

PLANE QUARTICS OVER \mathbb{Q} WITH COMPLEX MULTIPLICATION

PINAR KILIÇER, HUGO LABRANDE, REYNALD LERCIER,
CHRISTOPHE RITZENTHALER, JEROEN SIJSLING, AND MARCO STRENG

ABSTRACT. We give examples of smooth plane quartics over \mathbb{Q} with complex multiplication over $\overline{\mathbb{Q}}$ by a maximal order with primitive CM type. We describe the required algorithms as we go; these involve the reduction of period matrices, the fast computation of Dixmier–Ohno invariants, and reconstruction from these invariants. Finally, we discuss some of the reduction properties of the curves that we obtain.

INTRODUCTION

Abelian varieties with complex multiplication (CM) are a fascinating common ground between algebraic geometry and number theory, and accordingly have been studied since a long time ago. One of the highlights of their theoretical study was the proof of Kronecker’s *Jugendtraum*, which describes the ray class groups of imaginary quadratic fields in terms of the division points of elliptic curves. Hilbert’s twelfth problem asked for the generalization of this theorem to arbitrary number fields, and while the general version of this question is still open, Shimura and Taniyama [50] gave an extensive partial answer for CM fields by using abelian varieties whose endomorphism algebras are isomorphic to these fields. A current concrete application of the theory of CM abelian varieties is in public key cryptography, where one typically uses this theory to construct elliptic curves with a given number of points [8].

Beyond the theoretically well-understood case of elliptic curves, there are constructions of curves with CM Jacobians in both genus 2 [52, 60, 7] and 3 [27, 63, 33]. Note that in genus 2 every curve is hyperelliptic, which leads to a relatively simple moduli space; moreover, the examples in genus 3 that we know up to now are either hyperelliptic or Picard curves, which again simplifies considerations. This paper gives the first 19 conjectural examples of “generic” CM curves of genus 3, in the sense that the curves obtained are smooth plane quartics with trivial automorphism group. More precisely, it conjecturally completes the list of curves of genus 3 over \mathbb{Q} whose endomorphism rings over $\overline{\mathbb{Q}}$ are maximal orders of sextic fields (see Theorem 1.1). The other curves of genus 3 with such endomorphism rings are either hyperelliptic or Picard curves. The hyperelliptic ones were known to Weng [63], except for three curves that were computed by Balakrishnan, Ionica,

Date: February 12, 2018.

2010 Mathematics Subject Classification. 13A50, 14H25, 14H45, 14K22, 14Q05.

Key words and phrases. complex multiplication, genus 3, plane quartics, explicit aspects.

The third and fourth author acknowledge support from the CysMoLog “défi scientifique émergent” of the Université de Rennes 1. The authors would like to thank Enea Milio and the anonymous referee for various comments that were helpful for the improvement of the exposition.

Kılıçer, Lauter, Vincent, Somoza and Streng by using the methods and SAGEMATH implementation of [3, 2]. The Picard curves had all previously appeared in work by Koike-Weng [27] and Lario-Somoza [33].

To construct our curves, we essentially follow the classical path; first we determine the period matrices, then the corresponding invariants, then we reconstruct the curves from rational approximations of these invariants, and finally we heuristically check that the curves obtained indeed have CM by the correct order. In genus 3, however, all of these steps are somewhat more complicated than was classically the case.

The proven verification that the curves obtained indeed have CM by the correct order is left for another occasion; we restrict ourselves to a few remarks. First of all, there are no known equivalents in genus 3 of the results that bound the denominators of Igusa class polynomials [35]. In fact very little is known on the arithmetic nature of the Shioda and Dixmier–Ohno invariants that are used in genus 3, and a theoretical motivation for finding our list was to have concrete examples to aid with the generalization of the results in loc. cit.

Using the methods in [9] one could still verify the endomorphism rings of our curves directly; this has already been done for the simplest of our curves, namely

$$X_{15} : x^4 - x^3y + 2x^3z + 2x^2yz + 2x^2z^2 - 2xy^2z + 4xyyz^2 - y^3z + 3y^2z^2 + 2yz^3 + z^4 = 0.$$

The main restriction for applying these methods to the other examples is the time required for this verification. At any rate, the results in the final section of this paper are coherent with the existence of a CM structure with the given order.

The CM fields that give rise to our curves were determined by arithmetic methods in [22, 26]. This also gives us Riemann matrices that we can use to determine periods and hence the invariants of our quartic curves. However, we do need to take care to reduce our matrices in order to get good convergence properties for their theta values. The theory and techniques involved are discussed in Section 1.

With our reduced Riemann matrices in hand, we want to calculate the corresponding theta values. We will need these values to high precision so as to later recognize the corresponding invariants. The fast algorithms needed to make this feasible were first developed in [30] for genus 2; further improvements are discussed in Section 2.1. In the subsequent Section 2.2 we indicate how these values allow us to obtain the Dixmier–Ohno invariants of our smooth plane quartic curves. This is based on formulas obtained by Weber [62, 16].

The theory of reconstructing smooth plane quartics from their invariants was developed in [42] and is a main theme of Section 3. Equally important is the performance of these algorithms, which was substantially improved during the writing of this paper; starting from a reasonable tuple of Dixmier–Ohno invariants over \mathbb{Q} , we now actually obtain corresponding plane quartics over \mathbb{Q} with acceptable coefficients, which was not always the case before. In particular, we developed a “conic trick” which enables us to find conics with small discriminant in the course of Mestre’s reconstruction algorithms for general hyperelliptic curves (by loc. cit., the reconstruction methods for non-hyperelliptic curves of genus 3 reduce to Mestre’s algorithms for the hyperelliptic case). Section 3 discusses these and other speed-ups and the mathematical background from which they sprang. Without them, our final equations would have been too large to even write down.

We finally take a step back in Section 4 to examine the reduction properties of these curves, as well as directions for future work, before giving our explicit list of curves in Section 5.

1. RIEMANN MATRICES

Let A be a principally polarized abelian variety of dimension g over \mathbb{C} , such as the Jacobian $A = J(C)$ of one of the curves that we are looking for. Then by integrating over a symplectic basis of the homology and normalizing, the manifold A gives rise to a point τ in the Siegel upper half space \mathcal{H}_g , well-defined up to the action of the symplectic group $\mathrm{Sp}_{2g}(\mathbb{Z})$. The elements of \mathcal{H}_g are also known as *Riemann matrices*. In Section 1.1, we give the list, due to Kılıçer and Streng, of all fields K that can occur as endomorphism algebra of a simple abelian threefold over \mathbb{Q} with complex multiplication over \mathbb{Q} . In Section 1.2, we recall Van Wamelen's methods for listing all Riemann matrices with complex multiplication by the maximal order of a given field. In Section 1.3, we show how to reduce Riemann matrices to get Riemann matrices with better convergence properties.

1.1. The CM fields. Let A be an abelian variety of dimension g over a field k of characteristic 0, let K be a number field of degree $2g$ and let \mathcal{O} be an order in K . We say that A has CM by \mathcal{O} (over \bar{k}) if there exists an embedding $\mathcal{O} \rightarrow \mathrm{End}(A_{\bar{k}})$.

If A is simple over \bar{k} and has CM by the full ring of integers \mathcal{O}_K of K , then we have in fact $\mathcal{O}_K \cong \mathrm{End}(A_{\bar{k}})$ and K is a *CM field*, i.e., a totally imaginary quadratic extension K of a totally real number field F [32].

The *field of moduli* of a principally polarized abelian variety A/k is the residue field of the corresponding point in the moduli space of principally polarized abelian varieties. It is also the intersection of the fields of definition of A in \bar{k} [28, p.37]. In particular, if A is defined over \mathbb{Q} , then its field of moduli is \mathbb{Q} . The field of moduli of a curve or an abelian variety is not always a field of definition [48]. However, we have the following theorem.

Theorem 1.1. *There are exactly 37 isomorphism classes of CM fields K for which there exist principally polarized abelian threefolds A/\mathbb{Q} with field of moduli \mathbb{Q} and $\mathrm{End}(A) \cong \mathcal{O}_K$. The set of such fields is exactly the list of fields given in Table 1.*

For each such field K , there is exactly one such principally polarized abelian variety A up to \mathbb{Q} -isomorphism, and this variety is the Jacobian of a curve X of genus 3 defined over \mathbb{Q} . In particular, the abelian variety A itself is defined over \mathbb{Q} .

Proof. The first part, up to and including uniqueness of A , is exactly Theorem 4.1.1 of Kılıçer's thesis [22]. These 37 cases are listed in Table 1. Therefore we need only prove the statement on the field of definition, which can be done here directly from the knowledge of the CM field. By the theorem of Torelli [34, Appendix], k is a field of definition for the principally polarized abelian threefold A if and only if it is a field of definition for X . This implies that the field of moduli of X equals \mathbb{Q} , and we have to show that this field of moduli is also a field of definition.

In genus 3 all curves descend to their field of moduli, except for plane quartics with automorphism group $\mathbb{Z}/2\mathbb{Z}$ and hyperelliptic curves with automorphism group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (see [38, 40]). We finish by showing that neither of these occurs in Table 1. If $\mathbb{Q}(i)$ is a subfield of K , then by Weng [63, §4.4–4.5], the curve X is hyperelliptic with automorphism group containing $\mathbb{Z}/4\mathbb{Z}$, in which case it descends to its field of moduli. We therefore assume the contrary. If the curve X over \mathbb{Q} is

hyperelliptic, then its automorphism group is the group μ_K itself. Since this group is cyclic, it cannot be isomorphic to $\neq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and the curve X descends to its field of moduli. If X is non-hyperelliptic, then its automorphism group is $\mu_K/\{\pm 1\}$. Because of our assumption on K , this group is not isomorphic to $\mathbb{Z}/2\mathbb{Z}$, and again X descends to \mathbb{Q} . \square

Table 1 gives a list of cyclic sextic CM fields K , arranged as follows. Let K be such a field. Then it has an imaginary quadratic subfield k and totally real cubic subfield F . In Table 1, the number d_k is the discriminant of k ; the polynomial p_F is a defining polynomial for F . These two entries of the table define the field K . The number f_F is the conductor of F , and d_K is the discriminant of K . The entry $\#$ is the order of the automorphism group of the Jacobian of the corresponding curve, which is nothing but the number of roots of unity in K . The ‘‘Type’’ column indicates whether the conjectured model of the curve is hyperelliptic (H), Picard (P), or a plane quartic with trivial automorphism group (G). The ‘‘Curve’’ column gives a reference to the conjectured model over \mathbb{Q} of the curve. The cases 1, 2, 3, 5, . . . , 20 correspond to the smooth plane quartics X_i in Section 5.

In the hyperelliptic cases, curves can be reconstructed by applying the SAGE-MATH [58] code of Balakrishnan, Ionica, Lauter and Vincent [2] (based on [63, 3]) and MAGMA [5] functionality due to Lercier and Ritzenthaler for hyperelliptic reconstruction in genus 3 [37].

Some of these curves were already computed by Weng [63]. The final cases 4, 25, 26 were found by Balakrishnan, Ionica, Kılıçer, Lauter, Somoza, Streng and Vincent and will appear online soon. The Picard curves can be obtained as a special case of our construction, but are more efficiently obtained using the methods of Koike–Weng [27] and Lario–Somoza [33]. The rational models in [63, 27, 33] as well as those that can be obtained with [2, 37] are correct up to some precision over \mathbb{C} . In case 23, the hyperelliptic model was proved to be correct in Tautz–Top–Verberkmoes [57, Proposition 4]. The hyperelliptic model $y^2 = x^7 - 1$ for case 36 is a classical result (see Example (II) on page 76 in Shimura [49]) and the Picard model $y^3 = x^4 - x$ for case 37 is similar (e.g. Bouw–Cooley–Lauter–Lorenzo–Manes–Newton–Ozman [6, Lemma 5.1]); both can be proven by exploiting the large automorphism group of the curve.

Remark 1.2. In fact the curve in Case 4 also admits a hyperelliptic defining equation over \mathbb{Q} , which is not automatic; *a priori* it is a degree 2 cover of conic that we do not know to be isomorphic to \mathbb{P}^1 . However, in this case the algorithms in [9] show that the conjectural model obtained is correct, so that also in this case a hyperelliptic model exists over the field of moduli \mathbb{Q} .

In this paper, we construct models for the generic plane quartic cases.

1.2. Obtaining Riemann matrices from CM fields. Let \mathcal{L} be a lattice of full rank $2g$ in a complex g -dimensional vector space V . The quotient V/\mathcal{L} is a complex Lie group, called a *complex torus*. This complex manifold is an abelian variety if and only if it is projective, which is true if and only if there exists a *Riemann form* for \mathcal{L} , that is, an \mathbb{R} -bilinear form $E : V \times V \rightarrow \mathbb{R}$ such that $E(\mathcal{L}, \mathcal{L}) \subset \mathbb{Z}$ and such that the form

$$\begin{aligned} V \times V &\longrightarrow \mathbb{R} \\ (u, v) &\longmapsto E(u, iv) \end{aligned} \tag{1.3}$$

Case	$-d_k$	p_F	f_F	$-d_K$	h_K^*	#	Type	Curve
1	7	$X^3 + X^2 - 4X + 1$	13	$7^3 \cdot 13^4$	1	2	G	X_1 (§ 5)
2	7	$X^3 - 3X - 1$	3^2	$3^8 \cdot 7^8$	1	2	G	X_2 (§ 5)
3	7	$X^3 + 8X^2 - 51X + 27$	$7 \cdot 31$	$7^5 \cdot 31^4$	1	2	G	X_3 (§ 5)
4	7	$X^3 + 6X^2 - 9X + 1$	$3^2 \cdot 7$	$3^8 \cdot 7^5$	1	2	H	[2, 37] + see §1.1
5	7	$X^3 + X^2 - 30X + 27$	$7 \cdot 13$	$7^5 \cdot 13^4$	1	2	G	X_5 (§ 5)
6	7	$X^3 + 4X^2 - 39X + 27$	$7 \cdot 19$	$7^5 \cdot 19^4$	1	2	G	X_6 (§ 5)
7	7	$X^3 + X^2 - 24X - 27$	73	$7^3 \cdot 73^4$	4	2	G	X_7 (§ 5)
8	7	$X^3 + 2X^2 - 5X + 1$	19	$7^3 \cdot 19^4$	4	2	G	X_8 (§ 5)
9	8	$X^3 + X^2 - 4X + 1$	13	$2^9 \cdot 13^4$	1	2	G	X_9 (§ 5)
10	8	$X^3 + X^2 - 2X - 1$	7	$2^9 \cdot 7^4$	1	2	G	X_{10} (§ 5)
11	8	$X^3 + X^2 - 10X - 8$	31	$2^9 \cdot 31^4$	4	2	G	X_{11} (§ 5)
12	11	$X^3 + X^2 - 2X - 1$	7	$7^4 \cdot 11^3$	1	2	G	X_{12} (§ 5)
13	11	$X^3 + X^2 - 14X + 8$	43	$11^3 \cdot 43^4$	4	2	G	X_{13} (§ 5)
14	11	$X^3 + 2X^2 - 5X + 1$	19	$11^3 \cdot 19^4$	4	2	G	X_{14} (§ 5)
15	19	$X^3 + 2X^2 - 5X + 1$	19	19^5	1	2	G	X_{15} (§ 5)
16	19	$X^3 - 3X - 1$	3^2	$3^8 \cdot 19^3$	4	2	G	X_{16} (§ 5)
17	19	$X^3 + 9X^2 - 30X + 8$	$3^2 \cdot 19$	$3^8 \cdot 19^5$	1	2	G	X_{17} (§ 5)
18	19	$X^3 + 7X^2 - 66X - 216$	$13 \cdot 19$	$13^4 \cdot 19^5$	1	2	G	X_{18} (§ 5)
19	43	$X^3 + X^2 - 14X + 8$	43	43^5	1	2	G	X_{19} (§ 5)
20	67	$X^3 + 2X^2 - 21X - 27$	67	67^5	1	2	G	X_{20} (§ 5)
21	4	$X^3 + 2X^2 - 5X + 1$	19	$2^6 \cdot 19^4$	1	4	H	[63, §6 3rd ex.]
22	4	$X^3 - 3X - 1$	3^2	$2^6 \cdot 3^8$	1	4	H	[63, §6 2nd ex.]
23	4	$X^3 + X^2 - 2X - 1$	7	$2^6 \cdot 7^4$	1	4	H	[57] (also [63, §6 1st ex.])
24	4	$X^3 + X^2 - 10X - 8$	31	$2^6 \cdot 31^4$	4	4	H	[63, §6 4th ex.]
25	4	$X^3 + X^2 - 14X + 8$	43	$2^6 \cdot 43^4$	4	4	H	[2, 37] + see §1.1
26	4	$X^3 + 3X^2 - 18X + 8$	$3^2 \cdot 7$	$2^6 \cdot 3^8 \cdot 7^4$	4	4	H	[2, 37] + see §1.1
27	3	$X^3 + X^2 - 4X + 1$	13	$3^3 \cdot 13^4$	1	6	P	[27, 6.1(3)] (also [33, 4.1.3])
28	3	$X^3 + X^2 - 2X - 1$	7	$3^3 \cdot 7^4$	1	6	P	[27, 6.1(2)] (also [33, 4.1.2])
29	3	$X^3 + X^2 - 10X - 8$	31	$3^3 \cdot 31^4$	1	6	P	[27, 6.1(4)] (also [33, 4.1.4])
30	3	$X^3 + X^2 - 14X + 8$	43	$3^3 \cdot 43^4$	1	6	P	[27, 6.1(5)] (also [33, 4.1.5])
31	3	$X^3 + 3X^2 - 18X + 8$	$3^2 \cdot 7$	$3^9 \cdot 7^4$	1	6	P	[33, 4.2.1.1]
32	3	$X^3 + 6X^2 - 9X + 1$	$3^2 \cdot 7$	$3^9 \cdot 7^4$	1	6	P	[33, 4.2.1.2]
33	3	$X^3 + 3X^2 - 36X - 64$	$3^2 \cdot 13$	$3^9 \cdot 13^4$	1	6	P	[33, 4.2.1.3]
34	3	$X^3 + 4X^2 - 15X - 27$	61	$3^3 \cdot 61^4$	4	6	P	[33, 4.3.1]
35	3	$X^3 + 2X^2 - 21X - 27$	67	$3^3 \cdot 67^4$	4	6	P	[33, 4.3.2]
36	7	$X^3 + X^2 - 2X - 1$	7	7^5	1	14	H	$y^2 = x^7 - 1$
37	3	$X^3 - 3X - 1$	3^2	3^9	1	18	P	$y^3 = x^4 - x$

TABLE 1. CM fields in genus 3 whose maximal orders give rise to CM curves with field of moduli \mathbb{Q} , sorted by the order # of the group of roots of unity.

is symmetric and positive definite. The Riemann form is called a *principal polarization* if and only if the form E on \mathcal{L} has determinant equal to 1. We call a basis $(\lambda_1, \dots, \lambda_{2g})$ of \mathcal{L} *symplectic* if the matrix of E with respect to the basis is given in terms of $g \times g$ blocks as

$$\Omega_g = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}. \quad (1.4)$$

For every principal polarization, there exists a symplectic basis. If we write out the elements of a symplectic basis as column vectors in terms of a \mathbb{C} -basis of V , then we get a $g \times 2g$ *period matrix*.

The final g elements of a symplectic basis of \mathcal{L} for E form a \mathbb{C} -basis of V , so we use this as our basis of V . Then the period matrix takes the form $(\tau \mid I_g)$, where the $g \times g$ complex matrix τ has the following properties:

- (1) τ is symmetric,
- (2) $\text{Im}(\tau)$ is positive definite.

The set of such matrices forms the Siegel upper half space \mathcal{H}_g . Conversely, from every Riemann matrix τ , we get the complex abelian variety

$$\mathbb{C}^g / (\tau\mathbb{Z}^g + \mathbb{Z}^g) \quad (1.5)$$

which we can equip with a Riemann form given by Ω_g with respect to the basis given by the columns of $(\tau \mid I_g)$.

Given a CM field K , Algorithm 1 of Van Wamelen [60] (based on the theory of Shimura–Taniyama [50]) computes at least one Riemann matrix for each isomorphism class of principally polarized abelian variety with CM by the maximal order of K . For details, and an improvement which computes *exactly* one Riemann matrix for each isomorphism class, see also Streng [55, 54]. In our implementation, we could simplify the algorithm slightly, because the group appearing in Step 2 of [60, Algorithm 1] is computed by Kılıçer [22, Lemma 4.3.4] for the fields in Table 1.

1.3. Reduction of Riemann matrices. There is an action on the Siegel upper half space \mathcal{H}_g by the symplectic group

$$\text{Sp}_{2g}(\mathbb{Z}) = \{M \in \text{GL}_{2g}(\mathbb{Z}) : M^t \Omega_g M = \Omega_g\}, \quad (1.6)$$

given by

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} (\tau) = (A\tau + B)(C\tau + D)^{-1}. \quad (1.7)$$

The isomorphism class of principally polarized abelian variety $(\mathbb{C}^g / (\tau\mathbb{Z}^g + \mathbb{Z}^g), \Omega_g)$ of Section 1.2 depends only on the orbit of τ under the action of $\text{Sp}_{2g}(\mathbb{Z})$, so we change τ into an $\text{Sp}_{2g}(\mathbb{Z})$ -equivalent matrix on which the theta constants have faster convergence. For this, we use [31, Algorithm 2 in §4.1]. To avoid numerical instability, we replace the condition $|\tau'_{1,1}| \leq 1$ in Step 3 of loc. cit. by $|\tau'_{1,1}| < 0.99$. The result of this reduction then is a matrix $\tau \in \mathcal{H}_g$ such that the real parts of all entries have absolute value $\leq \frac{1}{2}$, such that the upper left entry has absolute value $|\tau_{1,1}| \geq 0.99$ and such that the imaginary part $Y = \text{Im}(\tau)$ is *Minkowski-reduced*, i.e.,

- (a) for all $j = 1, \dots, g$ and all $v = (v_1, \dots, v_g) \in \mathbb{Z}^g$ with $\gcd(v_j, \dots, v_g) = 1$, we have ${}^t v Y v \geq Y_{jj}$, and
- (b) for all $j = 1, \dots, g-1$, we have $Y_{jj+1} \geq 0$.

For example, taking $i \neq j$ and $v = e_i \pm e_j$ in (a) gives $Y_{ii} \pm 2Y_{ij} \geq 0$, while taking $j = 1$ and $v = e_i$ in (a) gives $Y_{ii} \geq Y_{11}$, so

$$|Y_{ij}| \leq \frac{1}{2} Y_{ii}, \quad Y_{11} \leq Y_{ii}. \quad (1.8)$$

We also have

$$\text{Im}(\tau_{1,1}) \geq \sqrt{0.99^2 - 0.5^2} > 0.85. \quad (1.9)$$

We have implemented this algorithm, as well as a version with Minkowski reduction replaced by LLL reduction, which scales better with g than Minkowski reduction. For a self-contained exposition including a proof that the LLL-version of the algorithm terminates, see the first arXiv version¹ of our paper, and for an alternative approach with LLL reduction, see Deconinck, Heil, Bobenko, van Hoeij, and Schmies [10].

¹ <https://arxiv.org/abs/1701.06489v1>

1.4. Conclusion and efficiency. It takes only a minute to compute the reduction with either the Minkowski or the LLL version of the reduction algorithm for all our Riemann matrices. We did not notice any difference in efficiency of numerical evaluations of Dixmier–Ohno invariants (as in Section 2) between the Minkowski-version of the reduction and the LLL-version of the reduction. Without reduction, we were unable to do the computations to sufficient precision for reconstructing all the curves. We conclude that for $g = 3$, there is no reason to prefer one of these algorithms over the other, but it is very important to use at least one of them. We do advise caution with the LLL-version, as the analysis in Section 2 below is valid only for Minkowski-reduced matrices.

2. COMPUTING THE DIXMIER–OHNO INVARIANTS

In this section, we show how given a Riemann matrix τ we can obtain an approximation of the Dixmier–Ohno invariants of a corresponding plane quartic curve. One procedure has been described in [20] and relies on the computation of derivatives of odd theta functions. Here we take advantage of the existence of fast strategies to compute the Thetanullwerte to emulate the usual strategy for such computations in the hyperelliptic case [63, 3]: we use an analogue of the Rosenhain formula to compute a special *Riemann model* for the curve from the Thetanullwerte, from which we then calculate an approximation of the Dixmier–Ohno invariants. By normalizing these, we find an explicit conjectural representative of the Dixmier–Ohno invariants as an element of a weighted projective space over \mathbb{Q} .

2.1. Fast computation of the Thetanullwerte from a Riemann matrix.

Definition 2.1. The *Thetanullwerte* or *theta-constants* of a Riemann matrix $\tau \in \mathcal{H}_3$ are defined as

$$\vartheta_{[a;b]}(0, \tau) = \sum_{n \in \mathbb{Z}^3} e^{i\pi(t(n+a)\tau(n+a) + 2^t(n+a)b)}, \quad (2.2)$$

where $a, b \in \{0, 1/2\}^3$. We define the *fundamental Thetanullwerte* to be those $\vartheta_{[a;b]}$ with $a = 0$; there are 8 of them.

In many applications, only the 36 so-called *even* Thetanullwerte are considered, which are those for which the dot product $4a \cdot b$ is even. The other Thetanullwerte turn out to always be equal to 0.

We further simplify notation by writing

$$\vartheta_{[a;b]} = \vartheta_i, \quad i = 2(b_0 + 2b_1 + 4b_2) + 2^4(a_0 + 2a_1 + 4a_2) \quad (2.3)$$

In other words, we number the Thetanullwerte by interpreting the reverse of the sequence $(2b||2a)$ as a binary expansion. This is the numbering used in, e.g., [13, 30]. For notational convenience, we write $\vartheta_{n_1, \dots, n_k}$ for the k -tuple $\vartheta_{n_1}, \dots, \vartheta_{n_k}$. In this section, we describe a fast algorithm to compute the Thetanullwerte with high precision. Note that it is sufficient to describe an algorithm that computes the fundamental Thetanullwerte; we can then compute the squares of all 64 Thetanullwerte by computing the fundamental ones at $\tau/2$, then use the following τ -duplication formula [21, Chap. IV]:

$$\vartheta_{[a;b]}(0, \tau)^2 = \frac{1}{2^3} \sum_{\beta \in \frac{1}{2}\mathbb{Z}^3/\mathbb{Z}^3} e^{-4i\pi^t a\beta} \vartheta_{[0;b+\beta]} \left(0, \frac{\tau}{2}\right) \vartheta_{[0;\beta]} \left(0, \frac{\tau}{2}\right). \quad (2.4)$$

We can then recover the 64 Thetanullwerte from their squares, by using a low-precision approximation of their value to decide on the appropriate square root. Both algorithms described in this subsection have been implemented in MAGMA [29].

2.1.1. Naive algorithm for the Thetanullwerte. A (somewhat) naive algorithm to compute the Thetanullwerte consists in computing the sum in Definition 2.1 until the remainder is too small to make a difference at the required precision. We show in this section that it is possible to compute the genus 3 Thetanullwerte up to precision P (that is, up to absolute difference of absolute value at most 10^{-P}) by using $O(\mathcal{M}(P)P^{1.5})$ bit operations. Here $\mathcal{M}(P)$ is the number of bit operations needed for one multiplication of P -bit integers. This running time is the same as for the general strategy given in [11], as analyzed in [30, Section 5.3].

Let $t_{m,n,p} = e^{i\pi(m,n,p)\tau^t(m,n,p)}$, so $\vartheta_0(\tau) = \sum_{m,n,p \in \mathbb{Z}} t_{m,n,p}$. Our algorithm computes the approximation

$$S_B = \sum_{m,n,p \in [-B,B]} t_{m,n,p} \quad (2.5)$$

of $\vartheta_0(\tau)$. The main idea is to use the following recurrence relation. Let $q_{jk} = e^{i\pi\tau_{jk}}$. Then we have

$$\begin{aligned} t_{m+1,n,p} &= t_{m,n,p} q_{11}^{2m} q_{11}^{2n} q_{12}^{2p} q_{13}, \\ t_{m,n+1,p} &= t_{m,n,p} q_{22}^{2m} q_{22}^{2n} q_{12}^{2p} q_{23}, \\ t_{m,n,p+1} &= t_{m,n,p} q_{33}^{2p} q_{33}^{2n} q_{23}^{2m} q_{13}. \end{aligned} \quad (2.6)$$

Algorithm 2.7 (Given a period matrix $\tau \in \mathcal{F}_3(\{N\})$ and a bound B , compute S_B).

- (i) $S_B \leftarrow t_{0,0,0} = 1$.
- (ii) For $m = 1, 2, \dots, B$ and $m = -1, -2, \dots, -B$:
- (iii) Compute $t_{m,0,0}$ using the recursion and add it to S_B .
- (iv) For $n = 1, 2, \dots, B$ and $n = -1, -2, \dots, -B$:
- (v) Compute $t_{m,n,0}$ using the recursion and add it to S_B .
- (vi) For $p = 1, 2, \dots, B$ and $p = -1, -2, \dots, -B$:
- (vii) Compute $t_{m,n,p}$ using recursion and add it to S_B .
- (viii) Return S_B .

This algorithm can be modified to compute approximations of any fundamental Thetanullwerte $\vartheta_{[0,b]}$ by adjusting the sign of each term (with a factor $(-1)^{(m,n,p) \cdot b}$). Hence, the computation of S_B reduces to the computation of the q_i and the use of the recursion relations to compute each term. We prove in the rest of the section that, for this algorithm to compute ϑ_0 up to 2^{-P} , taking $B = O(\sqrt{P})$ is sufficient. That is, we prove that

$$|\vartheta_0(\tau) - S_B| < 2^{-P} \quad \text{for an easily computable } B = O(\sqrt{P}). \quad (2.8)$$

This allows the computation of the genus 3 Thetanullwerte in $O(\mathcal{M}(P)P^{1.5})$; we refer to our implementation [29] of the naive algorithm for full details.

Our analysis is similar to the ones in [13, 30]. We use the following lemma, of which we defer the proof until the end of §2.1.1.

Lemma 2.9. *Let $Y = (Y_{ij})_{ij}$ be a Minkowski-reduced 3×3 positive definite symmetric real matrix. Then for all $n \in \mathbb{R}^3$ we have ${}^t n Y n \geq \frac{1}{100} Y_{11} {}^t n n$.*

Note that by (1.9), we have $\frac{1}{100}Y_{11} \geq 0.0085$. For the theoretical complexity bound $O(\sqrt{P})$, it will suffice to use this lemma as it is. However, for a practical algorithm, the $\frac{1}{100}Y_{11}$ is far from optimal, and we use the following better constant. Let

$$c_1 = \min(Y_{11} - Y_{12} - |Y_{13}|, Y_{22} - Y_{21} - Y_{23}, Y_{33} - Y_{32} - |Y_{31}|), \quad \text{and}$$

$$c = \max\left(c_1, \frac{1}{100}Y_{11}\right) \geq \frac{1}{100}Y_{11} \geq 0.0085,$$

which in practice tends to be much larger than $\frac{1}{100}Y_{11}$.

Lemma 2.10. *Let $Y = (Y_{ij})_{ij}$ be a Minkowski-reduced 3×3 positive definite symmetric real matrix. Then for all $n \in \mathbb{R}^3$ we have ${}^t n Y n \geq c {}^t n n$.*

Proof. In case $c = \frac{1}{100}Y_{11}$, use Lemma 2.9. Otherwise, we have $c = c_1$. Now, for $(m, n, p) \in \mathbb{R}^3$, using the inequalities $2|mn| \leq (m^2 + n^2)$ and $Y_{12}, Y_{23} \geq 0$ we have

$$\begin{aligned} \operatorname{Im}({}^t(m, n, p)\tau(m, n, p)) &\geq \\ (Y_{11} - Y_{12} - |Y_{13}|)m^2 + (Y_{22} - Y_{21} - Y_{23})n^2 + (Y_{33} - Y_{32} - |Y_{31}|)p^2 &\geq \\ c_1(m^2 + n^2 + p^2). &\quad \square \end{aligned}$$

Now we prove the complexity result (2.8). By Lemma 2.10, we have

$$\begin{aligned} |\vartheta_0(0, \tau) - S_B| &\leq 8 \sum_{\substack{m \text{ or } n \text{ or } p \geq B \\ \text{and } m, n, p \geq 0}} e^{-\pi c(m^2 + n^2 + p^2)} \\ &\leq 24 \sum_{m \geq B, n \geq 0, p \geq 0} e^{-\pi c(m^2 + n^2 + p^2)} \\ &\leq 24 \frac{e^{-\pi c B^2}}{(1 - e^{-\pi c})^3} \leq \exp(14.09 - \pi c B^2), \end{aligned} \quad (2.11)$$

since we have an absolute lower bound $c \geq 0.0085$. Therefore taking

$$B = \sqrt{(P \log(2) + 14.09)/(\pi c)} = O(\sqrt{P})$$

is enough to ensure that S_B is within 2^{-P} of ϑ_0 . This proves our complexity estimates for Algorithm 2.7, when combined with the following deferred proof.

Proof of Lemma 2.9. Suppose there is an $n \in \mathbb{R}^3$ with ${}^t n Y n < \frac{1}{100}Y_{11} {}^t n n$. Let $I \in \{1, 2, 3\}$ be such that $n_I^2 = \max_i n_i^2$. Let $\{I, J, K\} = \{1, 2, 3\}$. Without loss of generality, we have $Y_{II} = 1$ (scale Y) and $n_I = 1$ (scale n). Then $|n_i| \leq n_I = 1$ and $Y_{11} \leq Y_{II} = 1$.

Let $s_{ij} = s_{ji} = 1$ if $Y_{ij} \geq 0$ and $s_{ij} = s_{ji} = -1$ if $Y_{ij} < 0$. We get

$$\frac{3}{100} \geq \frac{1}{100}Y_{11} {}^t n n > {}^t n Y n = \sum_i n_i^2 (Y_{ii} - \sum_{j \neq i} |Y_{ij}|) + \sum_{\substack{\{i, j\} \\ \text{s.t. } i \neq j}} (n_i + s_{ij} n_j)^2 |Y_{ij}|. \quad (2.12)$$

By (1.8), we have $|Y_{ij}| \leq \frac{1}{2}Y_{ii}$, so all terms on the right hand side are non-negative.

We distinguish between three cases: I , $II+$ and $II-$.

Case I: There exists a $j \neq I$ with $s_{Ij} n_j > -\frac{3}{4}$.

Case $II\pm$: For all $j \neq I$, we have $s_{Ij} n_j \leq -\frac{3}{4}$ and $s_{13} = \pm 1$.

Proof in case I. Without loss of generality $j = J$. We take two terms from (2.12):

$$\begin{aligned} 0.03 &\geq (Y_{II} - |Y_{IJ}| - |Y_{IK}|) + (1 + s_{IJ}n_J)^2|Y_{IJ}| \\ &\geq Y_{II} + (-1 + (1/4)^2)|Y_{IJ}| - |Y_{IK}| \geq (1 - 15/32 - 1/2)Y_{II} \geq 0.031, \end{aligned} \quad (2.13)$$

which is a contradiction.

Proof in case II+. In this case, we have $s_{ij} = 1$ for all i and j . In particular, we have $n_J, n_K \leq -\frac{3}{4}$ both negative. We again take two terms from (2.12):

$$\begin{aligned} 3/100 &\geq n_J^2(Y_{JJ} - |Y_{IJ}| - |Y_{JK}|) + (n_J + n_K)^2|Y_{JK}| \\ &\geq n_J^2(Y_{JJ} - |Y_{IJ}|) \geq (3/4)^2 Y_{JJ} (1 - \frac{1}{2}) \geq (9/32)Y_{JJ}, \end{aligned} \quad (2.14)$$

so $Y_{JJ} \leq 8/75$. By symmetry, we also have $Y_{KK} \leq 8/75$. Using (2.12) again, we get

$$0.03 \geq (Y_{II} - |Y_{IJ}| - |Y_{JK}|) \geq Y_{II} - \frac{1}{2}Y_{JJ} - \frac{1}{2}Y_{KK} \geq 1 - 8/75 > 0.89, \quad (2.15)$$

which is another contradiction.

Proof in case II-. The proof in this case is different from the other two cases: we will show that Y is close to

$$X = \frac{1}{2} \begin{pmatrix} 2 & 1 & -1 \\ 1 & 2 & 1 \\ -1 & 1 & 2 \end{pmatrix}. \quad (2.16)$$

Let $(\varepsilon_{ij})_{ij} = Y - X$. We have $|n_i| = -s_{Ii}n_i \geq 3/4$ for all $i \in \{1, 2, 3\}$, hence (2.12) gives for all $\{i, j, k\} = \{1, 2, 3\}$:

$$0.06 > 0.03/n_i^2 \geq (Y_{ii} - |Y_{ij}| - |Y_{ik}|) \geq \frac{1}{2}Y_{ii} - s_{ik}Y_{ik} \geq 0. \quad (2.17)$$

With $X_{ii} = 1$ and $X_{ij} = \frac{1}{2}s_{ij}$, this becomes

$$0.06 > \frac{1}{2}\varepsilon_{ii} - s_{ik}\varepsilon_{ik} \geq 0. \quad (2.18)$$

As $\varepsilon_{II} = 0$, we get $0 \leq -s_{Ik}\varepsilon_{Ik} < 0.06$ for all $k \neq I$. Applying (2.18) again, but now with $k = I$, we get $\frac{1}{2}|\varepsilon_{ii}| < 0.06$ for all $i \neq I$. Applying (2.18) with $i = J$, $k = K$, we finally get $|\varepsilon_{JK}| < 0.12$. As Y is Minkowski-reduced, we have

$$\begin{aligned} 1 = Y_{II} &\leq (1, -1, 1)Y^t(1, -1, 1) \\ &= (1, -1, 1)X^t(1, -1, 1) + (1, -1, 1)(\varepsilon_{ij})_{ij}{}^t(1, -1, 1) \\ &\leq 0 + \sum_{i=1}^3 \sum_{j=1}^3 |\varepsilon_{ij}| < 0.72, \end{aligned} \quad (2.19)$$

contradiction. \square

2.1.2. Fast algorithm for the Thetanullwerte. In this section, we generalize the strategy described in genus 1 and 2 in [13] and ideas taken from [30, Chapter 7]. This leads to an evaluation algorithm with running time $O(\mathcal{M}(P) \log P)$.

We start, as in [13], by writing the τ -duplication formulas in terms of ϑ_i^2 . For example, we can write,

$$\vartheta_1(0, 2\tau)^2 = \frac{\sqrt{\vartheta_0^2 \sqrt{\vartheta_1^2}} + \sqrt{\vartheta_2^2 \sqrt{\vartheta_3^2}} + \sqrt{\vartheta_4^2 \sqrt{\vartheta_5^2}} + \sqrt{\vartheta_6^2 \sqrt{\vartheta_7^2}}}{4}(0, \tau). \quad (2.20)$$

These formulas match the iteration used in the definition of the genus 3 *Borchardt mean* \mathcal{B}_3 [13]. They can be seen as a generalization of the arithmetic-geometric mean to higher genus, since both involve Thetanullwerte and converge quadratically [13].

Applying the τ -duplication formula to the fundamental Thetanullwerte repeatedly gives (recall that we write $\vartheta_{n_1, \dots, n_k}$ for the k -tuple $\vartheta_{n_1}, \dots, \vartheta_{n_k}$)

$$\mathcal{B}_3(\vartheta_{0,1,\dots,7}(0,\tau)^2) = 1 \quad (2.21)$$

assuming one picks correct square roots $\vartheta_i(0, 2^k\tau)$ of $\vartheta_i(0, 2^k\tau)^2$. By the homogeneity of the Borchardt mean, we can write

$$\mathcal{B}_3\left(1, \frac{\vartheta_{1,\dots,7}(0,\tau)^2}{\vartheta_0(0,\tau)^2}\right) = \frac{1}{\vartheta_0(0,\tau)^2}. \quad (2.22)$$

We wish to use this equality to compute the right-hand side from the quotients of Thetanullwerte; this is a key ingredient to the quasi-linear running time of our algorithm. The difficulty here stems from the fact that the Borchardt mean requires a technical condition on the square roots picked at each step (“good choice”) in order to get a quasi-linear running time, and sometimes these choices of square roots do not correspond to the values of ϑ_i we are interested in (i.e., would not give $1/\vartheta_0(0,\tau)^2$ at the end of the procedure). We sidestep this difficulty using the same strategy as [30]: we design our algorithm so that the square roots we pick always correspond to the values of ϑ_i we are interested in, even when they do not correspond to “good choices” of the Borchardt mean. This slows down the convergence somewhat; however, one can prove (using the same method as in [30, Lemma 7.2.2]) that after a number of steps that only depends on τ (and not on P), our choice of square roots always coincides with “good choices”. After this point, only $\log P$ steps are needed to compute the value with absolute precision P , since the Borchardt mean converges quadratically; this means that the right-hand side of Equation (2.22) can be evaluated with absolute precision P in $O(\mathcal{M}(P) \log P)$.

The next goal is to find a function \mathfrak{F} to which we can apply Newton’s method to compute these quotients of Thetanullwerte (and, ultimately, the Thetanullwerte). For this, we use the action of the symplectic group on Thetanullwerte to transform (2.22) and get relationships involving the coefficients of τ . Using the action of the matrices described in [13, Chapitre 9], along with the Borchardt mean, we can build a function f with the property that

$$f\left(\frac{\vartheta_{1,\dots,7}(0,\tau)^2}{\vartheta_0(0,\tau)^2}\right) = (-i\tau_{11}, -i\tau_{22}, -i\tau_{33}, \tau_{12}^2 - \tau_{11}\tau_{22}, \tau_{13}^2 - \tau_{11}\tau_{33}, \tau_{23}^2 - \tau_{22}\tau_{33}) \quad (2.23)$$

However, the above function is a function from \mathbb{C}^7 to \mathbb{C}^6 ; this is a problem, as it prevents us from applying Newton’s method directly. As discussed in [30, Chapter 7], there are two ways to fix this: either work on the variety of dimension 6 defined by the fundamental Thetanullwerte, or add another quantity to the output and hope that the Jacobian of the system is then invertible. We choose the latter solution, and build a function $\mathfrak{F} : \mathbb{C}^7 \rightarrow \mathbb{C}^7$ by adding to the function f above an extra output, equal to $-i \det(\tau)$, which is motivated by the symplectic action of the matrix $\mathfrak{J} = \begin{pmatrix} 0 & -I_g \\ I_g & 0 \end{pmatrix}$ on the Thetanullwerte:

$$\vartheta_{0,1,2,3,4,5,6,7}^2(0, \mathfrak{J} \cdot \tau) = -i \det(\tau) \vartheta_{0,8,16,24,32,40,48,56}^2(0, \tau). \quad (2.24)$$

The following Algorithm 2.25 explicitly defines the function \mathfrak{F} that we will use.

Algorithm 2.25 (Given a 7-tuple $a_1, a_2, \dots, a_7 \in \mathbb{C}$, computes a number $\mathfrak{F}(a_1, \dots, a_7)$, defined by the steps in this algorithm. Here we are specifically interested in the value $\mathfrak{F}(\vartheta_{1,\dots,7}(0, \tau)^2/\vartheta_0(0, \tau)^2)$, so for clarity we abuse notation and denote a_i by $\vartheta_i(0, \tau)^2/\vartheta_0(0, \tau)^2$).

- (i) Compute $t_0 = \mathcal{B}_3(1, \vartheta_{1,\dots,7}(0, \tau)^2/\vartheta_0(0, \tau)^2)$.
- (ii) Compute $t_i = (1/t_0) \times \vartheta_i(0, \tau)^2/\vartheta_0(0, \tau)^2$.
- (iii) $t_i \leftarrow \sqrt{t_i}$, choosing the square root that coincides with the value of $\vartheta_i(0, \tau)$ (computed with low precision just to inform the choice of signs).
- (iv) Apply the τ -duplication formulas to the t_i to compute complex numbers that by abuse of notation we write as $\vartheta_i(0, 2\tau)^2$. (Here if $t_i = \vartheta_i(0, \tau)$, then “ $\vartheta_i(0, 2\tau)^2$ ” is really equal to $\vartheta_i(0, 2\tau)^2$.)
- (v) $r_1 \leftarrow \vartheta_{32}^2(0, 2\tau) \times \mathcal{B}_3(1, \vartheta_{32,33,34,35,0,1,2,3}^2(0, 2\tau)/\vartheta_0^2(0, 2\tau))$.
- (vi) $r_2 \leftarrow \vartheta_{16}^2(0, 2\tau) \times \mathcal{B}_3(1, \vartheta_{16,17,0,1,20,21,4,5}^2(0, 2\tau)/\vartheta_0^2(0, 2\tau))$.
- (vii) $r_3 \leftarrow \vartheta_8^2(0, 2\tau) \times \mathcal{B}_3(1, \vartheta_{8,0,10,2,12,4,14,6}^2(0, 2\tau)/\vartheta_0^2(0, 2\tau))$.
- (viii) $r_4 \leftarrow \vartheta_0^2(0, 2\tau) \times \mathcal{B}_3(1, \vartheta_{0,1,32,33,16,17,48,49}^2(0, 2\tau)/\vartheta_0^2(0, 2\tau))$.
- (ix) $r_5 \leftarrow \vartheta_0^2(0, 2\tau) \times \mathcal{B}_3(1, \vartheta_{0,32,2,34,8,40,10,42}^2(0, 2\tau)/\vartheta_0^2(0, 2\tau))$.
- (x) $r_6 \leftarrow \vartheta_0^2(0, 2\tau) \times \mathcal{B}_3(1, \vartheta_{0,16,8,24,4,20,12,28}^2(0, 2\tau)/\vartheta_0^2(0, 2\tau))$.
- (xi) $r_7 \leftarrow \vartheta_0^2(0, 2\tau) \times \mathcal{B}_3(1, \vartheta_{0,8,16,24,32,40,48,56}^2(0, 2\tau)/\vartheta_0^2(0, 2\tau))$.
- (xii) Return $(r_1/2, r_2/2, r_3/2, r_4/4, r_5/4, r_6/4, r_7/8)$.

The final part of our algorithm applies Newton’s method to \mathfrak{F} , by starting with an approximation of the quotients of Thetanullwerte with large enough precision P_0 to ensure that the method converges. In practice, we found that a starting precision $P_0 = 450$ was on the one hand large enough to make Newton’s method converge quickly and on the other hand small enough so that the fast algorithm does not get slowed down too much by first doing the naive algorithm to precision P_0 . Since computing \mathfrak{F} is asymptotically as costly as computing the Borchardt mean, and since there is no extra asymptotic cost when applying Newton’s method if one doubles the working precision at each step, we get an algorithm which computes the genus 3 Thetanullwerte with P digits of precision with time $O(\mathcal{M}(P) \log P)$. This algorithm was implemented in MAGMA, along with the aforementioned naive algorithm. For our examples, the fast algorithm always gives a result with more than 2000 digits of precision in less than 10 seconds.

2.2. Computation of the Dixmier–Ohno invariants. Consider Thetanullwerte $(\vartheta_0(\tau), \dots, \vartheta_{63}(\tau)) \in \mathbb{C}^{64}$ as computed in the previous section. Then by Riemann’s vanishing theorem [45, V.th.5] and Clifford’s theorem [1, Chap.3,§1] the values correspond to a smooth plane quartic curve if and only if 36 of them are non-zero. If this condition is satisfied, the following procedure determines the equation of a plane quartic $X_{\mathbb{C}}$ for which there is a Riemann matrix τ that gives these Thetanullwerte.

Using [62, p.108] (see also [16]), we compute the *Weber moduli*

$$\begin{aligned} a_{11} &:= i \frac{\vartheta_{33}\vartheta_5}{\vartheta_{40}\vartheta_{12}}, & a_{12} &:= i \frac{\vartheta_{21}\vartheta_{49}}{\vartheta_{28}\vartheta_{56}}, & a_{13} &:= i \frac{\vartheta_7\vartheta_{35}}{\vartheta_{14}\vartheta_{42}}, \\ a_{21} &:= i \frac{\vartheta_5\vartheta_{54}}{\vartheta_{27}\vartheta_{40}}, & a_{22} &:= i \frac{\vartheta_{49}\vartheta_2}{\vartheta_{47}\vartheta_{28}}, & a_{23} &:= i \frac{\vartheta_{35}\vartheta_{16}}{\vartheta_{61}\vartheta_{14}}, \\ a_{31} &:= -\frac{\vartheta_{54}\vartheta_{33}}{\vartheta_{12}\vartheta_{27}}, & a_{32} &:= \frac{\vartheta_2\vartheta_{21}}{\vartheta_{56}\vartheta_{47}}, & a_{33} &:= \frac{\vartheta_{16}\vartheta_7}{\vartheta_{42}\vartheta_{61}}. \end{aligned} \quad (2.26)$$

Note that these numbers depend on only 18 of the Thetanullwerte. The three projective lines $\ell_i : a_{1i}x_1 + a_{2i}x_2 + a_{3i}x_3 = 0$ in $\mathbb{P}_{\mathbb{C}}^2$, together with the four lines

$$x_1 = 0, \quad x_2 = 0, \quad x_3 = 0, \quad x_1 + x_2 + x_3 = 0 \quad (2.27)$$

will form a so-called *Aronhold system* of bitangents to the eventual quartic $X_{\mathbb{C}}$. Considering the first three lines as a triple of points $((a_{1i} : a_{2i} : a_{3i}))_{i=1\dots 3}$ in $(\mathbb{P}^2)^3$, one obtains a point on a 6-dimensional quasiprojective variety. Its points parametrize the moduli space of smooth plane quartics with full level two structure [19].

From an Aronhold system of bitangents, one can reconstruct a plane quartic following Weber's work [62, p.93] (see also [46, 16]). We take advantage here of the particular representative (a_{1i}, a_{2i}, a_{3i}) of the projective points $(a_{1i} : a_{2i} : a_{3i})$ to simplify the algorithm presented in loc. cit. Indeed, normally that algorithm involves certain normalization constants k_i . However, in the current situation [16, Cor.2] shows that these constants are automatically equal to 1 for our choices of a_{ji} in (2.26), which leads to a computational speedup. Let $u_1, u_2, u_3 \in \mathbb{C}[x_1, x_2, x_3]$ be given by

$$\begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ \frac{1}{a_{11}} & \frac{1}{a_{12}} & \frac{1}{a_{13}} \\ \frac{1}{a_{21}} & \frac{1}{a_{22}} & \frac{1}{a_{23}} \end{bmatrix}^{-1} \cdot \begin{bmatrix} 1 & 1 & 1 \\ a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}. \quad (2.28)$$

Then $X_{\mathbb{C}}$ is the curve defined by the equation $(x_1u_1 + x_2u_2 - x_3u_3)^2 - 4x_1u_1x_2u_2 = 0$.

We now have a complex model $X_{\mathbb{C}}$ of the quartic curve that we are looking for. Note that there is no reason to expect $X_{\mathbb{C}}$ to be defined over \mathbb{Q} ; its coefficients will in general be complicated algebraic numbers that are difficult to recognize algebraically. To get around this problem, we first approximate its 13 *Dixmier-Ohno invariants*, which were defined in [12, 15, 17] (see [42, Sec.1.2] for a short description). These invariants

$$\underline{\mathbb{I}} = (I_3 : I_6 : I_9 : J_9 : I_{12} : J_{12} : I_{15} : J_{15} : I_{18} : J_{18} : I_{21} : J_{21} : I_{27}) \quad (2.29)$$

are homogeneous expressions in the coefficients of a ternary quartic form. Their degrees in the coefficients of such a form are

$$\underline{d} = (3, 6, 9, 9, 12, 12, 15, 15, 18, 18, 21, 21, 27). \quad (2.30)$$

Therefore the evaluation of these invariants at $X_{\mathbb{C}}$ (which we still denote by $\underline{\mathbb{I}}$) gives rise to a point in the weighted projective space $\mathbb{P}^{\underline{d}}$. Note that I_{27} is the discriminant of $X_{\mathbb{C}}$, which is non-zero.

For a ternary quartic form over $\overline{\mathbb{Q}}$ that is equivalent to a ternary quartic form over \mathbb{Q} , the tuple $\underline{\mathbb{I}}$ defines a \mathbb{Q} -rational point in $\mathbb{P}^{\underline{d}}$. This is not to say that the entries of $\underline{\mathbb{I}}$ itself are in \mathbb{Q} . However, we can achieve this by suitably normalizing

this tuple. When $I_3 \neq 0$ (as will always be the case for us), we can for instance use the normalization

$$\underline{I}^{\text{norm}} = \left(1, \frac{I_6}{I_3^2}, \frac{I_9}{I_3^3}, \frac{J_6}{I_3^3}, \frac{I_{12}}{I_3^4}, \frac{J_{12}}{I_3^4}, \frac{I_{15}}{I_3^5}, \frac{J_{15}}{I_3^5}, \frac{I_{18}}{I_3^6}, \frac{J_{18}}{I_3^6}, \frac{I_{21}}{I_3^7}, \frac{J_{21}}{I_3^7}, \frac{I_{27}}{I_3^9} \right). \quad (2.31)$$

Our program concludes by computing the best rational approximation of (the real part) of the Dixmier–Ohno invariants $\underline{I}^{\text{norm}}$ by using the corresponding (PARI [4]) function `BestApproximation` in MAGMA at increasing precision until the sequence stabilizes. In practice, this does not take an overly long time: we worked with less than 1000 decimal digits and the denominators involved never exceeded 100 decimal digits.

For some of the CM fields, we in fact obtain 4 isomorphism classes of principally polarized abelian varieties. But by Theorem 1.1, we know that exactly one of them has field of moduli \mathbb{Q} . Of course we do not know in advance which of the four complex tori under consideration has this property. In such a case, we use `BestApproximation` for each of the four cases and we observe that this succeeds (at less than 1000 decimal digits) for exactly one of them. We then only set aside the Dixmier–Ohno invariants of that case for later consideration.

Some manipulations, illustrated below with the case 15, then give us an integral representative $\underline{I}^{\text{min}}$ of the Dixmier–Ohno invariants for which the gcd of the entries is minimal. We denote this 13-tuple by

$$\underline{I}^{\text{min}} = (I_3^{\text{min}}, I_6^{\text{min}}, I_9^{\text{min}}, \dots, J_{21}^{\text{min}}, I_{27}^{\text{min}}).$$

Example 2.32. In case 15, the approximation that we obtain is

$$\underline{I}^{\text{norm}} = \left(1 : \frac{3967}{609408} : \dots : \frac{346304226226660371}{1980388294678257795596288} \right). \quad (2.33)$$

We first get an integral representative by taking λ to be the least common multiple of the denominators of $\underline{I}^{\text{norm}}$ and setting \underline{I}' be equal to

$$(\lambda, \lambda^2 I_6, \lambda^3 I_9, \lambda^3 J_9, \lambda^4 I_{12}, \lambda^4 J_{12}, \lambda^5 I_{15}, \lambda^5 J_{15}, \lambda^6 I_{18}, \lambda^6 J_{18}, \lambda^7 I_{21}, \lambda^7 J_{21}, \lambda^9 I_{27}).$$

We can now find the prime factors p of I_3 and look at the valuations at p of each entry of \underline{I}' . Since for an invariant I of degree $3n$, we have that

$$I \left(pF \left(\frac{x}{p}, y, z \right) \right) = p^{3n} I \left(F \left(\frac{x}{p}, y, z \right) \right) = p^{3n} p^{-4n} I(F) = \frac{I(F)}{p^n} \quad (2.34)$$

by this procedure, we can reduce the valuations at p of these invariants. Applying this as much as possible while preserving positive valuation, we find

$$\underline{I}^{\text{min}} = (2^5 \cdot 3 \cdot 23 : 2^3 \cdot 3967 : 2^3 \cdot 3 \cdot 5 \cdot 41 \cdot 173 \cdot 19309 : \dots : 2^5 \cdot 3^{27} \cdot 19^7). \quad (2.35)$$

Note that we cannot always get a representative with coprime entries; already in the case under consideration the prime 2 divides all the entries).

3. OPTIMIZED RECONSTRUCTION

Having the Dixmier–Ohno invariants at our disposal, it remains to reconstruct a corresponding plane quartic curve X over \mathbb{Q} . It was indicated in [42] how such a reconstruction can be obtained; however, the corresponding algorithms, the precursors of those currently at [41], were suboptimal in several ways. To start with, they would typically return a curve over a quadratic extension of the base field, without performing a further Galois descent. Secondly, the coefficients of these

reconstructed models were typically of gargantuan size. In this section we describe the improvements to the algorithms, incorporated in the present version of [41], that enabled us to obtain the simple equations in this paper.

The basic ingredients are the following. A Galois descent to the base field can be found by determining an isomorphism of X with its conjugate and applying an effective version of Hilbert's Theorem 90, as was also mentioned in [42]. After this, a reduction algorithm can be applied, based on algorithms by Elsenhans [14] and Stoll [53] that have been implemented and combined in the MAGMA function `MinimizeReducePlaneQuartic`. However, applying these two steps concurrently is an overly naive approach, since the Galois descent step blows up the coefficients by an unacceptable factor. We therefore have to look under the hood of our reconstruction algorithms and use some tricks to optimize them.

Recall from [42] that the reconstruction algorithm finds a quartic form F by first constructing a triple (b_8, b_4, b_0) of binary forms of degree 8, 4 and 0. Our first step is to reconstruct the form b_8 as efficiently as possible. This form is reconstructed from its Shioda invariants \underline{S} , which are algebraically obtained from the given Dixmier–Ohno invariants \underline{I}^{\min} . Starting from the invariants \underline{S} , the methods of [37] are applied, which furnish a conic C and a quartic H in \mathbb{P}^2 that are both defined over \mathbb{Q} . This pair corresponds to b_8 in the sense that over $\overline{\mathbb{Q}}$ the divisor $C \cap H$ on C can be transformed into the divisor cut out by b_8 on \mathbb{P}^1 . A priority in this reconstruction step is to find a conic C defined by a form whose discriminant is as small as possible.

3.1. Choosing the right conic for Mestre reconstruction. Let k be a number field whose rings of integers \mathcal{O}_k admits an effective extended GCD algorithm, which is for example the case when \mathcal{O}_k is a Euclidean ring. We indicate how over such a field we can improve the algorithms developed to reconstruct a hyperelliptic curve from its Igusa or Shioda invariants in genus 2 or genus 3 respectively [44, 36, 37].

Recall that Mestre's method for hyperelliptic reconstruction is based on Clebsch's identities [37, Sec.2.1]. It uses three binary covariants $q = (q_1, q_2, q_3)$ of order 2. From these forms, one can construct a plane conic $C_q : \sum_{1 \leq i, j \leq 3} A_{i,j} x_i x_j = 0$ and a degree $g + 1$ plane curve H_q over the ring of invariants. Here g is the genus of the curve that we wish to reconstruct.

Given a tuple of values of hyperelliptic invariants over k , we can substitute to obtain a conic and a curve that we again denote by C_q and H_q . Generically, one then recovers a hyperelliptic curve X with the given invariants by constructing the double cover of C_q ramified over $C_q \cap H_q$. Because the coefficients of the original universal forms C_q and H_q are invariants of the same degree, the substituted forms will be defined over k .

Finding a model of X of the form $y^2 = f(x)$ over k (also called a *hyperelliptic model*) is equivalent to finding a k -rational point on the conic C_q by [37, 39]. Algorithms to find such a rational point exist [51, 61] and their complexity is dominated by the time spent to factorize the discriminant of an integral model of C_q . While a hyperelliptic model may not exist over k , it can always be found over some quadratic extension of k . It is useful to have such an extension given by a small discriminant, which is in particular the case when C_q has small discriminant. Accordingly, we turn to the problem of minimizing $\text{disc}(C_q)$.

In order to do so, we use a beautiful property of Clebsch's identities. By [37, Sec.2.1.(5)], we have that

$$\text{disc}(C_q) = \det((A_{i,j})_{1 \leq i,j \leq 3}) = R_q^2/2 \quad (3.1)$$

where R_q is the determinant of q_1, q_2, q_3 in the basis x^2, xz, z^2 . If q'_3 is now another covariant of order 2, we can consider the *family* of covariants $q_{\lambda,\mu} = (q_1, q_2, \lambda q_3 + \mu q'_3)$, $\lambda, \mu \in k$. For this family, the multilinearity of the determinant shows that

$$R_{q_{\lambda,\mu}} = \lambda R_{(q_1, q_2, q_3)} + \mu R_{(q_1, q_2, q'_3)}. \quad (3.2)$$

The values $R_{(q_1, q_2, q_3)}$ and $R_{(q_1, q_2, q'_3)}$ are invariants that can be effectively computed and which are generically non-zero. (If either of these invariants is zero, then, one can usually take different covariants q_i ; if all of these fail to give non-zero values, then typically X has large reduced automorphism group and other techniques can be used.) The key point is that we can minimize the value of $R_{q_{\lambda,\mu}}$, and by (3.1) the value of $\text{disc}(C_{q_{\lambda,\mu}})$ with it, by using the extended Euclidean algorithm to minimize the combined linear contribution of λ and μ to the linear expression $R_{q_{\lambda,\mu}}$. This allows us to reduce the discriminant all the way to $\gcd(R_{(q_1, q_2, q_3)}, R_{(q_1, q_2, q'_3)})$ or beyond.

Note that we do not have $C_{q_{\lambda,\mu}} = \lambda^2 C_{(q_1, q_2, q_3)} + \mu^2 C_{(q_1, q_2, q'_3)}$. However, the coefficients of the family of conics $C_{q_{\lambda,\mu}}$ and of $H_{q_{\lambda,\mu}}$ can be quickly found in terms of the invariants and λ, μ by using the same interpolation techniques as in [37, Sec. 2.3].

3.2. Reconstruction of a plane quartic model from the invariants. With these precomputations out of the way, we now search for a binary octic form b_8 whose Shioda invariants come from the first step of the reconstruction algorithm of [42] applied to the Dixmier–Ohno invariants of case 15 (*cf.* Table 1). Except for this case and case 6, all the other cases give conics C with no rational point and as such, a Galois descent phase is needed to find a rational quartic (*cf.* Section 3.3). Case 15 is the easiest CM plane quartic that we have to reconstruct. From the associated Shioda invariants, we compute an invariant $R_{q_{\lambda,\mu}}$. By using the extended GCD algorithm and substituting the result for λ and μ , we are left with R_q equal to the left hand side coefficient $2^{61} \cdot 3^{18} \cdots 201049$. This factor is almost equal to the Dixmier–Ohno invariant I_{12}^{\min} , the discriminant of the covariant used in our quartic reconstruction. Indeed, the considerations in [42] show that our reconstruction algorithm fails when $I_{12}^{\min} = 0$, and more precisely that this failure occurs when trying to reconstruct b_8 via Mestre's method. Hence the primes which divide I_{12}^{\min} naturally appear in the discriminants of $C_{q_{\lambda,\mu}}$. A substantially smaller R_q cannot therefore be expected.

Now as we know the factorization of R_q , we can efficiently determine if the conic $C_{q_{\lambda,\mu}}$ has a rational point. Unexpectedly, it has one, and after a change of variable we map it to the point $(1 : 1 : 0)$. The conic is then $C = x^2 - y^2 - z^2$ and the corresponding quartic H has approximately 50-digit coefficients.

Finally, it remains to compute the geometric intersection $C \cap H$. This yields the octic b_8 . The forms b_0 and b_4 computed by the plane quartic reconstruction algorithm [42] are therefore defined over \mathbb{Q} as well. By applying the linear map $(\ell^*)^{-1}$ defined in *loc. cit.*, we get a plane quartic defined over \mathbb{Q} too. It remains to reduce the size of its coefficients as explained in Section 3.3 to obtain the equation given in Section 5.

3.3. Galois descent and minimization. Now suppose that we have in this way found a pair (C, H) as above, for which C has minimal discriminant. We can then further optimize this pair by applying the following two steps:

- (i) Minimize the defining equation of C by using the theory of quaternion algebras (implemented in the MAGMA function `MinimalModel`);
- (ii) Apply the reduction theory of point clusters [53] applied to the intersection $C \cap H$ (implemented in the MAGMA function `ReduceCluster`).

The second step above is more or less optional; typically it leads to a rather better H at the cost of a slightly worse C . Regardless, at the end of this procedure, we can construct a binary form b_8 over a quadratic extension K of \mathbb{Q} by parametrizing the conic C , and we then reconstruct b_4 and b_0 as in [42]. The associated ternary quartic form F is usually defined over a quadratic extension of \mathbb{Q} . Since its covariant $\rho(F)$ from [42] is a multiple of $y^2 - xz$, we can immediately apply the construction from [59] to obtain an element $[M] \in \text{PGL}_3(K)$ that up to a scalar λ transforms F into its conjugate $\sigma(F)$:

$$[\sigma(F)] = [F.M]. \quad (3.3)$$

In the cases under consideration we know that the curve defined by F descends because of the triviality of its automorphism group. This implies that the cocycle defined by the class $[M]$ lifts to $\text{GL}_3(K)$. Explicitly, let $M \in \text{GL}_3(K)$ be some representative of the class $[M]$. Then we have

$$M\sigma(M) = \pi \quad (3.4)$$

for some scalar matrix π . Conjugating this equality shows that in fact $\pi \in \mathbb{Q}$, and taking determinants yields $\delta\sigma(\delta) = \pi^3$, where δ is the determinant of M . Now let $M_0 = (\pi/\delta)M$. Then we have

$$M_0\sigma(M_0) = \frac{\pi}{\delta}M\frac{\sigma(\pi)}{\sigma(\delta)}\sigma(M) = \frac{\pi\sigma(\pi)\pi}{\delta\sigma(\delta)} = \frac{\pi^3}{\delta\sigma(\delta)} = 1. \quad (3.5)$$

We may therefore assume that $M \in \text{GL}_3(K)$ corresponds to a lifted cocycle. The Galois cohomology group $H^1(\text{Gal}(K|\mathbb{Q}), \text{GL}_3(K))$ is trivial; Hilbert's Theorem 90 can be used to construct a coboundary N for M , that is, a matrix in $\text{GL}_3(K)$ for which

$$M\sigma(N) = N. \quad (3.6)$$

After choosing a random matrix $R \in \text{GL}_3(K)$, one can in fact take

$$N = R + M\sigma(R). \quad (3.7)$$

We thus obtain a coboundary N corresponding to the cocycle M . If we put $F_0 = F.N$, then the class $[F_0]$ is defined over \mathbb{Q} . The transformed form F_0 itself still need not be defined over \mathbb{Q} , but this can be achieved by dividing it by one of its coefficients.

A complication is that the determinant of a random matrix N as in (3.7) typically has a rather daunting factorization. These factors can (and usually will) later show up as places of bad reduction of the descended form F_0 . It is therefore imperative to avoid a bad factorization structure of the determinant of N . This, however, can be ensured by performing a lazy factorization of this determinant and passing to a next random choice if the result is not satisfactory.

After we have obtained a form F_0 , one can apply the MAGMA function `Minimize-ReducePlaneQuartic`; this function combines a discriminant minimization step due to Elsenhans in [14] with the reduction theory of Stoll in [53]. Typically the first

of these steps leads to the most significant reduction of the coefficient size, since it applies a suitable transformation in $\mathrm{GL}_3(\mathbb{Q})$ whose determinant is a large prime, whereas the cluster reduction step is a further optimization involving only the subgroup $\mathrm{SL}_3(\mathbb{Z})$. As mentioned above, we can save some time in the minimization step by carrying over the primes in the factorization of the determinant of the coboundary N , since these will recur in the set of bad primes of F_0 .

All in all, we get the following randomized algorithm whose heuristic complexity is polynomial in the size of the Dixmier–Ohno invariants, if we assume that the factorizations of I_{12}^{\min} and I_{27}^{\min} are known, and that $\det N$ behaves as a random integer.

Algorithm 3.8 (Integral plane quartic reconstruction from its Dixmier–Ohno invariants \underline{I}^{\min} when the factorizations of I_{12}^{\min} and I_{27}^{\min} are known).

- (i) Repeat the following steps until $N \neq 0$ and the full factorization of $\det(N)$ is known.
 - (a) Calculate the Shioda invariants \underline{S} of b_8 (as explained in [37]).
 - (b) Evaluate the conic $C_{q_{\lambda,\mu}}$ at \underline{S} and determine (λ, μ) by using the extended Euclidean algorithm (so that $\mathrm{disc} C_{q_{\lambda,\mu}} \simeq I_{12}^{\min}$, see Section 3.1).
 - (c) Choose a point P on the conic $C_{q_{\lambda,\mu}}$ and use it to parametrize the conic.
(To achieve this, let P to be any rational point of $C_{q_{\lambda,\mu}}$ if it is easy to find. Otherwise intersect C_q with a random rational line with a defining equation of small height and let P be the quadratic point defined by this intersection.)
 - (d) Intersect $C_{q_{\lambda,\mu}}$ and $H_{q_{\lambda,\mu}}$ to obtain the octic b_8 , then calculate the forms b_4 and b_0 and reconstruct a quartic F via the map ℓ^* .
 - (e) If F is defined over \mathbb{Q} then set N to be the identity matrix of $\mathrm{GL}(3, \mathbb{Q})$, else let N be a random coboundary as in (3.7).
 - (f) Try to compute a factorization of $\det N$. If this fails within the allocated time, then start over.
- (ii) Let $F_0 = FN$ and divide the result by one of its coefficients, so that F_0 has coefficients in \mathbb{Q} .
- (iii) Reduce the coefficient size of F_0 (with `MinimizeReducePlaneQuartic`, using the prime factors of $\det N$ and I_{12}^{\min}).

One important practical speedup for Algorithm 3.8 exploits that if we take R in (3.7) to be integral, then the determinants of the random coboundaries that we compute in Step (i)(e) share the same denominator, namely that of π/δ , where π is as in (3.4) and where δ is the determinant of M . In turn, the quantity π/δ only depends on the choice of the random line in Step (i)(c). A straightforward optimization is thus to loop over the Steps (i)(a) – (d) until a lazy factorization of the denominator of $\det(1 + M)$ yields its full factorization (note that here M is the cocycle defined by equation (3.3) and $1 + M = R + M\sigma(R)$ for R the identity matrix). Once done, we can loop over the Steps (i)(e) – (i)(f) to test as many coboundaries $N = R + M\sigma(R)$ from random integral matrices R as needed, once more until the lazy factorization of the denominator of $\det N$ is its full factorization.

In the most difficult case, i.e., case 16 (*cf.* Table 1), the candidates for $\det N$ have approximately 500-digit denominators and 700-digit numerators. If we allow less than a second for the lazy factorization routine in MAGMA, then the total computation in the end takes less than 5 minutes on a laptop. In this case, the descended form $F_0 = F.N$ has 1500-digit coefficients! Once the discriminant minimization steps from [14] are done for each prime divisor of $\det N$, we are left with a form that “merely” has 50-digit coefficients. Stoll’s reduction method [53] then finally yields the 15-digit equation given in Section 5.

Remark 3.9. Bouyer and Streng [7, Algorithm 4.8] show how one can avoid factoring in the discriminant minimization of binary forms. Such a trick enabled them to eliminate the need for a loop like that in Step (i) of Algorithm 3.8 when considering curves of genus 2. It remains to be seen whether a similar trick applies to Elsenhans’s discriminant minimization of plane quartics [14]. If it does, then that would greatly speed up the reconstruction.

4. REMARKS ON THE RESULTS

Our (heuristic) results can be found in the next section; here we discuss some of their properties and perform a few sanity checks. The very particular pattern of the factorization of the discriminants is already a good indicator of the correctness of our computations. Note that as the Dixmier–Ohno invariants that we use involve denominators with prime factors in $\{2, 3, 5, 7\}$, we will not look at the valuation of our invariants at these primes.

As was mentioned in the introduction, one of the motivations for computing this list of curves was to have examples in hand to understand the possible generalization of the results of Goren–Lauter [18] in genus 2 to non-hyperelliptic curves of genus 3. In genus 2, all primes dividing the discriminant are primes of bad reduction for the curve. This bad reduction provides information on the structure of the endomorphism ring of the reduction of the Jacobian. This particular structure allows one, with additional work, to bound the primes dividing the discriminant. Taking this even further allowed Lauter–Viray [35] to find out exactly which prime powers divide the discriminant. Similar bounds on primes dividing invariants have been obtained by Kılıçer–Lauter–Lorenzo–Newton–Ozman–Streng for hyperelliptic [24] and Picard [24, 25] curves.

Beyond these cases, so for “generic” genus 3 CM curves X , the situation is more involved. Let us fix terminology for a prime by calling it

- (i) a *potentially plane prime* if, after extending the base field, X has good non-hyperelliptic reduction at this prime;
- (ii) a *potentially hyperelliptic prime* if, after extending the base field, X has good hyperelliptic reduction at this prime;
- (iii) a *geometrically bad prime* in the remaining cases.

The first case can be detected easily, but distinguishing the second from the third case from the knowledge of the Dixmier–Ohno invariants is a difficult task and will be the main result of [43]. Applying these forthcoming results to the list of curves of Section 5, it can be proved for those curves that all primes $p > 7$ dividing I_{27}^{\min} with exponents 7 and 14 are potentially hyperelliptic whereas the few primes that are not of this kind are geometrically bad. Primes $p > 7$ dividing $\text{disc } X / I_{27}^{\min}$ for the curves of Section 5 are all potentially plane primes.

This profusion of hyperelliptic primes is typical of the CM case. Since the curves that we consider are CM curves, their Jacobian has potentially good reduction at all primes. Therefore, a prime is bad for X if and only if the Jacobian of X reduces to a product of two abelian sub-varieties with a decomposable principal polarization. The locus of such abelian threefolds is of codimension 2 in the moduli space of principally polarized abelian threefolds, whereas the locus of Jacobians of hyperelliptic curves has codimension 1. We therefore expect that “most” of the non-potentially-plane primes dividing the discriminant of a CM plane quartic are potentially hyperelliptic primes.

It should be mentioned that the results of [43] do not provide a closed formula for the potentially hyperelliptic primes simply in terms of the CM-type and polarization. In fact we wish to conclude this section with two remarks on the primes dividing I_{27}^{\min} that suggest that new phenomena occur for potentially hyperelliptic primes of plane quartics that do not have an exact equivalent in lower genus and that will require new theoretical developments in order to be fully explained. First, unlike the factorization pattern of the discriminants in the genus-2 CM, hyperelliptic and Picard cases, the factorization pattern of the product b of the potentially hyperelliptic primes seems to fit with that of a random integer of size b . For example, in case 16 below we have $b = 19 \cdot 37 \cdot 79 \cdot 13373064392147$. Secondly, the following proposition (applied for instance to X_9 at the primes 233 and 857 which are both totally split) shows that the reduction of the Jacobian of X at a potentially hyperelliptic prime can still be absolutely simple.

Proposition 4.1. *Let A be an abelian variety over a number field k and suppose that A has CM by \mathcal{O}_K for a sextic cyclic CM field K . Let $\mathfrak{p} \subset \mathcal{O}_k$ be a prime lying over a rational prime p . Let n be the number of prime factors of $p\mathcal{O}_K$.*

Then possibly after extending k , the following holds for the reduction \overline{A} of A modulo \mathfrak{p} .

We have $\overline{A} \sim B^d$ where B is absolutely simple and

- (i) *If $n = 2$, then $d = 1$, $\overline{A} = B$ is absolutely simple, and $\text{End}(\overline{A}_{\overline{\mathbb{F}}_p}) \otimes \mathbb{Q}$ is a central simple division algebra of reduced degree 3 over the imaginary quadratic subfield K_1 of K . It is ramified exactly at the two primes over p of K_1 .*
- (ii) *If $n = 6$, then $d = 1$, $\overline{A} = B$ is absolutely simple, and $\text{End}(\overline{A}_{\overline{\mathbb{F}}_p}) \otimes \mathbb{Q} \cong K$.*
- (iii) *In all other cases, we have $d = 3$, \overline{A} is supersingular, $\text{End}(\overline{A}_{\overline{\mathbb{F}}_p}) \otimes \mathbb{Q}$ is the quaternion algebra $B_{p,\infty}$ over \mathbb{Q} ramified only at p and infinity, and $\text{End}(\overline{A}_{\overline{\mathbb{F}}_p}) \otimes \mathbb{Q}$ is the 3×3 matrix algebra over $B_{p,\infty}$.*

If A is the Jacobian of a curve, then in cases (i) and (ii) the curve has potentially good reduction. (In case (iii) both good and bad reduction can occur.)

Proof. By a theorem of Serre and Tate [47], the abelian variety A has potentially good reduction. Extend k so that it has good reduction and so that k contains the reflex field. The Shimura–Taniyama formula [50, Theorem 1(ii) in Section 13.1] then gives a formula for the Frobenius endomorphism of the reduction as an element $\pi \in \mathcal{O}_K$ up to units. A theorem in Honda–Tate theory [56, Théorème 1] then gives a formula for the endomorphism algebra in terms of this π . We did the computation for all possible splitting types of a prime in a cyclic sextic number field and found the above-mentioned endomorphism algebras over some finite extension of \mathbb{F}_p . Moreover, we found that the endomorphism algebra from loc. cit. in our

cases does not change when taking powers of π (i.e., extending k and the extension of \mathbb{F}_p further), so that these are indeed the endomorphism algebras over $\overline{\mathbb{F}_p}$.

Finally, suppose further that $A = J(X)$ and X does not have potentially good reduction. Then by [6, Corollary 4.3], we get that the reduction of A is not absolutely simple, which gives a contradiction in cases (i) and (ii). \square

5. DEFINING EQUATIONS

We now give the equations of the plane quartics that we obtained for the CM field listed in Table 1. The expressions of the invariants of the curves obtained are too unwieldy to be written down completely; in fact in some cases it is even difficult to factor all of them. Here we only show the factorizations of I_{27}^{\min} (the full list is available at [23]).

- \mathbf{X}_1 : $-4169x^4 - 956x^3y + 7440x^3z + 55770x^2y^2 + 43486x^2yz$
 $+ 42796x^2z^2 - 38748xy^3 - 30668xy^2z + 79352xyz^2 - 162240xz^3$
 $+ 6095y^4 + 19886y^3z - 89869y^2z^2 - 1079572yz^3 - 6084z^4 = 0$
with disc $X_1 = 2^{-27} \cdot 3^{-27} \cdot 13^{18} \cdot I_{27}^{\min}$ where $I_{27}^{\min} = -2^{57} \cdot 3^{27} \cdot 5^{12} \cdot 7^9 \cdot 37^{14} \cdot 15187^{14}$.
- \mathbf{X}_2 : $19x^4 + 80x^3y - 54x^3z - 24x^2y^2 - 34x^2yz + 77x^2z^2 - 88xy^3 - 28xyz^2$
 $+ 38xyz^2 + 516xz^3 + 30y^4 - 36y^3z - 135y^2z^2 + 452yz^3 + 4z^4 = 0$
with disc $X_2 = 2^{-27} \cdot 3^{-27} \cdot I_{27}^{\min}$ where $I_{27}^{\min} = 2^{29} \cdot 3^{35} \cdot 7^9 \cdot 701^{14}$.
- \mathbf{X}_3 : $-1210961x^4 + 5202144x^3y + 408700x^3z - 2479108x^2y^2 + 1908050x^2yz$
 $+ 8367272x^2z^2 - 4393072xy^3 - 6944000xy^2z + 6772756xyz^2 + 10594064xz^3$
 $+ 4978166y^4 - 8342100y^3z + 4611839y^2z^2 + 14080572yz^3 - 1387684z^4 = 0$
with disc $X_3 = -2^{-27} \cdot 3^{-18} \cdot 31^{18} \cdot I_{27}^{\min}$ where $I_{27}^{\min} = 2^{29} \cdot 3^{36} \cdot 5^{36} \cdot 7^7 \cdot 233^{14} \cdot 356399^{14}$.
- \mathbf{X}_5 : $115x^4 - 766x^3y - 1336x^3z + 1205x^2y^2 + 5178x^2yz + 4040x^2z^2 + 8216xy^3 + 1322xy^2z$
 $- 9484xyz^2 + 1144xz^3 - 8094y^4 + 9032y^3z + 9669y^2z^2 - 6292yz^3 - 4706z^4 = 0$
with disc $X_5 = 2^{-27} \cdot 3^{-27} \cdot 13^{18} \cdot I_{27}^{\min}$ where $I_{27}^{\min} = 2^{29} \cdot 3^{51} \cdot 7^7 \cdot 37^{14} \cdot 127^{14}$.
- \mathbf{X}_6 : $1444x^4 - 3134924x^3y + 5002016x^3z + 2321857x^2y^2 + 2257732x^2yz$
 $+ 1585968x^2z^2 - 3166884xy^3 + 6283512xy^2z + 1014570xyz^2 - 4791852xz^3$
 $+ 3312514y^4 - 7211392y^3z + 19540084y^2z^2 - 10746888yz^3 + 4167513z^4 = 0$
with disc $X_6 = 2^{-27} \cdot 3^{-27} \cdot 19^{18} \cdot I_{27}^{\min}$ where $I_{27}^{\min} = 2^{29} \cdot 3^{51} \cdot 7^7 \cdot 17^{12} \cdot 127^{14} \cdot 211^{14} \cdot 20707^{14}$.
- \mathbf{X}_7 : $-133225x^4 - 68935944x^3y + 92175713x^3z - 21721369x^2y^2 + 2990226x^2yz$
 $+ 86699691x^2z^2 + 18547032xy^3 + 37568944xy^2z + 108649086xyz^2 - 259362054xz^3$
 $+ 35272208y^4 + 266781024y^3z + 140110856y^2z^2 - 1192622568yz^3 + 173418831z^4 = 0$
with disc $X_7 = 2^{-27} \cdot 3^{-18} \cdot 7^{18} \cdot 73^{18} \cdot I_{27}^{\min}$ where $I_{27}^{\min} = -2^{29} \cdot 3^{36} \cdot 5^9 \cdot 7^7 \cdot 71^{14} \cdot 83^{12} \cdot 17665559^{14}$.
- \mathbf{X}_8 : $11x^4 - 8x^3y - 46x^3z + 216x^2y^2 + 306x^2yz + 1636x^2z^2 - 144xy^3 + 304xy^2z$
 $+ 15726xyz^2 + 7963xz^3 - 428y^4 + 684y^3z - 32779y^2z^2 - 16901yz^3 + 106789z^4 = 0$
with disc $X_8 = 2^{-27} \cdot 3^{-27} \cdot 7^9 \cdot 19^{18} \cdot I_{27}^{\min}$ where $I_{27}^{\min} = 2^{43} \cdot 3^{27} \cdot 7^{15} \cdot 499^{14}$.
- \mathbf{X}_9 : $96128x^4 + 232804x^3y + 5588x^3z + 51333x^2y^2 - 37020x^2yz - 5791396x^2z^2$
 $- 108416xy^3 - 49056xy^2z - 6947226xyz^2 - 214292xz^3 - 5880y^4$
 $- 581812y^3z + 2438436y^2z^2 + 1944852yz^3 + 87102093z^4 = 0$
with disc $X_9 = 2^{-27} \cdot 3^{-18} \cdot 13^{18} \cdot I_{27}^{\min}$ where $I_{27}^{\min} = -2^{42} \cdot 3^{18} \cdot 5^{12} \cdot 7^{14} \cdot 79^{14} \cdot 233^{14} \cdot 857^{14}$.
- \mathbf{X}_{10} : $348x^4 - 832x^3y - 4x^3z + 261x^2y^2 - 132x^2yz - 1680x^2z^2 + 224xy^3 - 168xy^2z$
 $+ 1986xyz^2 + 36xz^3 + 8y^4 - 236y^3z + 404y^2z^2 + 428yz^3 + 1989z^4 = 0$
with disc $X_{10} = 2^{-27} \cdot 3^{-18} \cdot I_{27}^{\min}$ where $I_{27}^{\min} = -2^{42} \cdot 3^{18} \cdot 7^{14} \cdot 41^{14} \cdot 71^{14}$.

$$\begin{aligned} \mathbf{X}_{11} : & 245137 x^4 + 3134444 x^3 y - 405198 x^3 z + 13885332 x^2 y^2 - 4713906 x^2 y z \\ & - 6576142 x^2 z^2 + 25220768 x y^3 - 13466052 x y^2 z - 40450004 x y z^2 + 6168379 x z^3 \\ & + 16002624 y^4 - 12848080 y^3 z - 51202207 y^2 z^2 + 21339374 y z^3 + 44888767 z^4 = 0 \\ \text{with disc } X_{11} = & 2^{-27} \cdot 3^{-18} \cdot 31^{18} \cdot I_{27}^{\min} \text{ where } I_{27}^{\min} = -2^{72} \cdot 3^{18} \cdot 7^{14} \cdot 23^{14} \cdot 47^{14} \cdot 27527^{14}. \end{aligned}$$

$$\begin{aligned} \mathbf{X}_{12} : & -2283766 x^4 - 40282205 x^3 y + 65256060 x^3 z + 86351004 x^2 y^2 - 44980176 x^2 y z \\ & - 98227040 x^2 z^2 + 34948793 x y^3 + 112406040 x y^2 z - 10691928 x y z^2 - 811765633 x z^3 \\ & - 46977843 y^4 + 27242836 y^3 z + 210065028 y^2 z^2 - 159829005 y z^3 - 57425706 z^4 = 0 \\ \text{with disc } X_{12} = & -2^{-45} \cdot 3^{-18} \cdot I_{27}^{\min} \text{ where } I_{27}^{\min} = 2^5 \cdot 3^{18} \cdot 7^{14} \cdot 11^9 \cdot 5711^{14} \cdot 73064203493^{14}. \end{aligned}$$

$$\begin{aligned} \mathbf{X}_{13} : & 13741849 x^4 - 33952358 x^3 y - 12314654 x^3 z - 79058925 x^2 y^2 + 321820356 x^2 y z \\ & - 449435767 x^2 z^2 + 24161786 x y^3 + 58585032 x y^2 z + 184173924 x y z^2 + 202615424 x z^3 \\ & + 10642401 y^4 + 150598482 y^3 z + 136602159 y^2 z^2 - 6607170137 y z^3 + 3720024064 z^4 = 0 \\ \text{with disc } X_{13} = & 2^{-36} \cdot 3^{-18} \cdot 11^{18} \cdot 43^{18} \cdot I_{27}^{\min} \text{ where } I_{27}^{\min} = 2^{20} \cdot 3^{18} \cdot 11^9 \cdot 547^{14} \cdot 11827^{14} \cdot 189169^{14}. \end{aligned}$$

$$\begin{aligned} \mathbf{X}_{14} : & 727950 x^4 - 1982567 x^3 y - 1449460 x^3 z + 2619975 x^2 y^2 - 7272852 x^2 y z \\ & + 12943560 x^2 z^2 + 1222070 x y^3 - 9541020 x y^2 z - 10154664 x y z^2 + 31717821 x z^3 \\ & + 3907465 y^4 + 7463256 y^3 z + 4691252 y^2 z^2 + 58884154 y z^3 + 10671882 z^4 = 0 \\ \text{with disc } X_{14} = & 2^{-45} \cdot 3^{-18} \cdot 19^{18} \cdot I_{27}^{\min} \text{ where } I_{27}^{\min} = 2^5 \cdot 3^{18} \cdot 11^{19} \cdot 101^{14} \cdot 107^{14} \cdot 8378707^{14}. \end{aligned}$$

$$\begin{aligned} \mathbf{X}_{15} : & x^4 - x^3 y + 2 x^3 z + 2 x^2 y z + 2 x^2 z^2 - 2 x y^2 z + 4 x y z^2 - y^3 z + 3 y^2 z^2 + 2 y z^3 + z^4 = 0 \\ \text{with disc } X_{15} = & 2^{-45} \cdot 3^{-27} \cdot I_{27}^{\min} \text{ where } I_{27}^{\min} = 2^5 \cdot 3^{27} \cdot 19^7. \end{aligned}$$

$$\begin{aligned} \mathbf{X}_{16} : & 66648606 x^4 - 10422787 x^3 y - 1171743077 x^3 z + 272093232 x^2 y^2 \\ & + 894539212 x^2 y z + 1758438152 x^2 z^2 - 239684773 x y^3 - 3355325973 x y^2 z \\ & + 21854285561 x y z^2 + 213880974126 x z^3 + 731104019 y^4 - 6282157788 y^3 z \\ & - 38790710054 y^2 z^2 + 288506848419 y z^3 + 1153356733618 z^4 = 0 \\ \text{with disc } X_{16} = & 2^{-45} \cdot 3^{-27} \cdot 19^{18} \cdot I_{27}^{\min} \text{ where } I_{27}^{\min} = 2^5 \cdot 3^{35} \cdot 19^7 \cdot 37^{14} \cdot 79^{14} \cdot 13373064392147^{14}. \end{aligned}$$

$$\begin{aligned} \mathbf{X}_{17} : & 3717829 x^4 - 1434896 x^3 y + 19525079 x^3 z - 23623031 x^2 y^2 + 55253545 x^2 y z \\ & + 168545160 x^2 z^2 + 36024736 x y^3 - 64558785 x y^2 z + 379342822 x y z^2 - 329255097 x z^3 \\ & + 42096963 y^4 + 115245505 y^3 z - 817353798 y^2 z^2 + 498157725 y z^3 - 34967215 z^4 = 0 \\ \text{with disc } X_{17} = & 2^{-36} \cdot 3^{-27} \cdot I_{27}^{\min} \text{ where } I_{27}^{\min} = 2^{20} \cdot 3^{77} \cdot 19^7 \cdot 1229^{14} \cdot 3913841117^{14}. \end{aligned}$$

$$\begin{aligned} \mathbf{X}_{18} : & 3278898472 x^4 + 35774613556 x^3 y - 172165788624 x^3 z - 42633841878 x^2 y^2 \\ & + 224611458828 x^2 y z + 362086824567 x^2 z^2 + 6739276447 x y^3 + 195387780024 x y^2 z \\ & + 1153791743988 x y z^2 - 3461357269578 x z^3 - 18110161476 y^4 - 549025255626 y^3 z \\ & - 482663555556 y^2 z^2 + 15534718882176 y z^3 - 61875497274721 z^4 = 0 \\ \text{with disc } X_{18} = & 2^{-36} \cdot 13^{18} \cdot I_{27}^{\min} \text{ where } I_{27}^{\min} = -2^{32} \cdot 19^7 \cdot 101^{14} \cdot 251^{14} \cdot 7468843725186901^{14}. \end{aligned}$$

$$\begin{aligned} \mathbf{X}_{19} : & -7 x^4 - 2 x^3 y + 16 x^3 z + 7 x^2 y^2 - 6 x^2 y z - 8 x^2 z^2 + 10 x y^3 + 14 x y^2 z \\ & + 2 x y z^2 - 15 x z^3 + y^4 + 10 y^3 z + 13 y^2 z^2 + 17 y z^3 + 14 z^4 = 0 \\ \text{with disc } X_{19} = & 2^{-36} \cdot 3^{-27} \cdot I_{27}^{\min} \text{ where } I_{27}^{\min} = 2^{20} \cdot 3^{27} \cdot 11^{14} \cdot 43^7. \end{aligned}$$

$$\begin{aligned} \mathbf{X}_{20} : & 42978499 x^4 + 91609890 x^3 y + 226411413 x^3 z - 152950386 x^2 y^2 + 225973290 x^2 y z \\ & + 64073952 x^2 z^2 + 26287800 x y^3 + 11918208 x y^2 z - 742181730 x y z^2 - 464894250 x z^3 \\ & - 29463649 y^4 + 198058830 y^3 z - 144994689 y^2 z^2 - 208213515 y z^3 + 85424183 z^4 = 0 \\ \text{with disc } X_{20} = & -2^{-45} \cdot I_{27}^{\min} \text{ where } I_{27}^{\min} = 2^5 \cdot 67^7 \cdot 1439^{14} \cdot 2739021126001^{14}. \end{aligned}$$

REFERENCES

- [1] E. Arbarello, M. Cornalba, P. A. Griffiths, and J. Harris. *Geometry of algebraic curves. Vol. I*, volume 267 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, New York, 1985.
- [2] J. S. Balakrishnan, S. Ionica, K. Lauter, and C. Vincent. Genus 3. Package available at <https://github.com/christellevincent/genus3>.
- [3] J. S. Balakrishnan, S. Ionica, K. Lauter, and C. Vincent. Constructing genus 3 hyperelliptic Jacobians with CM. [arXiv:1603.03832](https://arxiv.org/abs/1603.03832), 2016.
- [4] C. Batut, K. Belabas, D. Benardi, H. Cohen, and M. Olivier. *User's Guide to PARI-GP*, 1998. <https://pari.math.u-bordeaux.fr>.
- [5] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).
- [6] I. Bouw, J. Cooley, K. Lauter, E. Lorenzo García, M. Manes, R. Newton, and E. Ozman. Bad reduction of genus three curves with complex multiplication. In *Women in numbers Europe*, volume 2 of *Assoc. Women Math. Ser.*, pages 109–151. Springer, Cham, 2015.
- [7] F. Bouyer and M. Streng. Examples of CM curves of genus two defined over the reflex field. *LMS J. Comput. Math.*, 18(1):507–538, 2015.
- [8] R. Bröker and P. Stevenhagen. Elliptic curves with a given number of points. In *Algorithmic number theory*, volume 3076 of *Lecture Notes in Comput. Sci.*, pages 117–131. Springer, Berlin, 2004.
- [9] E. Costa, N. Mascot, J. Sijsling, and J. Voight. Rigorous computation of the endomorphism ring of a Jacobian. [arXiv:1707.01158](https://arxiv.org/abs/1707.01158), 2016.
- [10] B. Deconinck, M. Heil, A. Bobenko, M. van Hoeij, and M. Schmies. Computing Riemann theta functions. *Math. Comp.*, 73(247):1417–1442, 2004.
- [11] B. Deconinck and M. van Hoeij. Computing Riemann matrices of algebraic curves. *Phys. D*, 152/153:28–46, 2001. Advances in nonlinear mathematics and science.
- [12] J. Dixmier. On the projective invariants of quartic plane curves. *Adv. in Math.*, 64:279–304, 1987.
- [13] R. Dupont. *Moyenne arithmético-géométrique, suites de Borchardt et applications*. PhD thesis, École polytechnique, Palaiseau, 2006.
- [14] A.-S. Elsenhans. Good models for cubic surfaces. Preprint at https://math.uni-paderborn.de/fileadmin/mathematik/AG-Computeralgebra/Preprints-elsenhans/red_5.pdf.
- [15] A.-S. Elsenhans. Explicit computations of invariants of plane quartic curves. *J. Symbolic Comput.*, 68(part 2):109–115, 2015.
- [16] A. Fiorentino. Weber's formula for the bitangents of a smooth plane quartic. [arXiv:1612.02049](https://arxiv.org/abs/1612.02049), 2016.
- [17] M. Girard and D. R. Kohel. Classification of genus 3 curves in special strata of the moduli space. In Hess, F. (ed.) et al., *Algorithmic number theory. 7th international symposium, ANTS-VII, Berlin, Germany, July 23–28, 2006. Proceedings*. Berlin: Springer. Lecture Notes in Computer Science 4076, 346–360., 2006.
- [18] E. Z. Goren and K. E. Lauter. Class invariants for quartic CM fields. *Ann. Inst. Fourier (Grenoble)*, 57(2):457–480, 2007.
- [19] B. H. Gross and J. Harris. On some geometric constructions related to theta characteristics. In *Contributions to automorphic forms, geometry, and number theory*, pages 279–311. Johns Hopkins Univ. Press, Baltimore, MD, 2004.
- [20] J. Guàrdia. On the Torelli problem and Jacobian Nullwerte in genus three. [arXiv:0901.4376](https://arxiv.org/abs/0901.4376), 2009.
- [21] J.-I. Igusa. *Theta functions*, volume 194 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, New York, 1972.
- [22] P. Kılıçer. *The CM class number one problem for curves*. PhD thesis, Universiteit Leiden and Université de Bordeaux, 2016.
- [23] P. Kılıçer, H. Labrande, R. Lercier, C. Ritzenthaler, J. Sijsling, and M. Streng. CM plane quartics. Available at <https://arxiv.org/abs/1606.05594v2/anc/curves.txt>.
- [24] P. Kılıçer, K. Lauter, E. Lorenzo García, R. Newton, E. Ozman, and M. Streng. A bound on the primes of bad reduction for CM curves of genus 3. [arXiv:1609.05826](https://arxiv.org/abs/1609.05826), 2016.

- [25] P. Kılıçer, E. Lorenzo García, and M. Streng. Primes dividing invariants of CM Picard curves. [arXiv:1801.04682](https://arxiv.org/abs/1801.04682), 2018.
- [26] P. Kılıçer and M. Streng. Rational CM points and class polynomials for genus three. In preparation, 2016.
- [27] K. Koike and A. Weng. Construction of CM Picard curves. *Math. Comp.*, 74(249):499–518 (electronic), 2005.
- [28] S. Koizumi. The fields of moduli for polarized abelian varieties and for curves. *Nagoya Math. J.*, 48:37–55, 1972.
- [29] H. Labrande. Calculating theta functions in genus 3. Package available at <http://hlabrande.fr/pubs/fastthetaconstantsgenus3.m>.
- [30] H. Labrande. *Explicit computation of the Abel-Jacobi map and its inverse*. PhD thesis, Université de Lorraine and University of Calgary, Nov. 2016.
- [31] H. Labrande and E. Thomé. Computing theta functions in quasi-linear time in genus two and above. *LMS J. Comput. Math.*, 19(suppl. A):163–177, 2016.
- [32] S. Lang. *Complex multiplication*, volume 255 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, New York, 1983.
- [33] J.-C. Lario and A. Somoza. A note on Picard curves of CM-type. [arXiv:1611.02582](https://arxiv.org/abs/1611.02582), 2016.
- [34] K. Lauter. Geometric methods for improving the upper bounds on the number of rational points on algebraic curves over finite fields. *J. Algebraic Geom.*, 10(1):19–36, 2001. With an appendix by J.-P. Serre.
- [35] K. Lauter and B. Viray. An arithmetic intersection formula for denominators of Igusa class polynomials. *Amer. J. Math.*, 137(2):497–533, 2015.
- [36] R. Lercier and C. Ritzenthaler. Invariants and reconstructions for genus 2 curves in any characteristic, 2008. Available in MAGMA 2.15 and later.
- [37] R. Lercier and C. Ritzenthaler. Hyperelliptic curves and their invariants: geometric, arithmetic and algorithmic aspects. *J. Algebra*, 372:595–636, 2012.
- [38] R. Lercier, C. Ritzenthaler, F. Rovetta, and J. Sijsling. Parametrizing the moduli space of curves and applications to smooth plane quartics over finite fields. *LMS J. Comput. Math.*, 17(suppl. A):128–147, 2014.
- [39] R. Lercier, C. Ritzenthaler, and J. Sijsling. Fast computation of isomorphisms of hyperelliptic curves and explicit descent. In E. W. Howe and K. S. Kedlaya, editors, *Proceedings of the Tenth Algorithmic Number Theory Symposium*, pages 463–486. Mathematical Sciences Publishers, 2012.
- [40] R. Lercier, C. Ritzenthaler, and J. Sijsling. Explicit Galois obstruction and descent for hyperelliptic curves with tamely cyclic reduced automorphism group. *Math. Comp.*, 85(300):2011–2045, 2016.
- [41] R. Lercier, C. Ritzenthaler, and J. Sijsling. `quartic_reconstruction`; a MAGMA package for reconstructing plane quartics from Dixmier-Ohno invariants. Package available at https://github.com/JRSijsling/quartic_reconstruction, 2016.
- [42] R. Lercier, C. Ritzenthaler, and J. Sijsling. Reconstructing plane quartics from their invariants. [arXiv:1606.05594](https://arxiv.org/abs/1606.05594), 2016.
- [43] E. Lorenzo García, R. Lercier, and C. Ritzenthaler. Hyperelliptic reduction of plane smooth quartics. In preparation, 2017.
- [44] J.-F. Mestre. Construction de courbes de genre 2 à partir de leurs modules. In *Effective methods in algebraic geometry*, volume 94 of *Prog. Math.*, pages 313–334, Boston, 1991. Birkhäuser.
- [45] H. E. Rauch and H. M. Farkas. *Theta functions with applications to Riemann surfaces*. The Williams & Wilkins Co., Baltimore, Md., 1974.
- [46] C. Ritzenthaler. Point counting on genus 3 non hyperelliptic curves. In *Algorithmic number theory*, volume 3076 of *Lecture Notes in Comput. Sci.*, pages 379–394. Springer, Berlin, 2004.
- [47] J.-P. Serre and J. Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968.
- [48] G. Shimura. On the field of rationality for an abelian variety. *Nagoya Math. J.*, 45:167–178, 1971.
- [49] G. Shimura. On abelian varieties with complex multiplication. *Proc. London Math. Soc. (3)*, 34(1):65–86, 1977.
- [50] G. Shimura and Y. Taniyama. Complex multiplication of Abelian varieties and its applications to number theory. *Publ. Math. Soc. Japan*, 6, 1961.

- [51] D. Simon. Solving quadratic equations using reduced unimodular quadratic forms. Preprint available at <http://www.math.unicaen.fr/~simon/maths/qfsolve.html>, 2013.
- [52] A.-M. Spallek. *Kurven vom Geschlecht 2 und ihre Anwendung in Publik-Key-Kryptosystemen*. PhD thesis, Institut für Experimentelle Mathematik, Essen, 1994.
- [53] M. Stoll. Reduction theory of point clusters in projective space. *Groups Geom. Dyn.*, 5(2):553–565, 2011.
- [54] M. Streng. Sage package for using Shimura’s reciprocity law for Siegel modular functions. <http://www.math.leidenuniv.nl/~streng/recipe>.
- [55] M. Streng. Computing Igusa class polynomials. *Math. Comp.*, 83(285):275–309, 2014. [arXiv:0903.4766](https://arxiv.org/abs/0903.4766).
- [56] J. Tate. Classes d’isogénie des variétés abéliennes sur un corps fini (d’après Honda). In *Séminaire Bourbaki 1968/69*, volume 179 of *Lecture Notes in Math.*, pages 95–110. Springer, Berlin, 1971.
- [57] W. Tautz, J. Top, and A. Verberkmoes. Explicit hyperelliptic curves with real multiplication and permutation polynomials. *Canad. J. Math.*, 43(5):1055–1064, 1991.
- [58] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 7.4)*, 2016. <http://www.sagemath.org>.
- [59] S. M. van Rijnsouw. *Testing the equivalence of planar curves*. PhD thesis, Technische Universiteit Eindhoven, Eindhoven, 2001.
- [60] P. van Wamelen. Examples of genus two CM curves defined over the rationals. *Math. Comp.*, 68(225):307–320, 1999.
- [61] J. Voight. Identifying the matrix ring: algorithms for quaternion algebras and quadratic forms. In *Quadratic and higher degree forms*, volume 31 of *Dev. Math.*, pages 255–298. Springer, New York, 2013.
- [62] H. Weber. Theory of abelian functions of genus 3. (Theorie der Abel’schen Functionen vom Geschlecht 3.), 1876.
- [63] A. Weng. A class of hyperelliptic CM-curves of genus three. *J. Ramanujan Math. Soc.*, 16(4):339–372, 2001.

PINAR KILIÇER, CARL VON OSSIEZKY UNIVERSITÄT OLDENBURG, INSTITUT FÜR MATHEMATIK, 26111 OLDENBURG, GERMANY
E-mail address: pinarkilicer@gmail.com

HUGO LABRANDE, LORIA/INRIA LORRAINE, ÉQUIPE CARMEL, 615 RUE DU JARDIN BOTANIQUE, 54602 VILLERS-LÈS-NANCY CEDEX, FRANCE.

ISPIA, UNIVERSITY OF CALGARY, 2500 UNIVERSITY DR NW, CALGARY, ALBERTA, T2N 1N4, CANADA.
E-mail address: hugo@hlabrande.fr

REYNALD LERCIER, DGA MI, LA ROCHE MARGUERITE, 35174 BRUZ, FRANCE.

IRMAR, UNIVERSITÉ DE RENNES 1, CAMPUS DE BEAULIEU, 35042 RENNES, FRANCE.
E-mail address: reynald.lercier@m4x.org

CHRISTOPHE RITZENTHALER, IRMAR, UNIVERSITÉ DE RENNES 1, CAMPUS DE BEAULIEU, 35042 RENNES, FRANCE.
E-mail address: christophe.ritzenthaler@univ-rennes1.fr

JEROEN SIJSLING, INSTITUT FÜR REINE MATHEMATIK, UNIVERSITÄT ULM, HELMHOLTZSTRASSE 18, 89081 ULM, GERMANY
E-mail address: jeroen.sijssling@uni-ulm.de

MARCO STRENG, MATHEMATISCH INSTITUUT, UNIVERSITEIT LEIDEN, P.O. BOX 9512, 2300 RA LEIDEN, THE NETHERLANDS
E-mail address: streng@math.leidenuniv.nl