GENERIC MODELS FOR GENUS 2 CURVES WITH REAL MULTIPLICATION

ALEX COWAN, SAM FRENGLEY, AND KIMBALL MARTIN

Abstract. Explicit models of families of genus 2 curves with multiplication by $\sqrt{D}$ are known for $D = 2, 3, 5$. We obtain generic models for genus 2 curves over $\mathbb{Q}$ with real multiplication in 12 new cases, including all fundamental discriminants $D < 40$. A key step in our proof is to develop an algorithm for minimisation of conic bundles fibred over $\mathbb{P}^2$. We apply this algorithm to simplify the equations for the Mestre conic associated to the generic point on the Hilbert modular surface of fundamental discriminant $D < 100$ computed by Elkies–Kumar.

1. Introduction

Let C be a genus 2 curve over a field k of characteristic 0 and let $D > 0$ be a fundamental discriminant. Let $\mathrm{Jac}(C)$ denote the Jacobian of C. We say C has RM D if it has real multiplication by the quadratic order $\mathcal{O}_D$ of discriminant D, i.e., if $\mathcal{O}_D$ embeds into the ring of endomorphisms of $\mathrm{Jac}(C)$ fixed by the Rosati involution. Families of genus 2 curves with RM 5 and RM 8 have been known for some time (e.g., [Mes91a, Bru95, Ben99]), however these families do not provide simple ways to parametrise genus 2 curves with RM D over k (even up to twists, i.e., $\bar{k}$-isomorphism). Moreover the methods used to construct these families are very specific to $D = 5$ and $D = 8$.

In this paper we develop a method to (i) give generic models for genus 2 curves with RM D, and (ii) parametrise such curves up to twists. We successfully carry out this method for many fundamental discriminants D (including all 11 positive fundamental discriminants $D < 40$), under the assumption that k has characteristic 0.

Theorem 1.1. *Let $D \in \{5, 8, 12, 13, 17, 21, 24, 28, 29, 33, 37, 44, 53, 61\}$ and let k be a field of characteristic 0. Let $F_D(z, g, h, r, s; x) \in \mathbb{Q}(z, g, h, r, s)[x]$ be the sextic polynomial given in the electronic data associated to this paper* [CFM24]*. Let $\mathscr{L}_D/\mathbb{Q}$ denote the conic bundle given by the vanishing of*

$$z^2 - \lambda_D \quad \text{and} \quad r^2 - Ds^2 - q_D$$

in $\mathbb{A}^5$, where $\lambda_D, q_D \in \mathbb{Z}[g, h]$ are the polynomials defined via (1.1) *and Table 1 respectively. Then:*

(i) *The family of genus 2 curves given by the Weierstrass equations*

$$y^2 = F_D(z, g, h, r, s; x)$$

for $(z, g, h, r, s) \in \mathscr{L}_D(k)$ provides a generic model (in the sense of Remark 2.1) for genus 2 curves with RM D defined over k.

(ii) *Generically, two such curves are $\bar{k}$-isomorphic if and only if the corresponding points on $\mathscr{L}_D$ have the same image under the forgetful map $\mathscr{L}_D \to \mathbb{A}^2$ given by $(z, g, h, r, s) \mapsto (g, h)$.*

Theorem 1.1(i) provides families in 5 parameters satisfying 2 relations, but for many such D one can do much better. Indeed, when $D \leq 17$ we show in Section 7.2 that the threefold $\mathscr{L}_D$ is rational over $\mathbb{Q}$. By parametrising $\mathscr{L}_D$ we give generic families

Date: March 5, 2024.

in 3 parameters with no relations. In fact, when $D = 17$ a generic family exists in 2 parameters with no relations. To illustrate this we present the families for $D = 12$ and 17.

Corollary 1.2 (A generic RM 12 family)**.** *Let k be a field of characteristic 0. For each $a, b, c \in k$ consider the cubic k-algebra $L = k[r]/\xi(r)$ where*

$$\xi(r) = r^3 - 3(a^2 - 3b^2)r + 2(a^2 - 3b^2),$$

and let

$$\varphi(x) = (r^2 + (2a - 3b)r - (a^2 + 2a - 3b^2 - 3bc - 3b))x^2 - 6((a - 2b)r - ac - a + 2b)x \\ - 3(r^2 - (2a - 3b)r - (a^2 - 2a - 3b^2 + 3bc + 3b)).$$

If $\xi(r)$ has no repeated roots we write $f_{12}(a, b, c; x) = \mathrm{Nm}_{L/K}\,\varphi(x)$. If $f_{12}(a, b, c; x)$ has no repeated roots then the Jacobian J of the genus 2 curve C/k with Weierstrass equation $C : y^2 = f_{12}(a, b, c; x)$ has RM 12 over $\bar{k}$, and if $\mathrm{End}_{\bar{k}}(J)$ is abelian then the RM is defined over k. Moreover, this is a generic family of genus 2 curves with RM 12 over $\mathbb{Q}$.

Corollary 1.3 (A generic RM 17 family)**.** *Let k be a field of characteristic 0. For each $a, b \in k$ let*

$$\varphi(x) = (a^2 - 8ab + 4a - 9b^2 - 6b + 3)x^3 + 3(7ab - 3a + 7b^2 + 4b - 3)x^2 + 4(a^2 - 7ab \\ + 3a - 4b^2)x + 4(3ab - a + b^2 - b),$$

and

$$\psi(x) = 4(a^2b + 5ab^2 - 7ab + 2a - 6b^2 + 2b)x^3 + 4(6a^2b - 2a^2 - 12ab^2 + 11ab - 3a \\ + 14b^2 - 6b)x^2 + (4a^3 - 34a^2b + 16a^2 + 38ab^2 - 43ab + 9a - 43b^2 + 36b - 9)x \\ + 12a^2b - 4a^2 - 10ab^2 + 14ab - 4a + 11b^2 - 14b + 3.$$

If the sextic polynomial $f_{17}(a, b; x) = \varphi(x)\psi(x)$ has no repeated roots, the Jacobian J of the genus 2 curve C/k given by the Weierstrass equation $C : y^2 = f_{17}(a, b; x)$ has RM 17 over $\bar{k}$, and if $\mathrm{End}_{\bar{k}}(J)$ is abelian then the RM is defined over k. Moreover, this is a generic family of genus 2 curves with RM 17 over $\mathbb{Q}$.

Remark 1.4. In our proof of Corollaries 1.2 and 1.3 we obtain a map from the respective parameter spaces to the (g, h)-plane. This allows us to give simple conditions (exploiting Theorem 1.1) for when pairs of parameters correspond to (geometrically) isomorphic curves (see Proposition 7.3).

1.1. **Parametrising genus 2 curves with RM D.** Our approach to proving Theorem 1.1 is via moduli. Let $D > 0$ be a fundamental discriminant. The Hilbert modular surface $Y_-(D)$ of discriminant D provides a (coarse) moduli space for genus 2 curves with RM D together with the RM D action. Forgetting the choice of RM D realises $Y_-(D)$ as a double cover of the Humbert surface of discriminant D, which we denote $\mathcal{H}_D$. (For precise definitions, see Section 2.1).

For each fundamental discriminant $D < 100$ the Humbert surface $\mathcal{H}_D$ is $\mathbb{Q}$-birational to $\mathbb{A}^2$ and in each of these cases Elkies and Kumar [EK14] computed explicit rational parametrisations $\mathbb{Q}(\mathcal{H}_D) \cong \mathbb{Q}(g, h)$ together with rational maps $\mathbb{A}^2 \dashrightarrow \mathcal{M}_2$ realising the moduli interpretation of $\mathcal{H}_D$. Moreover, they give explicit $\mathbb{Q}$-birational models for $Y_-(D)$ in the form

$$z^2 = \lambda_D, \tag{1.1}$$

for each fundamental discriminant $D < 100$, where $\lambda_D \in \mathbb{Z}[g, h] \subset \mathbb{Q}(\mathcal{H}_D)$ is a squarefree polynomial.

D	q_D
5	$-6(10g+3)(15g+2)$
8	$4g+4h-7$
12	$-(h-1)(3h^3+9h^2-27g-4h-8)$
13	$-100g^2+385gh-48h^2+194g+168h-108$
17	1
21	$18g^2-12gh-12h^2-14$
24	$12gh^2-3g^2-2h^2+3$
28	$-2(19g^2+35h^2+84h+28)$
29	$-6g^2-6gh+65g-16h^2-156h+4$
33	1
37	$g^2+15gh+20g-27h^2+2h-11$
44	$(gh+h-1)(5g^3h+9g^2h+6g^2-4gh+18g-8h+19)$
53	$-(25h^2+42h+24)g^2-(h+1)^2(26h+7)g-11(h+1)^4$
61	$-3(3h^2+7h-1)g^2+2(9h^3+12h^2-10h-1)g-9h^4-3h^3+8h^2+8h-20$

TABLE 1. Rational functions $q_D \in \mathbb{Q}(\mathcal{H}_D)$ such that the Mestre conic L_D is isomorphic over $\mathbb{Q}(Y_-(D))$ to $X^2 - DY^2 - q_D Z^2 = 0$.

In fact, the Hilbert modular surface $Y_-(D)$ is itself rational if and only if $D = 5, 8, 12, 13, 17$ (see [vdG88, Theorem VII.3.4]). Elkies and Kumar also give rational parametrisations $\mathbb{Q}(Y_-(D)) \cong \mathbb{Q}(m, n)$ in these cases, together with the rational maps $(m, n) \mapsto (g, h)$ induced by forgetful morphisms $Y_-(D) \to \mathcal{H}_D$.

By construction, a k-rational point $(z, g, h) \in Y_-(D)$ corresponds to genus 2 curve $C/\bar{k}$ with RM D. Indeed, if $\mathrm{Aut}(C) \cong C_2$, then C admits a model over k if and only if the *Mestre obstruction* vanishes, i.e., if the *Mestre conic* associated to the image of (g, h) in $\mathcal{M}_2$ has a k-rational point (for more details see Section 2.2). We write L_D for the Mestre conic associated to the generic point of $\mathcal{H}_D$.

In general, the conic L_D has quite complicated coefficients in g and h, and there is no obvious simple criterion for the Mestre obstruction to vanish. An argument of Poonen (see Proposition 3.1) shows that L_D is isomorphic over $\mathbb{Q}(Y_-(D))$ to a conic of the form

$$\widetilde{L}_D \colon X^2 - DY^2 - q_D Z^2 = 0 \tag{1.2}$$

for some rational function $q_D \in \mathbb{Q}(\mathcal{H}_D) \subset \mathbb{Q}(Y_-(D))$. The proof of this result is non-constructive, and to actually find such a function q_D (as well as the requisite transformations) is not at all easy. The main step in the proof of Theorem 1.1 is to find such transformations, and in particular we have the following theorem.

Theorem 1.5. *For $D \in \{5, 8, 12, 13, 17, 21, 24, 28, 29, 33, 37, 44, 53, 61\}$, the Mestre conic L_D is isomorphic to $X^2 - DY^2 - q_D Z^2$ where $q_D \in \mathbb{Q}(g, h)$ is the polynomial of Elkies–Kumar coordinates (z, g, h) given in Table 1.*

Furthermore, for the 5 fundamental discriminants $D \in \{5, 8, 12, 13, 17\}$ such that $Y_-(D)$ is birational to $\mathbb{A}^2$, the Mestre conic L_D is isomorphic to $X^2 - DY^2 - p_D Z^2$ where $p_D \in \mathbb{Q}(m, n)$ is the polynomial in Elkies–Kumar coordinates (m, n) given in Table 2.

D	p_D
5	$m^2 - 5n^2 - 5$
8	$-(m+1)$
12	$-27m^2 + n^2 + 27$
13	$1803m^2 - 72mn + n^2 + 3168m - 1440n - 768$
17	1

TABLE 2. Rational functions $p_D \in \mathbb{Q}(m,n)$ such that the Mestre conic L_D is isomorphic to $X^2 - DY^2 - p_D Z^2 = 0$ when $Y_-(D)$ is rational.

Remark 1.6. It is natural to wonder about the significance of the curves that q_D and p_D cut out in $Y_-(D)$. We make some remarks about this in Section 9, including a conjecture for q_{40}, but this remains quite mysterious to us.

The first part of Theorem 1.5, together with Mestre's method of constructing a genus 2 curve from a rational point on L_D yields Theorem 1.1, which we recall gives models in 5 parameters with 2 relations. Using the latter part of this theorem for $D = 5, 8, 12, 13, 17$ provides models in 4 parameters with 1 relation. In fact Theorem 1.5 implies that for each $D \leq 17$, the Mestre conic bundle $\mathscr{L}_D \to Y_-(D)$ is a rational threefold. Parametrising $\mathscr{L}_D$ then allows us to give models in 3 parameters with no relations.

Conversely, the conic bundle $\mathscr{L}_D$ is never (uni-)rational when $D > 17$ since the Hilbert modular surface $Y_-(D)$ is not rational; see [vdG88, Theorem VII.3.4]. Note that, since q_D is a rational function on $\mathcal{H}_D$, equation (1.2) defines a conic over $\mathbb{Q}(\mathcal{H}_D)$. This conic spreads out to a conic bundle $\mathscr{L}_D^{\mathcal{H}} \to \mathcal{H}_D$ which, *a priori*, may be rational. In such cases it is possible to give a 4-parameter family $y^2 = f_D(a,b,c,z;x)$ subject to a single relation $z^2 = \Lambda(a,b,c)$ for some polynomial $\Lambda(a,b,c) \in \mathbb{Z}[a,b,c]$.

Question 1.7. *Does there exist a fundamental discriminant D such that $\mathscr{L}_D^{\mathcal{H}}$ is not geometrically (uni-)rational but $\mathcal{H}_D$ is a rational surface?*

When $D = 21$, 28, 29, 33, 37, 44, 53, and 61 we exhibit explicit parametrisations of the threefolds $\mathscr{L}_D^{\mathcal{H}}$, which may be found in [CFM24]. Moreover, we give a parametrisation of $\mathscr{L}_{24}^{\mathcal{H}}$ over $\mathbb{Q}(\sqrt{-2})$.

Note that $\mathscr{L}_D^{\mathcal{H}}$ is not birational to the Mestre conic bundle over $\mathcal{H}_D$. Rather, Proposition 3.1 implies that the Mestre conic over $\mathbb{Q}(\mathcal{H}_D)$ is isomorphic to a conic of the form $X^2 - D\lambda_D Y^2 - q_D Z^2 = 0$. It is not clear if the Mestre conic bundle over $\mathcal{H}_D$ is ever rational.

As mentioned above, when $D = 17$ we may remove one more parameter without losing genericity. This is because the Mestre obstruction vanishes whenever $D \equiv 1 \pmod 8$.

Theorem 1.8. *If $D \equiv 1 \pmod 8$ is a positive fundamental discriminant, then the Mestre conic L_D is isomorphic over $\mathbb{Q}(Y_-(D))$ to a conic of the form $X^2 - DY^2 - Z^2$, i.e., we can take $q_D = 1$.*

In Section 3 we prove Theorem 1.8 by studying the RM action on the 2-torsion on a Jacobian with RM D. When $D \equiv 1 \pmod 8$, the prime 2 splits in $\mathbb{Q}(\sqrt{D})$, and using this observation we prove that a genus 2 curve with such RM has a Weierstrass model of the form $y^2 = \varphi(x)\psi(x)$ for some cubic polynomials $\varphi(x), \psi(x) \in k[x]$ (see Lemma 3.5). These facts also allow us to get a relatively nice model in the case $D = 33$.

Theorem 1.8 implies that whenever $D \equiv 1 \pmod 8$, the image of the set of rational points on $Y_-(D)$ under the double covering map $Y_-(D) \to \mathcal{H}_D$ generically parametrises genus 2 curves with RM D over k (up to twist). However, Theorem 1.8 by itself is not sufficient to construct generic models.

1.2. **An outline of the proof of Theorem 1.1: Simplifying the Mestre conic.** To prove Theorems 1.1 and 1.5 we construct transformations which put the Mestre conic L_D into one of the form (1.2). In [CMb] the first and third authors carried this out using naive methods when $D = 5$. However, that approach is not practical for $D > 5$.

The main idea is to employ *minimisation*, similar to Tate's algorithm for elliptic curves. We regard a conic $L/\mathbb{Q}(t_1, t_2)$ as the generic fibre of a conic defined over $\mathbb{Z}[t_1, t_2]$. By repeatedly blowing-up singularities of the latter we are often able to *minimise* L, that is, find an isomorphic conic whose discriminant has minimal degree (viewed as an element of $\mathbb{Z}[t_1, t_2]$). However $\mathbb{Z}[t_1, t_2]$ is not a PID so, unlike when L is defined over $\mathbb{Q}$, this process turns out to be quite delicate as:

(1) most blow-ups introduce other bad primes, which may be worse, and
(2) this process is extremely sensitive to the order in which these blow-ups are made.

For most $D < 30$, with a lot of patience and various tricks, one can carry out this process "by hand" (i.e., human-directed calculations in `Magma` [BCP97]) to find q_D, however the complexity grows quickly with D.

In Section 5 we develop and implement an algorithm which automates this minimisation process. By running this algorithm we find the transformations necessary to prove Theorem 1.5. Applying these transformations we find the corresponding generic models (see Section 7). Our `Magma` implementation has been made available through the GitHub repository [CFM24].

The minimisation approach which we employ is likely well known to experts, but the automation aspect seems to be novel (and can be adapted to much more general situations than conics defined over 2-variable function fields). To be clear, we are not able to give an effective algorithm to minimise a conic in the sense of provably terminating with a solution. Rather, we give an algorithm to search through a tree of sequences of blow-ups, which involves carefully scoring and pruning paths. This is necessary since the whole search tree is massive (it is infinite) and individual blow-up calculations can get very slow. Runtimes for our algorithm can be found in Table 3. It is not clear that increasing computational resources would allow us to treat more discriminants.

Remark 1.9. The preliminary step in our approach has applications to reconstructing general genus 2 curves (i.e., without an RM condition) from their moduli. Mestre's original conic is given in a simple form in terms of Clebsch invariants, however, in practice, one often begins with Igusa–Clebsch invariants and writes the Mestre conic in terms of Igusa–Clebsch invariants. The resulting coefficients can be quite large even when the Igusa–Clebsch invariants are small. In Section 4.1 we present simplified forms of Mestre's conic in terms of Igusa–Clebsch invariants. In addition to simplifying our minimisation process, this can also be used to construct genus 2 curves from Igusa–Clebsch invariants with smaller coefficients than the standard procedure.

1.3. **Further remarks.** First, we say a little more about previous works on families of genus 2 curves with RM. In [Mes91a], Mestre constructed 2-parameter families with RM 5 and RM 8. These families, however, do not contain all twist classes over $\mathbb{Q}$. Brumer (see [Bru95, Has00]) constructed a 3-parameter family with RM 5 — it is not known if Brumer's family covers all twist classes over $\mathbb{Q}$. Bending [Ben98, Ben99] gave a versal family with RM 8 determined (up to quadratic twist) by three parameters $A, P, Q \in k$ (that is, every genus 2 curve with RM 8 arises in this way, but distinct parameters (A, P, Q) may correspond to $\bar{k}$-isomorphic curves). These constructions, however, are quite specific to discriminants 5 and 8. Moreover, it is not clear from these constructions which parameters yield isomorphic curves, either over k or $\bar{k}$.

To our knowledge, aside from being generic models, ours are the first explicit models of any families of genus 2 curves with RM D beyond the cases of $D = 5, 8$, and the recent work of [BFS23] for $D = 12$ with full $\sqrt{3}$-level structure. See Section 8 for comparisons between our models and existing families.

In [EK14], for many fundamental discriminants $D < 100$, Elkies and Kumar identified one or more curves on $Y_-(D)$ with no Brauer obstruction, which typically correspond to 1-parameter families of genus 2 curves over $\mathbb{Q}$ with RM D. (Note that modular curves on $Y_-(D)$ need not correspond to families of genus 2 curves where the RM is defined over $\mathbb{Q}$.) However, no explicit models were given.

One application of such explicit models is to estimate counts of genus 2 curves with RM D by discriminant or conductor, which translates into estimates of counts of weight 2 newforms with rationality field $\mathbb{Q}(\sqrt{D})$. In [CMa], we used existing models to prove lower bounds for such counts for $D = 5, 8$. Our models here should have similar applications to other discriminants D.

Acknowledgements. We thank Noam Elkies, Tom Fisher, and Jef Laga for helpful discussions. We are grateful to Bjorn Poonen for kindly explaining Proposition 3.1 and its proof to us, and allowing us to include it here.

The algorithms in the paper have been implemented in `Magma` and our implementation has been made publicly available through the GitHub repository [CFM24].

AC was supported by the Simons Foundation Collaboration Grant 550031. SF was supported by the Woolf Fisher and Cambridge Trusts and by Royal Society Research Fellows Enhanced Research Expenses RF\ERE\210398. KM was supported by the Japan Society for the Promotion of Science (Invitational Fellowship L22540), and the Osaka Central Advanced Mathematical Institute (MEXT Joint Usage/Research Center on Mathematics and Theoretical Physics JPMXP0619217849).

This work was also supported by the National Science Foundation under Grant No. DMS-1929284 while the authors were in residence at the Institute for Computational and Experimental Research in Mathematics in Providence, RI, during Collaborate@ICERM "Rational Genus 2 Curves with Real Multiplication." Calculations were performed using computational resources and services at the Center for Computation and Visualisation, Brown University. We thank ICERM and Brown University for their hospitality, and providing access to their OSCAR Supercomputer.

2. Background

2.1. **Real multiplication and Hilbert modular surfaces.**

Let k be a field of characteristic 0, and let C/k be a genus 2 curve. We equip the Jacobian $J = \mathrm{Jac}(C)$ with the canonical principal polarisation and for each endomorphism $\psi \in \mathrm{End}_{\bar{k}}(J)$ we write $\psi^\dagger$ for its image under the Rosati involution, that is $\psi^\dagger = \zeta^{-1} \circ \hat{\psi} \circ \zeta$ where ζ is the principal polarisation on J and $\hat{\psi}$ is the dual of ψ. Denote by $\mathrm{End}^\dagger_{\bar{k}}(J) \subset \mathrm{End}_{\bar{k}}(J)$ the subalgebra of endomorphisms fixed by the Rosati involution, i.e., for which $\psi = \psi^\dagger$.

Let D be a fundamental discriminant. If $\mathrm{End}^\dagger_k(J)$ contains the quadratic order $\mathcal{O}_D$ of discriminant D, we say J (and C) has real multiplication (RM) by $\mathcal{O}_D$, and abbreviate this as RM D.

Let $\mathcal{M}_2$ and $\mathcal{A}_2$ denote the (coarse) moduli spaces of genus 2 curves and principally polarised abelian surfaces, respectively. We define for the *Hilbert modular surface* $Y_-(D)$ *of discriminant* D to be the coarse moduli space parametrising pairs $(J/k, \iota)$ where J/k is a genus 2 Jacobian, and $\iota\colon \mathcal{O}_D \hookrightarrow \mathrm{End}^\dagger_k(J)$ is an injective ring homomorphism. (This is birational to the definition in terms of principally polarised abelian surfaces used in [vdG88] and [EK14].)

There is a natural forgetful map $Y_-(D) \to \mathcal{A}_2$ given functorially by forgetting ι. The (Zariski closure of) the image of this map is known as the *Humbert surface* (of discriminant D) and we denote it by $\mathcal{H}_D$.

Remark 2.1. Let $\mathscr{L}/k$ be a geometrically integral variety. Since a k-point on $Y_-(D)$ may not correspond to a genus 2 curve defined over k we adopt the following convention: A curve $\mathcal{C}/\mathbb{Q}(\mathscr{L})$ is said to be a *generic curve with RM D* if there exists a Zariski dense set $U \subset Y_-(D)$ such that if $P \in U(k)$ is the moduli of a genus 2 curve C/k, then P lifts to a point $P' \in \mathscr{L}(k)$ such that the specialisation of $\mathcal{C}$ at P' is $\bar{k}$-isomorphic to C.

2.2. **The Mestre conic and cubic.** Let $\mathrm{M}_3(R)$ for the R-algebra of 3×3 matrices with entries in R. If L/R is a conic given by the vanishing of a homogeneous degree 2 polynomial $Q(X,Y,Z) \in R[X,Y,Z]$ we define the Gram matrix of L to be the symmetric matrix $A \in \mathrm{M}_3(R)$ such that

$$Q(X,Y,Z) = \mathbf{x}^{\mathrm{T}} A \mathbf{x}.$$

The discriminant of the conic L (and the polynomial $Q(X,Y,Z)$) is defined to be the determinant $\Delta(L) = \Delta(Q) = \det A$.

Let $\mathcal{S} \subset \mathrm{Sym}^6(\mathbb{P}^1)$ be the moduli space parametrising 6 *distinct* (unordered) points in $\mathbb{P}^1$, equipped with the natural action of $\mathrm{Aut}(\mathbb{P}^1) \cong \mathrm{PGL}_2$. To each point $\boldsymbol{a} = \{a_1, ..., a_6\} \in \mathcal{S}(k)$ we may associate the genus 2 curve $C_{\boldsymbol{a}}/k$ given by the Weierstrass equation

$$C_{\boldsymbol{a}} : y^2 = \prod_{i=1}^{6} (x - a_i).$$

The isomorphism class of the curve $C_{\boldsymbol{a}}$ is invariant under the action of PGL_2 on $\mathcal{S}$. Since all genus 2 curves are hyperelliptic we therefore have a $\mathbb{Q}$-isomorphism $\mathcal{M}_2 \cong \mathcal{S}/\!\!/\mathrm{PGL}_2$. There exist $\mathrm{PGL}_2 \times S_6$-invariants in $\mathbb{Z}[a_1, ..., a_6]$, known as the *Igusa–Clebsch invariants*, of degrees 2, 4, 6, and 10 respectively such that the induced morphism $\mathcal{M}_2 \to \mathbb{P}(1,2,3,5)$ is $\mathbb{Q}$-birational, and is a $\mathbb{Q}$-isomorphism onto its image (see e.g., [Igu60]). We identify $\mathcal{M}_2$ with its image in $\mathbb{P}(1,2,3,5)$.

Consider a k-rational point $P = [I_2 : I_4 : I_6 : I_{10}] \in \mathcal{M}_2 \subset \mathbb{P}(1,2,3,5)$. By construction we may associate a genus 2 curve C/k to P if and only if the fibre of the morphism $\mathcal{S} \to \mathcal{M}_2$ above P has a k-rational point. Generically, this fibre is a PGL_2-torsor, hence for general P it is isomorphic to a conic $L(P)/k$. Mestre [Mes91b] proved that if P corresponds to a genus 2 curve $C/\bar{k}$ with $\mathrm{Aut}_{\bar{k}}(C) \cong C_2$ then $L(P)$ is isomorphic to the conic with (symmetric) Gram matrix $(A_{ij})_{i,j=1}^3$ whose upper triangular entries are

$$\begin{aligned}
A_{1,1} &= \frac{-3I_2^3 - 140I_2I_4 + 800I_6}{2^6 \cdot 3^4 \cdot 5^6}, \\
A_{1,2} &= \frac{9I_2^4 + 560I_2^2I_4 + 1600I_4^2 - 3000I_2I_6}{2^7 \cdot 3^7 \cdot 5^8}, \\
A_{1,3} &= \frac{-9I_2^5 - 700I_2^3I_4 + 12400I_2I_4^2 + 3600I_2^2I_6 - 48000I_4I_6 - 10800000I_{10}}{2^8 \cdot 3^9 \cdot 5^{10}} \\
A_{2,2} &= A_{1,3}, \\
A_{2,3} &= \frac{3I_2^6 + 280I_2^4I_4 + 6000I_2^2I_4^2 - 1400I_2^3I_6 + 8000I_4^3 - 52000I_2I_4I_6 + 120000I_6^2}{2^9 \cdot 3^{10} \cdot 5^{12}}, \\
A_{3,3} &= \frac{-9I_2^7 - 980I_2^5I_4 - 12800I_2^3I_4^2 + 4800I_2^4I_6 + 154000I_2I_4^3 + 162000I_2^2I_4I_6}{2^{10} \cdot 3^{13} \cdot 5^{14}} \\
&\quad - \frac{480000I_4^2I_6 + 450000I_2I_6^2 + 8100000I_2^2I_{10} + 162000000I_4I_{10}}{2^{10} \cdot 3^{13} \cdot 5^{14}}.
\end{aligned}$$

Mestre also constructs an explicit cubic curve $M(P) \subset \mathbb{P}^2$ which is defined over k. The curve $M(P)$ has the following property.

Proposition 2.2 (Mestre [Mes91b, §1.5])**.** *Let K/k be a field. If there exists a K-isomorphism $\psi\colon L(P) \cong \mathbb{P}^1$ (i.e., if $L(P)$ has a K-point), then the double cover of $\mathbb{P}^1$ ramified over $\psi(M(P) \cap L(P))$ is a genus 2 curve C/K with moduli $P \in \mathcal{M}_2(K)$.*

We do not reproduce the equations for $M(P)$ here, but they may be found in [Mes91b] and in the code attached to this paper [CFM24].

3. The Mestre conic associated to a Hilbert modular surface

Let $Y_-(D)$ be the Hilbert modular surface of fundamental discriminant D and let $\mathcal{H}_D \subset \mathcal{A}_2$ be the corresponding Humbert surface, as in Section 2.1. Let $P \in \mathcal{H}_D(k) \cap \mathcal{M}_2(k)$ be a k-rational point and consider a genus 2 curve $C/\bar{k}$ corresponding to P. We say that P is *suitably generic* if the endomorphism ring of the Jacobian of C is commutative and $\mathrm{Aut}(C) \cong \{\pm 1\}$. Similarly, we say that a point $P \in Y_-(D)(k)$ is suitably generic if its image in $\mathcal{H}_D(k)$ is suitably generic.

The following result and argument was kindly explained to us by Bjorn Poonen.

Proposition 3.1. *Let k be a field of characteristic 0 and let $P \in \mathcal{H}_D(k)$ be a suitably generic k-rational point. Let $\lambda(P) \in k$ be such that $k(Q) = k(\sqrt{\lambda(P)})$ where $Q \in Y_-(D)(\bar{k})$ is a preimage of P. Then the Mestre conic $L_D(P) \subset \mathbb{P}^2$ associated to P is k-isomorphic to a conic of the form*

$$X^2 - D\lambda(P)Y^2 - q_D(P)Z^2$$

for some $q_D(P) \in k$.

Remark 3.2. If P is the generic point of $\mathcal{H}_D$, then $\lambda_D := \lambda(P) \in \mathbb{Q}(\mathcal{H}_D)^\times$ is the function (unique up to multiplication by a square) such that $Y_-(D)$ is birational to the surface given by the vanishing of $z^2 - \lambda_D$ in $\mathbb{A}^1 \times \mathcal{H}_D$.

Proof. For simplicity write $\lambda = \lambda(P)$. By [Voi21, Theorem 5.5.3] it suffices to show that there exists a $k(\sqrt{\lambda D})$-rational point on $L_D(P)$.

Recall that we write $\mathcal{S}$ for the moduli space parametrising 6 distinct points in $\mathbb{P}^1$ and that we have an isomorphism $\mathcal{M}_2 \cong \mathcal{S} /\!\!/ \mathrm{PGL}_2$. The fibre of the quotient morphism $\mathcal{S} \to \mathcal{M}_2$ above P is a PGL_2-torsor, and by construction defines the same class in $H^1(k, \mathrm{PGL}_2)$ as $L_D(P)$.

Note that we may equivalently view $\mathcal{S}$ as the (coarse) moduli space parametrising pairs (C, ϕ) where C is a genus 2 curve, and $\phi\colon C \to \mathbb{P}^1$ is a morphism of degree 2. Define $\mathcal{N}$ to be the (coarse) moduli space parametrising triples (C, α, β) where C is a genus 2 curve and $\alpha, \beta \in |\mathcal{K}_C|$ are elements of the linear system of a canonical divisor $\mathcal{K}_C$ on C. Note that if $\mathrm{Aut}(C) \cong \{\pm 1\}$ then the degree 2 morphism $\phi\colon C \to \mathbb{P}^1$ is unique up to composition with an element of $\mathrm{Aut}(\mathbb{P}^1)$, and therefore $\phi^*(0), \phi^*(\infty) \in |\mathcal{K}_C|$.

Let $\mathcal{M}_2'$ denote the Zariski open subvariety of $\mathcal{M}_2$ where $\mathrm{Aut}(C) \cong \{\pm 1\}$ and define $\mathcal{S}' = \mathcal{S} \times_{\mathcal{M}_2} \mathcal{M}_2'$ and $\mathcal{N}' = \mathcal{N} \times_{\mathcal{M}_2} \mathcal{M}_2'$. We have a commutative diagram

$$\begin{array}{ccc} \mathcal{S}' & & \\ \downarrow & \searrow & \\ \mathcal{N}' & \longrightarrow & \mathcal{M}_2' \end{array}$$

where the morphism on the left is given by $(C, \phi) \mapsto (C, \phi^*(0), \phi^*(\infty))$. Hence $\mathcal{S}' \to \mathcal{N}'$ is a $\mathbb{G}_m$-torsor since $\mathbb{G}_m$ is isomorphic to the subgroup of $\mathrm{Aut}(\mathbb{P}^1)$ fixing the points 0 and ∞.

By Hilbert's Theorem 90 a $\mathbb{G}_m$-torsor is trivial, so it suffices to show that, over $k(\sqrt{\lambda D})$, there exists a section $P \to \mathcal{N}'$ of the morphism $\mathcal{S}' \to \mathcal{N}'$.

Choose a finite extension K/k such that there exists a genus 2 curve C/K corresponding to P. Let $J = \mathrm{Jac}(C)$ be the Jacobian of C. By construction, there exists an element $\tau \in \mathrm{End}_{\bar{k}}(J)$ such that $\tau^2 = D$. Since J has abelian geometric endomorphism algebra (by assumption) τ is defined over $K(\sqrt{\lambda})$ by [CMb, Proposition 2.1].

Note that the action of τ on J induces an action on $H^0(J, \Omega_J) \cong H^0(C, \Omega_C)$ which, after base-changing to $K(\sqrt{\lambda})$, we may assume is given by the matrix $\left(\begin{smallmatrix} 0 & 1 \\ D & 0 \end{smallmatrix}\right)$. Let $\omega_1, \omega_2 \in H^0(C, \Omega_C)$ be eigenvectors contained in the span of the $\sqrt{D}$ and $-\sqrt{D}$-eigenspaces of this action respectively.

It is clear that ω_1 and ω_2 are fixed by the action of $\mathrm{Gal}(\bar{k}/K(\sqrt{\lambda}, \sqrt{D}))$. Let

$$\chi_\lambda, \chi_D \colon \mathrm{Gal}(\bar{k}/K) \to \{\pm 1\}$$

denote the quadratic characters associated to $K(\sqrt{\lambda})$ and $K(\sqrt{D})$ respectively. Then for each $i = 1, 2$ the 1-form ω_i is fixed by the action of $\sigma \in \mathrm{Gal}(\bar{k}/K)$ if and only if $\chi_\lambda(\sigma)\chi_D(\sigma) = 1$. In particular both ω_1 and ω_2 are defined over $K(\sqrt{\lambda D})$.

By abuse of notation let $\omega_1, \omega_2 \in |\mathcal{K}_C|$ denote the degree 2 divisors cut out by the 1-forms ω_1 and ω_2 respectively. By the above discussion the point $(C, \omega_1, \omega_2) \in \mathcal{N}(\bar{k})$ is $K(\sqrt{\lambda D})$-rational, and since P is k-rational we in fact have $k(\sqrt{\lambda D}) = \bigcap_K K(\sqrt{\lambda D})$, where we range over all possible choices of K/k. Since K was arbitrary (C, ω_1, ω_2) is $k(\sqrt{\lambda D})$-rational as required. ☐

The following proposition shows that the Mestre obstruction vanishes identically on the Hilbert modular surface $Y_-(D)$ for any $D \equiv 1 \pmod 8$. Theorem 1.8 follows by taking the point $P \in Y_-(D)$ in Proposition 3.3 to be the generic point. That is, when $D \equiv 1 \pmod 8$ we may take $q_D(P) = 1$ in Proposition 3.1.

Proposition 3.3. *Let k be a field of characteristic coprime to $2D$ and let $P \in Y_-(D)(k)$ be a suitably generic k-rational point. The Mestre conic $L_D(P) \subset \mathbb{P}^2$ associated to P has a k-rational point whenever $D \equiv 1 \pmod 8$.*

Proof. If k is finite, then any conic has a k-rational point, so we may assume without loss of generality that k is infinite. We first need the following lemmas:

Lemma 3.4. *Let $D > 0$ be any fundamental discriminant. Suppose that p is a prime number which splits in $\mathcal{O}_D$ as a product of prime ideals $(p) = \mathfrak{p}\bar{\mathfrak{p}}$. Let k be a field of characteristic coprime to pD and let J/k be a principally polarised abelian surface with RM D defined over k. Denote by $e_p \colon J[p] \times J[p] \to \mu_p$ the p-Weil pairing induced by the principal polarisation on J. Then we have a direct sum decomposition of Galois modules $J[p] = J[\mathfrak{p}] \oplus J[\bar{\mathfrak{p}}]$ and moreover $e_p(x, y) = 1$ for each pair $x \in J[\mathfrak{p}]$ and $y \in J[\bar{\mathfrak{p}}]$.*

Proof. The decompostion $J[p] = J[\mathfrak{p}] \oplus J[\bar{\mathfrak{p}}]$ is an isomorphism of Galois modules since the action of $\mathcal{O}_D$ is defined over k.

We claim that for each $y \in J[\bar{\mathfrak{p}}]$ there exists $y' \in J[p]$ and $\eta \in \mathfrak{p}$ such that $y = \eta y'$. If there exists $\eta \in \mathfrak{p}$ such that $\eta J[p] = J[\bar{\mathfrak{p}}]$ then this is clear, so suppose that for each $a \in \mathfrak{p}$ we have $aJ[p] \subsetneq J[\bar{\mathfrak{p}}]$. Since $J[\mathfrak{p}]$ is an $\mathbb{F}_p$-module of rank 2 there exist $a, b \in \mathfrak{p}$ such that $\ker a \neq \ker b$. In particular $aJ[p] \neq bJ[p]$, so choosing $z \in J[p] \setminus (\ker a \cup \ker b)$ we see that $\{az, bz\}$ is an $\mathbb{F}_p$-basis for $J[\bar{\mathfrak{p}}]$ and therefore there exist $m, n \in \mathbb{Z}$ such that $y = (na + mb)z$.

The $\mathcal{O}_D$-action on J is invariant under the Rosati involution by assumption, and therefore we have $e_p(ax, y) = e_p(x, ay)$ for any $a \in \mathcal{O}_D$ and $x, y \in J[p]$. But $x \in \ker \eta$ since $\eta \in \mathfrak{p}$, and therefore $e_p(x, y) = e_p(x, \eta y') = e_p(\eta x, y') = 1$, as required. ☐

Lemma 3.5. *Let k be a field of characteristic coprime to $2D$, C/k a curve of genus 2, $D \equiv 1 \pmod 8$, and suppose that $J = \mathrm{Jac}(C)$ has RM D defined over k. Let $C : y^2 = f(x)$ be a Weierstrass equation for C, where $f(x) \in k[x]$ is a sextic polynomial.*

Then there exists a factorisation $f(x) = \varphi(x)\psi(x)$ as a product of two cubic polynomials over k.

Proof. Since $D \equiv 1 \pmod 8$ the ideal $(2) \subset \mathcal{O}_D$ splits as a product $(2) = \mathfrak{p}\bar{\mathfrak{p}}$. We equip J with the canonical principal polarisation and let $e_2\colon J[2] \times J[2] \to \mu_2$ denote the induced 2-Weil pairing on J.

Let $x, y \in J[\mathfrak{p}] \setminus \{O\}$ be distinct elements. We claim that $e_2(x, y) \neq 1$. Indeed, if $e_2(x, y) = 1$ then since $J[2]$ is spanned by x, y, and $J[\bar{\mathfrak{p}}]$, by Lemma 3.4 the 2-Weil pairing $e_2\colon J[2] \times J[2] \to \mu_2$ would be trivial, which is not the case.

Following [BD11, Section 4] let $x_1, ..., x_6 \in \bar{k}$ denote the roots of $f(x)$, and let $T_{i,j} \in \mathrm{Pic}^0(C/\bar{k})$ denote the divisor class $T_{i,j} = T_{j,i} = [(x_i, 0) - (x_j, 0)]$. By [Smi05, Lemma 8.1.4] we have $e_2(T_{i,j}, T_{s,t}) = (-1)^{\#\{i,j,s,t\}}$. In particular, since for each distinct $x, y \in J[\mathfrak{p}]\setminus\{O\}$ we have $e_2(x, y) = -1$, it may be assumed without loss of generality that $J[\mathfrak{p}] = \{O, T_{1,2}, T_{2,3}, T_{1,3}\}$. But the $\mathrm{Gal}(\bar{k}/k)$-action on $J(\bar{k})$ stabilises $J[\mathfrak{p}]$, so in particular $\mathrm{Gal}(\bar{k}/k)$ also stabilises $\{x_1, x_2, x_3\}$, and therefore $\varphi(x) = (x - x_1)(x - x_2)(x - x_3)$ is contained in $k[x]$. But then setting $\psi(x) = f(x)/\varphi(x)$ we obtain the factorisation $f(x) = \varphi(x)\psi(x)$, as required. □

Let $L = L_D(P)$ and $M = M_D(P)$ denote the Mestre conic and cubic associated to P respectively. Since k is infinite there exists a separable quadratic extension K/k such that L obtains a point over K, and $K \cap k(L \cap M) = k$. By construction the Mestre obstruction for P vanishes over K, and there exists a genus 2 curve C/K corresponding to P. The geometric endomorphism ring $\mathrm{End}_{\bar{k}}(\mathrm{Jac}(C))$ is abelian since P is assumed to be suitably generic. It follows from [CMb, Proposition 2.1] that $\mathrm{Jac}(C)$ has $\mathcal{O}_D$-multiplication over K, and therefore if $y^2 = f(x)$ is a Weierstrass equation for C. By Lemma 3.5 the polynomial $f(x)$ factors over K as a product of cubics $f(x) = \varphi(x)\psi(x)$.

Let $S \subset \mathbb{A}^1$ denote the K-variety cut out by the vanishing of the polynomial f. By construction we have a K-isomorphism of varieties $L \cap M \cong S$. In particular, over K, we have a decomposition $L \cap M = S_1 \amalg S_2$ where S_1 and S_2 are degree 3 K-rational divisors on L (isomorphic as K-varieties to the vanishing sets of $\varphi(x)$ and $\psi(x)$ respectively).

Since $K \cap k(L \cap M) = k$ the $\mathrm{Gal}(K/k)$-action on $L \cap M$ must stabilise S_1 and S_2. In particular both S_1 and S_2 are defined over k. But if $\mathcal{K}_L$ is a canonical divisor on L, then $S_1 - \mathcal{K}_L$ is a k-rational degree 1 divisor on L, and is therefore linearly equivalent to a k-rational point on L (since L has genus 0). □

4. Simplified models for the generic Mestre conic

Mestre's conic is quite simple in terms of Clebsch invariants, however the Clebsch invariants are quite complicated rational functions on the Elkies–Kumar model for the Humbert surface. In this section we present two simplifications of the Mestre conic, firstly in terms of Igusa–Clebsch invariants (see Section 4.1), and secondly in terms of certain related quantities defined by Elkies–Kumar [EK14] for Hilbert modular surfaces (see Section 4.2). In each case, we record the cubic form satisfying the analogue of Proposition 2.2 in the electronic data [CFM24].

We remark that the first simplification is useful for reconstructing genus 2 curves over number fields, say, from Igusa or Igusa–Clebsch invariants, as it tends to give genus 2 curves with much smaller coefficients than using Mestre's construction [Mes91b] directly.

4.1. Mestre conics for Igusa–Clebsch invariants.

Let $T^{(1)}$ be the Gram matrix for the Mestre conic Q_1, viewed over $R = k[I_2, I_4, I_6, I_{10}]$. The upper triangular coefficients of $T^{(1)}$ are given in Section 2.2.

Let e_i is the i-th standard basis vector of R^3 for $i = 1, 2, 3$. Viewing each of the monomials I_2, I_4, I_6, I_{10} as degree 1 over k, we see that $Q_1(e_1), Q_1(e_2), Q_1(e_3)$ have degrees 3, 5, 7. We will simplify the Mestre conic in terms of Igusa–Clebsch invariants by making some change of bases to lower the degree of the coefficients.

Let $v_1 = I_2e_2 + 450e_3$ and $v_2 = I_2e_1 + 450e_2$. Then $Q_1(v_1)$ has degree 5 and $Q_1(v_2)$ has degree 3. Let $T^{(2)}$ be the Gram matrix for Q_1 with respect to the basis $\{e_1, e_2, v_1\}$. Let $T^{(3)}$ be the Gram matrix for Q_2 with respect to $\{9000e_1, 1350v_2, 607500e_3\}$. Now the degrees of the diagonal terms of $T^{(3)}$ are 3, 3, and 5, with the degree 5 entry of $T^{(3)}$ being

$$\begin{aligned}T^{(3)}_{3,3} &= 267I_2^3I_4^2 + 1515I_2I_4^3 - 1485I_2^2I_4I_6 - 3600I_4^2I_6\\ &\quad + 2025I_2I_6^2 - 141750I_2^2I_{10} - 1215000I_4I_{10}.\end{aligned}$$

We can do one more simplification to get rid of the $I_2^2I_{10}$ and $I_2^3I_4^2$ terms from the lower right entry of $T^{(3)}$. Let $T^{(4)}$ be the Gram matrix for Q_3 with respect to the basis $\{e_1, e_2, \frac{v_3}{10}\}$ where $v_1 = 7I_4e_1 + e_2I_2 - 2e_3$. The upper triangular coefficients of $T^{(4)}$ are:

$$\begin{aligned}
T^{(4)}_{1,1} &= -3I_2^3 - 140I_2I_4 + 800I_6\\
T^{(4)}_{1,2} &= 7I_2^2I_4 + 80I_4^2 - 30I_2I_6\\
T^{(4)}_{1,3} &= -230I_2I_4^2 - 9I_2^2I_6 + 1040I_4I_6 + 108000I_{10}\\
T^{(4)}_{2,2} &= 117I_2I_4^2 - 360I_4I_6 - 81000I_{10}\\
T^{(4)}_{2,3} &= -50I_2^2I_4^2 + 20I_4^3 + 321I_2I_4I_6 - 540I_6^2 + 24300I_2I_{10}\\
T^{(4)}_{3,3} &= -200I_2I_4^3 + 920I_4^2I_6 - 27I_2I_6^2 + 102600I_4I_{10}
\end{aligned}$$

We will call this transformed Mestre conic the *IC-simplified Mestre conic.*

4.2. **Mestre conics for Elkies–Kumar models.** The Elkies–Kumar models for Hilbert modular surfaces have Igusa–Clebsch invariants of the form

$$(I_2, I_4, I_6, I_{10}) = (-24(B_1/A_1), -12A, 96(AB_1/A_1) - 36B, -4A_1B_2)$$

where A, A_1, B, B_1, B_2 are rational functions on the corresponding Humbert surface.

Let $T^{(1)}$ be the Gram matrix for the IC-simplified Mestre conic Q_1 in terms of A, A_1, B, B_1, and B_2. Let $T^{(2)}$ be $\frac{A_1^3}{2}$ times the Gram matrix for Q_1 with respect to the basis $\{\frac{1}{8}e_1, \frac{e_2}{36A_1}, \frac{1}{24}e_3\}$. The upper triangular entries of $T^{(2)}$ are

$$\begin{aligned}
T^{(2)}_{1,1} &= -225A_1^3B + 285AA_1^2B_1 + 324B_1^3\\
T^{(2)}_{1,2} &= 20A^2A_1^2 - 45A_1BB_1 + 36AB_1^2\\
T^{(2)}_{1,3} &= 1170AA_1^3B - 1050A^2A_1^2B_1 - 1125A_1^4B_2 + 486A_1BB_1^2 - 1296AB_1^3\\
T^{(2)}_{2,2} &= -60AA_1B + 4A^2B_1 + 125A_1^2B_2\\
T^{(2)}_{2,3} &= -20A^3A_1^2 - 405A_1^2B^2 + 234AA_1BB_1 - 144A^2B_1^2 + 1350A_1^2B_1B_2\\
T^{(2)}_{3,3} &= -4140A^2A_1^3B + 3840A^3A_1^2B_1 + 4275AA_1^4B_2\\
&\quad + 729A_1^2B^2B_1 - 3888AA_1BB_1^2 + 5184A^2B_1^3.
\end{aligned}$$

Let Q_2 be the associated ternary quadratic form with coefficients in $\mathbb{Z}[A, A_1, B, B_1, B_2]$. Note that A_1^4 divides the discriminant of Q_2. In attempting to kill off the $A^2B_1^3$ term from $Q_2(e_3)$, we can simplify $T^{(2)}_{3,3}$ quite a bit, and remove a factor of A_1^2 from the discriminant. Let $v_2 = 4Ae_1 + e_3$. Then

$$Q_2(v_2) = -27A_1^2(-60A_1A^2B + 175A_1^2AB_2 - 27B_1B^2),$$

so we let $T^{(3)}$ be the Gram matrix of Q_2 with respect to $\{e_1, e_2, \frac{v_2}{3A_1}\}$. The upper triangular coefficients of $T^{(3)}$ are

$$\begin{aligned}
T^{(3)}_{1,1} &= -225A_1^3B + 285AA_1^2B_1 + 324B_1^3 \\
T^{(3)}_{1,2} &= 20A^2A_1^2 - 45A_1BB_1 + 36AB_1^2 \\
T^{(3)}_{1,3} &= 90AA_1^2B + 30A^2A_1B_1 - 375A_1^3B_2 + 162BB_1^2 \\
T^{(3)}_{2,2} &= -60AA_1B + 4A^2B_1 + 125A_1^2B_2 \\
T^{(3)}_{2,3} &= 20A^3A_1 - 135A_1B^2 + 18ABB_1 + 450A_1B_1B_2 \\
T^{(3)}_{3,3} &= 180A^2A_1B - 525AA_1^2B_2 + 81B^2B_1.
\end{aligned}$$

We call the resulting quadratic form Q_3 the *RM-simplified Mestre conic.*

Note that A_1^2 divides the discriminant of Q_3, and A_1 divides the diagonal minors of $T^{(3)}$. While one can remove another factor of A_1 from the discriminant, we do not know how to do this without introducing other factors into the discriminant.

5. An algorithm for minimising a conic over $\mathbb{Q}(t_1, t_2)$

Let R be an integral domain and k its field of fractions. Suppose $L : Q(X, Y, Z) = 0$ is a conic over a polynomial ring $R[t_1, \ldots, t_m]$. We say L is *minimal* if its discriminant has minimal degree among the $k(t_1, \ldots, t_m)$-equivalence classes of L. We would also like a notion of a *reduced minimal form*, to encapsulate the idea that the coefficients are also simple as possible. If L is minimal and diagonal, then the coefficient degrees add up to the discriminant degree, and this should be considered reduced.

In this section we present algorithms to search for a reduced minimal form of L in a certain (algorithmically defined) subset of the $k(t_1, \ldots, t_m)$-equivalence class of L. These algorithms are tailored to our case of interest: Mestre conics for Hilbert modular surfaces over $\mathbb{Q}$. For concreteness and ease of exposition, we will assume in what follows L is a conic defined over $\mathbb{Z}[t_1, t_2]$. However, our algorithms can be adapted to more general settings, and much of it makes sense beyond the situation where L is a conic in $\mathbb{P}^2$ (see Remark 5.5).

Remark 5.1. In general, it may not be easy to verify whether L is minimal. In our situation, where L is the Mestre conic over a Hilbert modular surface $Y_-(D)$ with birational model $z^2 = \lambda_D$, Proposition 3.1 tells us that our Mestre conic can be put in the form $X^2 - D\lambda_D Y^2 - q_D Z^2$ for some polynomial $q_D \in \mathbb{Z}[g, h]$. For our purposes, we consider such a Mestre conic to be in *reduced minimal form* if q_D has no non-constant factors in $\mathbb{Z}[g, h]$ which are norms from $\mathbb{Q}(g, h)(\sqrt{D\lambda_D})$.

5.1. **Minimisation.** Let A be a discrete valuation ring with maximal ideal $\mathfrak{p} = (\pi)$. Let S/A be an affine scheme flat of relative dimension 1 over $\operatorname{Spec} A$ and suppose that S has smooth generic fibre. Explicitly we may take S to be given by the vanishing of polynomials $f_1, ..., f_\ell \in A[x_1, ..., x_n]$ in $\mathbb{A}^n_A$ such that $f_i \notin \pi A[x_1, ..., x_n]$ for all $i = 1, ..., \ell$. Assume that the point $\mathfrak{m} = (\pi, x_1, ..., x_n)$ lies on S (this is the origin on the special fibre of S). Following [Sil94, IV.7] we define the blow-up of S at $\mathfrak{m}$ to be the subscheme of $S \times \mathbb{P}^n_{\mathbb{Z}}$ given by the equations

$$x_i y_0 - \pi y_i \quad \text{and} \quad x_i y_j - x_j y_i$$

where $1 \leq i, j \leq n$.

Just as curve and surface singularities (over $\mathbb{C}$) may be resolved by iterated blow-ups and normalisations, we may hope that in our setting arithmetic blow-ups will (at least partially) resolve the singular points on the special fibre of S. Indeed, this approach is utilised in Tate's algorithm for finding the minimal regular model of an elliptic curve over a DVR [Sil94, IV.7]. We will refer to this process as *minimisation* in reference to the fact that when $E/\mathbb{Z}_{(p)}$ is an elliptic curve, repeatedly applying the above algorithm "minimises the exponent of p in the discriminant of E".

If B is a unique factorisation domain and $\pi \in B$ is a prime element, we denote by $v_\pi(x)$ the π-adic valuation of an element $x \in B$.

Example 5.2 (An algorithm for minimising a conic in $\mathbb{P}^2_{\mathbb{Q}}$)**.** In the following example we illustrate how arithmetic blow-ups allow us to reproduce the classical reduction algorithm for ternary quadratic forms over $\mathbb{Q}$. The approach we present here is a closely related to (a simplified form of) [CR03, Algorithm I].

Let $Q(X, Y, Z) \in \mathbb{Z}[X, Y, Z]$ be a (homogeneous) degree 2 polynomial which defines a non-singular curve $C \subset \mathbb{P}^2_{\mathbb{Q}}$. After possibly rescaling Q we may assume that the Gram matrix has entries in $\mathbb{Z}$ and that $\Delta(Q) \in \mathbb{Z}$.

For simplicity we avoid characteristic 2 and consider Q as defining a scheme $\mathcal{C} \subset \mathbb{P}^2_{\mathbb{Z}[1/2]}$. For each prime number $p \neq 2$ the fibre of $\mathcal{C}$ at p is singular if and only if $\Delta(Q) \equiv 0 \pmod{p}$. This suggests the following minimisation algorithm:

If $p^2 \mid \Delta(Q)$ we consider the scheme $\mathcal{C}_p = \mathcal{C} \times_{\mathbb{Z}[1/2]} \operatorname{Spec} \mathbb{Z}_{(p)}$. The singular subscheme of the special fibre at p consists of either a point, or a double line. Let $\overline{U} \in \mathrm{SL}_3(\mathbb{F}_p)$ be a matrix which transforms the singular locus to the point $(0:0:1) \in \mathbb{P}^2_{\mathbb{F}_p}$, respectively the line $\{Z = 0\} \subset \mathbb{P}^2_{\mathbb{F}_p}$. By the existence of Smith normal form, the matrix $\overline{U}$ lifts to a matrix $U \in \mathrm{SL}_2(\mathbb{Z})$, which we then apply to $\mathcal{C}$ by setting $M' = U^{\mathrm{T}} M U$. Since $\det(U) = 1$ this leaves $\Delta(Q)$ unchanged.

In the former case, choosing the affine patch where $Z = 1$, and setting $x = X/Z$ and $y = Y/Z$ we blow-up the singular point $\mathfrak{m} = (p, x, y)$ on $\mathcal{C}_p$. Since $p^2 \mid \Delta(Q)$ this is given (on an open subscheme of the blow-up) by the vanishing of the integral non-homogeneous quadratic form $Q(px, py, 1)/p^2$. After homogenising we obtain the ternary quadratic form $Q'(X, Y, Z) = Q(X, Y, p^{-1}Z)$. In particular $\Delta(Q') = \Delta(Q)/p^2$.

In the case of the double line at $Z = 0$, we set $Q'(X, Y, Z) = Q(X, Y, pZ)/p^k$ for some $k \in \{1, 2\}$. We have $\Delta(Q') = p^{2-3k}\Delta(Q)$.

It follows that after finitely many iterations $v_p(\Delta(Q)) \leq 1$. Repeating the above algorithm at each odd prime $p \mid \Delta(Q)$, then after finitely many steps we have $v_p(\Delta(Q)) \leq 1$. We refer to this as a *minimal model for* Q (away from the prime 2).

It is important to note that the "global" approach in Example 5.2 may fail when the base ring (in that case $\mathbb{Z}$) fails to be a principal ideal domain. More specifically, if A is an integral domain and $\mathfrak{p}$ is a maximal ideal of A it is not necessarily true (unless A is a PID) that we may lift a matrix $\overline{U} \in \mathrm{SL}_3(A/\mathfrak{p})$ to a matrix $U \in \mathrm{SL}_3(A)$.

Nevertheless, we will see that in practice applying Example 5.2 in the case when $A = \mathbb{Z}[t_1, t_2]$ provides a useful algorithm for minimising a ternary quadratic form $Q(X, Y, Z)$ with coefficients in $\mathbb{Z}[t_1, t_2]$, which we describe in Algorithm 5.3. Let $\pi \in \mathbb{Z}[t_1, t_2]$ be a prime factor of $\Delta(Q)$. While we cannot in general hope for a lift $U \in \mathrm{SL}_3(\mathbb{Z}[t_1, t_2])$ which moves the singular point (or line) on the special fibre to the origin (respectively $Z = 0$), we can always choose a lift $U \in \mathrm{M}_3(\mathbb{Z}[t_1, t_2]) \cap \mathrm{GL}_3(\mathbb{Z}[t_1, t_2]_{(\pi)})$. In this case we introduce a factor of $\det(U)^2$ into $\Delta(Q)$.

Let $L/\mathbb{Z}[t_1, t_2]$ be a conic given by a Gram matrix M with coefficients in $\mathbb{Z}[t_1, t_2]$. Let $\pi \in \mathbb{Z}[t_1, t_2]$ be an irreducible element. We define $\overline{L}_\pi$ to be the generic fibre of the reduction of L modulo the ideal (π). If $a, b, c \in \mathbb{Z}[t_1, t_2]$ we write $\operatorname{diag}(a, b, c)$ for the diagonal matrix with entries a, b, and c. For each matrix $U \in \mathrm{M}_3(\mathbb{Z}[t_1, t_2]) \cap \mathrm{GL}_3(\mathbb{Q}(t_1, t_2))$ we denote by $L^U/\mathbb{Z}[t_1, t_2]$ the conic with Gram matrix $U^T M U$.

Algorithm 5.3 `MinimiseAtPi`(L, π): Minimise the conic L at a prime $\pi \mid \Delta(L)$.
Input: A conic $L/\mathbb{Z}[t_1, t_2]$ and a prime element $\pi \in \mathbb{Z}[t_1, t_2]$ where $(\pi) \neq (2)$ and $\pi^2 \mid \Delta(L)$.
Output: A conic $L'/\mathbb{Z}[t_1, t_2]$ such that $v_\pi(\Delta(L')) \leq v_\pi(\Delta(L)) - 2$.

`Sing` $\leftarrow$ the singular subscheme of $\overline{L}_\pi$
if $\dim$ `Sing` $= 0$ **then**
  $\overline{U} \leftarrow$ a matrix in $\mathrm{SL}_3(\mathbb{Z}[t_1, t_2]/(\pi))$ which moves `Sing` to $(0 : 0 : 1)$
  $U \leftarrow$ a lift of $\overline{U}$ to $\mathrm{M}_3(\mathbb{Z}[t_1, t_2]) \cap \mathrm{GL}_3(\mathbb{Z}[t_1, t_2]_{(\pi)})$
  $L' \leftarrow L^U$
  $V \leftarrow \mathrm{diag}(1, 1, \pi^{-1})$
  $L' \leftarrow (L')^V$
else
  $\overline{U} \leftarrow$ a matrix in $\mathrm{SL}_3(\mathbb{Z}[t_1, t_2]/(\pi))$ which moves `Sing` to $\{Z = 0\}$
  $U \leftarrow$ a lift of $\overline{U}$ to $\mathrm{M}_3(\mathbb{Z}[t_1, t_2]) \cap \mathrm{GL}_3(\mathbb{Z}[t_1, t_2]_{(\pi)})$
  $L' \leftarrow L^U$
  $V \leftarrow \mathrm{diag}(1, 1, \pi)$
  $k \leftarrow v_\pi(L')$
  $L' \leftarrow \pi^{-k}(L')^V$
end if
return L'

Remark 5.4. Note that Algorithm 5.3 will typically increase Y^2 or Z^2-coefficient degrees if the diagonal degrees (i.e., X^2, Y^2, and Z^2-coefficients) of L are not in increasing order. In practice we therefore assume the diagonal degrees are increasing by permuting the variables X, Y, Z.

Remark 5.5. Algorithm 5.3 can be generalised to the case of a scheme $S/\mathbb{Z}[t_1, ..., t_m]$ of relative dimension zero or one equipped with a "bad prime element" $\pi \in \mathbb{Z}[t_1, ..., t_m]$. One such situation is when S is relative dimension zero and given by a single homogeneous polynomial $f(X, Y) \in \mathbb{Z}[t_1, ..., t_m][X, Y]$. This viewpoint is useful for simplifying birational models for (small degree) coverings $X \to \mathbb{P}^m$, by considering X to be a hypersurface in $\mathbb{P}^1_{\mathbb{Z}[t_1, .., t_m]}$ cut out by $f(X, Y)$.

Even more generally one may replace $\mathbb{Z}[t_1, ..., t_m]$ with a geometrically integral base scheme T.

5.2. **Searching for minimal models.** Let $L : Q(X, Y, Z) = 0$ be a conic over $\mathbb{Q}(t_1, t_2)$. By the diagonal coefficients of L, we mean the X^2, Y^2 and Z^2-coefficients of Q.

By rescaling, we may assume the coefficients of Q lie in $\mathbb{Z}[t_1, t_2]$ and have gcd 1. If $\pi \in \mathbb{Z}[t_1, t_2]$ is a non-unit such that π^2 divides a diagonal coefficient (e.g., the X^2-coefficient) and π divides each coefficient involving the same variable (e.g., the XY and XZ-coefficients), then we replace that variable with itself divided by π (e.g., replace X with X/π). Furthermore, if π divides two of the diagonal coefficients and their cross-term coefficient (e.g., the X^2, Y^2 and XY-coefficients), then we scale the other variable (e.g., Z) by π and divide the whole conic equation by π. If L satisfies all these assumptions, we say L is *minimal with respect to scaling transformations*, or for short, *scale minimal.* At each stage in our algorithm, we will assume our conics are scale minimal.

Our algorithm to search for a reduced minimal model for L consists of constructing a search tree of $\mathbb{Q}(t_1, t_2)$-equivalent conics. At each stage, three possible types of minimisation operations are allowed:

(M1) minimisation of the degree of L (i.e., minimisation "at infinity"),
(M2) minimisation at a rational factor from the discriminant, and

(M3) minimisation at a polynomial factor from the discriminant.

There are two immediate issues. First, for general conics it may not be easy to determine when we have found a minimal form, but in our situation we employ the notion of reduced minimal as in Remark 5.1. Second, this search tree may be infinite, since removing factors from the discriminant can introduce other factors (as discussed in Section 5.1). To address the second issue, we place some restrictions on our search process which are based on observations made after performing several minimisations "by hand."

In particular, we observed:

(P1) Minimising conics tends to be easier when the rational part of the discriminant is small.

(P2) Minimising conics tends to be easier when the sum of the diagonal coefficient degrees is close to the discriminant degree.

For a scale minimal conic L, let $\Delta(L) \in \mathbb{Z}[t_1, t_2]$ be the discriminant. We define $\Delta_{\mathbb{Q}}(L)$ to be the rational part of $\Delta(L)$, i.e., the content of $\Delta(L)$. Write $\Delta(L) = \Delta_{\mathbb{Q}}(L) \prod \pi_i^{e_i}$, where the $\pi_i \in \mathbb{Z}[t_1, t_2]$ are coprime irreducible polynomials. Let $\Delta_1(L) = \prod_{e_i=1} \pi_i$ be the "power-free part" of $\Delta(L)$, and $\Delta_2(L) = \prod_{e_i>1} \pi_i^{e_i}$ be the power-full part of $\Delta(L)$. By the diagonal degree sum of L, denoted $\operatorname{diag}\deg L$, we mean the sum of degrees of the diagonal coefficients. We define the *degree score* of L to be

$$\texttt{DegScore}(L) := \deg \Delta_2(L) + \operatorname{diag}\deg L - \deg \Delta(L).$$

Then our second observation (P2) means that we want to work with conics with low degree score. Note that a degree score of 0 corresponds to having squarefree discriminant and $\operatorname{diag}\deg L = \deg \Delta(L)$.

5.2.1. *The main algorithm.* First we outline our main algorithm, `MinimisationSearch`, which we present in Algorithm 5.6. We describe pieces of the algorithm in more detail later. The `MinimisationSearch` algorithm creates a search tree where the nodes are transformed conics, and will terminate if it finds a conic with degree score 0. The order in which the tree is searched depends on the path score of each leaf L in the tree. In computer science this type of search is known as a best-first search. In Section 5.3 we discuss several options for path scoring, but our default is the average slope score which is essentially the average rate of change of the degree score along the path from the root node L_0 to the node L.

In general, the output of the algorithm may or may not be minimal, in the sense we have defined above. However, in our situation, we diagonalise the resulting conic to put it into the form given in Proposition 3.1. When necessary, one can remove norm factors from the last coefficient to reach a reduced minimal form.

5.2.2. *The sub-algorithms.* We now present the various sub-algorithms used in Algorithm 5.6.

Our first sub-algorithm, Algorithm 5.7, applies Algorithm 5.3 to remove as many rational prime factors as possible from the discriminant of a conic L without increasing its diagonal degrees. The order in which rational factors are removed can make a difference, and in our implementation we minimise starting with the largest prime p. In practice we observed that this performs better than starting with smaller primes.

Our second sub-algorithm, Algorithm 5.8, decreases the diagonal degrees of L by minimising at the place at infinity in both the affine patch where $t_1 = 1$ and the affine patch where $t_2 = 1$. For a conic L with coefficients in $\mathbb{Z}[t_1, t_2]$ we define `SwapAffinePatch`(L, t_i) to be the function which homogenises the coefficients of L with a transcendental t_3, swaps t_i and t_3, dehomogenises the resulting coefficients over $\mathbb{Z}[t_1, t_2]$, and returns the scale minimal form of the resulting conic.

Algorithm 5.6 `MinimisationSearch(`L_0`)`: Search for a minimal model for L_0 by removing power-full factors from the discriminant.
Input: A conic $L_0/\mathbb{Q}(t_0, t_1)$.
Output: A minimal model for L_0.

visited $\leftarrow \{L_0\}$
queue $\leftarrow \{L_0\}$
while queue is not empty **do**
  if there exists $L_f \in$ queue with degree score 0 **then**
    return L_f
  end if
  $L \leftarrow$ an element of queue with minimal path score
  remove L from queue
  $L \leftarrow$ RationalMinimisation(L)
  $L \leftarrow$ DegreeMinimisation(L)
  if $L \notin$ visited **then**
    add L to visited
    add L to queue
  else
    for each irreducible polynomial $\pi \mid \Delta_2(L)$ **do**
      $L' \leftarrow$ PolynomialMinimisation(L, π)
      if $\mathrm{ord}_\pi \Delta(L') < \mathrm{ord}_\pi \Delta(L)$ and $L' \notin$ visited **then**
        add L' to visited
        add L' to queue
      end if
    end for
  end if
end while
return Fail

Our final sub-algorithm, Algorithm 5.9, removes an irreducible polynomial factor π from the discriminant of L without increasing the degree score.

Remark 5.10. We comment on our implementation of Algorithms 5.6–5.9.

(1) When trying Algorithms 5.7–5.9, we will try these algorithms on certain forms of L. By Remark 5.4, we want the diagonal degrees of L to be increasing, and so we try these algorithms on every permutation of $\{X, Y, Z\}$ such that the diagonal degrees are increasing. The resulting conic can be significantly more complicated depending on the permutation used. To keep the number of branches small, we only keep the resulting conic from one of these permutations, and it will be one with a minimal degree score.
(2) Both Algorithm 5.6 and the sub-algorithms 5.7–5.9 make certain choices about the order of our three minimisation operations (M1)–(M3), and when to no longer pursue certain search paths. In practice, we avoid sequences of operations which make the conic worse along the way. One can modify these algorithms to include more branches and and be less greedy by not fixing the order of minimisation operations and by allowing operations which make the conic worse. While this may allow us to find solutions we would not otherwise, in moderately complicated situations that we tested this less restrictive search tended to take much longer to complete.
(3) One can also randomise Algorithm 5.6 to help mitigate getting stuck in unproductive sections of the search tree. Namely, with some fixed probability, we

Algorithm 5.7 `RationalMinimisation(L)`: Minimise L at rational primes $p \mid \Delta_{\mathbb{Q}}(L)$.
Input: A conic $L/\mathbb{Q}(t_1, t_2)$.
Output: A model L' for L, obtained by minimising at rational primes subject to the condition that $\operatorname{diag}\deg L' \leq \operatorname{diag}\deg L$.

```
D ← Δ_Q(L)
for p | D do
    while p^2 | Δ_Q(L) do
        L' ← MinimiseAtPi(L, p)
        if |Δ_Q(L')| < |Δ_Q(L)| and diag deg L' ≤ diag deg L then
            L ← L'
        else
            break
        end if
    end while
end for
return L
```

Algorithm 5.8 `DegreeMinimisation(L)`: Minimise L at the place at infinity to decrease its degree.
Input: A conic $L/\mathbb{Q}(t_1, t_2)$.
Output: A model L' for L, obtained by minimising at the place at infinity subject to the condition that $\operatorname{diag}\deg L' \leq \operatorname{diag}\deg L$.

```
for i ∈ {1, 2} do
    L_i ← SwapAffinePatch(L, t_i)
    while t_i | Δ_2(L_i) do
        L'_i ← MinimiseAtPi(L_i, t_i)
        if diag deg L'_i ≤ diag deg L_i then
            L_i ← L'_i
        else
            break
        end if
    end while
    L_i ← SwapAffinePatch(L'_i, t_i)
end for
return the first element of (L, L_1, L_2) which minimises diag deg
```

Algorithm 5.9 `PolynomialMinimisation(L, π)`: minimise L at a prime $(\pi) \subset \mathbb{Q}[t_1, t_2]$.
Input: A conic $L/\mathbb{Q}(t_1, t_2)$.
Output: A model L' for L, obtained by minimising at the prime (π) subject to the condition that `DegScore`$(L') \leq$ `DegScore`(L).

```
L' ← MinimiseAtPi(L, π)
if DegScore(L') ≤ DegScore(L) then
    L ← L'
end if
return L
```

choose L uniformly at random among the leaves in the queue, as opposed to choosing one with minimal path score. This randomisation sometimes speeds up the search process.

(4) Sometimes a good choice of polynomial minimisation is not immediately apparent in the node score. To help identify such branches, we have also implemented a variant of the algorithm where after each polynomial minimisation, we immediately run `RationalMinimisation` and `DegreeMinimisation`. Sometimes this is slightly slower, and sometimes it is significantly faster.

5.3. **Scoring methods.** Algorithm 5.6 relies on a path score for each node to choose the next leaf in the search process. If we merely used the degree score, our search would be very slow (and potentially not terminate) when there is no good search path along a branch that starts with minimal degree scores. The path score (as well as randomisation) provides a balance between a purely greedy search and a breadth-first search.

First we define the *node score* of a node L to be its degree score plus the number primes $p \mid \Delta_{\mathbb{Q}}(L)$ dividing the rational part of the discriminant. This modification of the degree score is to account for principle (P1). With this node score in mind, we consider the following methods to define a path score. A lower path score is considered better.

- *Average slope score.* The path score of L is the difference between the node scores of L and the root L_0, divided by the number of nodes on the path from L_0 to L.
- *Penalised node score.* The path score of L is the node score plus a penalty which depends on the length of the path. Let n be the number of nodes on the path from the root L_0 to L, excluding L itself, whose node score is the same as the node score of L. We set the penalty to be $\frac{n^2}{4}$.
- *Alternating score.* Alternate the path score between the average slope and penalised node score methods.

The average slope score measures the rate at which the node score is decreasing, and prevents the search from spending too much time along paths where the node score does not improve much or at all. The penalised node score is closer to the greedy approach of only using the degree score (or rather the node score), but which, at least temporarily, avoids paths along which the path score does not improve at all after a few steps. The alternating score blends these two approaches.

6. The output of Algorithm 5.6

For each positive fundamental discriminant $D < 100$, Elkies–Kumar [EK14] give a rational parametrisation of the Humbert surface $\mathcal{H}_D$, together with a rational function $\lambda_D \in \mathbb{Q}(g,h) \cong \mathbb{Q}(\mathcal{H}_D)$ such that the Hilbert modular surface $Y_-(D)$ is birational to the affine surface cut out by the vanishing of $z^2 - \lambda_D$ in $\mathbb{A}^3$. For each such discriminant, we apply Algorithm 5.6 to try to transform the (IC or RM simplified; see Section 4) Mestre conic $L_D/\mathbb{Q}(g,h)$ into the form $X^2 - D\lambda_D Y^2 - q_D Z^2$, for some rational function $q_D \in \mathbb{Q}(g,h)$ (such a model is guaranteed to exist by Proposition 3.1).

For $D < 100$, we first pre-compute a list of "nice" changes of coordinates which minimises and reduces a factor of $\Delta(L_D)$, or the quantities (A_1, A, B_1, B, B_2) of Elkies–Kumar (see Remark 6.1). For each such change of variables, we run our algorithm for each of our 3 scoring methods for up to 48 hours. We also run the randomised version explained in Remark 5.10(3), taking the randomisation probability $p = \frac{1}{8}$.

Runtimes of successful cases for the first two scoring methods are summarised in Table 3. The second and third columns in Table 3 give the discriminant degrees and coefficient degrees of the initial Mestre conic L_D, as a measure of complexity. The next 2 columns list runtimes for the deterministic version of our algorithms with the average slope score and penalise node score methods. The last 2 columns list average runtimes (over 5 trials) for the randomised version of these 2 scoring methods. When $D = 33, 53, 61$ a change of variables was used and we record the runtimes using the change of variables that finished fastest for that scoring method.

Note the runtimes are wall times, not CPU times, so differences of a few seconds should be considered random noise. Calculations were run on the OSCAR supercomputer at Brown University.

In Table 3 bolded runtimes note where one (non-randomised) scoring method significantly outperformed the other. Note that sometimes the average slope score is much better than the penalised node score, and sometimes the converse is true. An extreme example is $D = 44$ which completes in under 12 minutes for the average slope score but does not finish before the 48-hour timeout for the penalised node score. The issue in this case is the penalised slope method gets stuck on a single minimisation computation. In spite of this, with a suitable initial change of variables it finishes in just over 31 minutes. Randomised versions also terminate, and the variant of the algorithm in Remark 5.10(4) finishes in 11 minutes. We also tested the alternating scoring method, and found it is faster for $D = 61$ (4h 7m), and while it often performs in between the other two scoring methods, it is much worse when $D = 24, 33, 37$.

Remark 6.1 ("Nice" changes of coordinates). In some cases (namely when $D = 33$, 53, and 61) we first needed to apply a projective linear change of coordinates to the model for $\mathcal{H}_D$ for our algorithm to successfully terminate. We arrive at several changes of coordinates using the `Magma` function `MinRedTernaryForm` developed by Elsenhans–Stoll [ES], and our own more naive reduction algorithms (which simply place the most singular points of a plane curve at infinity).

Often it happens that, for a given D, one random instance may result in a significant speed-up, but another random instance runs much slower, so on average no time is saved. The cases where randomisation usually results in a speed up are often the cases where many steps are required in the deterministic version (see Table 4). An extreme case is $D = 33$ using the penalised node score. In this case the deterministic version runs in 420 steps and takes about 5 times a long as a typical random instance. For $D = 44, 53, 61$, of 5 randomised trials using the penalised node score, 3, 2 and 1 instances, respectively, did not finish before the 48-hour timeout.

To get a better sense of how difficult it was to find a sequence of transformations to minimise L_D, compare with Table 4. The second column lists the number of polynomial factors of Δ_L occurring to at least a square power, i.e., the number of prime ideals $\mathfrak{p}$ in $\mathbb{Q}[g, h]$ where one needs to minimise. Sometimes these factors occur to higher powers, and the third column counts these with appropriate multiplicity. In particular, the third column in Table 4 tells us the smallest number of minimisation steps we expect to need to perform to carry out the minimisation completely. The fourth column reports, when using the average slope score, the number of steps (i.e., number of times the `while` loop is iterated) required to complete `MinimisationSearch`. The fifth column, again for average slope score, reports the depth of the final solution in the search tree. The last two columns report analogous data when using the penalised node score.

We note that runtimes and number of steps required are not perfectly correlated, as certain minimisation steps take much longer to run than others (e.g., compare the average slope with penalised node scores for $D = 33$ or $D = 61$). We expect that the best search paths typically avoid the most intensive minimisation calculations. Thus, using automated timeouts in the search process would likely increase efficiency (we have not implemented this).

D	$\deg \Delta_{L_D}$	$\deg L_D$	slope	pen. node	rand. slope	rand. node
5	11	7	1s	1s	1s	1s
8	13	7	6s	6s	6s	6s
12	29	15	1m 21s	**1m 1s**	1m 29s	1m 28s
13	20	10	1m 25s	1m 29s	1m 29s	1m 30s
17	32	16	48s	**29s**	1m 1s	30s
21	38	16	2m 24s	**2m 3s**	2m 9s	2m 12s
24	43	18	**19s**	28s	24s	43s
28	45	17	2h 39m	**15m 30s**	2h 18m	18m 27s
29	40	18	**1m 52s**	3m 1s	2m 10s	2m 50s
33*	50	26	**23m 6s**	1h 22m	30m 46s	15m 55s
37	48	18	**12m 21s**	49m 20s	12m 48s	40m 16s
44	96	42	**11m 42s**	>2d	13m 4s	>28h
53*	70	30	**13m 32s**	2h 50m	58m 50s	>20h
61*	78	32	**4h 41m**	7h 49m	4h 10m	>13h

Table 3. Approximate runtimes for minimising L_D with different scoring functions. Starred discriminants required initial change of variables and bold values correspond to cases where one scoring method significantly outperformed another.

	minimisation primes		slope score		pen. node score	
D	$\#\{\mathfrak{p}^2 \mid \Delta_L\}$	$\sum \lfloor \frac{v_{\mathfrak{p}}(\Delta_L)}{2} \rfloor$	steps	depth	steps	depth
5	2	2	2	2	2	2
8	3	3	4	4	4	4
12	5	5	14	8	**9**	8
13	4	4	8	7	**7**	7
17	5	6	22	10	**11**	10
21	6	8	19	12	**13**	**10**
24	8	9	**14**	12	51	12
28	8	11	1053	21	**56**	21
29	7	9	**16**	**9**	24	15
33*	8	11	**72**	**18**	420	23
37	8	10	**90**	17	241	17
44	10	12	**74**	**24**	—	—
53*	10	13	56	**19**	56	20
61*	11	15	413	**21**	**396**	22

Table 4. Numbers of steps to minimise L_D and depth of solutions. Starred discriminants required an initial change of variables and bold values correspond to cases where one scoring method outperforms another.

It is also interesting to note that for most $D \geq 29$, the two scoring methods are finding different paths to the minimal model (the depths are typically different).

7. Models for genus 2 curves with RM

Using the transformations computed as described in Section 6 we now prove our main results about generic models for genus 2 curves with RM D.

7.1. Proofs of Theorems 1.1 and 1.5.

Proof of Theorem 1.5. The polynomials $q_D \in \mathbb{Q}[g, h]$ are computed by applying the transformations calculated using Algorithm 5.6 to the generic Mestre conic L_D which is defined over $\mathbb{Q}(\mathcal{H}_D) \cong \mathbb{Q}(g, h)$. These transformations are too complicated to reproduce here, but are stored in the electronic data accompanying this article at [CFM24].

To determine the analogous polynomials p_D, we convert to Elkies–Kumar (m, n)-coordinates and again apply Algorithm 5.6. These transformations are also recorded at [CFM24]. □

Let $M_D/\mathbb{Q}(Y_-(D))$ be the Mestre cubic defined in Section 2.2 associated to the generic point on the Hilbert modular surface $Y_-(D)$. Recall that we write $\widetilde{L}_D/\mathbb{Q}(Y_-(D))$ for the transformed Mestre conic given by $X^2 - DY^2 - q_D Z^2 = 0$.

To deduce Theorem 1.1 it remains to apply Mestre's result (Proposition 2.2) to $\widetilde{L}_D$ and the corresponding transformed cubic. Note that $\widetilde{L}_D$ may not have a point (except when $D \equiv 1 \pmod 8$, see Theorem 1.8). To overcome this, we note that a point on the threefold $\mathscr{L}_D$ defined in Theorem 1.1 allows us to parametrise the conic $\widetilde{L}_D$, and hence recover the Weierstrass models in Theorem 1.1 via Proposition 2.2.

Proof of Theorem 1.1. Let $\widetilde{R}_D(X, Y, Z) \in \mathbb{Q}(Y_-(D))[X, Y, Z]$ be the homogeneous cubic form which defines the cubic curve obtained by applying the transformations stored in [CFM24] to the Mestre cubic M_D.

Consider a $\mathbb{Q}(\mathscr{L}_D)$-rational parametrisation $\mathbb{A}^1 \dashrightarrow \widetilde{L}_D$ given by $x \mapsto [\eta_0 : \eta_1 : \eta_2]$ for some polynomials $\eta_i \in \mathbb{Q}(\mathscr{L}_D)[x]$. Our choice of parametrisation was computed by stereographic projection away from the point $(r, s, 1) \in \widetilde{L}_D(\mathbb{Q}(\mathscr{L}_D))$ and is recorded in [CFM24].

It is simple to check using computer algebra (e.g., `Magma`) that $\widetilde{R}_D(\eta_0, \eta_1, \eta_2)$ is equal to $F_D(z, g, h, r, s; x)$ up to a constant factor in $\mathbb{Q}(\mathscr{L}_D)$. The claim in (i) follows immediately from Proposition 2.2, together with [CMb, Proposition 2.1].

For (ii), note that (g, h) are coordinates for the Elkies–Kumar model for the Humbert surface $\mathcal{H}_D$ (which is birational to a subvariety of $\mathcal{M}_2$). □

7.2. **Models when $Y_-(D)$ is rational.** As described in the introduction, when $D = 5$, 8, 12, 13, and 17 the threefold $\mathscr{L}_D$ is rational, which we now prove. In particular, we give generic families of genus 2 curves with RM D in three parameters with no relations. When $D = 5$ this model is given in [CMb, Remark 6.2].

Corollary 7.1. *Let k be a field of characteristic 0. For each $D \in \{5, 8, 12, 13, 17\}$ and $a, b, c \in k$ consider the degree 6 polynomial $f_D(a, b, c; x) \in k[x]$ recorded in* [CFM24]. *If $f_D(a, b, c; x)$ has no repeated roots, then the Jacobian J of the genus 2 curve C/k with Weierstrass equation $C : y^2 = f_D(a, b, c; x)$ has RM D over $\bar{k}$. Moreover if $\mathrm{End}_{\bar{k}}(J)$ is abelian, then the RM is defined over k.*

Corollary 1.2 and Corollary 1.3 explicate the $D = 12$ and $D = 17$ cases of Corollary 7.1. When $D = 8$ we have $f_8(a, b, c; x) = \mathrm{Nm}_{L/K}\, \varphi(x)$, where $L = k[r]/\xi(r)$,

$$\xi(r) = (-a^2 + 2b^2 - 1)r^3 - 3cr^2 + (4a^4 - 16a^2b^2 + 2a^2 + 16b^4 - 4b^2 - 2c^2 - 2)r - 2c,$$

and

$$\begin{aligned}\varphi(x) = {} & (2(2b-1)(a^2 - 2b^2 + 1)r^2 + 4c(a^2 - 2b^2 + 2b - 1)r - 4(4a^4b - 2a^4 + 2a^3c \\ & - 16a^2b^3 + 8a^2b^2 + 2a^2b - a^2 - 4ab^2c + 16b^5 - 8b^4 - 4b^3 + 2b^2 - 2b + 1)x^2 \\ & + 4(a(a^2 - 2b^2 + 1)r^2 + 2acr - 2(2a^5 - 8a^3b^2 + a^3 + 2a^2bc + 8ab^4 - 2ab^2 - a \\ & - 4b^3c))x + (2b+1)(a^2 - 2b^2 + 1)r^2 - 2c(a^2 - 2b^2 - 2b - 1)r - 2(4a^4b + 2a^4 \\ & + 2a^3c - 16a^2b^3 - 8a^2b^2 + 2a^2b + a^2 - 4ab^2c + 16b^5 + 8b^4 - 4b^3 - 2b^2 - 2b - 1).\end{aligned}$$

Remark 7.2. The concise presentations given for $D = 8$ and $D = 12$ (with the Weierstrass sextic being given as a norm from a cubic étale k-algebra) is a general phenomenon for genus 2 curves whose Jacobians admit a Richelot isogeny (see e.g., [BD11, Lemma 4.1]). In particular, every genus 2 curve with RM by an order of discriminant $D \equiv 0 \pmod 2$ admits a model of this form.

Similarly the simple presentation in Corollary 1.3 follows from Lemma 3.5. In contrast, we do not know of any simpler presentation when $D \equiv 5 \pmod 8$. It would be interesting to simplify the models $C : y^2 = f_D(a, b, c; x)$ which we give when $D = 5, 13$ (possibly by developing a satisfactory algorithm for minimising a coupled conic-cubic pair in $\mathbb{P}^2$).

Proof of Corollary 7.1. This follows from Theorem 1.5, analogously to Theorem 1.1. Let $\widetilde{L}'_D : X^2 - DY^2 - p_D Z^2 = 0$, where p_D is as in Table 2, and let $\widetilde{R}'_D(X, Y, Z) \in \mathbb{Q}(m, n)[X, Y, Z]$ be the associated cubic form (see [CFM24]). Let $\mathscr{L}'_D : r^2 - Ds^2 - p_D = 0$ be the Mestre conic bundle over $\mathbb{A}^2_{m,n}$.

In the electronic data associated to this article [CFM24] we record rational parametrisations $(a, b, c) \mapsto (m, n, r, s)$ of the threefolds $\mathscr{L}'_D$ for each $D \leq 17$.

Let $x \mapsto [\nu_0 : \nu_1 : \nu_2]$ be the $\mathbb{Q}(a, b, c)$-rational parametrisation of $\widetilde{L}'_D$ recorded in [CFM24]. When $D = 17$ such a parametrisation is given over $\mathbb{Q}(a, b)$. It is simple to check with computer algebra that $\widetilde{R}'_D(\nu_0, \nu_1, \nu_2)$ is equal to $f_D(a, b, c; x)$ up to a constant factor, and the claims follow from Proposition 2.2. □

Indeed, the proof of Corollary 7.1 also allows us to recall the forgetful maps from the parameter space to the Humbert surface $\mathcal{H}_D$, and we immediately deduce the following.

Proposition 7.3. *For $D \in \{5, 8, 12, 13, 17\}$, let $f_D(a, b, c; x) \in \mathbb{Z}[a, b, c][x]$ be the polynomials defined in Corollary 7.1 (and it is understood that c plays no role when D = 17). The natural map from the parameter space $\mathbb{A}^3$ to the Humbert surface $\mathcal{H}_D$ which associates to a point $(a, b, c) \in \mathbb{A}^3$ the genus 2 curve $C : y^2 = f_D(a, b, c; x)$ is given by*

$$(g, h) = \begin{cases} \left(\dfrac{m^2 - 5n^2 - 9}{30}, \dfrac{25(m+5)n^4 - 5\beta n^2 + (m+3)^3(m-2)^2}{12500}\right) & \text{if } D = 5, \\ \left(\dfrac{(m-1)(m+1)}{16(2n^2-1)}, \dfrac{-32n^4 + 8(2m^2+7m+9)n^2 - (m+3)^3}{16(2n^2-1)(m+1)}\right) & \text{if } D = 8, \\ \left(\dfrac{2(m-1)(m+1)(m^2n + 9m^2 - 8)}{27m^2 - n^2 - 27}, m\right) & \text{if } D = 12, \\ \left(\dfrac{2(m^3 + 150m^2 - 6(n-44)m - 16(9n+4))}{9(n^2 - 12m^3 + 3m^2)}, \right. & \\ \quad \left. \dfrac{267m^3 - 24(3n-148)m^2 + (n^2 - 1440n - 768)m + 128n^2}{54(n^2 - 12m^3 + 3m^2)}\right) & \text{if } D = 13, \\ \left(\dfrac{\gamma}{3}, \dfrac{(5\gamma+9)a + 6(\gamma+1)}{18(2a-3)}\right) & \text{if } D = 17 \end{cases}$$

where

$$\beta = 2m^3 + 10m^2 - 5m - 45,$$

$$\gamma = \frac{-3(4a^3 - 6a^2b + 12a^2 + 2ab^2 + 5ab + 7a - 3b^2 + 6b + 1)}{2(4a^3 - 4a^2b + 12a^2 + 2ab^2 + 9a - 3b^2 + 9b)},$$

and

$$
(m,n) = \begin{cases} \left(\dfrac{2(5a^2+5ac+b^2-5c^2+1)}{5a^2-b^2+5c^2-1}, \dfrac{-b(4a+2c)}{5a^2-b^2+5c^2-1} \right) & \textit{if } D=5, \\ \left(\dfrac{-2a^2+4b^2+c^2-2}{2(a^2-2b^2)}, \dfrac{-c}{2} \right) & \textit{if } D=8, \\ \left(\dfrac{-a^2+3b^2+3c^2+1}{a^2-3b^2+3c^2-1}, \dfrac{18c}{a^2-3b^2+3c^2-1} \right) & \textit{if } D=12, \\ \left(\dfrac{8(13b^2-a^2+c^2-6c-3)}{a^2-13b^2-c^2+3c-3}, \dfrac{24(5a^2-65b^2-31c^2-34c-9)}{a^2-13b^2-c^2+3c-3} \right) & \textit{if } D=13. \end{cases}
$$

In particular, for a generic pair $P, P' \in \mathbb{A}^3(k)$ the associated genus 2 curves are isomorphic over $\bar{k}$ if and only if the image of P and P' under the above map are equal.

8. Relation to known families

8.1. **Discriminant 8.** Bending [Ben98, Ben99] gave a versal family of genus 2 curves C/k with RM 8 by analysing the Richelot isogeny $\sqrt{2}\colon \mathrm{Jac}(C) \to \mathrm{Jac}(C)$. This family is given in terms of three parameters A, P, Q. This construction therefore induces a dominant rational map $\mathbb{A}^3 \dashrightarrow Y_-(8)$. By interpolating triples of A, P, Q it is simple to recover this rational map in terms of Elkies–Kumar's [EK14] model for $Y_-(8)$. The rational map $\mathbb{A}^3 \dashrightarrow Y_-(8)$ is given by taking $(A, P, Q) \mapsto (m, n)$.

$$
m = \frac{f_1(A,P,Q)}{f_3(A,P,Q)f_4(A,P,Q)^2} \qquad \text{and} \qquad n = \frac{-f_2(A,P,Q)}{f_3(A,P,Q)f_4(A,P,Q)}.
$$

Here, the polynomials $f_i(A, P, Q) \in \mathbb{Z}[A, P, Q]$ have degrees 20, 15, 10, and 5 for each $i = 1, 2, 3, 4$ respectively. The precise formulae are too complicated to reproduce here, but we include them in the electronic data associated to this article [CFM24].

8.2. **Discriminant 12.** Denote by $Y_-(12)[\sqrt{3}]$ the Hilbert modular surface of discriminant 12 with *full $\sqrt{3}$-level structure*. That is, $Y_-(12)[\sqrt{3}]$ is the surface whose k-points parametrise genus 2 Jacobians J/k with an RM 12 action $\iota\colon \mathcal{O}_{12} \to \mathrm{End}_k^{\dagger}(J)$, such that $\ker \iota(\sqrt{3})$ is contained in $J(k)$.

Bruin, Flynn, and Shnidman [BFS23] computed an explicit rational parametrisation $\mathbb{P}^2 \dashrightarrow Y_-(12)[\sqrt{3}]$ over $\mathbb{Q}$ and gave formulae for the generic genus 2 curve. By forgetting the level structure we obtain a natural forgetful morphism $Y_-(12)[\sqrt{3}] \to Y_-(12)$. This forgetful map is given in the models of Elkies–Kumar [EK14] and Bruin–Flynn–Shnidman [BFS23] by $[a : b : c] \mapsto (m, n)$ where

$$
m = \frac{(a-c)(a^2+ab-4ac+b^2+bc+c^2)F_1(a,b,c)}{F_2(a,b,c)} \quad \text{and} \quad n = \frac{-F_3(a,b,c)}{(a-c)^2F_2(a,b,c)}.
$$

Here the homogeneous polynomials $F_i(a, b, c) \in \mathbb{Z}[a, b, c]$ are given by

$$
\begin{aligned}
F_1(a,b,c) &= a^4 - a^3b - 8a^3c + 3a^2bc + 18a^2c^2 - ab^3 + 6ab^2c + 3abc^2 - 8ac^3 + b^4 - b^3c \\
&\quad - bc^3 + c^4, \\
F_2(a,b,c) &= a^7 - 11a^6c + 39a^5c^2 - 2a^4b^3 - 37a^4c^3 + 10a^3b^3c - 37a^3c^4 - 30a^2b^3c^2 \\
&\quad + 39a^2c^5 + ab^6 + 10ab^3c^3 - 11ac^6 + b^6c - 2b^3c^4 + c^7,
\end{aligned}
$$

and

$$F_3(a,b,c) = a^9 - 45a^8c + 414a^7c^2 - 3a^6b^3 - 1374a^6c^3 + 36a^5b^3c + 1260a^5c^4 - 99a^4b^3c^2 + 1260a^4c^5 + 3a^3b^6 - 60a^3b^3c^3 - 1374a^3c^6 + 9a^2b^6c - 99a^2b^3c^4 + 414a^2c^7 + 9ab^6c^2 + 36ab^3c^5 - 45ac^8 - b^9 + 3b^6c^3 - 3b^3c^6 + c^9.$$

9. On the polynomials p_D and q_D

It is natural to ask about the geometric significance of the polynomials p_D and q_D, i.e., the curves they cut out in $Y_-(D)$. Here we present some empirical observations, including a conjecture for q_{40}, the first case missing from Table 1.

First consider p_D for $D = 5, 8, 12, 13$, and 17. For each such D, the polynomial p_D is a factor of the discriminant $\Delta(L_D)$ of the original Mestre conic L_D, written in terms of (m,n). In all of the cases except $D = 8$, the polynomial p_D is also a factor of λ_D, viewed as a polynomial in m and n. In the case $D = 17$, where $p_D = 1$, we remark that there is a quadratic factor of both $\Delta(L_D)$ and λ_D which is a norm from $\mathbb{Q}(m,n)(\sqrt{17})$. It is not clear how one might identify *a priori* which factor(s) of $\Delta(L_D)$ should contribute to p_D.

For q_D, the situation is even more mysterious. Consider the 12 q_D's in Table 1 such that $q_D \neq 1$. In each such case, q_D is not a factor of the original Mestre conic discriminant $\Delta(L_D)$. When $D = 12$ or $D = 44$, the lowest degree factor of q_D is a factor of $\Delta(L_D)$. It is not even apparent during our minimisation steps in Algorithm 5.6 what q_D should be—it is often not until we diagonalise at the end of our minimisation process that q_D appears!

For $D = 5, 8, 12$, or 13, writing q_D in terms of (m,n) gives a rational function which contains p_D as factor of the numerator ($D = 5, 13$) or denominator ($D = 8, 12$). At least when $D = 5, 8$, the rational functions $q_D(m,n)$ and $p_D(m,n)$ differ by a norm from $\mathbb{Q}(m,n)(\sqrt{D})$. For example, $q_5 = -6(10g+3)(15g+2) = -(m^2-5n^2)(m^2-5n^2-5)$. Here the curves $g = -\frac{3}{10}$ and $g = -\frac{2}{15}$ on $Y_-(5)$ are somewhat special: they have no $\mathbb{Q}$-rational points and do not lie in the image of the map from (m,n) to (g,h) (see [CMb, Section 5] for details).

Now consider the case $D = 21$. Recall from [EK14] that

$$\lambda_{21} = 189g^6 - 594g^5h + 621g^4h^2 - 216g^3h^3 - 378g^4 + 1116g^3h - 954g^2h^2 + 184gh^3 + 16h^4 + 205g^2 - 522gh + 349h^2 - 16,$$

and by Theorem 1.5 we have

$$q_{21} = 18g^2 - 12gh - 12h^2 - 14.$$

In Figure 1 we plot the real values (g,h) such that $\lambda_{21} = 0$ (red) and $q_{21} = 0$ (blue).

We see that there are four points where λ_{21} vanishes to order at least 2 on the curve $q_{21} = 0$: one pair where

$$27g^2 - 25 = 0 \quad \text{and} \quad 27h^2 - 1 = 0,$$

and one pair where

$$27g^4 + 342g^2 - 289 = 0 \quad \text{and} \quad 3h^4 + 27h^2 - 25 = 0.$$

Indeed, the resultants with respect to g and h are given by

$$\mathrm{Res}_g(\lambda_{21}, q_{21}) = 746496(27h^2-1)^2(3h^4+27h^2-25)^2$$

and

$$\mathrm{Res}_h(\lambda_{21}, q_{21}) = 64(27g^2-25)^2(27g^4+342g^2-289)^2.$$

We observed similar behaviour when $D = 24$ and $D = 28$.

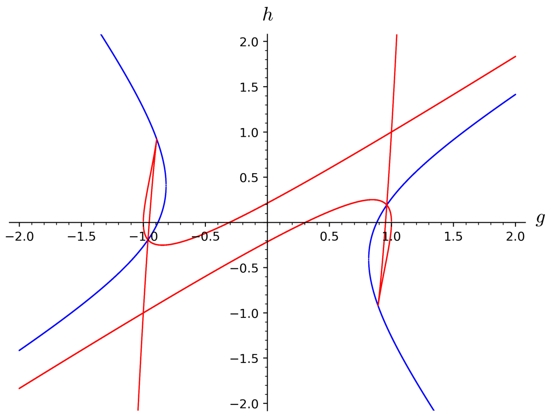

FIGURE 1. For $D = 21$, the real values (g, h) such that $\lambda_{21} = 0$ (red) and $q_{21} = 0$ (blue).

When $D = 40$, the singular points of the plane curve defined by the vanishing of the polynomial

$$\lambda_{40} = (g^2 - h^2 - 1)(9g^4 - 17g^2h^2 + 8h^4 - 12g^3 + 12gh^2 + 7g^2 - 8h^2 + 10g + 2)$$

occur at the points where

$$\begin{aligned} g - 8 = 0 &\quad \text{and} \quad 2h^2 - 125 = 0, \\ g - 9 = 0 &\quad \text{and} \quad h^2 - 80 = 0, \\ 3g + 1 = 0 &\quad \text{and} \quad h = 0. \end{aligned}$$

With the ansatz that q_{40} is quadratic in g and h with rational coefficients and imposing that q_{40} vanishes at the points given by the equations above, we see that q_{40} is proportional to

$$-15g^2 + 14h^2 + 10g + 5. \tag{9.1}$$

The expression in (9.1) is not identically a norm in $\mathbb{Q}(\sqrt{40})$ for $g, h \in \mathbb{Q}$, but is a norm for all of the 16 points (g, h) corresponding to genus 2 curves given in [EK14, Section 17.3], and thus seems to us to be a reasonable guess for an admissible choice of q_{40}.

REFERENCES

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. Computational algebra and number theory (London, 1993). MR1484478 ↑1.2

[BD11] Nils Bruin and Kevin Doerksen, *The arithmetic of genus two curves with* $(4, 4)$*-split Jacobians*, Canad. J. Math. **63** (2011), no. 5, 992–1024. MR2866068 ↑3, 7.2

[Ben98] Peter R. Bending, *Curves of genus* 2 *with* $\sqrt{2}$*-multiplication*, Ph.D. Thesis, 1998. ↑1.3, 8.1

[Ben99] ______, *Curves of genus 2 with sqrt2 multiplication*, arXiv e-prints (November 1999), math/9911273. ↑1, 1.3, 8.1

[BFS23] Nils Bruin, E. Victor Flynn, and Ari Shnidman, *Genus two curves with full* $\sqrt{3}$*-level structure and Tate-Shafarevich groups*, Selecta Math. (N.S.) **29** (2023), no. 3, Paper No. 42, 33. MR4594581 ↑1.3, 8.2

[Bru95] Armand Brumer, *The rank of* $J_0(N)$, 1995, pp. 3, 41–68. Columbia University Number Theory Seminar (New York, 1992). MR1330927 ↑1, 1.3

[CFM24] Alex Cowan, Sam Frengley, and Kimball Martin, *GitHub repository*, 2024. `https://github.com/SamFrengley/genus-2-RM.git`. ↑1.1, 1.1, 1.2, 1.3, 2.2, 4, 7.1, 7.1, 7.2, 8.1

[CMa] Alex Cowan and Kimball Martin, *Counting modular forms by rationality field. Preprint. arXiv:2301.10357*. ↑1.3

[CMb] ______, *Moduli for rational genus 2 curves with real multiplication for discriminant 5*. J. Théor. Nombres Bordeaux, to appear. *arXiv:2206.05752*. ↑1.2, 3, 3, 7.1, 7.2, 9

[CR03] J. E. Cremona and D. Rusin, *Efficient solution of rational conics*, Math. Comp. **72** (2003), no. 243, 1417–1441. MR1972744 ↑5.2

[EK14] Noam Elkies and Abhinav Kumar, *K3 surfaces and equations for Hilbert modular surfaces*, Algebra Number Theory **8** (2014), no. 10, 2297–2411. MR3298543 ↑1.1, 1.3, 2.1, 4, 6, 8.1, 8.2, 9, 9

[ES] Andreas-Stephan Elsenhans and Michael Stoll, *Minimization of hypersurfaces*. Math. Comp., to appear. *arXiv:2110.04625*. ↑6.1

[Has00] Ki-ichiro Hashimoto, *On Brumer's family of RM-curves of genus two*, Tohoku Math. J. (2) **52** (2000), no. 4, 475–488. MR1793932 ↑1.3

[Igu60] Jun-ichi Igusa, *Arithmetic variety of moduli for genus two*, Ann. of Math. (2) **72** (1960), 612–649. MR114819 ↑2.2

[Mes91a] J.-F. Mestre, *Familles de courbes hyperelliptiques à multiplications réelles*, Arithmetic algebraic geometry (Texel, 1989), 1991, pp. 193–208. MR1085260 ↑1, 1.3

[Mes91b] Jean-François Mestre, *Construction de courbes de genre* 2 *à partir de leurs modules*, Effective methods in algebraic geometry (Castiglioncello, 1990), 1991, pp. 313–334. MR1106431 ↑2.2, 2.2, 4

[Sil94] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR1312368 ↑5.1

[Smi05] Benjamin Andrew Smith, *Explicit endomorphisms and correspondences*, Ph.D. Thesis, 2005. ↑3

[vdG88] Gerard van der Geer, *Hilbert modular surfaces*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 16, Springer-Verlag, Berlin, 1988. MR930101 ↑1.1, 1.1, 2.1

[Voi21] John Voight, *Quaternion algebras*, Graduate Texts in Mathematics, vol. 288, Springer, Cham, 2021. MR4279905 ↑3

Department of Mathematics, Harvard University, Cambridge, MA 02138 USA
Email address: `cowan@math.harvard.edu`

School of Mathematics, University of Bristol, Bristol, BS8 1UG, UK
Email address: `sam.frengley@bristol.ac.uk`

Department of Mathematics, University of Oklahoma, Norman, OK 73019 USA
Email address: `kimball.martin@ou.edu`