$$y^2 = x^6 + x^3 + w,$$

cf. section 8.3. We then have

$$J_2 = 6 - 240w = 0$$

Hence, $w = -\frac{1}{40}$.

□

In the next section we will focus on genus two curves over $\mathbb{Q}$.

7. Genus 2 curves defined over $\mathbb{Q}$

Let $\mathcal{X}$ be a genus two curve defined over $\mathbb{Q}$. The moduli point in $\mathcal{M}_2$ corresponding to $\mathcal{X}$ is given by $\mathfrak{p} = (i_1, i_2, i_3)$. Since i_1, i_2, i_3 are rational functions in terms of the coeffiecients of $\mathcal{X}$, then $i_1, i_2, i_3 \in \mathbb{Q}$.

The converse isn't necessarily true. Let $\mathfrak{p} = (i_1, i_2, i_3) \in \mathcal{M}_2(\mathbb{Q})$. The universal equation of a genus 2 curve corresponding to $\mathfrak{p}$ is determined in [47], which is defined over a quadratic number field K. The main questions we want to consider is what percentage of the rational moduli points are defined over $\mathbb{Q}$? How can we determine a minimal equation for such curves?

The quotient space $C := \mathcal{X}/\mathrm{Aut}(\mathcal{X})$ is a genus zero curve, i.e. is isomorphic to a conic which is determined as follows. Let $\mathbf{x} = (x_1, x_2, x_3)$ be a coordinate in $\mathbb{P}^2$ and

$$C: \ \psi(x_1, x_2, x_3) := \mathbf{x}^t M \mathbf{x} \tag{26}$$

be the corresponding conic for the symmetric matrix M given as in Eq. (18).

There is also a cubic L given by the equation

$$L: \sum_{1 \le j,k,l \le 3} a_{jkl} x_j x_k x_l = 0 \tag{27}$$

where the coefficients a_{jkl} are given explicitly in terms of the invariants in [47].

Lemma 7 ([55]). *The genus 2 curve $\mathcal{X}$ is the intersection of the conic C and the cubic L.*

Mestre's algorithm has been implemented in Magma, Maple, Sage. For an implementation in Sage see Bouyer/Streng and their paper [16]. However, all these implementations have had issues. For example, the implementation in Sage will not work for curves with $J_2 = 0$.

Example 3. *Let $\mathcal{X}$ be the genus 2 curve given by the equation*

$$y^2 = x^6 + x^5 + x + 1/6.$$

One can check that for this curve the Igusa-Clebsch invariants are

$$[\,0,\ -32000,\ 5120000/3,\ 295116800000/81\,]$$

and the algorithm fails in this case.

Theorem 6. [47, Thm. 2] *For every point $\mathfrak{p} \in \mathcal{M}_2 \setminus \{D = 0\}$ such that $\mathfrak{p} \in \mathcal{M}_2(k)$, for some number field K, there is a pair of genus-two curves $\mathcal{C}^{\pm}$ given by*

$$\mathcal{C}^{\pm}: \quad y^2 = \sum_{i=0}^{6} a_{6-i}^{\pm}\, x^i\ ,$$

corresponding to $\mathfrak{p}$, such that $a_i^{\pm} \in K(d)$, $i = 0, \ldots, 6$ as given explicitly in [47, Eq. 41].

Proof. The proof is exactly the same as [47, Thm. 4], other then the fact that the coefficients are expressed in terms of i_1, i_2, i_3. We can take $J_2, \ldots, J_{10}$ as in Eq. (5.5). Substituting in formulas Eq. (B) we get,

(28)

$$\begin{aligned}
A &= -\frac{1}{120}\\
B &= \frac{1}{2^5 \cdot 3^5 \cdot 5^4}\,(36 + 5i_1)\\
C &= \frac{1}{2^8 \cdot 3^8 \cdot 5^6}\,(25i_2 + 180i_1 - 216)\\
D &= \frac{1}{2^{12} \cdot 3^{14} \cdot 5^{10}}\,(2700i_2 - 675i_1^2 - 250i_1i_2 - 86400000i_3 + 13500i_1 - 34992)
\end{aligned}$$

Then d^2 in [47] becomes

(29)

$$\begin{aligned}
d^2 = -\frac{1}{2^{50} \cdot 3^{56} \cdot 5^{30}}\,&(9i_1^7 + 2i_1^6i_2 - 27i_1^6 - 18i_1^4i_2^2 - 4i_1^3i_2^3 + 331776i_1^5i_3 + 54i_1^3i_2^2 + 9i_1i_2^4\\
&+ 2i_2^5 - 55240704i_1^4i_3 - 47278080i_1^3i_2i_3 - 8294400i_1^2i_2^2i_3 - 27i_2^4 + 161243136i_1^3i_3\\
&+ 107495424i_1^2i_2i_3 - 52254720i_1i_2^2i_3 - 12441600i_2^3i_3 - 9459597312000i_1^2i_3^2\\
&- 2866544640000i_1i_2i_3^2 + 161243136i_2^2i_3 + 111451255603200i_1i_3^2\\
&+ 20639121408000i_2i_3^2 - 264180754022400000i_3^3 - 240734712102912i_3^2)\cdot\\
&\cdot (675i_1^2 + 250i_1i_2 - 13500i_1 - 2700i_2 + 86400000i_3 + 34992)
\end{aligned}$$

Notice that d^2 has two significant factors: one is J_{30} which correspond exactly to the locus of the curves with extra involutions, and the other one is the Clebsch invariant D expressed in terms of i_1, i_2, i_3. Substituting A, B, C, D for the expressions in Eq. (28) we get $a_0, \ldots, a_6$ in terms of i_1, i_2, i_3 as in the Appendix. □

Remark 4. *Notice that the above theorem does not provide an equation for the curve if the Clebsch invariant $D = 0$.*

7.1. **Genus 2 curve with** $\mathrm{Aut}(\mathcal{X}) \cong V_4$**.** The above theorem is valid for any point $\mathfrak{p} \in \mathcal{M}_2$, including the points $\mathfrak{p} \in \mathcal{M}_2$ with $V_4 \hookrightarrow \mathrm{Aut}(\mathfrak{p})$. On contrary, Mestre's approach which has been implemented in many computer algebra packages is valid only for $\mathfrak{p} \in \mathcal{M}_2$ with $\mathrm{Aut}(\mathfrak{p}) \cong C_2$.

Let $\mathcal{X}$ be a genus 2 curve with $\mathrm{Aut}(\mathcal{X}) \cong V_4$. The V_4 locus has dimension two and is parametrized by the parameters u, and v as explained above. The rational model of a genus 2 curve with automorphism group V_4 given in terms of this parameters u, and v has equation given as follows

(30)
$$\begin{aligned} f(x,z) = &\left(v^2+u^2v-2\,u^3\right)x^6+2\,\left(u^2+3\,v\right)\left(v^2-4\,u^3\right)x^5z+\\ &+\left(15\,v^2-u^2v-30\,u^3\right)\left(v^2-4\,u^3\right)x^4z^2+4\,\left(5\,v-u^2\right)\left(v^2-4\,u^3\right)^2x^3z^3+\\ &+\left(v^2-4\,u^3\right)^2\left(15\,v^2-u^2v-30\,u^3\right)x^2z^4+2\,\left(v^2-4\,u^3\right)^3\left(u^2+3\,v\right)xz^5+\\ &+\left(v^2-4\,u^3\right)^3\left(v^2+u^2v-2\,u^3\right)z^6 \end{aligned}$$

where u, and v are expressed in terms of the absolute invariants (i_1, i_2, i_3) as in [74]. The discriminant of the form is

$$\Delta_f = 2^{36}\,\left(u^2+18\,u-4\,v-27\right)^2\left(4\,u^3-v^2\right)^{15}u^{30}.$$

The case $\Delta_f = 0$ correspond exactly to the cases when $|\,\mathrm{Aut}(\mathfrak{p})| > 4$ which is treated below. Notice that the factors 2 and u have exponents ≥ 30.

7.2. **Genus 2 curve with** $\mathrm{Aut}(\mathcal{X}) \cong D_4$**.** Let $\mathcal{X}$ be a genus 2 curve with $\mathrm{Aut}(\mathcal{X}) \cong D_4$. The D_4 locus is a dimension one locus parametrized by the parameter s, as proved in [61, Lemma 3]ants. The rational model of a genus 2 curve with automorphism group D_4 given in terms of this parameter s is as follows

$$y^2 = x^5 + x^3 + s\,x$$

where s can be expressed in terms of the absolute invariants (i_1, i_2, i_3) as follows

$$s = -\frac{3}{4}\frac{345\,i_1^2+50\,i_1i_2-1296i_1-90i_2}{2925i_1^2+250\,i_1i_2-54000i_1-9450i_2+139968}.$$

The discriminant is $\Delta_f = 2^4\cdot s^3\,(4\,s-1)^2$.

7.3. **Genus 2 curve with** $\mathrm{Aut}(\mathcal{X}) \cong D_6$**.** Now let us consider the case when $\mathcal{X}$ is a genus 2 curve with $\mathrm{Aut}(\mathcal{X}) \cong D_6$. The D_6 locus is a dimension one locus parametrized by the parameter w as proved in [61, Lemma 3]. The rational model of a genus 2 curve with automorphism group D_6 given in terms of this parameter w is as follows

$$y^2 = x^6 + x^3 + w$$

where the parameter w given in terms of the absolute invariants (i_1, i_2, i_3) is

$$w = \frac{1}{4}\frac{540i_1^2+100i_1i_2-1728i_1+45i_2}{2700i_1^2+1000i_1i_2+204525i_1+40950i_2-708588}$$

The discriminant of the form is $\Delta_f = -3^6\cdot w^2\,(4\,w-1)^3$.

Hence, for every point $\mathfrak{p} \in \mathcal{M}_2$ we can find an equation of a curve C corresponding to $\mathfrak{p}$. Below we give an example to illustrate how this work in our code in Sage.

Example 4. *Consider the curve*

$$y^2 = 4294967297\,t^6 + 77309411328\,t^5 + 579820584969\,t^4 + 2319282339816\,t^3 + 5218385264643\,t^2 + 6262062317592\,t + 3131031158771$$

By using the functions above we find that this curve has automorphism group D_6. Hence, we compute $w = 2^{33}$. The equation of a curve over $\mathbb{Q}$ isomorphic (over $\mathbb{C}$) to our curve is

$$y^2 = x^6 + x^3 + 2^{33}$$

In the next section we will see if we can transform this curve over $\mathbb{Q}$ to another curve with smaller coefficients.

In the next section we will see how to minimize the discriminant of a genus two curve when its equation is given in Weierstrass form.

8. Minimal discriminant for Weierstrass equations

Let K be a field with a discrete valuation $\mathfrak{v}$ and ring of integers $\mathcal{O}_K$ and C an irreducible, smooth, algebraic curve of genus $g \geq 1$ defined over K and function field $K(C)$. The discriminant $\mathfrak{D}_{C/K}$ is an important invariant of the function field of the curve and therefore of the curve. Since the discriminant is a polynomial given in terms of the coefficients of the curve, then it is an ideal in the ring of integers $\mathcal{O}_K$ of K. The valuation of this ideal is a positive integer. A classical question is to find an equation of the curve such that this valuation is minimal, in other words the discriminant is minimal.

When $g = 1$, so that C is an elliptic curve, there is an extensive theory of the minimal discriminant ideal $\mathfrak{D}_{C/K}$. Tate [80] devised an algorithm how to determine the Weierstrass equation of an elliptic curve with minimal discriminant as part of his larger project of determining Neron models for elliptic curves. Such ideas were extended for genus 2 in [43]. Here we mostly follow [58].

For a binary form $f(x, z)$ and a matrix $M = \begin{bmatrix} a, b \\ c, d \end{bmatrix}$, such that $M \in GL_2(k)$, we have that $f^M := f(aX + bZ, cX + dZ)$ has discriminant

$$\Delta(f^M) = (\det M)^{\frac{d(d-1)}{2}} \cdot \Delta(f)$$

This property of the discriminant is crucial in our algorithm which is explained later.

8.1. Discriminant of a curve.

The concept of a minimal discriminant for elliptic curves was defined by Tate and others in the 1970-s; see [80]. Such definitions and results were generalized by Lockhart in [44] for hyperelliptic curves.

Let us assume now that K is an algebraic number field with field of integers $\mathcal{O}_K$. Let M_K be the set of all inequivalent absolute values on K and M_K^0 the set of all non-archimedean absolute values in M_K. We denote by $K_\mathfrak{v}$ the completion of K for each $\mathfrak{v} \in M_K^0$ and by $\mathcal{O}_\mathfrak{v}$ the valuation ring in $K_\mathfrak{v}$. Let $\mathfrak{p}_v$ be the prime ideal in $\mathcal{O}_K$ and $\mathfrak{m}_v$ the corresponding maximal ideal in $K_\mathfrak{v}$. Let $(\mathcal{X}, P)$ be a superelliptic curve of genus $g \geq 2$ over K.

If $\mathfrak{v} \in M_K^0$ we say that $\mathcal{X}$ is **integral at** $\mathfrak{v}$ if $\mathcal{X}$ is integral when viewed as a curve over $K_\mathfrak{v}$. We say that $\mathcal{X}$ is **minimal at** $\mathfrak{v}$ when it is minimal over $K_\mathfrak{v}$.

An equation of $\mathcal{X}$ over K is called **integral** (resp. **minimal**) over K if it is integral (resp. minimal) over $K_\mathfrak{v}$, for each $\mathfrak{v} \in M_K^0$.

Next we will define the minimal discriminant over K to be the product of all the local minimal discriminants. For each $\mathfrak{v} \in M_K^0$ we denote by $\Delta_\mathfrak{v}$ the minimal discriminant for $(\mathcal{X}, P)$ over $K_\mathfrak{v}$. The **minimal discriminant** of $(\mathcal{X}, P)$ over K is the ideal

$$\Delta_{\mathcal{X}/K} = \prod_{\mathfrak{v} \in M_K^0} \mathfrak{m}_\mathfrak{v}^{\mathfrak{v}(\Delta_\mathfrak{v})}$$

We denote by $\mathfrak{a}_\mathcal{X}$ the ideal $\mathfrak{a}_\mathcal{X} = \prod_{\mathfrak{v} \in M_K^0} \mathfrak{p}_\mathfrak{v}^{\mathfrak{v}(\Delta_\mathfrak{v})}$.

Let $\mathcal{X}$ be a genus two curve with equation $y^2 = f(x)$. The discriminant of $\mathcal{X}$ is the discriminant of $f(x)$, hence $J_{10}(f)$, a degree 10 polynomial in terms of the coefficients of $f(x)$.

Let $M \in GL_2(K)$ such that $\det M = \lambda$. Then, $\Delta(f^M) = \lambda^{30}\,\Delta(f)$. Assume $\Delta(f) = p^\alpha \cdot N$, where $\alpha > 30$, for some prime p and some integer N such that $(p, N) = 1$. We perform the coordinate change

$$x \to \frac{1}{p} x$$

on $f(x)$. Then, the new discriminant is $\Delta' = \frac{1}{p^{30}} \cdot p^\alpha \cdot N = p^{\alpha-30} \cdot N$. Hence, we have the following

Lemma 8. *A genus 2 curve $\mathcal{X}_g$ with integral equation*

$$y^2 = a_6 x^6 + \cdots a_1 x + a_0$$

has minimal discriminant if $\mathfrak{v}(\Delta) < 30$.

Thus, we factor Δ as a product of primes, say $\Delta = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, and take u to be the product of those powers of primes with exponents $\alpha_i \geq 30$. Then, the transformation $x \mapsto \frac{1}{p^u} \cdot x$ will reduce the discriminant.

8.2. **Twists.** Of course we can make the discriminant as small as we want it if we allow twists.

Let $\mathcal{X}$ be hyperelliptic curve with an extra automorphism of order $n \geq 2$. Then, from [62] we know that the equation of $\mathcal{X}$ can be written as

$$y^2 = f(x^n)$$

If $\mathcal{X}$ is given with such equation over $\mathbb{Q}$ and discriminant

$$\Delta = u\,N, \quad \textit{such that} \quad (u, N) = 1$$

then for any transformation $\tau : x \mapsto u^{-\frac{n}{30}} \cdot x$ would lead to $\mathcal{X}^\tau$ defined over $\mathbb{Q}$ and isomorphic to $\mathcal{X}$ over $\mathbb{C}$. Hence, $\mathcal{X}^\tau$ is a twist of $\mathcal{X}$ with discriminant

$$\Delta' = \frac{1}{u} \cdot u\,N = N,$$

Hence, in this case we can reduce the discriminant even further.

Lemma 9. *Let $\mathcal{X}$ be a genus 2 curve with $\mathrm{Aut}(\mathcal{X}) \cong V_4$. Assume that $\mathcal{X}$ has equation over $\mathbb{Q}$ as $y^2 = f(x^2)$. Then, $\mathcal{X}$ has minimal discriminant Δ if $\mathfrak{v}(\Delta) < 15$.*

If $\mathrm{Aut}(\mathcal{X}) \cong D_6$ and $\mathcal{X}$ has equation over $\mathbb{Q}$ as $y^2 = f(x^3)$. Then, $\mathcal{X}$ has minimal discriminant Δ if $\mathfrak{v}(\Delta) < 10$.

Proof. The proof is an immediate consequence of the above remarks. □

The following gives a universal curve with minimal discriminant for the V_4-locus.

Lemma 10. *Let $\mathcal{X}$ be a genus 2 curve such that $\mathrm{Aut}(\mathcal{X}) \cong V_4$ and (u, v) the corresponding dihedral invariants. Then, $\mathcal{X}$ has minimal discriminant and is defined over its field of moduli when given by the equation*

$$y^2 = b_6 x^6 + \cdots + b_1 x + b_0 \tag{31}$$

where

$$\begin{aligned}
b_6 &= -\frac{\left(2\,u^3 - u^2 v - v^2\right)}{2^6 u^6} \\
b_5 &= -2\frac{\left(u^2 + 3\,v\right)\left(4\,u^3 - v^2\right)}{2^5 u^5} \\
b_4 &= \frac{\left(30\,u^3 + u^2 v - 15\,v^2\right)\left(4\,u^3 - v^2\right)}{2^4 u^4} \\
b_3 &= -4\,\frac{\left(u^2 - 5\,v\right)\left(4\,u^3 - v^2\right)^2}{2^3 u^3} \\
b_2 &= -\frac{\left(30\,u^3 + u^2 v - 15\,v^2\right)\left(4\,u^3 - v^2\right)^2}{2^2 u^2} \\
b_1 &= -\frac{\left(u^2 + 3\,v\right)\left(4\,u^3 - v^2\right)^3}{u} \\
b_0 &= \left(2\,u^3 - u^2 v - v^2\right)\left(4\,u^3 - v^2\right)^3
\end{aligned}$$

Proof. We know that the equation of the curve in Eq. (30) is defined over its field of moduli. Let

$$\sigma : (x, y) \mapsto \left(\frac{1}{2u}\,x, \frac{1}{(2u)^6}\,y\right).$$

Then the discriminant of the new curve $\mathcal{X}^\sigma$ is

$$\Delta_f = 2^6 \ \left(u^2 + 18\,u - 4\,v - 27\right)^2 \ \left(4u^3 - v^2\right)^{15}.$$

Since all exponents are < 15, this discriminant can not be further reduced over $\mathbb{Q}$. The equation of the curve in this case becomes as in Eq. (31).

□

Notice that for any curve $\mathcal{X}$ with $\mathrm{Aut}(\mathcal{X}) \cong V_4$, we have $u \neq 0$, so the curve in Eq. (31) is defined everywhere.

In the next section we will see that smaller discriminant doesn't necessarily mean small coefficients. We illustrate below with an example.

Example 5. *Let $u = 35$ and $v = 6$. Using the function*

```
RatModSha_uv (35, 6)
```

we get

```
(-4)*(19591*t^6+106564876*t^5-55428309960*t^4+35132884438720*t^3
+9503959738981440*t^2+313299704915023 1296*t-98758721142240034304)
```

Notice that this curve has large coefficients. Especially, when we have that for $u = 35$ and $v = 6$ we get corresponding $(a, b) = (2, 3)$ and therefore a curve

$$y^2 = x^6 + 2x^4 + 3x^3 + 1$$

As it is shown in [71], it is almost always true that the curve $y^2 = x^6 + ax^4 + bx^2 + 1$ has smaller coefficients when such $a, b \in \mathbb{Q}$ do exist.

9. Constructing the databases

Now that we have all the necessary results we are ready to construct all three dictionaries.

9.1. **Curves with height ≤ 10: the dictionary $\mathcal{L}_1$.** In order to create the list $\mathcal{L}_1$ we first compile a list of all 7-tuples $(a_0, \ldots, a_6)$ and from this list eliminate all the tuples with $J_{10} = 0$. Then, for each tuple we compute the moduli point $\mathfrak{p} = (i_1, i_2, i_3)$ and all the other invariants as described in the previous sections.

Table 1. The number of curves for a given height

h	$\mathbb{P}^6$	# of curves	V_4	D_4	D_6
1	1 093	230	28	11	2
2	37 969	8 593	230	40	7
3	409 585	88 836	1054	112	26

Remark 5. *The bound for the number of genus 2 curves of height* h *is* $< (2h+1)^7$. *For example, for* $\mathrm{h} = 1$ *this bound is* $< 3^7 = 2187$. *In fact, as shown in Table 1 the number of such curves is 230, all of which are listed in* [71, Table 2, 3].

In the Table 1 we display the number of curves with extra automorphism for a given height h.

9.2. **Curve with extra involutions: the dictionary $\mathcal{L}_2$.** The list $\mathcal{L}_2$ was computed in [71] for $1 \leq \mathrm{h} \leq 100$. Since every genus 2 curve with extra automorphisms can be written (over $\mathbb{C}$) as

$$y^2 = x^6 + ax^4 + bx^2 + 1 \tag{32}$$

we create the list of tuples $(1, 0, b, 0, a, 0, 1)$ for $a, b \leq \mathrm{h}$. We go through the lists and delete the ones which have $J_{10} = 0$. This number is displayed in [71, Table 1] for $1 \leq \mathfrak{h} \leq 100$, including information on how many points from $\mathcal{L}_2$ are already in $\mathcal{L}_1$, how many of these curves have automorphism group D_4 and how many have automorphism group D_6.

Table 2. Curves with extra involutions and height $\mathrm{h} \leq 101$

h	$J_{10} \neq 0$	new pts. in $\mathcal{M}_2$	D_4	D_6	Total pts
1	8	4	1	0	5
2	24	9	3	0	14
3	47	12	4	0	26
4	79	17	6	0	43
5	119	20	7	0	63
6	167	25	9	0	88
7	223	28	11	0	116
8	287	33	13	0	149
9	359	36	15	0	185
10	439	41	17	0	226

In [71] it is discussed when such curves have minimal height and how a reduction as in [2] is easier to perform in this case. In Table 2 we display only the first ten rows of Table 1 from [71].

There are 20 697 curves in $\mathcal{L}_2$, such that for each h we have roughly 4 h curves. So it is expected that the number of curves of height $\leq h$, with equation Eq. (32), defined over $\mathbb{Q}$ is $\leq 4\frac{\mathrm{h}(\mathrm{h}+1)}{2}$; see Beshaj [71] for more details.

The first curve with automorphism group isomorphic to D_4 occurs for $\mathrm{h} = 1$. It is only one such curve, namely the curve with equation

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

The are only two curves with automorphism group isomorphic to D_6, which occur for $\mathrm{h} = 79$ and $\mathrm{h} = 83$. namely the curve

$$y^2 = x^6 + 79x^4 - 17x^2 + 1$$

and the curve

$$y^2 = x^6 + 83x^6 + 19x^2 + 1.$$

There are 195 curves with automorphism group isomorphic to D_4. For the largest height $\mathrm{h} = 101$ there are 405 curves two of which have automorphism group isomorphic to D_4.

In [2] is proved the following theorem:

Theorem 7 ([2]). *Let $\mathfrak{p} \in \mathcal{M}_2(\mathbb{Q})$ be such that $\mathrm{Aut}(\mathfrak{p}) \cong V_4$. There is a genus 2 curve $\mathcal{X}$ corresponding to $\mathfrak{p}$ with equation $y^2 z^4 = f(x^2, z^2)$, where*

$$f(x, z) = x^6 - s_1 x^4 z^2 + s_2 x^2 z^4 - z^6. \tag{33}$$

If $f \in \mathbb{Z}[x, z]$, then $f(x, z)$ or $f(-z, x)$ is a reduced binary form.

It is interesting to not that from 20 292 such curves we found only 57 which do not have minimal absolute height. For more details see the discussion in the last section of [2].

9.3. **Curves with small moduli height: the dictionary $\mathcal{L}_3$.** For the last dictionary $\mathcal{L}_3$ we create a list of all points $[x_0 : x_1 : x_2 : x_3]$ of projective height $\leq \mathfrak{h}$ in $\mathbb{P}^3(\mathbb{Q})$, for some integer $\mathfrak{h} \geq 1$. Each such point correspond to the point $[J_2^5 : J_4 J_2^3 : J_6 J_2^2 : J_{10}]$. The number of such tuples (up to equivalence in $\mathbb{P}^3$) is given in column 2 of Table 3. Not all such points correspond to a genus 2 curve. We delete all the points such that $x_3 = 0$ since they correspond to the cases when $J_{10} = 0$. What is left on the list is the number of points in the moduli space $\mathcal{M}_2$ with moduli height $\leq \mathfrak{h}$. This number is given in the third column in the Table 3.

For each given point $\mathfrak{p} = (r, i_1, i_2, i_3)$ in this list we find the equation of the curves as described above. As we already know we don't get a curve defined over $\mathbb{Q}$ in each case. The number of points which are defined over $\mathbb{Q}$ is given in column four. From those points $\mathfrak{p} \in \mathcal{M}_2$ such that the field of definition is $\mathbb{Q}$, the number of points with automorphisms is given in column five.

The following question is natural: What percentage of rational points $\mathfrak{p} \in \mathcal{M}_2(\mathbb{Q})$ with a fixed moduli height $\mathfrak{h}$ have $\mathbb{Q}$ as a field of definition, when $\mathfrak{h}$ becomes arbitrarily large? In other words, what is the limit

$$\lim_{\mathfrak{h} \to \infty} \frac{n_3}{n_2}?$$

TABLE 3. Genus 2 curves with bounded moduli height

$\mathfrak{h}$	$\mathbb{P}^3(\mathbb{Q})$ n_1	$\mathfrak{p} \in \mathcal{M}_2(\mathbb{Q})$ n_2	$M_{\mathfrak{p}} = F_{\mathfrak{p}}$ n_3	$\lvert \operatorname{Aut}(\mathfrak{p})\rvert > 2$ n_4	ratio
1	40	27	20	15	0.25
2	272	223	124	75	0.4
3	1120	975	514	243	0.53
4	2928	2639	1311	507	0.61
5	6928	6351	3056	1035	0.66
6	12768	11903	5561	1587	0.71
7	23760	22319	9963	2667	0.73
8	38128	36111	15648	3771	0.76
9	60640	57759	24214	5427	0.78
10	88448	84703	34936	7107	0.8
11	131088	125903	50630	9867	0.81
12	177712	171375	68046	12123	0.82
13	248080	239727	93229	16011	0.83
14	324736	314655	120358	19395	0.84
15	427968	415583	157569	23907	0.85
16	542720	528031	199136	28419	0.86
17	700032	681887	252947	35139	0.86
18	857328	836591	307964	40251	0.87
19	1076928	1051871	381219	48675	0.87

Lemma 11. *For large enough moduli height $\mathfrak{h} \in \mathcal{M}_2(\mathbb{Q})$, the majority of genus 2 curves with moduli height $\mathfrak{h}$ are not defined over $\mathbb{Q}$.*

Proof. Let $\mathfrak{p} \in \mathcal{M}_2(\mathbb{Q})$ with moduli height $\mathfrak{h}_0$. Then, $\mathfrak{p} = (i_1, i_2, i_3)$ for $i_1, i_2, i_3 \in \mathbb{Q}$. The equation of a curve $\mathcal{X}$ corresponding to $\mathfrak{p}$ is the intersection of the conic $C: \ \psi(x_1, x_2, x_3) = 0$ and the cubic $L: \ \phi(x_1, x_2, x_3) = 0$ which are both defined over $\mathbb{Q}$, since their equations are given in terms of i_1, i_2, i_3. The intersection $C \cap L$ is obtained as the resultant of the corresponding equations with respect to one of the variables x_1, x_2, x_3. This resultant contains a square root which is given in terms of i_1, i_2, i_3; see [47]. $\mathcal{X}$ is defined over $\mathbb{Q}$ if and only if the expression inside the square root is a complete square. Since this is a surface in $\mathbb{Q}^3$, the set of points of fixed projective height which make it a complete square has measure zero. This completes the proof. □

Next we will consider a similar question. What percentage of curves defined over $\mathbb{Q}$ don't have extra automorphisms when $\mathfrak{h}$ becomes arbitrary large? In other words, what it the limit

$$\lim_{\mathfrak{h}\to\infty} \frac{n_3 - n_4}{n_3}?$$

Thus, we want to determine the ratio of points of height $\mathfrak{h}$ in $\mathcal{M}_2(\mathbb{Q})$ for which $M_{\mathfrak{p}} \neq F_{\mathfrak{p}}$ over the total number of points of height $\mathfrak{h}$ in $\mathcal{M}_2(\mathbb{Q})$ as $\mathfrak{h} \to \infty$.

Lemma 12. *For large enough moduli height $\mathfrak{h}$, the majority of genus 2 curves with moduli height $\mathfrak{h}$ don't have extra automorphisms.*

Proof. The number of points with height $\mathfrak{h}$ in the projective space increases as $\mathfrak{h}$ increases. However, such points $\mathfrak{p} = (i_1, i_2, i_3)$ have to satisfy the equation $J_{30} = 0$ when they have automorphisms. □

There is another database of genus 2 curves described in [15] which is has all the curves with discriminant < 1000. We checked our database to see how many of our curves would be with small discriminant. We have to warn the reader that our definition of the discriminant is just J_{10} and slightly different from what is used in [15]. The majority of curves in the third dictionary have small discriminant, but this is not a surprise since small moduli height forces J_{10} to be small. Only one curve in the second dictionary has $|J_{10}| < 1000$. Six curves in the first dictionary have $|J_{10}| < 10000$. It would be interesting to see exactly how the database in [13] and [15] intersect.

Appendix A. Functions of the genus 2 package

Genus 2 package

Input: a sextic polynomial $f(t)$

`J2`	Igusa invariant J_2
`J4`	Igusa invariant J_4
`J6`	Igusa invariant j_6
`J10`	Igusa invariant J_{10}
`J30`	J_{30}: the V_4-locus
`Igusa`	Igusa invariants $[J_2, J_4, J_6, J_{10}]$
`Clebsch`	Invariants [A, B, C, D]
`i_1`	absolute invariant i_1
`i_2`	absolute invariant i_2
`i_3`	absolute invariant i_3
`j1`	Igusa function j_1
`j2`	Igusa function j_2
`j3`	Igusa function j_3
`RatMod`	Rational model of the curve over when such model exists.
`RatModSha`	Rational model of the curve over its minimal field of definition as in Shaska [74]
`RatModMe`	Rational model over $\mathbb{Q}$, when such model exists, as in Mestre [55]
`height`	Height of the sextic
`EquivBin`	Checks if sextics are equivalent
`RatModTable`	Rational Model from the Table of minimal models
`MinField`	Minimal field of definition
`Info`	Displays information about the curve $y^2 = f(t)$
`RatForm`	Rational Model from Malmendier/Shaska [47]

Input: the moduli point (i_1, i_2, i_3)

`J30_j`	J_{30} in terms of i_1, i_2, i_3
`Igusa_i`	$J_2, \ldots, J_{10}$
`Clebsch_i`	Invariants [A, B, C, D]
`ClebschMatrix`	ClebschMatrix in terms of invariants i_1, i_2, i_3
`Cubic`	Cubic defined in Eq. (27)
`Conic`	Conic defined in Eq. (26)
`L_D4`	Locus of curves with group D_4
`L_D6`	Locus of curves with group D_6
`AutGroup`	Automorphism group of the curve
`Sh_u_v`	Shaska invariants u, v
`ModHeight`	Modular height

Moduli Space

`curves_moduli`	Computes the number of rational points of height $\mathfrak{h}$ in the moduli space and how many of those have a rational model
`NumbCurvMod`	This function computes the total number of rational points of moduli height $\mathfrak{h}$, how many of them have a rational model over $\mathbb{Q}$, how many of them have automorphisms and the ratio=obstruction/ fine points
`moduli_points`	Computes the number of rational points of height $\mathfrak{h}$ in the moduli space
`MoPtsCurvAut`	Moduli points with automorphisms

Creating the databases

`Curves(h, L)`	Creates the dictionary $\mathcal{L}_1$ of curves with height h
`CurvesAut(h, L)`	Creates the dictionary $\mathcal{L}_2$ of curves with automorphisms
`CurvHe`	Number of curves with height h
`SelfRec(f)`	Checks if a sextic is self reciprocal
`CurvHeW(h, w)`	Number of curves with height h and w
`NCWT(h, w)`	Number of curves with height h and twists w
`CurvesTabOverQ(h, w)`	Counts the number of curves over $\mathbb{Q}$, including twist, for given height.

Appendix B. Basic Invariants and relations among them

Clebsch invariants A, B, C are in terms of the coefficients

$$
\begin{aligned}
A =& \, 2\,a_6\,a_0 - \frac{1}{3}\,a_5\,a_1 + \frac{2}{15}\,a_4\,a_2 - \frac{1}{20}\,a_3^2 \\
B =& -\Big(\frac{4}{225}\,a_6\,a_2\,a_4\,a_0 - \frac{2}{75}\,a_6\,a_2\,a_3\,a_1 + \frac{8}{1125}\,a_6\,a_2^3 - \frac{2}{75}\,a_5\,a_3\,a_4\,a_0 \frac{2}{225}\,a_5 a_3^2\,a_1 \\
& - \frac{2}{1125}\,a_5\,a_3\,a_2^2 + \frac{8}{1125}\,a_4^3\,a_0 - \frac{2}{1125}\,a_4^2\,a_3\,a_1 + \frac{14}{5625}\,a_4^2\,a_2^2 - \frac{2}{225}\,a_5\,a_2\,a_4\,a_1 \\
& + \frac{2}{45}\,a_5^2\,a_2\,a_0 + \frac{2}{45}\,a_6\,a_1^2\,a_4 - \frac{2}{9}\,a_6\,a_1\,a_5\,a_0 - \frac{8}{5625}\,a_4\,a_3^2\,a_2 + \frac{2}{3}\,a_6^2\,a_0^2 \\
& + \frac{2}{75}\,a_6\,a_0\,a_3^2 + \frac{1}{3750}\,a_3^4\Big) \\
C =& -\frac{2}{46875}\,a_4^3\,a_2^3 - \frac{1}{5625}\,a_4^4\,a_1^2 - \frac{1}{5625}\,a_5^2\,a_2^4 - \frac{2}{9}\,a_6^3\,a_0^3 + \frac{11}{5625}\,a_6\,a_2\,a_3^2\,a_4\,a_0 \\
& - \frac{7}{1125}\,a_6\,a_2^2\,a_5\,a_0\,a_3 + \frac{4}{225}\,a_6\,a_2\,a_4\,a_1\,a_5\,a_0 - \frac{1}{562500}\,a_3^6 + \frac{8}{1125}\,a_6^2\,a_2^3\,a_0 \\
& - \frac{8}{28125}\,a_6\,a_2^4\,a_4 + \frac{1}{9375}\,a_6\,a_2^3\,a_3^2 + \frac{1}{5625}\,a_5\,a_3^4\,a_1 + \frac{1}{90}\,a_5^3\,a_3\,a_0^2 - \frac{2}{28125}\,a_5\,a_3^3\,a_2^2 \\
& - \frac{8}{28125}\,a_4^4\,a_2\,a_0 + \frac{8}{1125}\,a_4^3\,a_6\,a_0^2 + \frac{1}{9375}\,a_4^3\,a_3^2\,a_0 - \frac{2}{28125}\,a_4^2\,a_3^3\,a_1 - \frac{1}{225}\,a_4^2\,a_5^2\,a_0^2 \\
& - \frac{2}{140625}\,a_4^2\,a_3^2\,a_2^2 + \frac{1}{90}\,a_6^2\,a_1^3\,a_3 - \frac{1}{225}\,a_6^2\,a_1^2\,a_2^2 + \frac{2}{140625}\,a_4\,a_3^4\,a_2 - \frac{1}{3750}\,a_6\,a_0\,a_3^4 \\
& - \frac{1}{75}\,a_6^2\,a_0^2\,a_3^2 + \frac{14}{225}\,a_6^2\,a_2\,a_0^2\,a_4 - \frac{1}{3750}\,a_6\,a_2\,a_3^3\,a_1 - \frac{2}{45}\,a_6\,a_2\,a_5^2\,a_0^2 - \frac{1}{3750}\,a_5\,a_3^3\,a_4\,a_0 \\
& + \frac{1}{2250}\,a_5^2\,a_3^2\,a_0\,a_2 + \frac{7}{28125}\,a_5\,a_3\,a_4\,a_2^3 + \frac{1}{2250}\,a_5\,a_3\,a_4^2\,a_1^2 + \frac{7}{28125}\,a_4^3\,a_2\,a_3\,a_1 \\
& + \frac{2}{1125}\,a_4^3\,a_1\,a_5\,a_0 - \frac{1}{5625}\,a_5\,a_2^2\,a_4^2\,a_1 + \frac{2}{1125}\,a_5\,a_2^3\,a_6\,a_1 + \frac{1}{2250}\,a_5^2\,a_2^2\,a_3\,a_1 \\
& + \frac{1}{9}\,a_6^2\,a_1\,a_0^2\,a_5 + \frac{1}{2250}\,a_6\,a_1^2\,a_3^2\,a_4 - \frac{2}{45}\,a_6^2\,a_1^2\,a_0\,a_4 - \frac{2}{1875}\,a_6\,a_2^2\,a_4^2\,a_0 \\
& + \frac{1}{1875}\,a_6\,a_2^2\,a_4\,a_3\,a_1 - \frac{1}{75}\,a_6^2\,a_2\,a_0\,a_3\,a_1 + \frac{1}{1875}\,a_5\,a_3\,a_4^2\,a_2\,a_0 - \frac{1}{75}\,a_5\,a_3\,a_6\,a_0^2\,a_4 \\
& - \frac{7}{11250}\,a_5\,a_3^2\,a_4\,a_2\,a_1 + \frac{1}{90}\,a_5\,a_3^2\,a_6\,a_0\,a_1 - \frac{1}{225}\,a_5^2\,a_3\,a_4\,a_1\,a_0 \\
& - \frac{7}{1125}\,a_4^2\,a_6\,a_0\,a_3\,a_1 - \frac{1}{225}\,a_5\,a_2\,a_6\,a_1^2\,a_3
\end{aligned}
$$

Clebsch invariants A, B, C, D in terms of the Igusa invariants J_2, J_4, J_6, J_{10}

$$
\begin{aligned}
A =& \, -\frac{1}{2^3 3\cdot 5}\,J_2\,, \\
B =& \, \frac{1}{2^3 3^3 5^4}\left(J_2^2 + 20\,J_4\right)\,, \\
C =& \, -\frac{1}{2^5 3^5 5^6}\left(J_2^3 + 80\,J_2 J_4 - 600\,J_6\right)\,, \\
D =& \, -\frac{1}{2^8 3^9 5^{10}}\left(9\,J_2^5 + 700\,J_2^3 J_4 - 3600\,J_2^2 J_6 - 12400\,J_2 J_4^2 + 48000\,J_4\,J_6 + 10800000\,J_{10}\right)
\end{aligned}
$$

The entries of the Clebsch matrix M.

$$
\begin{aligned}
A_{11} &= 2\,C + \frac{1}{3}\,A\,B\,,\\
A_{22} &= A_{13} = D\,,\\
A_{33} &= \frac{1}{2}\,B\,D + \frac{2}{9}\,C\,(B^2 + A\,C)\,,\\
A_{23} &= \frac{1}{3}\,B\,(B^2 + A\,C) + \frac{1}{3}\,C\,(2\,C + \frac{1}{3}\,A\,B)\,,\\
A_{12} &= \frac{2}{3}\,(B^2 + A\,C)
\end{aligned}
$$

Igusa invariants J_2, J_4, J_6, J_{10} we display them below in terms of the coefficients

$$
\begin{aligned}
J_2 &= 6a_3^2 - 240a_0a_6 + 40a_1a_5 - 16a_2a_4\\
J_4 &= 48a_0a_4^3 + 48a_2^3a_6 + 4a_2^2a_4^2 + 1620a_0^2a_6^2 + 36a_1a_3^2a_5 - 12a_1a_3a_4^2 - 12a_2^2a_3a_5 + 300a_1^2a_4a_6\\
&\quad + 300a_0a_5^2a_2 + 324a_0a_6a_3^2 - 504a_0a_4a_2a_6 - 180a_0a_4a_3a_5 - 180a_1a_3a_2a_6 + 4a_1a_4a_2a_5\\
&\quad - 540a_0a_5a_1a_6 - 80a_1^2a_5^2\\
J_6 &= 176a_1^2a_5^2a_3^2 + 64a_1^2a_5^2a_4a_2 + 1600a_1^3a_5a_4a_6 + 1600a_1a_5^3a_0a_2 - 160a_0a_4^4a_2 - 96a_0^2a_4^3a_6\\
&\quad + 60a_0a_4^3a_3^2 + 72a_1a_3^4a_5 - 24a_1a_3^3a_4^2 - 119880a_0^3a_6^3 - 320a_1^3a_5^3 - 160a_2^4a_4a_6 - 96a_2^3a_0a_6^2\\
&\quad + 60a_2^3a_3^2a_6 - 24a_2^2a_3^3a_5 + 8a_2^2a_3^2a_4^2 - 900a_2^2a_1^2a_6^2 - 24a_2^3a_4^3 - 36a_2^4a_5^2 - 36a_1^2a_4^4\\
&\quad + 424a_0a_4^2a_2^2a_6 - 2240a_1^2a_5^2a_0a_6 + 2250a_1^3a_3a_6^2 + 492a_0a_4^2a_2a_3a_5 + 20664a_0^2a_4a_6^2a_2\\
&\quad + 3060a_0^2a_4a_6a_3a_5 - 468a_0a_4a_3^2a_2a_6 - 198a_0a_4a_3^3a_5 - 640a_0a_4a_2^2a_5^2 + 3472a_0a_4a_2a_5a_1a_6\\
&\quad - 18600a_0a_4a_1^2a_6^2 - 876a_0a_4^2a_1a_6a_3 + 492a_1a_3a_2^2a_4a_6 - 238a_1a_3^2a_2a_4a_5 + 76a_1a_3a_2a_4^3\\
&\quad + 3060a_1a_3a_0a_6^2a_2 + 1818a_1a_3^2a_0a_6a_5 + 26a_1a_3a_2^2a_5^2 - 1860a_1^2a_3a_2a_5a_6 + 330a_1^2a_3^2a_6a_4\\
&\quad + 76a_2^3a_4a_3a_5 - 876a_2^2a_0a_6a_3a_5 + 616a_2^3a_5a_1a_6 + 2250a_0^2a_5^3a_3 - 10044a_0^2a_6^2a_3^2\\
&\quad + 28a_1a_4^2a_2^2a_5 - 640a_1^2a_4^2a_2a_6 + 26a_1^2a_4^2a_3a_5 - 1860a_1a_4a_0a_5^2a_3 + 616a_1a_4^3a_0a_5\\
&\quad - 18600a_0^2a_5^2a_6a_2 + 59940a_0^2a_5a_6^2a_1 + 330a_0a_5^2a_3^2a_2 + 162a_0a_6a_3^4 - 900a_0^2a_5^2a_4^2\\
&\quad - 198a_1a_3^3a_2a_6\\
J_{10} &= a_6^{-1}Res_X\left(f, \frac{\partial f}{\partial X}\right)
\end{aligned}
$$

(34)

$$
\begin{aligned}
&t_2^6t_3 - 15265260t_2^5t_3 - 27949860t_2^4t_3^2 - 118098t_2^3t_3^3 + 14693280768t_2^5 + 93437786558880t_2^4t_3\\
&- 878290475269680t_2^3t_3^2 + 85811055510240t_2^2t_3^3 - 1139016237660t_2t_3^4 + 3486784401t_3^5\\
&- 223154201664000000t_2^4 - 2877286739295420000000t_2^3t_3 - 24696580101686910000000t_2^2t_3^2\\
&- 1098180181016955000000t_2t_3^3 - 70607384120250000t_3^4 + 13556617751088000000000000t_2^3\\
&+ 433843541357670112500000000t_2^2t_3 - 66256910147680796250000000t_2t_3^2\\
&+ 57191981137402500000000t_3^3 - 41178226418929800000000000000000t_2^2\\
&- 3270773656259838098437500000000000t_2t_3 - 231627523606480125000000000000000t_3^2\\
&+ 625394313737496337500000000000000000000t_2 + 469045735303122253125000000000000000000t_3\\
&- 379927045595529025031250000000000000000000000 = 0
\end{aligned}
$$

$$
\begin{aligned}
a_{111} &= \frac{2}{9}\,(A^2C - 6BC + 9D),\\
a_{112} &= \frac{1}{9}\,(2B^3 + 4ABC + 12C^2 + 3AD),
\end{aligned}
$$

$$
\begin{aligned}
a_{113} = a_{122} &= \frac{1}{9}\left(AB^3 + \frac{4}{3}A^2BC + 4B^2C + 6AC^2 + 3BD\right),\\
a_{123} &= \frac{1}{18}\left(2B^4 + 4AB^2C + \frac{4}{3}A^2C^2 + 4BC^2 + 3ABD + 12CD\right),\\
a_{133} &= \frac{1}{18}\left(AB^4 + \frac{4}{3}A^2B^2C + \frac{16}{3}B^3C + \frac{26}{3}ABC^2 + 8C^3 + 3B^2D + 2ACD\right),\\
a_{222} &= \frac{1}{9}\left(3B^4 + 6AB^2C + \frac{8}{3}A^2C^2 + 2BC^2 - 3CD\right),\\
a_{223} &= \frac{1}{18}\left(-\frac{2}{3}B^3C - \frac{4}{3}ABC^2 - 4C^3 + 9B^2D + 8ACD\right),\\
a_{233} &= \frac{1}{18}\left(B^5 + 2AB^3C + \frac{8}{9}A^2BC^2 + \frac{2}{3}B^2C^2 - BCD + 9D^2\right),\\
a_{333} &= \frac{1}{36}\left(-2B^4C - 4AB^2C^2 - \frac{16}{9}A^2C^3 - \frac{4}{3}BC^3 + 9B^3D + 12ABCD + 20C^2D\right)
\end{aligned}
$$

References

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

[2] ———, *Reduction theory of binary forms*, Advances on superelliptic curves and their applications, 2015, pp. 84–116. MR3525574

[3] ———, *Integral minimal weierstrass equations of genus 2 curves*, Algebraic curves and their fibrations in mathematical physics and arithmetic geometry, 2016.

[4] ———, *Integral models of binary forms with minimal height.*, Ph.D. Thesis, 2016.

[5] ———, *Minimal weierstrass equations for genus 2 curves* (201612), available at 1612.08318.

[6] L. Beshaj, A. Elezi, and T. Shaska, *Theta functions of superelliptic curves*, Advances on superelliptic curves and their applications, 2015, pp. 47–69. MR3525572

[7] L. Beshaj, V. Hoxha, and T. Shaska, *On superelliptic curves of level n and their quotients, I*, Albanian J. Math. **5** (2011), no. 3, 115–137. MR2846162

[8] L. Beshaj and T. Shaska, *Decomposition of some jacobian varieties of dimension 3*, Artificial intelligence and symbolic computation, 2015, pp. 193–204.

[9] L. Beshaj, T. Shaska, and C. Shor, *On Jacobians of curves with superelliptic components*, Riemann and Klein surfaces, automorphisms, symmetries and moduli spaces, 2014, pp. 1–14. MR3289629

[10] L. Beshaj, T. Shaska, and E. Zhupa, *The case for superelliptic curves*, Advances on superelliptic curves and their applications, 2015, pp. 1–14. MR3525570

[11] 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

[12] L. Beshaj and T. Yamauchi, *On prym varieties for the coverings of some singular plane curves* (201609), available at 1609.03981.

[13] Lubjana Beshaj and Tony Shaska, *Algebraic curves, http://www.algcurves.org*, 2017.

[14] Oskar Bolza, *On binary sextics with linear transformations into themselves*, Amer. J. Math. **10** (1887), no. 1, 47–70. MR1505464

[15] Andrew R. Booker, Jeroen Sijsling, Andrew V. Sutherland, John Voight, and Dan Yasaki, *A database of genus 2 curves over the rational numbers* (201602), available at 1602.03715.

[16] Florian Bouyer and Marco Streng, *Examples of CM curves of genus two defined over the reflex field*, LMS J. Comput. Math. **18** (2015), no. 1, 507–538. MR3376741

[17] Mariela Carvacho, enRubén A. Hidalgo, and ulSaúl Quispe, *Jacobian variety of generalized Fermat curves*, Q. J. Math. **67** (2016), no. 2, 261–284. MR3509993

[18] Francisco-Javier Cirre and enRubén A. Hidalgo, *Normal coverings of hyperelliptic real Riemann surfaces*, Riemann and Klein surfaces, automorphisms, symmetries and moduli spaces, 2014, pp. 59–75. MR3289633

[19] A. Clebsch and P. Gordan, *Theorie der Abelschen Functionen*, Physica-Verlag, Würzburg, 1967. Thesaurus Mathematicae, (Neudrucke wichtiger mathematischer Werke), Band 7. MR0485106

[20] Henri Cohen and Gerhard Frey, *Handbook of elliptic and hyperelliptic curve cryptography*, 2010.
[21] Artur Elezi and Tony Shaska, *Weight distributions, zeta functions and Riemann hypothesis for linear and algebraic geometry codes*, Advances on superelliptic curves and their applications, 2015, pp. 328–359. MR3525583
[22] P. Gaudry and É. Schost, *On the invariants of the quotients of the Jacobian of a curve of genus 2*, Applied algebra, algebraic algorithms and error-correcting codes (Melbourne, 2001), 2001, pp. 373–386. MR1913484
[23] Michael Griffin, Andreas Malmendier, and Ken Ono, SU(2)*-Donaldson invariants of the complex projective plane*, Forum Math. **27** (2015), no. 4, 2003–2023. MR3365787
[24] J. Gutierrez and T. Shaska, *Hyperelliptic curves with extra involutions*, LMS J. Comput. Math. **8** (2005), 102–115. MR2135032 (2006b:14049)
[25] R. A. Hidalgo and T. Shaska, *On the field of moduli of superelliptic curves* (2016), available at 1606.03160.
[26] enRubén A. Hidalgo, *Edmonds maps on the Fricke-Macbeath curve*, Ars Math. Contemp. **8** (2015), no. 2, 275–289. MR3322704
[27] Ruben A. Hidalgo and Pilar Johnson, *Field of moduli of generalized Fermat curves of type* $(k, 3)$ *with an application to non-hyperelliptic dessins d'enfants*, J. Symbolic Comput. **71** (2015), 60–72. MR3345315
[28] Ruben A. Hidalgo and ulSaúl Quispe, *Fields of moduli of some special curves*, J. Pure Appl. Algebra **220** (2016), no. 1, 55–60. MR3393450
[29] enRubén A. Hidalgo and Sebastian Reyes, *Fields of moduli of classical Humbert curves*, Q. J. Math. **63** (2012), no. 4, 919–930. MR2999991
[30] Ruben A. Hidalgo, anSebastián Reyes-Carocca, and María Elisa Valdés, *Field of moduli and generalized Fermat curves*, Rev. Colombiana Mat. **47** (2013), no. 2, 205–221. MR3199693
[31] Ruben A. Hidalgo and Rubí E. Rodríguez, *A remark on the decomposition of the Jacobian variety of Fermat curves of prime degree*, Arch. Math. (Basel) **105** (2015), no. 4, 333–341. MR3395480
[32] Jun-ichi Igusa, *Arithmetic variety of moduli for genus two*, Ann. of Math. (2) **72** (1960), 612–649. MR0114819
[33] ———, *On Siegel modular forms of genus two*, Amer. J. Math. **84** (1962), 175–200. MR0141643
[34] ———, *On Siegel modular forms genus two. II*, Amer. J. Math. **86** (1964), 392–412. MR0168805
[35] ———, *On the desingularization of Satake compactifications*, Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965), 1966, pp. 301–305. MR0217076
[36] ———, *On the graded ring of theta-constants. II*, Amer. J. Math. **88** (1966), 221–236. MR0200482
[37] ———, *A desingularization problem in the theory of Siegel modular functions*, Math. Ann. **168** (1967), 228–260. MR0218352
[38] ———, *Modular forms and projective invariants*, Amer. J. Math. **89** (1967), 817–855. MR0229643
[39] M. Izquierdo and T. Shaska, *Cyclic curves over the reals*, Advances on superelliptic curves and their applications, 2015, pp. 70–83. MR3525573
[40] V. Krishnamoorthy, T. Shaska, and H. Völklein, *Invariants of binary forms*, Progress in Galois theory, 2005, pp. 101–122. MR2148462 (2006b:13015)
[41] Michael Laska, *An algorithm for finding a minimal Weierstrass equation for an elliptic curve*, Math. Comp. **38** (1982), no. 157, 257–260. MR637305 (84e:14033)
[42] Kristin Lauter and Tonghai Yang, *Computing genus 2 curves from invariants on the Hilbert moduli space*, J. Number Theory **131** (2011), no. 5, 936–958. MR2772480
[43] Qing Liu, *Modèles entiers des courbes hyperelliptiques sur un corps de valuation discrète*, Trans. Amer. Math. Soc. **348** (1996), no. 11, 4577–4610. MR1363944 (97h:11062)
[44] P. Lockhart, *On the discriminant of a hyperelliptic curve*, Trans. Amer. Math. Soc. **342** (1994), no. 2, 729–752. MR1195511 (94f:11054)
[45] K. Magaard, T. Shaska, S. Shpectorov, and H. Völklein, *The locus of curves with prescribed automorphism group*, Sūrikaisekikenkyūsho Kōkyūroku **1267** (2002), 112–141. Communications in arithmetic fundamental groups (Kyoto, 1999/2001). MR1954371

[46] A. Malmendier and T. Shaska, *The satake sextic in elliptic fibrations on k3* (201609), available at 1609.04341.
[47] ———, *A universal pair of genus-two curves* (2016), available at 1607.08294.
[48] Andreas Malmendier, *The eigenvalue equation on the Eguchi-Hanson space*, J. Math. Phys. **44** (2003), no. 9, 4308–4343. MR2003960
[49] ———, *Donaldson invariants of* $\mathbb{C}\mathrm{P}^1 \times \mathbb{C}\mathrm{P}^1$ *and mock theta functions*, Commun. Number Theory Phys. **5** (2011), no. 1, 203–229. MR2833320
[50] ———, *The signature of the Seiberg-Witten surface*, Surveys in differential geometry. Volume XV. Perspectives in mathematics and physics, 2011, pp. 255–277. MR2815730
[51] ———, *Kummer surfaces associated with Seiberg-Witten curves*, J. Geom. Phys. **62** (2012), no. 1, 107–123. MR2854198
[52] Andreas Malmendier and David R. Morrison, *K3 surfaces, modular forms, and non-geometric heterotic compactifications*, Lett. Math. Phys. **105** (2015), no. 8, 1085–1118. MR3366121
[53] Andreas Malmendier and Ken Ono, *Moonshine for* M_{24} *and Donaldson invariants of* $\mathbb{C}\mathrm{P}^2$, Commun. Number Theory Phys. **6** (2012), no. 4, 759–770. MR3068406
[54] ———, SO(3)*-Donaldson invariants of* $\mathbb{C}\mathrm{P}^2$ *and mock theta functions*, Geom. Topol. **16** (2012), no. 3, 1767–1833. MR2967063
[55] J.-F. Mestre, *Construction de courbes de genre 2 a partir de leurs modules*, Effective methods in algebraic geometry **94 of Progr. Math.** ((Castiglioncello, 1990)), 313–334.
[56] E. Previato, T. Shaska, and G. S. Wijesiri, *Thetanulls of cyclic curves of small genus*, Albanian J. Math. **1** (2007), no. 4, 253–270. MR2367218 (2008k:14066)
[57] R. Sanjeewa and T. Shaska, *Determining equations of families of cyclic curves*, Albanian J. Math. **2** (2008), no. 3, 199–213. MR2492096 (2010d:14043)
[58] Rachel Shaska, *Equations of curves with minimal discriminant* (201407), available at 1407.7064.
[59] T. Shaska, *Curves of genus 2 with* (N, N) *decomposable Jacobians*, J. Symbolic Comput. **31** (2001), no. 5, 603–617. MR1828706
[60] ———, *Curves of genus two covering elliptic curves*, ProQuest LLC, Ann Arbor, MI, 2001. Thesis (Ph.D.)–University of Florida. MR2701993
[61] ———, *Genus 2 curves with* $(3, 3)$*-split Jacobian and large automorphism group*, Algorithmic number theory (Sydney, 2002), 2002, pp. 205–218. MR2041085
[62] ———, *Determining the automorphism group of a hyperelliptic curve*, Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, 2003, pp. 248–254 (electronic). MR2035219 (2005c:14037)
[63] ———, *Genus 2 fields with degree 3 elliptic subfields*, Forum Math. **16** (2004), no. 2, 263–280. MR2039100
[64] ———, *Some special families of hyperelliptic curves*, J. Algebra Appl. **3** (2004), no. 1, 75–89. MR2047637
[65] ———, *Genus two curves covering elliptic curves: a computational approach*, Computational aspects of algebraic curves, 2005, pp. 206–231. MR2182041 (2006g:14051)
[66] ———, *Subvarieties of the hyperelliptic moduli determined by group actions*, Serdica Math. J. **32** (2006), no. 4, 355–374. MR2287373
[67] ———, *Some open problems in computational algebraic geometry*, Albanian J. Math. **1** (2007), no. 4, 297–319. MR2367221
[68] ———, *Some remarks on the hyperelliptic moduli of genus 3*, Comm. Algebra **42** (2014), no. 9, 4110–4130. MR3200084
[69] ———, *Genus two curves with many elliptic subcovers*, Comm. Algebra **44** (2016), no. 10, 4450–4466. MR3508311
[70] T. Shaska and L. Beshaj, *The arithmetic of genus two curves*, Information security, coding theory and related combinatorics, 2011, pp. 59–98. MR2963126
[71] ———, *Heights on algebraic curves*, Advances on superelliptic curves and their applications, 2015, pp. 137–175. MR3525576
[72] T. Shaska and C. Shor, *The q-weierstrass points of genus 3 hyperelliptic curves with extra automorphisms*, arXiv preprint arXiv:1307.8177 (2013).
[73] ———, *Theta functions and symmetric weight enumerators for codes over imaginary quadratic fields*, Des. Codes Cryptogr. **76** (2015), no. 2, 217–235. MR3357243

[74] T. Shaska and H. Völklein, *Elliptic subfields and automorphisms of genus 2 function fields*, Algebra, arithmetic and geometry with applications (2000), 703–723.
[75] T. Shaska and G. S. Wijesiri, *Theta functions and algebraic curves with automorphisms*, Algebraic aspects of digital communications, 2009, pp. 193–237. MR2605301 (2011e:14057)
[76] T. Shaska, G. S. Wijesiri, S. Wolf, and L. Woodland, *Degree 4 coverings of elliptic curves by genus 2 curves*, Albanian J. Math. **2** (2008), no. 4, 307–318. MR2470579
[77] Goro Shimura, *On the field of rationality for an abelian variety*, Nagoya Math. J. **45** (1972), 167–178. MR0306215 (46 #5342)
[78] C. Shor and T. Shaska, *Weierstrass points of superelliptic curves*, Advances on superelliptic curves and their applications, 2015, pp. 15–46. MR3525571
[79] Michael Stoll and John E. Cremona, *On the reduction theory of binary forms*, J. Reine Angew. Math. **565** (2003), 79–99. MR2024647 (2005e:11091)
[80] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), 1975, pp. 33–52. Lecture Notes in Math., Vol. 476. MR0393039 (52 #13850)
[81] Paul van Wamelen, *Examples of genus two CM curves defined over the rationals*, Math. Comp. **68** (1999), no. 225, 307–320. MR1609658
[82] eAndré Weil, *The field of definition of a variety*, Amer. J. Math. **78** (1956), 509–524. MR0082726 (18,601a)
[83] Myungjun Yu, *Selmer ranks of twists of hyperelliptic curves and superelliptic curves.*, J. Number Theory **160** (2016), 148–185 (English).

Department of Mathematics, The University of Texas at Austin, Austin, TX 78712
E-mail address: beshaj@math.utexas.edu

Departamento de Matemática y Estadística, Universidad de La Frontera, Temuco, Chile.
E-mail address: ruben.hidalgo@ufrontera.cl

Department of Mathematics and Statistics, Oakland University, Mathematics and Science Center,, Rochester, MI 48309
E-mail address: kruk@oakland.edu

Department of Mathematics, Utah State University, Logan, UT 84322
E-mail address: andreas.malmendier@usu.edu

Departamento de Matemática y Estadística,, Universidad de La Frontera, Temuco, Chile.
E-mail address: saul.quispe@ufrontera.cl

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