Algorithmic Number Theory Symposium XVII, Groningen, July 6-10, 2026

CURVES OF GENUS TWO WITH MAPS OF EVERY DEGREE TO A FIXED ELLIPTIC CURVE

EVERETT W. HOWE

Abstract. We show that up to isomorphism there are exactly twenty pairs (C, E), where C is a genus-2 curve over $\mathbf{C}$, where E is an elliptic curve over $\mathbf{C}$, and where for every integer $n > 1$ there is a map of degree n from C to E. We also show that for every genus-2 curve C, there is an integer n with $1 < n \leq 59$ such that there is no minimal degree-n map from C to an elliptic curve.

1. Introduction

Curves of genus two that have nonconstant maps to elliptic curves have been studied for nearly 200 years, beginning with work of Legendre in 1828. Below, we will briefly review some of the work of the early researchers in the field — Legendre, Jacobi, Weierstrass, Kowalevski, Poincaré, Picard, Goursat, Brioschi, and others — but for now we will simply note that the problem we consider in this paper is one that could have been understood by these authors, with just a little tweaking of the terminology. Namely, we address the question of whether there exists a genus-2 curve C over the complex numbers $\mathbf{C}$, and an elliptic curve E over $\mathbf{C}$, such that for every $n > 1$ there exists a degree-n morphism from C to E. ("Is there a hyperelliptic integral that can be reduced, via transformations of every degree $n > 1$, to expressions involving the same elliptic integral?")

Perhaps surprisingly, the answer is yes.

Theorem 1. *Up to isomorphism, there are exactly twenty pairs (C, E) such that*

(1) *C is a curve of genus 2 over the complex numbers $\mathbf{C}$;*
(2) *E is an elliptic curve over $\mathbf{C}$; and*
(3) *for every $n > 1$ there is a map of degree n from C to E.*

Suppose (C, E) is one of these twenty pairs. If we choose a base point P on C, then the set of maps from C to E that take P to the origin of E correspond by duality to embeddings of E into $\operatorname{Jac} C$. These embeddings (plus the zero map) form a $\mathbf{Z}$-lattice in the $\mathbf{Q}$-vector space $\operatorname{Hom}(E, \operatorname{Jac} C) \otimes \mathbf{Q}$, whose dimension is at most twice the rank of $\operatorname{End} E$. In our examples, we obtain $\mathbf{Z}$-modules of rank 4, and the degree function is a quadratic form on each such module. The twenty pairs give rise to only four different quadratic forms on $\mathbf{Z}^4$, up to isomorphism. These quadratic

Date: 5 June 2026.
2020 *Mathematics Subject Classification.* Primary 14H45; Secondary 11G05, 11G10, 11G15, 11G30.
Key words and phrases. Hyperelliptic curve, elliptic curve, abelian surface, split Jacobian, quadratic form.

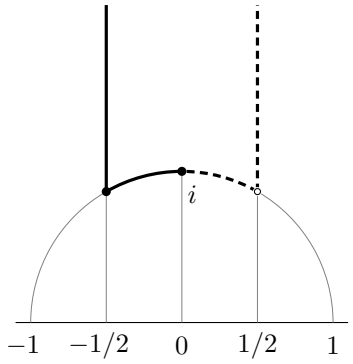

FIGURE 1. A strict fundamental domain $\mathcal{F}_1$ for $\Gamma(1)$

forms are

$$\begin{aligned} q_1 &:= 2w^2 + 3x^2 + 3y^2 + 4z^2 + 2xy \\ q_2 &:= 2w^2 + 2x^2 + 3y^2 + 3z^2 + 2wz + 2xy \\ q_3 &:= 2w^2 + 3x^2 + 3y^2 + 4z^2 + 2wx + 2wy + 2xz + 2yz \\ q_4 &:= 2w^2 + 3x^2 + 4y^2 + 6z^2 - 2wx + 2wz + 2xy + 4yz, \end{aligned}$$

and so in the course of proving Theorem 1 we will need the following result.

Proposition 2. *Each of the quaternary quadratic forms q_1, q_2, q_3, q_4 represents every integer greater than* 1.

Let $\mathcal{F}_1$ be the strict fundamental domain for $\Gamma(1)$ depicted in Figure 1. Suppose (C, E) is one of the twenty pairs from Theorem 1, and let τ be the element of $\mathcal{F}_1$ that corresponds to E. We will show that E has complex multiplication, so that τ is an element of an imaginary quadratic field. We will also show that the curve C has a period matrix of the form

$$\begin{pmatrix} 1 & 0 & \tau/2 & 1/2 \\ 0 & 1 & 1/2 & \sigma/2 \end{pmatrix}$$

where τ is as above and where σ lies in the strict fundamental domain $\mathcal{F}_2$ for $\Gamma(2)$ depicted in Figure 2. (That there is a period matrix of this form, for any genus-2 curve with a map of degree 2 to an elliptic curve, is essentially a result of Picard [37, 38].) Table 1 gives the value of τ and σ for the each of the twenty pairs, along with the discriminants Δ_E and Δ_F of the endomorphism rings of E and F, and the quadratic form associated to the pair (C, E). Pairs (C, E) that have the same values of Δ_E and Δ_F can be obtained from one another by Galois conjugation.

A map φ from a curve C to an elliptic curve E is said to be *minimal* if it does not factor through an isogeny $F \to E$ of degree greater than 1. We note that for our pairs (C, E), for some values of n there are no minimal maps $C \to E$ of degree n. This follows from two more general results that we prove in Section 7 by using work of Kani.

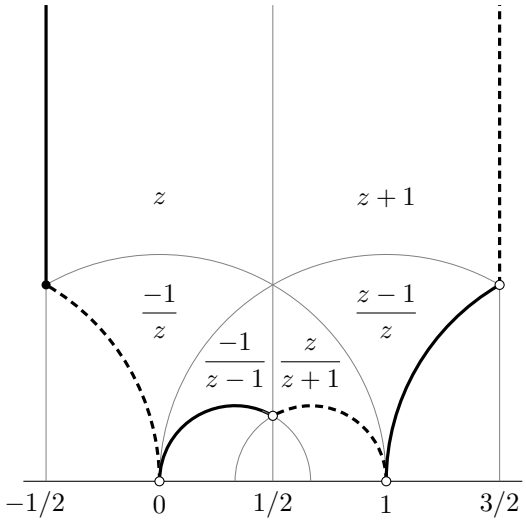

FIGURE 2. A strict fundamental domain $\mathcal{F}_2$ for $\Gamma(2)$, whose closure is tiled with images of the closure of the strict fundamental domain $\mathcal{F}_1$. The tiles are labeled by the Möbius transformation that takes $\mathcal{F}_1$ to the given tile. Note that $(3+\sqrt{-3})/2$ and $(3+\sqrt{-3})/6$ are not included in $\mathcal{F}_2$.

Theorem 3. *Let C be a curve of genus 2 over $\mathbf{C}$. Then for some n in the set $\{2,3,4,5,6,7,8,9,11,12,13,19,31,59\}$, there does not exist an elliptic curve E for which there exists a minimal map of degree n from C to E.*

Theorem 4. *Let k be a positive integer and let*

$$\begin{aligned} N = 2^6 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43 \cdot 47 \cdot 53 \cdot 59 \cdot 61 \cdot 67 \cdot 71 \cdot \\ 73 \cdot 79 \cdot 83 \cdot 97 \cdot 103 \cdot 107 \cdot 109 \cdot 113 \cdot 127 \cdot 131 \cdot 139 \cdot 151 \cdot 157 \cdot 163 \cdot \\ 167 \cdot 173 \cdot 179 \cdot 181 \cdot 191 \cdot 197 \cdot 199 \cdot 211 \cdot 223 \cdot 227 \cdot 239 \cdot 263 \cdot 271 \cdot \\ 277 \cdot 283 \cdot 293 \cdot 311 \cdot 359 \cdot 383 \cdot 431 \cdot 439 \cdot 479 \cdot 503 \cdot 599 \cdot 631 \cdot 719 \cdot \\ 727 \cdot 743 \cdot 751 \cdot 823 \cdot 839 \cdot 863 \cdot 887 \cdot 911 \cdot 983 \cdot 991 \cdot 1031 \cdot 1039 \cdot 1063 \cdot \\ 1103 \cdot 1151 \cdot 1223 \cdot 1231 \cdot 1303 \cdot 1319 \cdot 1327 \cdot 1439 \cdot 1487 \cdot 1511\,. \end{aligned}$$

If C is a curve of genus 2 over $\mathbf{C}$, then for some n in $\{2,3,13,kN\}$ there does not exist an elliptic curve E for which there exists a minimal map of degree n from C to E.

The structure of this paper follows that of the proof of Theorem 1. In Section 2 we recall some facts about genus-2 curves with degree-2 maps to elliptic curves. In particular, the following proposition is fundamental to our proof.

Proposition 5. *Suppose C is a genus-2 curve with a degree-2 map φ to an elliptic curve E. Then there is a unique elliptic curve F, a degree-2 map $\chi\colon C \to F$, and an isomorphism $\psi\colon E[2] \to F[2]$ such that the kernel of $\varphi^* \times \chi^*\colon E \times F \to \operatorname{Jac} C$ is*

No.	Δ_E	Δ_F	τ	σ	Form
1.	-4	-100	$\sqrt{-1}$	$5\sqrt{-1}$	q_2
2.				$(12+5\sqrt{-1})/13$	
3.	-8	-32	$\sqrt{-2}$	$\sqrt{-2}/4$	q_1
4.				$(4+\sqrt{-2})/4$	
5.				$(1+\sqrt{-2})/2$	
6.				$(2+\sqrt{-2})/4$	
7.		-72		$(6+\sqrt{-2})/6$	q_3
8.				$(2+3\sqrt{-2})/2$	
9.	-12	-3	$\sqrt{-3}$	$(-1+\sqrt{-3})/2$	q_3
10.				$(1+\sqrt{-3})/2$	
11.	-16	-4	$2\sqrt{-1}$	$\sqrt{-1}$	q_1
12.				$1+\sqrt{-1}$	
13.	-20	-20	$\sqrt{-5}$	$\sqrt{-5}$	q_2
14.			$(-1+\sqrt{-5})/2$	$(3+\sqrt{-5})/7$	
15.	-24	-24	$\sqrt{-6}$	$(2+\sqrt{-6})/2$	q_3
16.			$\sqrt{-6}/2$	$(6+\sqrt{-6})/7$	
17.	-36	-36	$3\sqrt{-1}$	$(6+3\sqrt{-1})/5$	q_4
18.				$(4+3\sqrt{-1})/5$	
19.			$(-1+3\sqrt{-1})/2$	$1+3\sqrt{-1}$	
20.				$(3+\sqrt{-1})/3$	

TABLE 1. Data for the twenty pairs (C, E) from Theorem 1

the graph of ψ and such that the following diagram commutes:

$$\begin{array}{ccc} E\times F & \xrightarrow{\left[\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right]} & E\times F \\ {\scriptstyle \varphi_*\times\chi_*}\uparrow & & \downarrow{\scriptstyle \varphi^*\times\chi^*} \\ \operatorname{Jac} C & \xrightarrow{2} & \operatorname{Jac} C\,. \end{array} \tag{1}$$

The pair (χ, ψ) is unique up to composition with automorphisms of F. Conversely, given two elliptic curves E and F and an isomorphism $\psi\colon E[2] \to F[2]$, there is a genus-2 curve C and a degree-2 map $C \to E$ that gives rise to F and ψ as above, unless ψ is the restriction to $E[2]$ of an isomorphism $E \to F$, in which case there is no such curve C.

Corollary 6. *Let notation be as in Proposition 5, and let ω be a nonconstant map from C to E. Let α be the endomorphism $\varphi_*\omega^*\colon E \to E$ and let β be the morphism $\chi_*\omega^*\colon E \to F$. Then $\deg\omega = (\deg\alpha + \deg\beta)/2$, and for every $P \in E[2]$ we have $\beta(P) = \psi(\alpha(P))$.*

There is a converse statement, as well.

Corollary 7. *Let notation be as in Proposition 5, and suppose $\alpha\colon E \to E$ and $\beta\colon E \to F$ are morphisms such that for every $P \in E[2]$, we have $\beta(P) = \psi(\alpha(P))$. Then there is a nonconstant map $\omega\colon C \to E$ with $\deg\omega = (\deg\alpha + \deg\beta)/2$ such that $\alpha = \varphi_*\omega^*$ and $\beta = \chi_*\omega^*$.*

Suppose C is a genus-2 curve that has maps of every degree $n > 1$ to an elliptic curve E. In Section 3 we apply Corollary 6 to the degree-3 and degree-4 maps from C to E, and use the resulting information to deduce restrictions on the endomorphism ring of E and on the relationship between E and F. In particular, we prove the following proposition.

Proposition 8. *Suppose C is a genus-2 curve that has maps of degree 2, 3, and 4 to an elliptic curve E. Let F be the curve associated as in Proposition 5 to a degree-2 map from C to E. Then for one of the possibilities for p and Δ listed below, the endomorphism ring of E has discriminant Δ, and there is a cyclic isogeny from E to F of degree p.*

(1) $p = 1$ *and* $-\Delta \in \{3, 4, 7, 11, 12, 16, 19, 20, 24, 27, 28\}$.
(2) $p = 2$ *and* $-\Delta \in \{4, 7, 8, 12, 15, 16, 20, 23, 24, 31, 36, 39, 40\}$.
(3) $p = 3$ *and* $-\Delta \in \{3, 4, 8, 11, 12, 16, 19, 20\}$.
(4) $p = 5$ *and* $-\Delta \in \{3, 4, 7, 8, 11, 12, 15, 16, 19, 31, 35, 40, 76, 91, 104, 115, 124, 131, 136, 139, 140\}$.

After Proposition 8, we see that only finitely many pairs (E, F) can occur. Suppose (E, F) is a pair satisfying the conclusion of Proposition 8 for some p and Δ, and suppose ψ is one of the six isomorphisms $E[2] \to F[2]$. We can compute the curve C associated to this data as in the second statement of Proposition 5, if such a C exists. For each such C and E, we can compute a $\mathbf{Z}$-basis for $\mathrm{Hom}(C, E)$, and using Corollary 7 we can compute the positive definite quadratic form given by the degree map. It is then an easy matter to check whether this form represents all integers n with $1 < n < 32$, which is obviously a necessary condition for the form to represent all integers $n > 1$. Our method for doing this is explained in Section 4, and Magma [4] code for carrying out the computation is available on the GitHub repository mentioned in Section 4.*

It turns out that each quadratic form arising in this way that represents all the integers from 2 to 31 is equivalent to one of the forms q_1, q_2, q_3, and q_4 given above, and therefore the (C, E) pairs that we have found satisfy the conditions of Theorem 1. It is then a simple matter to compute the data presented in Table 1, and to see that there are only 20 such pairs.

In Section 5 we compute models for the curves C. In Section 6 we prove Proposition 2, and in Section 7 we prove Theorems 3 and 4.

Remark 9. We note here that there is a result similar to Theorem 1 for fields of positive characteristic, if we restrict our attention to *ordinary* curves. Namely, if C is an ordinary genus-2 curve over an algebraically closed field K of positive characteristic, and if C has maps of every degree $n > 1$ to an elliptic curve E, then C is the reduction of one of the curves from Theorem 1. This follows from Serre-Tate lifting ([28],[36]), which shows that an ordinary example over K can be lifted to an example in characteristic 0. Note, however, that in general not all of

*We ran all of the code mentioned in this paper on an Apple M4 Max chip running Magma V2.29-6 on MacOS Tahoe 26.2.

the curves in the theorem will have good ordinary reduction modulo a given prime, so there will not necessarily be 20 examples of such curves over a given K.

We have not investigated the situation for non-ordinary curves over a field of positive characteristic. The endomorphism ring of a supersingular elliptic curve is a $\mathbf{Z}$-module of rank 4, so in some sense it should be easier for there to exist maps α and β as in Corollary 7 that can produce an ω of a given degree. For this reason, we expect that over some fields there will be examples of (C, E) pairs that are not reductions of our 20 curves in characteristic zero.

Remark 10. Here we give some historical background. As we mentioned at the beginning of this section, the study of genus-2 curves with maps to elliptic curves goes back nearly two centuries. In §12 of the third supplement to his *Traité des fonctions elliptiques* [34], published in 1828, Legendre shows how several "ultra-elliptic" integrals involving expressions of the form $\sqrt{x(1-x^2)(1-k^2x^2)}$ can be expressed in terms of elliptic integrals. Jacobi, in a postscript to his 1832 review [22, 23] of Legendre's book, notes that Legendre's examples can be generalized; rephrased in modern terminology, Jacobi's observation is that every hyperelliptic curve of the form

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

admits a degree-2 map to an elliptic curve. Legendre's examples come by taking $\lambda = -1$. Later, Königsberger [29] and Picard [37, §9] each proved that every genus-2 curve with a degree-2 map to an elliptic curve occurs in Jacobi's family.

The study of genus-2 curves with maps to elliptic curves continued, and flourished, in the latter half of the 19th century, with the focus shifting to the period matrices of such curves and the endomorphism rings of their Jacobians. In an 1874 paper, not published in a journal until 1884, Kowalevski [30] quotes an unpublished result of Weierstrass that describes the period matrices of curves whose associated abelian integrals can be reduced to elliptic integrals; in 1884 Poincaré [39] provided a proof of Weierstrass's theorem. For the special case of genus-2 curves, a better version of Weierstrass's result was given (independently) by Picard [37], and in 1884 Picard showed that his result can also be deduced directly from that of Weierstrass [38]. At the very end of the 19th century, Humbert published a series of papers [19, 20, 21] concerning genus-2 curves whose Jacobians have endomorphism rings larger than $\mathbf{Z}$; Humbert's curves having "singular relations with square invariant" have zero-divisors in their endomorphism rings, and hence have maps to elliptic curves.

Research in these matters has continued to this day. In more modern terminology, one can fix an integer $n > 1$ and study the moduli space of triples (C, E, φ), where $\varphi\colon C \to E$ is a map of degree n from a curve of genus 2 to an elliptic curve. (Usually one demands in addition that the map be minimal, in the sense defined above.) Some work concerns the general case (see for example [14, 24, 27]), but there is also interest in considering specific small values of n and constructing more or less explicit models of the corresponding moduli space, perhaps also giving equations for the triples (C, E, φ) themselves.

For $n = 2$, Jacobi's previously-cited work gives such equations over algebraically closed fields; in [18], the authors analyze the situation over non-algebraically closed fields. For the case $n = 3$, there are works spanning 141 years, including [2, 3, 5, 6, 15, 16, 17, 31, 40]. The case $n = 4$ is considered in older [1] and more recent [8] research, and there is work on the case $n = 5$ as well [35]. The paper [32] considers

all n up to 11, but is more focused on models for the moduli space itself rather than on the triples (C, E, φ), partly because the known models for C become quite complicated even for $n = 4$.

2. Consequences of the existence of a degree-2 map

In this section we prove Proposition 5 and its corollaries.

Proof of Proposition 5. Suppose C is a genus-2 curve over $\mathbf{C}$ with a degree-2 map φ to an elliptic curve E. Then the special case $N = 2$ of [24, Theorem 1.5] shows that there is another elliptic curve F and an isomorphism $\psi\colon E[2] \to F[2]$ such that the Jacobian of C is isomorphic to the quotient of $E \times F$ by the graph of ψ, and such that there is a degree-2 map $\chi\colon C \to F$.

Furthermore, if we let $G \subset (E \times F)[2]$ be the graph of ψ, then the isogeny $\varphi^* \times \chi^*\colon E \times F \to \operatorname{Jac} C$ has kernel G, and we have a diagram

$$\begin{array}{ccc} E \times F & \xrightarrow{\left[\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right]} & E \times F \\ \downarrow{\scriptstyle \varphi^* \times \chi^*} & & \uparrow{\scriptstyle \varphi_* \times \chi_*} \\ \operatorname{Jac} C & \xrightarrow{1} & \operatorname{Jac} C\,. \end{array}$$

We can then extend this diagram so that the compositions of the horizontal arrows on the top line and on the bottom line are the multiplication-by-2 maps:

$$\begin{array}{ccccc} E \times F & \xrightarrow{\left[\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right]} & E \times F & \xrightarrow{\left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]} & E \times F \\ \downarrow{\scriptstyle \varphi^* \times \chi^*} & & \uparrow{\scriptstyle \varphi_* \times \chi_*} & & \downarrow{\scriptstyle \varphi^* \times \chi^*} \\ \operatorname{Jac} C & \xrightarrow{1} & \operatorname{Jac} C & \xrightarrow{2} & \operatorname{Jac} C\,. \end{array}$$

The right half of this diagram is nothing other than diagram (1), which is what we want to show exists. The uniqueness of the pair (χ, ψ) up to automorphisms of F is part of [24, Theorem 1.5], and the converse follows from this as well. □

Remark 11. We note that we can give a period matrix for the Jacobian of C in terms of the period matrices for E and F and the isomorphism ψ, as follows. First, E has a period lattice Λ_E of the form $\langle 1, \tau \rangle$ for a unique τ in the fundamental domain $\mathcal{F}_1$, and there is a unique σ in the fundamental domain $\mathcal{F}_2$ such that

- $\Lambda_F := \langle 1, \sigma \rangle$ is a period matrix for F, and
- the isomorphism $\psi\colon E[2] \to F[2]$ sends the 2-torsion point $1/2 \bmod \Lambda_E$ of $E(\mathbf{C})$ to the 2-torsion point $\sigma/2 \bmod \Lambda_F$ of $F(\mathbf{C})$, and the point $\tau/2 \bmod \Lambda_E$ of $E(\mathbf{C})$ to the point $1/2 \bmod \Lambda_F$ of $F(\mathbf{C})$.

Then we can take

$$\Lambda_C := \begin{pmatrix} 1 & 0 & \tau/2 & 1/2 \\ 0 & 1 & 1/2 & \sigma/2 \end{pmatrix} \tag{2}$$

to be a period matrix for the Jacobian of C. This is essentially a result of Picard; see [37] and [38].

We also know the sesquilinear form on $\mathbf{C}^2$ that represents the principal polarization on $\operatorname{Jac} C$, because it is derived from the product polarization on $\Lambda_E \times \Lambda_F$. Namely, if δ is any multiple of $\sqrt{-1}$ and we write $\tau = a + b\delta$ and $\sigma = c + d\delta$ for

real numbers a, b, c, d, then the sesquilinear form applied to elements (z_1, z_2) and (w_1, w_2) of $\mathbf{C}^2$ gives the value

$$\text{Trace}_{\mathbf{C}/\mathbf{R}}\left(\frac{w_1\bar{z}_1}{b\delta} + \frac{w_2\bar{z}_2}{d\delta}\right). \tag{3}$$

One can check that the matrix of values of this pairing, applied to pairs of column vectors in the basis for Λ_C given above, is

$$\begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

so the pairing does indeed give a principal polarization on Λ_C.

Proof of Corollary 6. Let $\alpha = \varphi_*\omega^*$ and $\beta = \chi_*\omega^*$, and let $\widehat{\alpha}$ and $\widehat{\beta}$ be the dual morphisms of α and β. We can extend diagram (1) as follows:

$$\begin{array}{ccccccc} & & E \times F & \xrightarrow{\left[\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right]} & E \times F & & \\ & \overset{\alpha\times\beta}{\nearrow} & \uparrow{\scriptstyle \varphi_*\times\chi_*} & & \downarrow{\scriptstyle \varphi^*\times\chi^*} & \overset{\widehat{\alpha}+\widehat{\beta}}{\searrow} & \\ E & \xrightarrow{\omega^*} & \operatorname{Jac} C & \xrightarrow{2} & \operatorname{Jac} C & \xrightarrow{\omega_*} & E\,. \end{array} \tag{4}$$

Following the bottom edge of the diagram gives us multiplication by $2\deg\omega$ on E. The map from E to E we get from following the top edges of the diagram is the sum of the endomorphisms $\widehat{\alpha}\alpha$ and $\widehat{\beta}\beta$ of E. But $\widehat{\alpha}\alpha$ is multiplication by $\deg\alpha$, and $\widehat{\beta}\beta$ is multiplication by $\deg\beta$, so we see that $2\deg\omega = \deg\alpha + \deg\beta$, as claimed.

Let P be a point of order 2 on E. Then the image of P under the map from the lower left of the diagram to the $E \times F$ on the upper right is the pair $(\alpha(P), \beta(P))$, while the image of P in rightmost copy of $\operatorname{Jac} C$ is 0, because the middle map from $\operatorname{Jac} C$ to $\operatorname{Jac} C$ is multiplication by 2. Therefore, $(\alpha(P), \beta(P))$ lies in the kernel of the isogeny $\varphi^*\times\chi^*$, which is the graph of ψ, and it follows that $\beta(P) = \psi(\alpha(P))$. □

Proof of Corollary 7. Given α and β as in the statement of the corollary, consider the following diagram:

$$\begin{array}{ccccccc} & & E \times F & \xrightarrow{\left[\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right]} & E \times F & & \\ & \overset{\alpha\times\beta}{\nearrow} & \uparrow{\scriptstyle \varphi_*\times\chi_*} & & \downarrow{\scriptstyle \varphi^*\times\chi^*} & \overset{\widehat{\alpha}+\widehat{\beta}}{\searrow} & \\ E & & \operatorname{Jac} C & \xrightarrow{2} & \operatorname{Jac} C & & E\,. \end{array} \tag{5}$$

Our goal is to produce a morphism $\omega\colon C \to E$ that will allow us to extend this diagram to diagram (4).

By assumption, we have $\beta(P) = \psi(\alpha(P))$ for every $P \in E[2]$, so the kernel of the map $\widehat{\alpha} + \widehat{\beta}$ from $E \times F$ to E contains the kernel of $\varphi^* \times \chi^*$. It follows that there is a map $\varpi\colon \operatorname{Jac} C \to E$ that we can use to complete the triangle on the right-hand side of (5). (We note that this map is unique, because $\varphi^* \times \chi^*$ is an isogeny.)

Choose an Abel–Jacobi embedding of C into its Jacobian, and let ω be the composition of this embedding with ϖ. Then we automatically have $\varpi = \omega_*$, and by duality we find that $\omega^*\colon E \to \operatorname{Jac} C$ completes the triangle on the left-hand side of (5). This gives us (4), and proves the corollary. □

3. Consequences of the existence of maps of degree 3 and 4

In this section we prove Proposition 8. We begin with a lemma that records some facts about endomorphism rings of elliptic curves with noncyclic endomorphisms of small degree.

Lemma 12. *Let E be an elliptic curve over $\mathbf{C}$ that has a cyclic endomorphism α, and let Δ be the discriminant of the endomorphism ring of E.*

(1) *If* $\deg\alpha = 2$, *then* $-\Delta \in \{4, 7, 8\}$.
(2) *If* $\deg\alpha = 3$, *then* $-\Delta \in \{3, 8, 11, 12\}$.
(3) *If* $\deg\alpha = 4$, *then* $-\Delta \in \{7, 12, 15, 16\}$.
(4) *If* $\deg\alpha = 5$, *then* $-\Delta \in \{4, 11, 16, 19, 20\}$.
(5) *If* $\deg\alpha = 6$, *then* $-\Delta \in \{8, 15, 20, 23, 24\}$.
(6) *If* $\deg\alpha = 7$, *then* $-\Delta \in \{3, 7, 12, 19, 24, 27, 28\}$.
(7) *If* $\deg\alpha = 10$, *then* $-\Delta \in \{4, 15, 24, 31, 36, 39, 40\}$.
(8) *If* $\deg\alpha = 35$, *then* $-\Delta \in \{19, 31, 35, 40, 59, 76, 91, 104, 115, 124, 131, 136, 139, 140\}$.

Proof. Since E has a cyclic endomorphisms of positive degree, its endomorphism ring $\mathcal{O}$ is an imaginary quadratic order, and $\mathcal{O} \cong \mathbf{Z}[(\Delta + \sqrt{\Delta})/2]$. If we write $\alpha = x + y(\Delta + \sqrt{\Delta})/2$ for integers x and y, then x and y must be coprime to one another (because α is cyclic), and we have $\deg\alpha = x^2 + \Delta xy + y^2(\Delta^2 - \Delta)/4$. Given a value for $\deg\alpha$, it is a simple matter to find the discriminants Δ for which it is possible to find coprime x and y satisfying the equality above. We leave the details to the reader. □

Proof of Proposition 8. Suppose C is a genus-2 curve over $\mathbf{C}$ that has maps of degree 2, 3, and 4 to an elliptic curve E. Let φ be a degree-2 map from C to E, and let the elliptic curve F, the degree-2 map $\chi\colon C \to F$, and the isomorphism $\psi\colon E[2] \to F[2]$ be as in Proposition 5.

By Corollary 6, the existence of the degree-3 map from C to E implies that there is an endomorphism α of E and a morphism $\beta\colon E \to F$ such that $\deg\alpha + \deg\beta = 6$, and such that

$$\beta(P) = \psi(\alpha(P)) \quad \text{for all } P \in E[2]\,. \tag{6}$$

In particular, (6) implies that

$$\#(\ker\alpha)[2] = \#(\ker\beta)[2]\,. \tag{7}$$

We enumerate the possibilities below. Note that Lemma 12 tells us the possible discriminants of the endomorphism ring of an elliptic curve with a cyclic isogeny of certain degrees, and we use this without further comment in the list below to indicate how each possibility is covered by one of the cases in the statement of the proposition.

1. $\deg\alpha = 0$ and $\deg\beta = 6$. This cannot happen, because $\#(\ker\alpha)[2] = 4$ while $\#(\ker\beta)[2] = 2$, contradicting (7).
2. $\deg\alpha = 1$ and $\deg\beta = 5$. This implies that F is 5-isogenous to E. We explore this case further in the discussion below.
3. $\deg\alpha = 2$ and $\deg\beta = 4$. By (7), we see that β must be a cyclic isogeny. More specifically, (6) implies that $\ker\alpha$ is contained in $\ker\beta$, so β is the composition of α with a 2-isogeny from E to F. This possibility therefore falls under the case $p = 2$ of the statement of the proposition.

4. $\deg\alpha = 3$ and $\deg\beta = 3$. This falls under the case $p = 3$ of the statement of the proposition.
5. $\deg\alpha = 4$ and $\deg\beta = 2$. We see from (7) that α must be a cyclic isogeny. Therefore this falls under the case $p = 2$ of the statement of the proposition.
6. $\deg\alpha = 5$ and $\deg\beta = 1$. This falls under the case $p = 1$ of the statement of the proposition.
7. $\deg\alpha = 6$ and $\deg\beta = 0$. Equation (7) shows that this case cannot occur.

The only possibility not covered by the conclusion of the proposition is that E is arbitrary and F is 5-isogenous to E. For the rest of the proof we will assume that we are in this case.

Now we consider the consequences of the existence of a degree-4 map from C to E. Corollary 6 implies that there is an endomorphism α of E and a morphism $\beta\colon E \to F$ such that $\deg\alpha + \deg\beta = 8$, with (6) and (7) holding. We list the possibilities, and again use Lemma 12 without comment to show which cases of the proposition covers them.

1. $\deg\alpha = 0$ and $\deg\beta = 8$. From (7) we see that $\ker\beta$ must contain $E[2]$, so β is the composition of a 2-isogeny $E \to F$ with the multiplication-by-2 map on E. We see that F must be 2-isogenous to E. Since F is also 5-isogenous to E, we see that E has an endomorphism of degree 10. We find that this possibility falls under the case $p = 2$ of the proposition.
2. $\deg\alpha = 1$ and $\deg\beta = 7$. We will discuss this case below.
3. $\deg\alpha = 2$ and $\deg\beta = 6$. This falls under the case $p = 5$ of the statement of the proposition.
4. $\deg\alpha = 3$ and $\deg\beta = 5$. This falls under the case $p = 5$ of the statement of the proposition.
5. $\deg\alpha = 4$ and $\deg\beta = 4$. If α is cyclic, then this falls under the case $p = 5$ of the statement of the proposition. If α is not cyclic, then by (7) neither is β, which means that $F \cong E$. Therefore, there is an endomorphism of E of degree 5. This falls under the case $p = 1$ of the statement of the proposition.
6. $\deg\alpha = 5$ and $\deg\beta = 3$. This falls under the case $p = 3$ of the statement of the proposition.
7. $\deg\alpha = 6$ and $\deg\beta = 2$. This falls under the case $p = 5$ of the statement of the proposition.
8. $\deg\alpha = 7$ and $\deg\beta = 1$. This falls under the case $p = 1$ of the statement of the proposition.
9. $\deg\alpha = 8$ and $\deg\beta = 0$. By (7) we see that α cannot be cyclic, so it is the composition of multiplication-by-2 with an endomorphism of E of degree 2. This falls under the case $p = 5$ of the statement of the proposition.

This leaves us with one situation unaddressed: when there is both a 5-isogeny from E to F and a 7-isogeny from E to F, so that E has an endomorphism of degree 35. If the endomorphism ring of E does not have discriminant -59, then Lemma 12 shows that this situation falls under the case $p = 5$ of the proposition. To finish the proof of the proposition, we must show that the case of discriminant -59 cannot occur.

Suppose, in the situation of the proposition, that the endomorphism ring of the elliptic curve E has discriminant -59 and that F is both 5-isogenous and 7-isogenous to E. Since there are isogenies from E to F of coprime degrees, F must

also have endomorphism ring with discriminant -59. We check that then there are morphisms from E to F of degrees 0, 3, 5, and 7, and no other degrees less than 9, and that there are endomorphisms of E of degrees 0, 1, and 4, and no other degrees less than 9.

Since we are assuming that there is a degree-3 map from C to E, Corollary 6 says that there is an $\alpha_3 \in \operatorname{End} E$ and a $\beta_3 \in \operatorname{Hom}(E, F)$ such that $\deg \alpha_3 + \deg \beta_3 = 6$ and such that $\beta_3(P) = \psi(\alpha_3(P))$ for all $P \in E[2]$. The only possibility is that $\deg \alpha_3 = 1$ and $\deg \beta_3 = 5$. Note that $\alpha_3 = \pm 1$, so in fact $\beta_3(P) = \psi(P)$ for all $P \in E[2]$.

Likewise, since there is a degree-4 map from C to E there is an $\alpha_4 \in \operatorname{End} E$ and a $\beta_4 \in \operatorname{Hom}(E, F)$ such that $\deg \alpha_4 + \deg \beta_4 = 8$ and such that $\beta_4(P) = \psi(\alpha_4(P))$ for all $P \in E[2]$. The only possibility is $\deg \alpha_4 = 1$ and $\deg \beta_4 = 7$, so that $\alpha_4 = \pm 1$ and $\beta_4(P) = \psi(P)$ for all $P \in E[2]$.

If we let $\widehat{\beta}_4$ be the dual isogeny of β_4, so that $\widehat{\beta}_4 \beta_4 = 7$, then $P = \widehat{\beta}_4(\psi(P))$ for all $P \in E[2]$. Therefore, if we set $\gamma = \widehat{\beta}_4 \beta_3$, then γ is a degree-35 endomorphism of E that acts trivially on $E[2]$. That implies that $\gamma - 1$ kills $E[2]$, so $\gamma - 1 = 2\delta$ for some $\delta \in \operatorname{End} E$.

But we check that the only elements of norm 35 in $\operatorname{End} E \cong \mathbf{Z}[\frac{1+\sqrt{-59}}{2}]$ are $\frac{\pm 9 \pm \sqrt{-59}}{2}$, and none of these can be written as $1 + 2\delta$ for $\delta \in \mathbf{Z}[\frac{1+\sqrt{-59}}{2}]$. Therefore, $\operatorname{End} E$ cannot have discriminant -59. □

Remark 13. We choose to exclude the discriminant -59 from the statement of Proposition 8, even though its exclusion complicates the proof, because including it would make one of our later computational steps slightly more awkward. See Remark 16.

4. Enumerating possible examples

Proposition 8 gives our first step toward our proof of Theorem 1 by specifying a finite list of possible pairs (E, F) from which to construct examples of pairs (C, E) as in Theorem 1. In this section we explain how a computer calculation gives our second step toward the proof, by greatly reducing the number of possibilities.

Proposition 14. *Let C and E be as in Theorem 1, let $\varphi\colon C \to E$ be a degree-2 map, let F be as in Proposition 5, and let Δ_E and Δ_F be the discriminants of the endomorphism rings of E and F, respectively. Then the pair (Δ_E, Δ_F) is one of the following*:

$$\begin{array}{llllll} (-3,-3) & (-7,-7) & (-8,-72) & (-12,-12) & (-16,-16) & (-20,-20) \\ (-4,-4) & (-8,-8) & (-11,-11) & (-12,-48) & (-16,-64) & (-24,-24) \\ (-4,-100) & (-8,-32) & (-12,-3) & (-16,-4) & (-19,-19) & (-36,-36). \end{array}$$

In the cases where $\operatorname{End} E$ *and* $\operatorname{End} F$ *have the same discriminant Δ, the curves E and F are isomorphic to one another when $-\Delta \in \{3, 4, 7, 8, 11, 12, 16, 19, 20\}$ and are not isomorphic to one another when $-\Delta \in \{24, 36\}$.*

Proof. Our proof is computational, and Magma programs for carrying out the computation are available at https://github.com/everetthowe/many-maps.

We narrow down our possibilities by using a weakened form of Corollary 6. Given two elliptic curves E and F, if there exists an isomorphism $\psi\colon E[2] \to F[2]$ such that E, F, and ψ are as in Proposition 5, then for every $n > 1$ there exists

an endomorphism α_n of E and a homomorphism $\beta_n\colon E \to F$ such that $2n = \deg\alpha_n + \deg\beta_n$, and such that (6) holds. It follows that (7) also holds, and this is the weaker condition that we will check.

Given the j-invariants of E and F, we can use the classical modular polynomials Ψ_m to determine whether there are endomorphisms of E, and homomorphisms $E \to F$, of any given (small) degree and with kernels containing a given number of 2-torsion points. The polynomial Ψ_m has the property that there is a cyclic degree-m isogeny between two elliptic curves with j-invariants j_1 and j_2 if and only if $\Psi_m(j_1, j_2) = 0$. Every isogeny β can be factored into a cyclic isogeny composed with multiplication by a rational integer, and $\#(\ker\beta)[2]$ is determined by the parity of the degree of the cyclic isogeny and the parity of the rational integer.

To prove the proposition, we run through all (Δ, p) pairs listed in Proposition 8. For each Δ, we construct the number field K that contains the j-invariants of the elliptic curves E whose endomorphism rings have discriminant Δ; this is simply the number field defined by the Hilbert class polynomial for Δ, whose roots are precisely the j-invariants in question. Then, for one such root j_E, we use the classical modular polynomial Ψ_p to construct an extension L of K that contains the j-invariants j_F of the elliptic curves F that are p-isogenous to E.

For each such pair (j_E, j_F), we use the method sketched above to compute the set S_E of all pairs (m, d) of integers such that there is an endomorphism of E of degree m and with kernel containing exactly d points of order 2, for $m \le 62$. We compute the analogous set S_F corresponding to homomorphisms $E \to F$. Then, for every n from 2 to 31, we check to see whether we can find an $(m_1, d_1) \in S_E$ and an $(m_2, d_2) \in S_F$ with $d_1 = d_2$ and with $m_1 + m_2 = 2n$.

For all of the pairs (j_E, j_F) that meet this requirement, we output the discriminants of the endomorphism rings of E and F, and we note whether $j_E = j_F$. (We can compute the discriminant of $\operatorname{End} F$ by finding the discriminant whose Hilbert class polynomial is equal to the minimal polynomial of j_F.) The computation gives us the list of discriminant pairs listed in the proposition, and tells us whether $E \cong F$ when the discriminants are equal. □

Remark 15. Magma includes many of the classical modular polynomials Ψ_m for $m < 62$ in its standard distribution, but not all of them. It does include those for prime powers less than 61. We obtained Ψ_{61} from Andrew Sutherland's web page; it was calculated using the methods of [7]. For m with more than one prime factor, we write $m = ab$ for coprime a and b, and note that $\Psi(x, y)$ can be computed by taking the z-resultant of $\Psi(x, z)$ and $\Psi(y, z)$.

Remark 16. The quadratic order of discriminant -59 has class number 3, so there are three elliptic curves with this endomorphism ring; call them E, F, and F'. Let S_E and S_F be as in the penultimate paragraph of the proof of Proposition 14. We find that for every n from 2 to 31, there is an $(m_1, d_1) \in S_E$ and an $(m_2, d_2) \in S_F$ with $d_1 = d_2$ and with $m_1 + m_2 = 2n$, so E and F meet the "weaker condition" mentioned in the second paragraph of the proof. However, as we saw in the proof of Proposition 8, there do not exist $\alpha_3, \alpha_4 \in \operatorname{End} E$ and $\beta_3, \beta_4 \in \operatorname{Hom}(E, F)$ with $6 = \deg\alpha_3 + \deg\beta_3$ and $8 = \deg\alpha_4 + \deg\beta_4$ and with (6) holding for both pairs. It is for this reason that we made a special argument to exclude $p = 5$, $\Delta = -59$ from the conclusion of Proposition 8.

Let $\mathcal{O}$ be an imaginary quadratic order corresponding to one of the discriminants listed in Proposition 14, and let $\mathcal{O}_{\max}$ be the maximal order containing it. We check that the class number of $\mathcal{O}$ is at most 2, and that if $\mathcal{O}_{\max} \neq \mathcal{O}$ then the class number of $\mathcal{O}_{\max}$ is 1. This makes it particularly easy to find the elements of the fundamental domains $\mathcal{F}_1$ and $\mathcal{F}_2$ that correspond to elliptic curves with one of these endomorphism rings. Namely, if an order $\mathcal{O} = \mathbf{Z}[\theta]$ has class number 1, then the lattice $\langle 1, \theta \rangle$ has CM by $\mathcal{O}$, and the image ϑ of θ in the upper half-plane gives rise to the unique elliptic curve over $\mathbf{C}$ with CM by $\mathcal{O}$. It is a simple matter to find the element τ of $\mathcal{F}_1$ that is in the $\mathrm{PSL}_2(\mathbf{Z})$-orbit of ϑ. The elements of $\mathcal{F}_2$ that correspond to the elliptic curve with CM by $\mathcal{O}$ are simply the images of τ under the Möbius transformations listed in Figure 2.

If $\mathcal{O} = \mathbf{Z}[\theta]$ has class number 2, then in addition to the values of τ in $\mathcal{F}_1$ and $\mathcal{F}_2$ specified above, we must find the τ corresponding to a nonprincipal ideal of $\mathcal{O}$. If $\mathcal{O}$ is maximal, we find a nonprincipal prime ideal I of $\mathcal{O}$ lying over a rational prime p and we write $I = \langle p, \gamma \rangle$ for some $\gamma \in \mathcal{O}$. Then we let ϑ be the image of γ/p in the upper half-plane, and in the same way as above we find the elements τ of $\mathcal{F}_1$ and $\mathcal{F}_2$ that lie in the $\mathrm{PSL}_2(\mathbf{Z})$-orbit of ϑ.

If $\mathcal{O}$ has class number 2 and is nonmaximal, then as we noted above its corresponding maximal order $\mathcal{O}_{\max}$ has class number 1. Let f be the conductor of $\mathcal{O}$. Then the class group of $\mathcal{O}$ is isomorphic to the quotient of the group $U := (\mathcal{O}_{\max}/f\mathcal{O}_{\max})^\times/(\mathbf{Z}/f\mathbf{Z})^\times$ by the image of $\mathcal{O}_{\max}^\times$ in U (see [10, Eq (7.25), p. 116]). If $\gamma \in \mathcal{O}_{\max}$ represents a nontrivial element of this quotient group, then we let ϑ be the image of γ/f in the upper half-plane, and proceed as before.

We are now in a position to compute the values of τ and σ such that the period lattice (2) with polarization (3) corresponds to the Jacobian of a curve with maps of every degree $n > 1$ to the elliptic curve corresponding to the element τ of $\mathcal{F}_1$.

Proposition 17. *The pairs (τ, σ) listed in Table 1 are exactly the elements of $\mathcal{F}_1 \times \mathcal{F}_2$ such that the period matrix (2) and polarization (3) correspond to a curve from Theorem 1 whose associated elliptic curve corresponds to $\tau \in \mathcal{F}_1$.*

Proof. Our proof is computational, and Magma programs for carrying out the computation are available at https://github.com/everetthowe/many-maps.

For every pair (Δ_E, Δ_F) in Proposition 14, we let $K = \mathbf{Q}(\sqrt{\Delta_E}) \cong \mathbf{Q}(\sqrt{\Delta_F})$ and we specify an embedding K into $\mathbf{C}$ by choosing one of the square roots of Δ_E in K and declaring that it has positive imaginary part. Then we compute the values of τ in $K \cap \mathcal{F}_1$ corresponding to Δ_E as described above, and the values of $\rho \in K \cap \mathcal{F}_1$ corresponding to Δ_F. For each ρ we compute its images σ in $K \cap \mathcal{F}_2$; but if $\Delta_E = \Delta_F$ and $-\Delta_E \in \{3, 4, 7, 8, 11, 12, 16, 19, 20\}$ we only do so when $\rho = \tau$, and if $\Delta_E = \Delta_F$ and $-\Delta_E \in \{24, 36\}$ we only do so when $\rho \neq \tau$.

For each pair (τ, σ) we obtain, we perform the following calculation. Let Λ be the lattice in $K^2 \subset \mathbf{C}^2$ generated by the vectors

$$b_1 := (1, 0)\,, \qquad b_2 := (0, 1)\,, \qquad b_3 := (\tau/2, 1/2)\,, \qquad b_4 := (1/2, \sigma/2)\,.$$

We write elements of Λ as $\mathbf{Z}$-linear combinations of these vectors.

Let Λ_E be the lattice in $K \subset \mathbf{C}$ generated by 1 and τ. If Λ, with its principal polarization (3), is the Jacobian of a genus-2 curve C, then the maps from C to E that take a fixed base point to the origin of E correspond to embeddings of Λ_E into Λ. Such an embedding is determined by where it sends $1 \in \Lambda_E$, and the image

$x \in \Lambda$ must have the property that $\tau x \in \Lambda$; in other words, x must be an element of the sublattice $\mathrm{M} := \Lambda \cap \tau^{-1}\Lambda$ of Λ.

If Λ is the Jacobian of a curve C, then the degree of the map from C to E corresponding to an element x of M is equal to the value of the pairing (3) applied to τx and x. Write $\langle \tau x, x \rangle$ for the value of this pairing. If we compute four elements c_1, c_2, c_3, c_4 of Λ that generate M, we can then compute the Gram matrix of the quadratic form q on $\mathbf{Z}^4$ that sends a vector (n_1, n_2, n_3, n_4) to $\langle \tau x, x \rangle$, where $x = n_1 c_1 + \cdots + n_4 c_4$.

Given the Gram matrix of q, we can compute all of $v \in \mathbf{Z}^4$ with $q(v) \leq 31$. Let S be this set of vectors, and let V be the set $\{q(v) : v \in S\}$. If $1 \in V$ then we know that Λ is not the Jacobian of a genus-2 curve C, because there can be no degree-1 map from a genus-2 curve to E. On the other hand, if V does not contain 1, then Λ does correspond to a curve C, and if V does not contain every integer between 2 and 31 then C certainly does not have maps of every degree to E.

Thus, we can remove from consideration every pair (τ, σ) for which the set V is not equal to $\{2, \ldots, 31\}$.

On the other hand, for every pair (τ, σ) for which the set V is equal to $\{2, \ldots, 31\}$, we can check to see whether the quadratic form q is isomorphic to one of the forms q_1, q_2, q_3, or q_4. When we perform this calculation, we find that in fact every such q *is* isomorphic to one of the forms q_i. So for each such q, we output the values Δ_E, Δ_F, τ, σ, and i.

When we do so, we find that the output matches Table 1. This proves Theorem 1. □

5. Models of the curves

Given values Δ_E, Δ_F, τ, and σ from a row of Table 1, let K be a number field in which the Hilbert class polynomials of Δ_E and Δ_F split. We can compute models over K for elliptic curves E and F with period lattices Λ_E and Λ_F homothetic to $\langle 1, \tau \rangle$ and $\langle 1, \sigma \rangle$, respectively. Let L be an extension of K over which the 2-torsion points of E and F are rational. By complex approximation we can identify the 2-torsion points P_1, P_τ, and $P_{1+\tau}$ of $E(L)$ corresponding to the values $1/2$, $\tau/2$, and $(1+\tau)/2$ modulo Λ_E, and similarly we can compute the analogously-defined 2-torsion points Q_1, Q_σ, and $Q_{1+\sigma}$ on $F(L)$. Let ψ be the isomorphism $E[2] \to F[2]$ that sends P_1 to Q_σ and P_τ to Q_1. Then we can use the formulas from [18, §2] to compute a curve C over L that corresponds to E, F, and ψ as in Proposition 5.

Once we have a curve C in hand, we can try to find a twist of it that is rational over its field of moduli and that has a relatively simple defining equation. ("Relatively simple" is an inexact expression, so creating these models is not an exact science.)

By this method, we have found the models for the curves in Theorem 1 that we present in Table 2. Since we define the curves in terms of elements of abstract number fields, and not by specific complex numbers, each of the equations corresponds to several curves from Theorem 1 — namely, the ones with the same values of Δ_E and Δ_F.

Example 18. For the first curve on the list, we will present a basis for the rank-4 $\mathbf{Z}$-module of maps from C to E that take the point $(1, 0)$ to the origin of E. We give the reasonably simple formulas here; Magma code that verifies (8) can be found in the GitHub repository mentioned in Section 4.

Δ_E	Δ_F	Polynomial f
-4	-100	$x^6 - 3x^4 + (2 + r^{24})x^2 - r^{24}$ where $r^2 - r - 1 = 0$
-8	-32	$x^6 + (32r^3 - 31r^2 + 8r - 18)x^4 + (8r^3 - 8r^2 + 16r)x^2 + 8$ where $r^4 - 2r^2 - 1 = 0$
-8	-72	$x^6 + (-2r - 33)x^4 + (-116r - 189)x^2 - 2r + 5$ where $r^2 - 6 = 0$
-12	-3	$x^6 + (3r - 6)x^4 + (-12r + 9)x^2 + 4$ where $r^2 + 1 = 0$
-16	-4	$x^6 + (6r + 9)x^4 + (72r - 30)x^2 + 16r$ where $r^2 - 2 = 0$
-20	-20	$x^5 + 5x^3 + 5x$
-24	-24	$x^6 - 21x^4 + 48x^3 - 45x^2 + 48x - 23$
-36	-36	$x^5 - (8r - 12)x^4 - (73r + 6)x^3 - (168r + 252)x^2 - (72r + 423)x$ where $r^2 + 3 = 0$

TABLE 2. For each pair Δ_E, Δ_F, we give a polynomial f such that $y^2 = f$ is an equation for the corresponding curves C from Table 1

Let i and s satisfy $i^2 = -1$ and $s^2 = 5$, and let $r = (s+1)/2$, so that $r^2 - r - 1 = 0$. Our curve C is

$$y^2 = x^6 - 3x^4 + (2 + r^{24})x^2 - r^{24},$$

and we let E be the elliptic curve

$$w^2 = z^3 + 9sz$$

with j-invariant 1728.

Define rational functions P_2, Q_2, P_3, and Q_3 by

$$P_2 := \frac{36sr^6}{x^2 - 1} \qquad Q_2 := \frac{-18sr^3}{(x^2 - 1)^2}$$

$$P_3 := \frac{-3r(x+1)(x^2 - 6r^3x + r^{12})}{(x-1)(sx + r^6)^2} \qquad Q_3 := \frac{-9r((1-2s)x^2 - 2x - r^6)}{(x-1)^2(sx + r^6)^3}$$

and define maps from C to E by

$$\begin{aligned}
\varphi_1 &: \quad (x, y) \to (\ \ P_2,\ yQ_2) \\
\varphi_2 &: \quad (x, y) \to (-P_2, iyQ_2) \\
\varphi_3 &: \quad (x, y) \to (\ \ P_3, iyQ_3) \\
\varphi_4 &: \quad (x, y) \to (-P_3,\ yQ_3).
\end{aligned}$$

These maps all send the point $(1,0)$ on C to the identity of E. Then one can check that for integers a, b, c, d, we have

$$\deg(a\varphi_1 + b\varphi_2 + c\varphi_3 + d\varphi_4) = 2a^2 + 2b^2 + 3c^2 + 3d^2 + 2ad + 2bc = q_2(a,b,c,d)\,, \tag{8}$$

where q_2 is the quadratic form given in the introduction.

Remark 19. The code in our GitHub repository also includes similar presentations of the curves and maps for the cases $\Delta_E = \Delta_F = -20$ and $\Delta_E = \Delta_F = -36$. We hope to add more examples as time allows.

Remark 20. The examples with $\Delta_E = \Delta_F$ (rows 13 through 20 in Table 1) have a remarkable property: Each C has maps of every degree to *two different* (but Galois conjugate) elliptic curves. If the existence of any (C, E) pairs as in Theorem 1 is surprising, then surely it is even more surprising to find curves C with more than one choice for E!

6. Quaternary quadratic forms representing all integers greater than 1

In this section we will prove Proposition 2. It is easy to check that each of the four forms q_1, q_2, q_3, q_4 represents the integer 4, and it is clearly the case that if a form represents n then it also represents $4n$. Thus, it will suffice for us to show that each of the four forms represents every integer $n > 1$ that is not a multiple of 4. We give a separate argument for each of the four forms.

6.1. The quadratic form q_1.

Recall that

$$q_1 = 2w^2 + 3x^2 + 3y^2 + 4z^2 + 2xy\,.$$

Suppose $n > 1$ is not a multiple of 4. Let d be the integer defined by

$$d = \begin{cases} 0 & \text{if } n \equiv 2, 3, 5 \bmod 8 \\ 1 & \text{if } n \equiv 1, 6, 7 \bmod 8\,. \end{cases}$$

Then $n - 4d^2$ is a positive integer and $n - 4d^2 \equiv 2, 3, 5 \bmod 8$; a result of Dickson [12, Theorem VI] then shows that we may write

$$n - 4d^2 = a^2 + 2b^2 + 2c^2$$

for some integers a, b, c. By considering the right-hand side of this equality modulo 8, we check that b and c cannot both have the opposite parity to a, so by switching b and c if necessary we can ensure that $a \equiv b \bmod 2$. Now we simply set

$$w = c \qquad y = (b-a)/2$$
$$x = (a+b)/2 \qquad z = d$$

and note that $n = q_1(w, x, y, z)$.

6.2. The quadratic form q_2.

Recall that

$$q_2 = 2w^2 + 2x^2 + 3y^2 + 3z^2 + 2wz + 2xy\,.$$

Suppose $n > 1$ is not a multiple of 4. Let d be the integer defined by

$$d = \begin{cases} 0 & \text{if } 3n \equiv 1, 2, 5, 6, 7 \bmod 8 \\ 1 & \text{if } 3n \equiv 3 \bmod 8\,. \end{cases}$$

Then $3n-5d^2$ is a positive integer and $3n-5d^2 \equiv 1, 2, 5, 6, 7 \bmod 8$. Another result of Dickson [11, Theorem 15] shows that we may write

$$3n - 5d^2 = a^2 + b^2 + 5c^2$$

for some integers a, b, c. It follows that

$$a^2 + b^2 \equiv c^2 + d^2 \bmod 3\,,$$

so by exchanging a and b, if necessary, we may assume that $a^2 \equiv c^2 \bmod 3$ and $b^2 \equiv d^2 \bmod 3$, and by replacing a and b with their negatives, if necessary, we may assume that in fact $a \equiv c \bmod 3$ and $b \equiv d \bmod 3$. Now let

$$w = c \qquad\qquad y = (b-d)/3$$
$$x = d \qquad\qquad z = (a-c)/3$$

and note that $n = q_2(w, x, y, z)$.

6.3. **The quadratic form q_3.** Recall that

$$q_3 = 2w^2 + 3x^2 + 3y^2 + 4z^2 + 2wx + 2wy + 2xz + 2yz\,.$$

Let $n > 1$ be an integer that is not a multiple of 4. Let d be the integer defined by

$$d = \begin{cases} 0 & \text{if } n \equiv 2, 3, 6, 7 \bmod 8 \\ 1 & \text{if } n \equiv 1, 5 \bmod 8\,. \end{cases}$$

Then $n-3d^2$ is a positive integer and $n-3d^2 \equiv 2, 3, 6, 7 \bmod 8$. Yet another result of Dickson [12, Theorem XI] shows that we may write

$$n - 3d^2 = a^2 + 2(b^2 + bc + c^2)$$

for some integers a, b, c. Now, b and c cannot both be even, because in that case we would have $n-3d^2 \equiv a^2 \bmod 8$, while we know that $n-3d^2$ is not congruent to a square modulo 8. By replacing (b, c) with $(b+c, -c)$ if necessary, we can ensure that one of the numbers b, c is even and the other odd. Then by switching b and c, if necessary, we can ensure that $a+c+d$ is even. Now set

$$w = b + (a+c+d)/2 \qquad\qquad y = c - (a+c+d)/2$$
$$x = -(a+c+d)/2 \qquad\qquad z = d$$

and note that $n = q_2(w, x, y, z)$.

6.4. **The quadratic form q_4.** Recall that

$$q_4 = 2w^2 + 3x^2 + 4y^2 + 6z^2 - 2wx + 2wz + 2xy + 4yz\,.$$

Our proof in this case depends on the parity of n. First let us suppose that $n > 1$ is an even integer that is not a multiple of 4. Then n is congruent to 2 or 6 modulo 8, so Legendre's three-square theorem [33, pp. 398–399] says that we may write

$$n = a^2 + b^2 + c^2$$

for some integers a, b, c. By permuting these integers and changing their signs, if necessary, we may assume that $a \equiv b \bmod 3$. Then we may set

$$w = (2a+b)/3 \qquad\qquad y = (a-b+3c)/6$$
$$x = 0 \qquad\qquad z = (b-a)/3\,.$$

These numbers are integers; the only thing that may not be clear immediately is whether y is integral at 2, but that can be verified by noting that

$$a - b + 3c \equiv a + b + c \equiv a^2 + b^2 + c^2 \equiv n \equiv 0 \bmod 2\,.$$

One can easily check that $n = q_4(w, x, y, z)$.

Now suppose that $n > 1$ is odd. Let $d = 3$, and note that the three-square theorem shows that we may write

$$4n - d^2 = a^2 + b^2 + c^2$$

for some integers a, b, c. Considering this equality modulo 4, we see that a, b, and c must all be odd, and by permuting them and changing their signs (if necessary) we can assume that $a \equiv b \bmod 3$ and $a \equiv b + c + d \bmod 4$. Now set

$$w = (2a + b + d)/6 \qquad y = (a - b + 3c - d)/12$$
$$x = d/3 \qquad z = (b - a)/6\,.$$

Our assumptions on a, b, c, and d show that w, x, y, z are integers, and it is easy to check that $n = q_4(w, x, y, z)$.

This proves Proposition 2. □

7. Empty intersections of Humbert surfaces

A point in the moduli space $\mathcal{M}_2$ of genus-2 curves lies on the Humbert surface H_{n^2} if and only if the curve it represents has a minimal map of degree n to an elliptic curve. Since a map $C \to E$ of prime degree is necessarily minimal, Theorem 1 shows that the intersection $\cap_p H_{p^2}$ is nonempty, where p ranges over the set of all primes. (Keep in mind that the Humbert surface H_{n^2} has roughly n^3 components, so one's geometric intuition about intersections of surfaces in threefolds must be tempered with some combinatorics to get a full picture of the situation.)

This leads to the motivation behind Theorems 3 and 4: Can we show that there are finite collections of Humbert surfaces H_{n^2} with trivial intersection? And, hearkening back to our geometric intuition, can we find *four* Humbert surfaces H_{n^2} whose intersection is empty, as one would expect if we were dealing with a random collection of irreducible surfaces? Or, does the combinatorics of their many components interfere with this seemingly reasonable expectation? Work of Kani sheds light on the situation, and guides our proofs of these two theorems.

Kani [25, Theorem 20] shows that to every genus-2 curve C one can associate a positive definite quadratic form q_C in at most 3 variables, with integer coefficients, known as the *refined Humbert invariant* of C. The invariant q_C has the property that C has a minimal map of degree n to some elliptic curve if and only if q_C represents n^2 primitively; that is, if and only if there is an integer vector v with coprime entries such that $q_C(v) = n^2$. Kani also shows [26] that a positive-definite ternary quadratic form with integer coefficients that is *primitive* — that is, one whose coefficients generate the unit ideal — occurs as refined Humbert invariant if and only if it does not take on any values that are 2 or 3 modulo 4. Theorems 3 and 4 are therefore corollaries of the following proposition concerning ternary quadratic forms.

Proposition 21. *Let q be a primitive positive definite ternary quadratic form with integer coefficients that does not represent 1 and that does not represent any integer congruent to 2 or 3 modulo 4. Then*:

(1) *For some n in the set $D_1 := \{2, 3, 4, 5, 6, 7, 8, 9, 11, 12, 13, 19, 31, 59\}$, the form q does not primitively represent n^2.*
(2) *Let N be as in Theorem 4 and let k be a positive integer. For some n in the set $D_2 := \{2, 3, 13, kN\}$, the form q does not primitively represent n^2.*

Proof. Let D be either of the sets D_1 and D_2. Suppose there were a positive definite integer ternary form q that does not represent 1, and that does not represent any integer that is 2 or 3 modulo 4, but that primitively represents all n^2 with $n \in D$. In particular, this q must primitively represent 4, 9, and 169. We write q in Minkowski-reduced form as $ax^2 + by^2 + cz^2 + 2rxy + 2sxz + 2tyz$. (Note that a priori, r, s, and t may be half-integers.)

The condition that q only represent integers that are 0 and 1 mod 4 implies that a, b, and c must be 0 or 1 mod 4. By considering the values of q at triples (x, y, z) with all entries in $\{-1, 0, 1\}$ we find that the same congruence condition implies that the half-integers r, s, and t are in fact integers.

By replacing some of the variables with their negations, we can assume that $r \geq 0$ and $s \geq 0$, and if $rs = 0$ then we may assume that $t \geq 0$. And finally, since the form is reduced, from [9, Lemma 1.2, p. 257] we see that

$$\begin{array}{lll} 2r \leq a & 2t \leq a + b + 2r - 2s & 2t \geq -b \\ 2s \leq a & 2t \leq a + b - 2r + 2s & 2t \geq 2r + 2s - a - b\,. \\ 2t \leq b & & \end{array}$$

We know from [41, Satz 7, p. 281] that the sequence (a, b, c) is the sequence of successive minima for q. Since q represents 4 but does not represent 1, we must have $a = 4$. Since $4x^2$ does not represent 9, we must have $b \in \{4, 5, 8, 9\}$.

We check that for $b \in \{4, 5, 8, 9\}$ and $r \in \{0, 1, 2\}$, if the quadratic form $ax^2 + by^2 + 2rxy$ does not represent integers that are 2 or 3 mod 4 then it also does not represent 169. Since we are assuming that q does represent 169, the third succesive minimum of q must be at most 169; in other words, $c \leq 169$.

Now we can enumerate all of the values of a, b, c, r, s, and t meeting the conditions above. For each resulting ternary form q, we check whether it represents all of the integers in D_1 and D_2 as follows.

The elements of D_1 are small enough that we can simply check by brute force whether q primitively represents all of them. Magma code in our GitHub repository carries out this computation, and verifies that none of the q we must consider represents every element of D_1. This proves statement (1).

To prove statement (2), we must show that none of the q produced above primitively represents $(kN)^2$. To accomplish this, it will suffice for us to produce, for each of the q we must consider, a prime power m that divides N^2 such that q does not primitively represent any multiple of m.

Lemma 22, below, gives a quick method that often can find such a prime power m. We apply the lemma to each of the q we must consider. If the lemma does not provide us with such an m, the brute force method sketched in Remark 23 produces an m that divides 2^{12} such that q does not primitively represent any multiple of m. Since 2^{12} divides N^2, this computation verifies statement (2) of the proposition. □

Lemma 22 (Compare to [13, Prop. 3.1]). *Let $q = ax^2+by^2+cz^2+2rxy+2sxz+2tyz$ be a nondegenerate quadratic form with integer coefficients, let M be the matrix*

$$\begin{pmatrix} a & r & s \\ r & b & t \\ s & t & c \end{pmatrix},$$

and for $1 \le i \le 3$ let M_i be the upper left $i \times i$ submatrix of M. Let $A = \det M_1$, $B = (\det M_2)/(\det M_1)$, and $C = (\det M_3)/(\det M_2)$. Suppose that p is an odd prime such that A, B, C, r/a, s/a, and $(rs-at)/(ab-r^2)$ are all integral at p, and suppose that the parities of the p-adic valuations of A, B, and C are not all equal. Finally, suppose that $-A/B$, $-A/C$, and $-B/C$ are all nonsquares in $\mathbf{Q}_p$.

If m is an integer whose p-adic valuation is greater than that of A, B, and C, then q does not primitively represent m.

Proof. We note that if we set

$$u := x + \left(\frac{r}{a}\right)y + \left(\frac{s}{a}\right)z, \qquad v := y - \left(\frac{rs-at}{ab-r^2}\right)z, \qquad w := z,$$

then $q = Au^2 + Bv^2 + Cw^2$, and our assumptions on the integrality of A, B, C, r/a, s/a, and $(rs-at)/(ab-r^2)$ show that q is in fact isomorphic over $\mathbf{Z}_p$ to the diagonal form $q' := Au^2 + Bv^2 + Cw^2$. Therefore it suffices to show that q' does not primitively represent m.

Reorder A, B, and C so that A and B have p-adic valuations of the same parity. Suppose that q' represents m over $\mathbf{Z}_p$, and let u, v, and w be elements of $\mathbf{Z}_p$ with $m = Au^2 + Bv^2 + Cw^2$.

We claim that each summand in this last equality has valuation at least that of m. For suppose not. Because our valuation is non-Archimedean, if any of the summands has valuation less than that of m, then at least two of them must have that same valuation, in order for there to be cancellation that will increase the valuation of the sum. Since C has different parity of valuation than A and B, it must be that Au^2 and Bv^2 have equal valuation, say equal to e, and that Au^2+Bv^2 has valuation greater than e. The p-adic expansions of the summands must then look like

$$\begin{aligned} Au^2 &= \quad \alpha p^e + \text{higher-order terms} \\ Bv^2 &= -\alpha p^e + \text{higher-order terms} \end{aligned}$$

with α a unit. But then

$$-\left(\frac{Au^2}{Bv^2}\right) = 1 + \text{higher-order terms}, \tag{9}$$

which is enough to show that $-(Au^2)/(Bv^2)$ is a square in $\mathbf{Z}_p$, because p is odd. This contradicts our assumption that $-A/B$ is not a square. Therefore, Au^2, Bv^2, and Cw^2 each have valuation greater than that of m, so each of u, v, and w has positive valuation, so they are not coprime. □

Remark 23. The requirement in Lemma 22 that p be odd is necessary in order for (9) to contradict the assumption that $-A/B$ is a nonsquare. Rather than try to spell out a variation of the lemma for $p = 2$, we instead simply note that for small powers m of 2, we can check by brute force whether we can have $q(x, y, z) \equiv 0 \bmod m$ for values of x, y, and z that are not all even. (The amount of brute force needed can be reduced slightly by diagonalizing q over $\mathbf{Q}_2$; see the Magma code for details.)

References

[1] Oskar Bolza, *Ueber die Reduction hyperelliptischer Integrale erster Ordnung und erster Gattung auf elliptische durch eine Transformation vierten Grades*, Math. Ann. **28** (1886), no. 2-3, 447–456.

[2] ———, *Zur Reduction hyperelliptischer Integrale erster Ordnung auf elliptische mittels einer Transformation dritten Grades*, Math. Ann. **50** (1898), no. 2-3, 314–324. MR 1511001

[3] ———, *Zur Reduction hyperelliptischer Integrale erster Ordnung auf elliptische mittels einer Transformation dritten Grades*, Math. Ann. **51** (1898), no. 3, 478–480. MR 1511037

[4] 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). MR 1484478

[5] Francesco Brioschi, *Sur la réduction de l'intégrale hyperelliptique à l'elliptique par une transformation du troisième degré*, Ann. Sci. École Norm. Sup. (3) **8** (1891), 227–230. MR 1508859

[6] Reinier Bröker, Everett W. Howe, Kristin E. Lauter, and Peter Stevenhagen, *Genus-2 curves and Jacobians with a given number of points*, LMS J. Comput. Math. **18** (2015), no. 1, 170–197. MR 3349314

[7] Reinier Bröker, Kristin Lauter, and Andrew V. Sutherland, *Modular polynomials via isogeny volcanoes*, Math. Comp. **81** (2012), no. 278, 1201–1231. MR 2869057

[8] 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. MR 2866068

[9] J. W. S. Cassels, *Rational quadratic forms*, London Mathematical Society Monographs, vol. 13, Academic Press, Inc., 1978, pp. xvi+413. MR 522835

[10] David A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, third ed., AMS Chelsea Publishing, Providence, RI, 2022, With contributions by Roger Lipsett. MR 4502401

[11] Leonard Eugene Dickson, *Ternary quadratic forms and congruences*, Ann. of Math. (2) **28** (1926/27), no. 1-4, 333–341. MR 1502786

[12] ———, *Integers represented by positive ternary quadratic forms*, Bull. Amer. Math. Soc. **33** (1927), no. 1, 63–70. MR 1561323

[13] A. G. Earnest and B. L. K. Gunawardana, *Local criteria for universal and primitively universal quadratic forms*, J. Number Theory **225** (2021), 260–280. MR 4235261

[14] Gerhard Frey and Ernst Kani, *Curves of genus 2 covering elliptic curves and an arithmetical application*, Arithmetic algebraic geometry (Texel, 1989), Progr. Math., vol. 89, Birkhäuser Boston, Boston, MA, 1991, pp. 153–176. MR 1085258

[15] Édouard Goursat, *Sur la réduction des intégrales hyperelliptiques*, Bull. Soc. Math. France **13** (1885), 143–162. MR 1503964

[16] ———, *Sur un cas de réduction des intégrales hyperelliptiques du second genre*, C. R. Acad. Sci., Paris **100** (1885), 622–624.

[17] Charles Hermite, *Sur un exemple de réduction d'intégrales abéliennes aux fonctions elliptiques*, Ann. Soc. Sci. Bruxelles Sér. I **1** (1876), 1–16.

[18] Everett W. Howe, Franck Leprévost, and Bjorn Poonen, *Large torsion subgroups of split Jacobians of curves of genus two or three*, Forum Math. **12** (2000), no. 3, 315–364. MR 1748483

[19] Georges Humbert, *Sur les fonctiones abéliennes singulières. Premier mémoire*, J. Math. Pures Appl. (5) **5** (1899), 233–350.

[20] ———, *Sur les fonctiones abéliennes singulières. Deuxième mémoire*, J. Math. Pures Appl. (5) **6** (1900), 279–386.

[21] ———, *Sur les fonctiones abéliennes singulières. Troisième mémoire*, J. Math. Pures Appl. (5) **7** (1901), 97–123.

[22] Carl Gustav Jacob Jacobi, *Anzeige von Legendre* Traité des fonctions elliptiques, troisième supplément, J. Reine Angew. Math. **8** (1832), 413–417.

[23] ———, *Anzeige von Legendre* Traité des fonctions elliptiques, troisième supplément, Gesammelte Werke. Bände I, Verlag von G. Reimer, Berlin, 1881, pp. 373–382.

[24] Ernst Kani, *The number of curves of genus two with elliptic differentials*, J. Reine Angew. Math. **485** (1997), 93–121. MR 1442190

[25] ———, *Elliptic subcovers of a curve of genus 2. I. The isogeny defect*, Ann. Math. Qué. **43** (2019), no. 2, 281–303. MR 3996071

[26] ———, *The refined Humbert invariant for abelian product surfaces with complex multiplication*, preprint, 2025.
[27] Ernst Kani and Wolfgang Schanz, *Modular diagonal quotient surfaces*, Math. Z. **227** (1998), no. 2, 337–366. MR 1609061
[28] Nicholas M. Katz, *Serre-Tate local moduli*, Algebraic surfaces (Orsay, 1976–78), Lecture Notes in Math., vol. 868, Springer, Berlin, 1981, pp. 138–202. MR 638600
[29] Leo Königsberger, *Ueber die Transformation des zweiten Grades für die Abelschen Functionen erster Ordnung*, J. Reine Angew. Math. **67** (1867), 58–77. MR 1579358
[30] Sophie Kowalevski, *Über die Reduction einer bestimmten Klasse Abel'scher Integrale 3^{ten} Ranges auf elliptische Integrale*, Acta Math. **4** (1884), no. 1, 393–414. MR 1554643
[31] Robert M. Kuhn, *Curves of genus 2 with split Jacobian*, Trans. Amer. Math. Soc. **307** (1988), no. 1, 41–49. MR 936803
[32] Abhinav Kumar, *Hilbert modular surfaces for square discriminants and elliptic subfields of genus 2 function fields*, Res. Math. Sci. **2** (2015), Art. 24, 46. MR 3427148
[33] Adrien-Marie Legendre, *Essai sur la théorie des nombres*, Chez Duprat, Paris, 1798.
[34] ———, *Traité des fonctions elliptiques et des intégrales Eulériennes, avec des tables pour en faciliter le calcul numérique. Tome troisième*, Imprimerie de Huzard-Courcier, Paris, 1828.
[35] Kay Magaard, Tanush Shaska, and Helmut Völklein, *Genus 2 curves that admit a degree 5 map to an elliptic curve*, Forum Math. **21** (2009), no. 3, 547–566. MR 2526800
[36] Peter Norman, *Lifting abelian varieties*, Invent. Math. **64** (1981), no. 3, 431–443. MR 632983
[37] Emile Picard, *Sur la réduction du nombre des périodes des intégrales abéliennes et, en particulier, dans le cas des courbes du second genre*, Bull. Soc. Math. France **11** (1883), 25–53. MR 1503909
[38] ———, *Remarque sur la réduction des intégrales abéliennes aux intégrales elliptiques*, Bull. Soc. Math. France **12** (1884), 153–155. MR 1503942
[39] Henri Poincaré, *Sur la réduction des intégrales abéliennes*, Bull. Soc. Math. France **12** (1884), 124–143. MR 1503940
[40] Tanush Shaska, *Genus 2 fields with degree 3 elliptic subfields*, Forum Math. **16** (2004), no. 2, 263–280. MR 2039100
[41] Bartel Leendert van der Waerden, *Die Reduktionstheorie der positiven quadratischen Formen*, Acta Math. **96** (1956), 265–309. MR 82513

Independent mathematician, San Diego, CA 92104, USA
Email address: however@alumni.caltech.edu
URL: http://ewhowe.com