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

ABELIAN SURFACES OF SMALL CONDUCTOR FROM GENUS 3 DOUBLE COVERS

RAYMOND VAN BOMMEL, CÉLINE MAISTRET, JIA SHI,
AND ANDREW V. SUTHERLAND

Abstract. We describe the construction of a database of roughly half a million abelian surfaces over $\mathbb{Q}$ of small conductor arising as Pryms associated to a genus 3 double cover of a genus 1 curve. Our construction uses a method that provides a degree of control over the primes of bad reduction.

Contents

1. Introduction

Tables of elliptic curves of small conductor compiled by Cremona [17] and others are now a key component of the L-functions and modular forms database (LMFDB) [31]. These tables have a long history of service to the number theory community, and they have proven to be a rich source of problems and applications for computational number theorists. The fact that the conductors are small is crucial to the utility of this dataset in the LMFDB, as it makes it feasible to explicitly match them to modular forms (via the modularity theorem [12]) and compute their L-functions. In 2015 a database of 66 158 genus 2 curves $C/\mathbb{Q}$ with minimal discriminant $|\Delta_{\min}| \le 10^6$ was added to the LMFDB [6]. These small discriminant curves necessarily have (Jacobians with) small conductors, but most small conductor curves do not have small discriminants. This is due in large part to the presence

Date: May 2026.

of primes of *almost good reduction* (see Definition 2.5), which divide the discriminant but not the conductor; these primes can be much larger than the conductor itself, as can be seen in the examples of [35].

More recently a larger database of genus 2 curves $C/\mathbb{Q}$ of small conductor was compiled by Booker and the fourth author [5, 50], and is now available in the alpha release of the LMFDB [32]. This includes more than 6 million genus 2 curves of conductor $N \leq 10^6$, more than 90 times as many as are known with $|\Delta_{\min}| \leq 10^6$. But this new database of genus 2 curves necessarily omits many abelian surfaces of small conductor, because most abelian surfaces over $\mathbb{Q}$ do not arise as a Jacobian. Products of elliptic curves already account for more than 27 million distinct isogeny classes of abelian surfaces over $\mathbb{Q}$ of conductor less than 10^6, and Weil restrictions of elliptic curves defined over quadratic fields account for many more.

Extensive tables of elliptic curves over $\mathbb{Q}$ and quadratic fields can be found in the LMFDB. Provided one is willing to assume modularity (now known for $\mathbb{Q}$ and all real quadratic fields, as well as many imaginary quadratic fields), there are rigorous methods to enumerate all such elliptic curves up to a given conductor bound. But this is not the case for geometrically simple abelian surfaces, and after the recent heuristic compilation of genus-2 curves of small conductor, the next most interesting case to consider is geometrically simple abelian surfaces over $\mathbb{Q}$ that are not principally polarised (hence not Jacobians of curves), such as those that arise as Prym varieties associated to a genus 3 cover of an elliptic curve. The necessity of considering such examples was demonstrated by the abelian surface of conductor 550 discovered in the process of constructing a database of genus 3 nonhyperelliptic curves [48], which arises as the Prym variety associated to a smooth plane quartic curve that admits a degree-2 map to an elliptic curve. It corresponds to one of nine weight-2 paramodular forms of level $N \leq 1000$ in the heuristic tables of Poor and Yuen [38, 39, 40, 41] for which no corresponding Jacobian is known. Its existence was predicted by the paramodular conjecture of Brumer and Kramer [14, 15].

This motivates our current work: a heuristic algorithm to construct abelian surfaces of small conductor that arise as Prym varieties associated to double covers of an elliptic curve. A key feature of our approach, unlike the methods used to construct databases of genus 2 curves, is our ability to control, to a certain extent, the primes of bad reduction. This not only allows us to construct many new geometrically simple abelian surfaces of small conductor, it also allows us to construct many Jacobians of genus 2 curves of small conductor that were not previously known. This notably includes ten genus 2 curves whose Jacobians have good reduction away from 2, extending the list of 512 curves found by Robin Visser [51]; see Section 5.1 for a list of these curves.

We should emphasise that our algorithm is necessarily heuristic, and we can make no claims of completeness. For any fixed dimension g and set of primes S, the set of abelian varieties of dimension g over $\mathbb{Q}$ with good reduction away from S is known to be finite (this is Shafarevich's conjecture, proved by Faltings [19]), but for $g > 1$ no algorithm is known to enumerate this set. Indeed, this is a major open problem whose solution would yield an algorithm for determining the set of rational points on a curve of genus $g \geq 2$ over $\mathbb{Q}$, as shown in [1]. We have the more modest goal of constructing many (but not necessarily all) abelian surfaces over $\mathbb{Q}$ with good reduction away from a specified set of primes.

To construct such abelian surfaces as Prym varieties, we study degree-2 covers of genus 1 curves. Our approach is to start with an elliptic curve E over $\mathbb{Q}$ and prescribe the branch points of the putative cover.

To do so, we pick a rational effective divisor D on E of degree 4, such that all prime divisors in D occur with multiplicity 1. Assuming there exists a rational divisor D' such that $D \sim 2D'$ in the divisor class group of E, there exists a rational function f with $\operatorname{div}(f) = D - 2D'$. The cover $\phi\colon C \to E$ is obtained by adjoining the square root of f to the function field of E, and by Riemann-Hurwitz, C is a curve of genus 3. We denote the Prym variety associated to this cover ϕ by A.

Remark 1.1. Note that the divisor D does not determine the cover ϕ. There are two degrees of freedom. The divisor D' can be replaced by $D' + T$ for a 2-torsion element $T \in \operatorname{Pic}^0(E)$. If $T \neq 0$, this gives rise to a different curve C' that generally is not isomorphic to C, even over $\overline{\mathbb{Q}}$; see also Remark 4.1. It is also possible to replace the function f by $d \cdot f$ for some $d \in \mathbb{Q}^*$. This gives a quadratic twist of the original cover ϕ. We can check for quadratic twists of small conductor in a post-processing step.

Similar to the case of hyperelliptic curves, where the stable reduction (i.e., the special fibre of a stable model) is understood through the degeneration of the branch points of the map to $\mathbb{P}^1$ (see [25]), we study the stable reduction of the genus 3 cover through the degeneration of the branch points on the genus 1 curve. The method is more subtle in the case of the genus 3 cover, as the stable reduction of the cover is not entirely determined by the degeneration of the branch locus alone. For example, in the case in which all the branch points coincide (see Proposition 2.7 or the corresponding row in Table 1), it cannot be determined from the branch locus alone whether the stable reduction has one or two connected components above the genus 1 curve. Indeed, it does not suffice to determine the degeneration of the branch locus; the degeneration of the whole divisor $D - 2D'$ must be considered.

This is detailed in Section 2, where we carefully curated some basic cases for which the Prym variety has conductor exponent 0 or 1. The cases chosen have relatively simple degenerations of the branch points, meaning that they are not too unlikely to occur in a search, while also giving rise to a small conductor exponent in the Prym. The results for odd primes p are summarised in Table 1. In this table, N_E, N_C, and N_A are the conductor exponents of E, $\operatorname{Jac}(C)$, and A, respectively, $\mathcal{C}_p$ is the special fibre of a regular model of C, $\mathcal{E}_p$ is the special fibre of a regular model of E that separates the branch points of the cover, black points indicate branch points, thick lines indicate components of multiplicity 2, dotted lines indicate chains of $\mathbb{P}^1$s, and all components have geometric genus 0 and multiplicity 1 unless otherwise indicated. For the prime $p = 2$, we give a sufficient criterion for C and the Prym to have good reduction at 2, see Proposition 2.9. We note that these results are far from exhaustive. However, the same method can be used to study many other possible degenerations in the case that p is odd. As with hyperelliptic curves, the criterion for $p = 2$ is rather ad hoc and we do not expect it to generalise easily.

The rest of the paper is organised as follows. In Section 2 we cover the mathematical background and technical details of the double covers we construct. Section 3 addresses the problem of computing the conductor of the Pryms associated to these double covers, and describes an efficient heuristic algorithm for doing so. Section 4 discusses the computations we ran to construct many Pryms of small conductor,

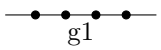
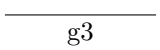
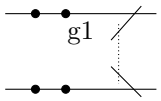
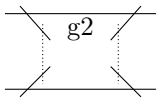
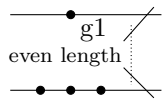
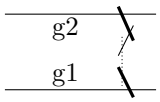
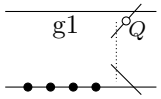
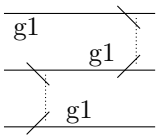
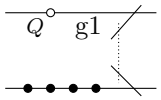
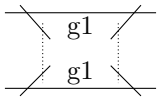
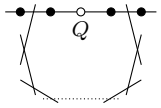
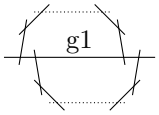
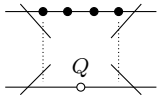
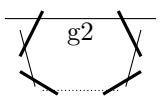
Prop.	$\mathcal{E}_p$	N_E	$\mathcal{C}_p$	stable reduction of C	N_C	N_A
2.3		0		good	0	0
2.4		0		genus 2 with 1 self-intersection	1	1
2.6		0		genus 2 and genus 1 intersecting in a node	0	0
2.7(i)		0		three genus 1s linked in a chain	0	0
2.7(ii)		0		two genus 1s intersecting twice	1	1
2.8(i)		1		genus 1 with 2 self-intersections	2	1
2.8(ii)		1		genus 2 with 1 self-intersection	1	0

TABLE 1. Results from Section 2 for odd primes.

and Section 5 summarises our computational results, which include the enumeration of more than 100 million genus 3 double covers, among which we found nearly half a million distinct isogeny classes of Prym varieties with conductors below 2^{20}, of which more than 80 000 were not previously known. This includes more than 8,000 that are isogenous to a genus 2 Jacobian that was not previously known.

1.1. **Acknowledgments.** We would like to warmly thank the referees for their careful reading of this manuscript and their helpful suggestions and comments. The first and second authors were supported by the second author's Royal Society Dorothy Hodgkin Fellowship. The third and fourth authors were supported by Simons Foundation award 550033. We would like to thank Tim Dokchitser and Gergely Jakovac for their help computing models of curves in the experiments that led to the results in this paper. We also thank Andrew Booker for providing the code we used to test the functional equation, and Nils Bruin for helpful comments.

2. PRYMS WITH PRESCRIBED LOCAL DATA

2.1. **Generalities.** Recall from the introduction that the genus 3 cover $\phi\colon C \to E$ was constructed by adjoining the square root of a function f whose divisor is $D - 2D'$. First we show that C has tame reduction at all primes $p > 3$.

Proposition 2.1. *Let $\phi\colon C \to E$ be a degree 2 map from a genus 3 curve C to a genus 1 curve E, all defined over $\mathbb{Q}$. Let $p > 3$ be a prime number. Then C has tame reduction at p.*

Proof. Because E is of genus 1, E attains stable reduction over a field extension $K/\mathbb{Q}$ that is at most tamely ramified at p since $p > 2 \cdot \text{genus}(E) + 2 = 4$. Let $B \subset E$ be the branch locus of the map ϕ, and let $K(B)$ be the Galois extension of K generated by the coordinates of the points in B. The Galois group $\text{Gal}(K(B)/K)$ acts as a subgroup of $S_{|B|} = S_4$, and therefore $K(B)/K$ is at most tamely ramified at all primes above p. By [30, Thm. 2.3], the curve C has stable reduction over an extension field $L/K(B)$ of degree at most 2. This extension is also at most tamely ramified at all primes above p, and hence p is a prime of tame reduction for C. □

Remark 2.2. The conductor of the Prym variety is the quotient of the conductor of the Jacobian of the genus 3 curve by the conductor of E. Therefore, by Proposition 2.1, to understand the conductor of the Prym variety at primes $p > 3$, it suffices to understand the tame conductor exponent of C and the conductor exponent of E at these primes.

2.2. **Local data at odd primes.** Let C, E, ϕ, f, D, and D' be as before. In order to understand the geometric properties of C at a prime $p > 2$, we look at how the divisor $D - 2D'$ degenerates modulo powers of p. For the purpose of this work, we will assume that E has stable reduction at p, even though it would be possible to also study the case in which E does not have stable reduction using this method. As discussed in the introduction, the approach is very similar to that of hyperelliptic curves. In the hyperelliptic case, D consists of the Weierstraß points on $\mathbb{P}^1$, and D' is $(g+1)\cdot\infty$, and it only matters how D degenerates. In our case it also matters how D' degenerates. The following is an adaptation of a method for hyperelliptic curves that is explicitly described in [25, Sect. 4], and can be found in more generality in [30, Lemma 1.9].

We construct a tree-like regular model $\mathcal{E}/\mathbb{Z}_p^{\text{unr}}$ that separates all the points in D and D' by repeatedly blowing up, starting from a semi-stable regular model of E over $\mathbb{Z}_p^{\text{unr}}$. The function f gives rise to a rational function $\tilde{f} \in K(\mathcal{E})$, because E and $\mathcal{E}$ have the same function field.

Similar to [25, Sect. 4], we define a divisor D_{odd} (called C in loc. cit.) which captures the odd part of $\text{div}(\tilde{f})$, and a divisor B such that $2B = D_{\text{odd}} - \text{div}(\tilde{f})$. Then we construct a cover $\mathcal{C}$ of $\mathcal{E}$ by taking $\text{Spec}(\mathcal{O}_{\mathcal{E}} \oplus \mathcal{L}^{-1})$, where the bundle $\mathcal{L}$ is defined as $\mathcal{O}_{\mathcal{E}}(B)$. The model $\mathcal{C}/\mathbb{Z}_p^{\text{unr}}$ of C is then a regular model, see [25, Prop. 4.3].

Note that $\text{div}(\tilde{f})$ can also contain vertical divisors of $\mathcal{E}$. The divisor $\text{div}(\tilde{f})$ must have the property that the intersection product satisfies $\text{div}(\tilde{f}) \cdot V = 0$ for any vertical divisor V of $\mathcal{E}$. This uniquely determines the vertical part of $\text{div}(\tilde{f})$ up to multiples of the whole special fibre $\mathcal{E}_p$ of $\mathcal{E}$, see [27, Thm. III.3.6]. In [25, Sect. 4], this is made explicit in terms of the number of points in D and D' whose reduction lies in a certain vertical component or in a lower component in the tree. If $\tilde{f}$ has odd order at a vertical component of $\mathcal{E}$, then the unique component above it will have multiplicity 2, and if $\tilde{f}$ has even order then the components above it will have multiplicity 1. Therefore, if there are no vertical components in D_{odd}, then the

model $\mathcal{C}$ is semi-stable. If not, then $\mathcal{C}$ will become semi-stable after a ramified extension of degree 2, see for example [30, Thm. 2.3].

The following propositions list some configurations for which the conductor exponent of C (and hence A) is small. A pictorial summary of these can be found in Table 1.

Proposition 2.3. *Suppose that E has good reduction at p. If the four points in D reduce to distinct points in $E \bmod p$, then, after a quadratic twist by p if necessary, C has good reduction at p.*

Proof. In this case, no blow-ups are necessary and $\mathcal{E}$ can be taken to be a smooth model of E. If $\widetilde{f}$ happens to have odd order at the vertical divisor, then we do a quadratic twist. That is, we replace f by $p \cdot f$, and the resulting function has even order at the vertical divisor. Now the constructed cover $\mathcal{C}$ is regular and semi-stable. The special fibre $\mathcal{C}_p$ is a degree-2 cover, branched at a degree 4 divisor on $\mathcal{E}_p$, i.e., $\mathcal{C}_p$ is a smooth curve of genus 3. □

Proposition 2.4. *Suppose that E has good reduction at p. If exactly two points in D reduce to the same point in $E \bmod p$, then, after a quadratic twist by p if necessary, C has stable reduction at p, with special fibre being a genus 2 curve with a self-intersection.*

Proof. Let us first assume the points occurring in D are defined over $\mathbb{Q}_p^{\mathrm{unr}}$. Then $\mathcal{E}$ is obtained by blowing up a smooth model several times, and its special fibre is a genus 1 curve with two branch points, and attached to that genus 1 curve, there is a chain of $\mathbb{P}^1$s with the two other branch points at the end (as in Table 1). Since there is an even number of branch points on each vertical component, $\tilde{f}$ either has even order at all vertical components or odd order at all vertical components. We multiply f again by the appropriate power of p to make sure it has even order at all vertical components. Using Riemann-Hurwitz, we see that the special fibre $\mathcal{C}_p$ consists of a genus 2 component lying above the genus 1 curve in $\mathcal{E}_p$, and a loop of $\mathbb{P}^1$s attached to the genus 2 component.

Suppose the points in D reducing to the same point in $E \bmod p$ are defined over a ramified degree 2 extension of $\mathbb{Q}_p^{\mathrm{unr}}$. Then, after extending the base field to this degree-2 extension, $\tilde{f}$ has even order at all vertical components, and we get a stable model as in the previous case over this degree-2 extension. If inertia mirrors the chain of $\mathbb{P}^1$s and hence acts non-trivially on the genus 2 component, we can multiply $\tilde{f}$ by p to make inertia act trivially on the genus 2 component. Therefore, after twisting if necessary, C has the stable reduction at p as claimed. □

The following proposition is the first case in which we get a prime of almost good reduction. Let us first recall the definition of almost good reduction.

Definition 2.5. The curve C is said to have *almost good reduction* if C has bad reduction at p and the Jacobian of C has good reduction at p.

This happens when the curve has stable reduction and the special fibre of the stable model has no loops. In this case, the reduction of the Jacobian is isogenous to the product of the Jacobians of the irreducible components of this special fibre. As a consequence, C has conductor exponent 0 at p, even though C has bad reduction at p.

Proposition 2.6. *Suppose that E has good reduction at p and that all points in D are defined over $\mathbb{Q}_p^{\mathrm{unr}}$. Let n be a positive integer and assume that three of the points in D reduce to the same point in $E \bmod p^{2n}$, but no two of them reduce to the same point in $E \bmod p^{2n+1}$. Suppose furthermore that the fourth point reduces to a different point in $E \bmod p$. Then, after a quadratic twist by p if necessary, C has almost good reduction at p, with special fibre consisting of a genus 2 curve intersecting a genus 1 curve.*

Proof. After twisting if necessary, the special fibre of $\mathcal{C}$ becomes a genus 2 curve connected with a genus 1 curve through a chain of $\mathbb{P}^1$s which alternately have multiplicity 2 and 1. The $\mathbb{P}^1$s with multiplicity 2 in the special fibre can be contracted by Castelnuovo's criterion, obtaining a regular semi-stable model, which gives the desired reduction.

Note that in the twisting that we just did, we used that $2n$ is even. Indeed, if the three points reduce to the same point modulo an odd power of p, then the chain of $\mathbb{P}^1$s has even length. This means that the cover is ramified at either the vertical genus 1 component or the final vertical genus 0 component with the three branch points. In this case, twisting will not make the cover unramified, as it will only swap the components at which the cover is ramified with the ones at which it is unramified. □

Proposition 2.7. *Suppose that E has good reduction at p, $D = P_1 + P_2 + P_3 + P_4$ and $D' = P_4 + Q$, where $P_1, \dots, P_4, Q$ are defined over $\mathbb{Q}_p^{\mathrm{unr}}$. Moreover, assume that P_1, P_2, P_3, P_4 reduce to the same point on E modulo p^n, for some positive integer n, such that no two reduce to the same point modulo p^{n+1}.*

(i) *If Q also reduces to that point modulo p, then, after a quadratic twist if necessary, C has almost good reduction, with special fibre consisting of three genus 1 curves in a chain.*
(ii) *If Q reduces to a different point modulo p, then, after a quadratic twist if necessary, C has stable reduction, with special fibre consisting of two genus 1 curves intersecting twice.*

Proof. In both cases, after a quadratic twist if necessary, the cover $\mathcal{C} \to \mathcal{E}$ does not have any vertical components in its branch divisor. It remains to understand the cover above the vertical genus 1 component. Since the cover has no ramification points on that component, there are two possibilities: a genus 1 curve mapping to the genus 1 curve through a 2-isogeny, or two disjoint copies of the genus 1 curve. To distinguish these two cases we consider the restriction of the divisor $\mathrm{div}(\tilde{f})$ to the vertical genus 1 component.

If Q reduces to the same point as P_1, P_2, P_3, P_4, then the restriction of $\mathrm{div}(\tilde{f})$ to the vertical genus 1 component is 0, and the cover is locally given by adjoining the square root of a constant function, i.e., the cover consists of two disjoint genus 1 curves.

If Q reduces to a different point, then the restriction of $\mathrm{div}(\tilde{f})$ to the vertical genus 1 component is $2\overline{Q} - 2\overline{P_1}$, where $\overline{P_1}$ is the intersection point with the chain of $\mathbb{P}^1$s leading to the branch points. In this case $\tilde{f}$ does not restrict to a constant function on the vertical genus 1 component, and the cover is a 2-isogeny.

In both cases, the chain of $\mathbb{P}^1$s can be contracted to obtain the desired stable reduction. □

Proposition 2.8. *Suppose that E has multiplicative reduction at p. Let $\mathcal{E}$ be its minimal regular (semi-stable) model. Suppose that $D = P_1 + P_2 + P_3 + P_4$ and $D' = P_4 + Q$, with $P_1, \dots, P_4, Q$ defined over $\mathbb{Q}_p^{\mathrm{unr}}$. Moreover, assume that P_1, P_2, P_3, P_4 reduce to distinct smooth points on the same irreducible component of $\mathcal{E}_p$.*

(i) *If Q reduces to a smooth point on the same irreducible component of $\mathcal{E}_p$, then, after a quadratic twist if necessary, C has stable reduction, with special fibre consisting of a genus 1 curve with two self-intersections.*

(ii) *If not, then, after a quadratic twist if necessary, C has stable reduction, with special fibre consisting of a genus 2 curve with a self-intersection.*

Proof. The special fibre of $\mathcal{E}$ is an n-gon for some positive integer n, with components $C_1, \dots, C_n$ in that order. Without loss of generality, we assume that the reductions of $P_1, \dots, P_4$ lie on C_n. Note that the reduction of Q is a smooth point, because Q is defined over $\mathbb{Q}_p^{\mathrm{unr}}$. Because $D - 2D' = 0$ on E, this implies that Q can only be on the same component as $P_1, \dots, P_4$, or on the exact opposite component $C_{n/2}$ in case n is even. In particular, if n is odd, we are always in case (i).

In case (i), we have that the vertical part of $\mathrm{div}(\tilde{f})$ is $0 + m \cdot \sum_{i=1}^{n} C_i$ for some $m \in \mathbb{Z}$. Multiplying f by p^{-m}, twisting the cover if necessary, we may assume that $\mathrm{div}(\tilde{f})$ has no vertical part. Then the cover is ramified above C_n with four ramification points, and unramified above all other components C_i. Hence, $\mathcal{C}_p$ consists of a genus 1 curve with 2 loops of $\mathbb{P}^1$s, and there is stable reduction as claimed.

In case (ii), we have that the vertical part of $\mathrm{div}(\tilde{f})$ is

$$C_1 + 2C_2 + 3C_3 + \ldots + \tfrac{n}{2} C_{\frac{n}{2}} + (\tfrac{n}{2} - 1) C_{\frac{n}{2}+1} + \ldots + 2C_{n-2} + C_{n-1} + m \cdot \sum_{i=1}^{n} C_i,$$

for some $m \in \mathbb{Z}$, which we again can assume to be 0, twisting the cover if necessary. Now the cover above the components is:

- ramified at six points on C_n (the points P_1, P_2, P_3, P_4 and the intersection points with the adjacent components), giving rise to a genus 2 curve in $\mathcal{C}_p$;
- fully ramified above the odd-numbered components C_{2k+1}, giving rise to a genus 0 component with multiplicity 2 on $\mathcal{C}_p$ above each such component;
- ramified at two points on the other even-numbered components C_{2k}, giving rise to a genus 0 component with multiplicity 1 on $\mathcal{C}_p$ above each such component.

Just as in the proof of Proposition 2.6, the components of multiplicity 2 can be contracted due to Castelnuovo's criterion. Hence, we get a genus 2 curve with a loop of $\mathbb{P}^1$s, and there is stable reduction as claimed. □

2.3. **Local data at the even prime.** Since the cover is of degree 2, the prime $p = 2$ behaves differently. Recall that an elliptic curve given by $y^2 = x^3 - n$ has good reduction if and only if $v_2(n) \equiv 4 \bmod 6$ and $\frac{n}{2^{v_2(n)}} \equiv 3 \bmod 4$, see for example [2, Table 1]. Indeed, in this case, changing coordinates if necessary, we may assume that $v_2(n) = -2$ and $n \equiv \frac{3}{4} \bmod 1$. Replacing y by $y + \frac{1}{2}$ then yields an integral Weierstraß model with good reduction at 2. The next proposition is inspired by the fact that the four ramification points in this example have 2-adic distance $2^{-\frac{2}{3}}$.

Proposition 2.9. *Suppose that E has good reduction at 2. Let $\mathcal{E}$ be a good Weierstraß model of E over $\mathbb{Z}_2$ with projective coordinates x, y, z. Suppose $D = P_1 + P_2 + P_3 + P_4$ with P_1, P_2, P_3 defined over $\overline{\mathbb{Q}_2}$, and fix $P_4 = 0_E$ and $D' = 2 \cdot 0_E$. Let v_2*

be the valuation on $\overline{\mathbb{Q}_2}$ *normalised so that* $v_2(2) = 1$. *Assume that* $P_i = (x_i : 1 : z_i)$ *with* $v_2(x_i), v_2(z_i) > 0$, *for all* $i = 1, 2, 3$, *and that the* 2*-adic distances between the points are* $2^{-\frac{2}{3}}$, *i.e.* $\min(v_2(x_i - x_j), v_2(z_i - z_j)) = \frac{2}{3}$ *for all* $i \neq j$. *Then, after twisting if necessary, the curve* C *has good reduction at* 2.

Proof. The 2-adic distance between P_i and P_4 is $2^{-\frac{2}{3}}$. By definition, this means that $\min(v_2(x_i), v_2(z_i)) = \frac{2}{3}$. Let

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

be the integral Weierstraß model $\mathcal{E}$. We consider the 2-adic valuations of the separate terms for the points P_1, P_2, P_3. By the non-archimedean property, we find that $v_2(z_i) = v_2(x_i^3)$. In particular, $v_2(z_i) = 2$ and $v_2(x_i) = \frac{2}{3}$.

The function f whose square root we adjoin to get the genus 3 curve lies in the Riemann-Roch space $\mathcal{L}(3 \cdot 0_E) = \langle 1, \frac{x}{z}, \frac{y}{z} \rangle$. We normalise f so that the coefficient of $\frac{y}{z}$ is 1, i.e. $f = \frac{y}{z} + c_1\frac{x}{z} + c_2$. Note that f has zeros at P_1, P_2, P_3. As $v_2(1) = 0$, $v_2(\frac{x_i}{z_i}) = -\frac{4}{3}$, and $v_2(\frac{y_i}{z_i}) = -2$, the term $c_1\frac{x_i}{z_i}$ is the only term whose valuation is not an integer. We therefore must have $-2 = v_2(\frac{y_i}{z_i}) = v_2(c_2)$, and also $v_2(c_1\frac{x_i}{z_i}) > -2$, that is, $v_2(c_1) \geq 0$. In particular, $c_2 \in \frac{1}{4} + \mathbb{Z}$ or $c_2 \in \frac{3}{4} + \mathbb{Z}$. In the latter case, we multiply f by -1 to obtain $c_2 \in \frac{1}{4} + \mathbb{Z}$.

Now the genus 3 curve C obtained by adjoining a square root of f, after twisting if necessary, can be put into a long form $w^2 + w + \frac{1}{4} = f$, and by subtracting $\frac{1}{4}$ on both sides we obtain a model with good reduction at 2. □

2.4. **Conductor exponent of the Prym.** By Remark 2.2, the different situations that we studied above have immediate consequences for the conductor of the Prym variety associated to the cover $C \to E$.

Corollary 2.10. *The conductor exponents presented in Table 1 are correct.*

Proof. The conductor exponent N_C of C at p is defined by the action of inertia on the Tate module, see for example [13]. In all cases considered in Table 1, the stable reduction was obtained after at most a ramified extension of degree 2. Therefore, N_C has no wild part, and we only need to determine its tame part. Since C has stable reduction in all cases, this translates into computing the dimension of the homology of the dual graph of $\mathcal{C}_p$, i.e. the number of loops in $\mathcal{C}_p$. □

In the case of Proposition 2.9, where $p = 2$, the curve C has good reduction at p and hence the conductor exponents of C and A are 0.

3. Computing the conductor of the Prym

The methods of the previous section allow us to control the primes of bad reduction for the Pryms we construct and give us some information about the conductor exponents at these primes, but not enough to determine the conductor of the Prym variety A associated to a genus 3 double cover $\phi\colon C \to E$ of an elliptic curve E. While in principle one can compute the conductor of A as the quotient of the conductors of $\mathrm{Jac}(C)$ and E, this approach is impractical, as there are no efficient methods available for computing the conductor of the Jacobian of a general genus 3 curve over $\mathbb{Q}$. Partial results are known in some special cases, such as when C is a Picard curve [7, 9], a Ciani quartic [8], or a hyperelliptic curve [34], but even in these special cases the available methods are not fast enough for our purposes.

We instead adopt the heuristic approach used for existing databases of genus 2 and genus 3 curves over $\mathbb{Q}$ of small conductor [6, 48], including the database of genus 2 curves found in the LMFDB. We now assume that the L-function $L(A,s) = \sum_{n\geq 1} a_n n^{-s}$ of our abelian surface $A/\mathbb{Q}$ satisfies the expected functional equation

$$\Lambda(A,s) = \varepsilon N^{1-s}\Lambda(A,2-s), \tag{1}$$

where $\varepsilon = \pm 1$ is the root number and $\Lambda(A,s) = \Gamma_{\mathbb{C}}(s)^2 L(A,s)$ is the completed L-function of A (here $\Gamma_{\mathbb{C}}(s) \coloneqq 2(2\pi)^{-s}\Gamma(s)$ with $\Gamma(s) \coloneqq \int_0^\infty t^{s-1}e^{-t}dt$). As explained in [6, §5.2], given a purported conductor N, root number ε, and Dirichlet coefficients a_n for $n \leq B = b\sqrt{N}$, where $b \geq 5$ is a fixed constant, there is an explicit numerical test that must be satisfied if (1) holds and these purported values are all correct, and is unlikely to be satisfied whenever this is not the case.

Increasing b strengthens this test, but also requires us to compute more Dirichlet coefficients; we used $b = 12$ for our computations. For the sake of efficiency we first perform computations at standard double precision (53 bits) and accept the possibility of rounding errors that may arise from the use of floating-point arithmetic. After the fact, we can use interval arithmetic as implemented in [24] to rigorously verify our computations, subject to our assumption that (1) holds. This assumption is implied by the conjectured modularity of A, but this conjecture remains open, so even with interval arithmetic, all our conductor computations are conditional.

For any fixed N there are only finitely many possibilities for ε and the a_n for $n \leq B$. If our numerical test of (1) fails for all possibilities, then we know that N is not the conductor of A (under our assumption). For any particular genus 3 double cover $C \to E$, the prime divisors of N must divide the discriminant of C, and the results of Brumer and Kramer in [13] imply that the conductor exponent $v_p(N)$ is bounded by $20, 10, 9, 4$ for $p = 2$, $p = 3$, $p = 5$, $p \geq 7$, respectively. There are thus only finitely many possibilities for N that can arise in any given A, and we can efficiently enumerate them. Ruling out all but one possibility suffices to determine the conductor N, subject to our assumption that (1) holds. Ruling out all $N \leq N_{\max}$, where $N_{\max}$ determines the conductors we consider "small", suffices to prove that $N > N_{\max}$, under the same assumption. This is often much easier than determining the exact value of N.

Let us now sketch the algorithm. We are given a genus 3 double cover $C \to E$, an upper bound $N_{\max}$ on the conductor N of the associated Prym A, an upper bound $r_{\max}$ on $\operatorname{rad}(N)$ (the product of the prime divisors of N), and an upper bound $L_{\max}$ on the number of tests of the functional equation (1) we are willing to apply. Our goal is to compute N or conclude that one of these bounds has been violated (the algorithm returns `failure` in the latter case).

1. Compute the discriminant Δ of C and factor it using trial division over primes $p \leq \sqrt{N_{\max}}$. If this does not factor Δ up to a prime-power cofactor, return `failure`.
2. For each prime $p|\Delta$ compute lower and upper bounds on $v_p(N)$, taking into account $v_p(\Delta)$ and any applicable bounds from Table 1.
3. Compute the set S of integers $N \leq N_{\max}$ with prime factors $p|\Delta$ satisfying the $v_p(N)$ bounds from Step 2 with $\operatorname{rad}(N) \leq r_{\max}$.
4. For each $N \in S$, compute the number L_N of combinations of ε and pairs (a_p, a_{p^2}) over $p|N$ that are compatible with $v_p(N)$, using the Weil bounds

and constraints on degrees of bad Euler factors.[1] Sort S by L_N and truncate if needed to make $\sum_{N\in S} L_N \le L_{\max}$. Return `failure` if $S = \emptyset$.

5. Compute $a_p(A) = a_p(C) - a_p(E)$ for $p \nmid \Delta$ with $p \le B := b\sqrt{N_{\max}}$.
   Compute $a_{p^2}(A) = a_{p^2}(C) - a_p(C)a_p(E) + p$ for $p \nmid \Delta$ with $p \le \sqrt{B}$.
6. For each candidate conductor N in the ordered set S, test (1) using each of the possibilities for $\varepsilon = \pm 1$ and the pairs (a_p, a_{p^2}) over $p|N$ determined in Step 4. If the test passes for more than one choice, return `error`; if the test passes for exactly one choice, return N and the values of ε and the (a_p, a_{p^2}) pairs that worked; otherwise, proceed to the next $N \in S$.
7. Return `failure`.

In our computations we used $r_{\max} := 2^{10}$ and $N_{\max} := 2^{20}$, yielding $B \approx 12288$, and found that $b = 12$ was sufficient to ensure the algorithm never returned `error`.

For the computation in Step 5, for primes $p \le \sqrt{B} \approx 111$ we used naïve point-counting to compute $\#E(\mathbb{F}_p)$, $\#C(\mathbb{F}_p)$, and $\#C(\mathbb{F}_{p^2})$, from which we can derive $a_p(A)$ and $a_{p^2}(A)$. For the remaining $p \le B \approx 12288$ we compute $a_p(A) = a_p(C) - a_p(E)$ by applying average polynomial-time algorithms to compute $a_p(C) \bmod p$ for $p \le B$ in $O(B \log^3 B)$ time (we used `smalljac` [26] to compute $a_p(E)$). When C is a hyperelliptic curve $y^2 = f(x)$, we use the algorithm described in [21, 49], and when C is a smooth plane quartic $f(x, y, z) = 0$, we use the algorithm described in [16]. In the latter case we may exploit the fact that C is a double cover of a genus 1 curve via [16, Remark 5.26]. Note that for $p > 64$ the Weil bounds imply $|a_p(A)| \le 4\sqrt{p} \le p/2$, so $a_p(A)$ is uniquely determined by $a_p(A) \bmod p$.

Remark 3.1. The asymptotic complexity of our implementation of Step 5 is $\tilde{O}(B^{3/2})$. This is suboptimal, but for $\sqrt{B} \approx 111$ it is the most efficient approach in practice. There is an asymptotically more efficient approach that uses a combination of the L-polynomial lifting algorithms described in [44, 45] to lift the L-polynomial of A from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}$ in $O((\log p)^{2+o(1)})$ expected time, which yields an $\tilde{O}(B)$ Las Vegas algorithm to compute the L-polynomials $L_p(T)$ of A for primes $p \le B$ of good reduction for C that is much more efficient in practice than using Harvey's general-purpose average polynomial-time algorithm for arithmetic schemes [20]. While we did not use this algorithm to compute conductors, we did use it to identify Prym varieties A with $\mathrm{End}(A_{\overline{\mathbb{Q}}}) = \mathbb{Z}$ via Zywina's algorithm [52], which requires full L-polynomials for more values of p than we needed to compute conductors.

Remark 3.2. Genus 3 curves $C/\mathbb{Q}$ that are not smooth plane quartics are always hyperelliptic over $\overline{\mathbb{Q}}$ but need not admit a hyperelliptic model $y^2 = f(x)$ over $\mathbb{Q}$. There is an average polynomial-time algorithm that can be applied to such curves [22], but as explained in Remark 5.1, we can always realise a quadratic twist of our Prym using a hyperelliptic model, so we did not use this algorithm.

By caching precomputed quadratic residues and roots of cubic polynomials over $\mathbb{F}_{p^2}$ for $p \le \sqrt{B}$ we are able to ensure that the naïve point-counting performed in Step 5 takes negligible time (a few milliseconds), and the speed of the average polynomial-time algorithms in [16, 21, 49] ensured that the total time for Step 5 was typically under 2 seconds. In most cases the computation of the conductor was dominated by Step 6, since the number of combinations L_N of ε and pairs (a_p, a_{p^2})

[1] For example, [43, Corollary II.2] implies that for $p > 5$ we have $\deg L_p(T) = 4 - v_p(N)$.

for $p|N$ may be quite large. Keeping $r_{\max}$ small helps to control this, but to ensure that the computations remain manageable we set $L_{\max} := 2^{28}$, which forces the algorithm to terminate Step 6 if the number of tests exceeds $L_{\max}$.

With this constraint in place the average running time of the algorithm was around 15 seconds on the 2.45 GHz AMD Milan CPUs that we used. In roughly 5/6 of the cases the $L_{\max}$ constraint prevented the algorithm from considering all possible $N \le N_{\max}$ with $\mathrm{rad}(N) \le r_{\max}$, so it is very likely that we missed many Pryms whose conductors satisfy our search parameters. But adding the $L_{\max}$ constraint reduces the average running time of the algorithm by more than a factor of 10, allowing us to process many more Pryms.

4. Constructing a database of Pryms of small conductor

To construct genus 3 covers $\phi\colon C \to E$ that will produce a Prym variety A of small conductor, we control the primes of bad reduction for both E and C via our selection of E, the ramification points of ϕ, and the number field K (of degree at most 4) over which these ramification points are defined. We start by placing constraints on the bad primes we will allow. In order to make the conductor computations manageable, we want the primes dividing the conductor to be fairly small (the larger the prime, the greater the number of possible Euler factors), and we also want the number of bad primes to be small. We also want to constrain the archimedean valuation of the conductor, but this is actually less critical than controlling the number of possible bad Euler factors, which can lead to a combinatorial explosion in our heuristic algorithm for computing the conductor, as explained in the previous section.

For our database, which we do not claim to be complete in any way, we decided to impose a bound of $r_{\max} := 2^{10}$ on the conductor radical $\mathrm{rad}(N)$ (the product of its prime divisors), which ensures that both the size and number of primes dividing the conductor are small. Subject to this constraint, our goal is to search for Prym varieties with conductors $N \le N_{\max} := 2^{20}$, a bound we chose because it suffices to cover all abelian surfaces with good reduction away from 2 (this choice turned out to be fortuitous, as explained in Section 5.1), but the bound on N plays no role in the initial stage.

We begin by assembling a list of elliptic curves $E/\mathbb{Q}$ whose conductors have radical bounded by 2^{10} (this isn't strictly necessary, as primes dividing the conductor of E need not divide the conductor of A, but they usually will). Fortunately the LMFDB contains a large (but far from complete) set of such elliptic curves, including all $E/\mathbb{Q}$ with good reduction away from $2, 3, 5, 7$ and all $E/\mathbb{Q}$ with conductor less than 500 000. For the number field K, we consider all number fields of degree up to 4 with $|\Delta_K| \le 2^{20}$, all of which are included in the LMFDB.

We then iterate over pairs (E, K) and for each pair we compute the Mordell-Weil group of $E(K)$, which we require to be strictly larger than $E(\mathbb{Q})$ whenever $K \ne \mathbb{Q}$ (otherwise there is no point in considering K). For each pair we provisionally compute a set of generators for the Mordell-Weil groups $E(\mathbb{Q})$ and $E(K)$ and then iterate over integer linear combinations of these generators to construct ramification points; this set of generators might not be complete because we impose a height bound to keep the computation feasible (indeed, no rigorous algorithm is known to compute $E(\mathbb{Q})$, or even its rank). We want to keep the (naïve) heights of the points we choose small, so we restrict the absolute values of the integer coefficients

we use in our integer linear combinations to at most 5 and reduce this bound as needed to keep the total number of integer linear combinations reasonably small (we imposed a bound of $3^9 = 19683$ on the total number of choices of ramification points to consider for each pair).

We then apply the following constraints.

- The ramification points P_1, P_2, P_3, P_4 must be distinct, and their sum must be divisible by 2; in other words, $P_1+P_2+P_3+P_4 = 2Q$ for some $Q \in E(K)$. We now take $D' = [0_E] + [Q]$.
- The product of the primes p that divide N_E or Δ_K, or the norm of a prime of K modulo which P_1, P_2, P_3, P_4 are not distinct must be at most 2^{10}, as these primes will likely become primes of bad reduction for C.
- The defining polynomial of the quadratic extension of the function field of E obtained by adjoining the square root of the selected function f with $\mathrm{div}(f) = [P_1] + [P_2] + [P_3] + [P_4] - 2[Q] - 2[0_E]$ must not be too large (we restricted its print length to 2000 characters).
- The (not necessarily minimal) discriminant $\Delta(C)$ of the genus 3 cover $C/\mathbb{Q}$ can have at most one prime factor greater than 2^{10}, with $|\Delta| \leq 10^{5000}$.
- The minimal discriminant $\Delta_{\min}(C)$ can contain at most 7 prime divisors, and the product of the primes p with $v_p(\Delta) \in [1, 11]$ cannot exceed 2^{10}.

Note that we allow $\Delta_{\min}(C)$ to have radical greater than 2^{10} provided that the extra primes occur with exponent at least 12. The motivation for this is that the C we construct will often have one or more primes of almost good reduction (see Definition 2.5) that are bad for C but good for $\mathrm{Jac}(C)$; such primes will not divide the conductor of A. One does not encounter primes of almost good reduction in the current database of genus 2 curves in the LMFDB, but that is only because the current database was constructed using a bound of 2^{20} on the minimal discriminant. This makes it nearly impossible for almost good primes to appear, since such primes must have discriminant exponent at least 12. But in the new database of more than 6 million genus 2 curves of small conductor (but not necessarily small discriminant) that is now available in the alpha version of the LMFDB [32], primes of almost good reduction are quite common and appear in almost half the curves.

Remark 4.1. In addition to enumerating ramification points, we also iterate over non-trivial points in $E(\mathbb{Q})[2]$, which we may add to the point Q that is used to construct the genus 3 cover. If T is a 2-torsion point, then $Q + T$ also satisfies all the requirements listed above, but it may produce a different cover and a non-isogenous Prym; see also Remark 1.1.

The first phase of the computation iterates over pairs (E, K) and integer linear combinations of K-rational points to find genus 3 covers $C \to E$ that satisfy the constraints above, and computes an isogeny invariant of each Prym using the *trace hash* defined in [6, §5.2]. This is a linear combination of $a_p(A)$ values for $p \in [2^{12}, 2^{13}]$ computed in the finite field with $2^{61} - 1$ elements using coefficients derived from the digits of π. This range of p conveniently avoids the primes of bad reduction, and because the trace hash is a linear function, we can compute the trace hash for A as the difference of the trace hashes for C and E. This typically takes less than a second to compute using average polynomial-time algorithms. The trace hash is necessarily an isogeny invariant, and as long as the database is not too large and not

too many of the $a_p(A)$ are zero, one expects the trace hash to uniquely distinguish the Prym's isogeny class from other isogeny classes in the dataset.

Of course one always needs to consider the birthday paradox, and some hash collisions may have occurred, but Pryms with distinct trace hashes cannot be isogenous, and this is useful to know. In our computations we also introduced a *twist hash*, which is computed in the same way as the trace hash, but using $|a_p(A)|$ rather than $a_p(A)$, making it invariant under quadratic twisting as well as isogeny. This twist hash gives an efficient way to certify that two abelian surfaces are not isogenous to any quadratic twists of each other.

In the second phase of the computation we attempt to compute the conductors of all the Pryms $C \to E$ that have been enumerated. There is a tradeoff between spending effort on computing conductors versus enumerating more Pryms whose conductors might be easier to compute, so we set an upper bound on the total number of conductor and Euler factor combinations we are willing to consider for a single Prym. Setting this bound to $L_{\max} := 2^{28}$ meant that on average we spent about 15 seconds attempting to compute the conductor of each Prym. As can be seen in the next section, we successfully computed a heuristic conductor less than 2^{20} in only about 1 in 200 cases, but in nearly 1 in 6 cases we were able to prove that the conductor is greater than 2^{20} using fewer than $L_{\max} := 2^{28}$ combinations (and around 15 seconds of wall time, on average).

We should emphasise that our conductor computations are heuristic for two distinct reasons: (a) they depend on the unproven assumption that $L(A, s)$ has an analytic continuation that satisfies the functional equation (1) and (b) in our computations we only consider conductors that satisfy the bounds imposed by $N \le N_{\max}$ and $\mathrm{rad}(N) \le r_{\max}$, we terminate our computation as soon as we find a conductor and a choice of root number and bad Euler factors that works, and we use floating-point calculations rather than interval arithmetic. As noted in Section 3, one can remove heuristic (b) by running a more extensive computation that considers every conductor N supported on primes dividing the minimal discriminant of C, uses interval arithmetic to make the numerical tests of (1) fully rigorous, and verifies that there is only one value of N for which the numerical test succeeds. We have not yet attempted this computation, but we plan to do so in the future.

Notwithstanding these provisions, as can be seen in the next section, for about 80 percent of the nearly half a million Pryms for which we provisionally computed the conductor there was a previously known genus 2 curve with a matching trace hash and the same conductor. The conductors of these genus 2 curves have all been rigorously computed under assumption (a), and for about 10 percent of them (those for which the modularity criteria of [11] apply), (a) is actually known to hold. This gives us confidence that our heuristic conductor computations are correct.

5. Computational Results

We undertook the enumeration described in the preceding section in a large parallel computation run on Google's cloud platform, using roughly 250 000 cores, most of which were 2.45 GHz AMD Milan CPUs (Zen 3 architecture). The total CPU time spent was on the order of 100 CPU years, with about half spent enumerating Pryms and half spent computing conductors (we chose parameters to ensure a close to 50/50 division of labor). Tables 2 and 3 summarise the results of the enumeration phase, while Table 4 provides statistics on the Pryms of small conductor that were

found, a surprising number of which are isogenous to Jacobians of genus 2 curves over $\mathbb{Q}$, several thousand of which were not previously known. See Section 5.1 for some particularly interesting examples.

objects	**count**
Elliptic curves E with $\mathrm{rad}(N_E) \le 2^{10}$ in the LMFDB	315 607
Number fields K of degree ≤ 4 with $\lvert\Delta_K\rvert \le 2^{20}$ and $\mathrm{rad}(\Delta_K) \le 2^{10}$	12 821
Pairs (E, K) with $\mathrm{rad}(N_E\Delta_K) \le 2^{10}$ and $n(E_K) > n(E)$	42 504 851
Genus 3 double covers $C \to E$ arising from some pair (E, K)	117 615 804
Nonhyperelliptic C	81 601 322
Hyperelliptic C	36 014 482
Hyperelliptic C that required twisting (see Remark 5.1)	546 281
C that also cover a genus 2 curve (see Remark 5.2)	13 077 189
Smooth plane quartic genus 2 covers	6 040 037
Hyperelliptic genus 2 covers	7 037 152

TABLE 2. Pryms constructed. Here $n(E)$ and $n(E_K)$ count Mordell-Weil generators (including torsion generators). The $E/\mathbb{Q}$ we considered include all $E/\mathbb{Q}$ with $N_E \le 500\,000$ or $\mathrm{rad}(N_E)|210$.

Remark 5.1. Every irreducible smooth projective genus 3 curve $C/\mathbb{Q}$ is either a smooth plane quartic or hyperelliptic in the sense that C admits a degree-2 map to a genus zero curve $Y/\mathbb{Q}$. If $Y \simeq \mathbb{P}^1$ then C admits a rational hyperelliptic model of the form $y^2 = f(x)$ with $f \in \mathbb{Q}[x]$, but otherwise C need not admit such a model; over $\mathbb{Q}$ it can be defined as the intersection of a hypersurface $w^2 = f(x, y, z)$ and a conic $Y\colon g(x, y, z) = 0$ in weighted projective space, where f and g are ternary quartic and quadratic forms, respectively. The base change of C to a quadratic extension $K/\mathbb{Q}$ over which Y has a rational point will admit a hyperelliptic model with coefficients in K whose Shioda invariants (see [46]) are rational. In general, there may not be a curve defined over $\mathbb{Q}$ with a given set of rational Shioda invariants (the field of definition may differ from the field of moduli, even for hyperelliptic curves with extra automorphisms, see [23, p. 86]), but in our situation we know by construction that $\mathbb{Q}$ is a field of definition for C, and that the reduced automorphism group has even order (due to the nonhyperelliptic involution induced by the map $C \to E$), so we can use the algorithm of Lercier and Ritzenthaler [28, 29] implemented in Magma [10] to construct a hyperelliptic curve $\tilde{C}\colon y^2 = f(x)$ with $f \in \mathbb{Q}[x]$ that has the same Shioda invariants as C; see [29, Lemma 1.6]. The curve $\tilde{C}$ won't necessarily be a degree-2 cover of E, but it will be a degree-2 cover of a genus 1 curve $\tilde{E}$ whose Jacobian is a quadratic twist of E, which we can find by enumerating quadratic characters ramified only at the primes of bad reduction of $\tilde{C}$. By applying this quadratic twist to the double cover $\tilde{C} \to \tilde{E}$ we obtain a double cover $\tilde{C}' \to E$ whose associated Prym variety is a quadratic twist of our original Prym (even though $\tilde{C}'$ is *not* a quadratic twist of our original geometrically hyperelliptic $C/\mathbb{Q}$).

Remark 5.2. As explained in [33], over an algebraically closed field, we can always find a Jacobian that is isogenous to our Prym. When C is hyperelliptic we are generically in the $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ stratum (curves with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \hookrightarrow \mathrm{Aut}(C)$,

see [33]) of the moduli space of hyperelliptic genus 3 curves, and over $\overline{\mathbb{Q}}$ we can define C via a hyperelliptic model $y^2 = f(x^2)$ with $\deg(f) = 4$, and then $\mathrm{Jac}(C) \sim \mathrm{Jac}(C_1) \times \mathrm{Jac}(C_2)$, with $C_1 \colon y^2 = f(x)$ of genus 1 and $C_2 \colon y^2 = xf(x)$ of genus 2, with $\mathrm{Jac}(C_2)$ isogenous to our Prym [33, Prop. 1.1]. When C is nonhyperelliptic we are generically in the $\mathbb{Z}/2\mathbb{Z}$ stratum (curves with $\mathbb{Z}/2\mathbb{Z} \hookrightarrow \mathrm{Aut}(C)$, see [33]) of the moduli space of nonhyperelliptic genus 3 curves, and even over $\mathbb{Q}$ we can always define C with a model of the form $y^4 + h(x,z)y^2 + f(x,z) = 0$, where f and h are binary forms of degrees 4 and 2, respectively, by choosing a model for which the $\mathbb{Z}/2\mathbb{Z}$ involution is $y \mapsto -y$ (efficient code for doing this can be found in our GitHub repository [4]). Over $\overline{\mathbb{Q}}$ we can factor $f(x,z)$ into a product of binary quadratic forms and apply the formulas of Ritzenthaler-Romagny [42] to obtain equations for curves C_1, C_2 of genus $1, 2$ such that $\mathrm{Jac}(C) \sim \mathrm{Jac}(C_1) \times \mathrm{Jac}(C_2)$, with $\mathrm{Jac}(C_2)$ isogenous to our Prym. We call models for C of the form above *even models*. In our setting, we have a degree-2 map $\phi \colon C \to E$ to a genus 1 curve. In the nonhyperelliptic case, we can always choose an even model, but we may not be able to construct the curve C_2 over $\mathbb{Q}$ (as noted in Ritzenthaler-Romagny [42], the necessary rationality condition is not always satisfied). The reverse is true in the hyperelliptic case: we may not be able to construct an even model over $\mathbb{Q}$ (there is a quadratic equation related to the involution induced by ϕ that must have a rational root), but whenever this is possible we immediately get an equation over $\mathbb{Q}$ for C_2. Magma code that efficiently checks these rationality conditions and produces a genus 2 curve C_2 equipped with a map $C \to C_2$ can be found in our GitHub repository [4]. We exploit this whenever possible, as it is much easier to compute the conductor (and the L-function) of $\mathrm{Jac}(C_2)$ than of the Prym A which we can access only indirectly.

Remark 5.3. As noted in Remark 5.2, when the genus 3 curve C admits both the Prym map $C \to E$ and a degree-2 map $C \to C_2$ to a genus 2 curve, then we have associated isogeny decompositions $\mathrm{Jac}(C) \sim A \times E$ and $\mathrm{Jac}(C) \sim \mathrm{Jac}(C_2) \times E'$, where A is the abelian surface corresponding to the Prym variety and E' is an elliptic curve which may be isogenous to E but need not be. If $E' \sim E$ then $A \sim \mathrm{Jac}(C_2)$ and we have $L(A,s) = L(C_2,s)$. This will necessarily occur when there is only one involution to work with, as the map $C \to C_1$ induced by our even model for C (see Remark 5.2) will force $\mathrm{Jac}(C_1) \sim E$, but this need not hold when there are additional involutions, for example, when C is a Ciani quartic with automorphism group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. This is actually useful, because if we find that $\mathrm{Jac}(C_1)$ is not isogenous to E then we immediately get a factorisation of $\mathrm{Jac}(C)$ and our Prym into a product of elliptic curves, that is, there must exist a third elliptic curve E'' for which $\mathrm{Jac}(C) \sim E \times E' \times E''$. Indeed, $A \sim E' \times E''$ and $\mathrm{Jac}(C_2) \sim E \times E''$. With an equation for C_2 in hand, it is not hard to find E''.

Data for the small conductor Pryms whose isogeny classes are tabulated in Table 4 is available in the GitHub repository associated to this paper [4]. For each genus 3 double cover $C \to E$ we provide the following data:

- The conductor N (subject to heuristics (a) and (b) noted in Section 3).
- The trace hash h (an isogeny class invariant).

objects	lower bound
Isogeny classes of Pryms	80 904 678
that contain a genus 2 Jacobian	12 226 239
Isogeny classes of nonhyperelliptic Pryms	55 699 050
that contain a genus 2 Jacobian	5 833 651
Isogeny classes of hyperelliptic Pryms	27 390 870
that contain a genus 2 Jacobian	6 538 719
Isogeny classes of Pryms up to quadratic twist	25 549 552
that contain a genus 2 Jacobian	7 071 149
Isogeny classes of nonhyperelliptic Pryms up to quadratic twist	20 061 326
that contain a genus 2 Jacobian	3 912 828
Isogeny classes of hyperelliptic Pryms up to quadratic twist	7 261 867
that contain a genus 2 Jacobian	3 473 381

TABLE 3. Isogeny classes of Pryms enumerated.

objects	count
Isogeny classes of Pryms of conductor $\leq 2^{20}$	454 153
that contain a previously known genus 2 Jacobian	373 048
that contain a genus 2 Jacobian via Remark 5.2	235 089
that were previously unknown	8 586
Isogeny classes of generic ($\mathrm{End}(A_{\overline{\mathbb{Q}}}) = \mathbb{Z}$) Pryms of conductor $\leq 2^{20}$	236 850
that contain a previously known genus 2 Jacobian	217 298
that contain a genus 2 Jacobian via Remark 5.2	165 829
that were previously unknown	6 836

TABLE 4. Isogeny classes of Pryms with conductor $\leq 2^{20}$; all counts assume that heuristically computed conductors are correct and isogeny classes are uniquely identified by their trace hashes.

- An integral equation for C (either a smooth plane quartic $f(x, y, z) = 0$ or a hyperelliptic curve $y^2 + h(x)y = f(x)$).
- Weierstrass coefficients a_1, a_2, a_3, a_4, a_6 for a minimal integral model of E.
- The root number ε and the Euler factors $L_p(T)$ for primes $p|\Delta(C)$ that were used to deduce N via the functional equation (1).
- In cases where Remark 5.2 applies we provide an integral equation for the genus 2 curve C_2 whose Jacobian is isogenous to the Prym variety A.

The previously unknown isogeny classes of genus 2 curves over $\mathbb{Q}$ of conductor $N \leq 2^{20}$ may contain multiple $\mathbb{Q}$-isomorphism classes of Jacobians. These can be exhaustively enumerated via [3], and we plan to do this before adding our data to the LMFDB.

5.1. **Genus 2 curves over $\mathbb{Q}$ of 2-power conductor.** In his 1996 invited talk *Computational aspects of curves of genus at least* 2 at the second Algorithmic Number Theory Symposium (ANTS II), Bjorn Poonen [37] proposed the problem of enumerating all genus 2 curves over $\mathbb{Q}$ whose Jacobians have good reduction away

from 2; this was shortly after the easier problem of enumerating all genus 2 curves over $\mathbb{Q}$ with good reduction away from 2 had been solved by Smart [47], building on previous joint work with Merriman [36]. Little progress was made on this problem in the next two decades, but there is substantial recent progress due to Robin Visser. In his doctoral thesis [51] Visser presents a list of 512 genus 2 curves $C/\mathbb{Q}$ whose Jacobians have good reduction away from 2, obtained through a wide variety of means and extensive search. We are happy to add ten new curves to this list:

N	$\lvert D\rvert$	curves
2^{14}	$2^{54}3^{22}11^{22}$	$\pm y^2 = 7161x^6 + 7722x^5 - 40887x^4 - 74844x^3 + 46431x^2 + 17226x - 5313$
2^{16}	$2^{49}3^{22}11^{22}$	$\pm y^2 = 5115x^6 + 26928x^5 + 18117x^4 + 5016x^3 + 19305x^2 - 22968x + 7359$
2^{20}	$2^{54}13^{22}$	$\pm y^2 = 3107x^6 + 17576x^5 + 18642x^4 + 37284x^2 - 70304x + 24856$
2^{20}	$2^{54}13^{22}$	$\pm y^2 = 1287x^6 - 9854x^5 - 5993x^4 + 100308x^3 + 93873x^2 - 9854x - 18863$
2^{20}	$2^{54}13^{22}$	$\pm y^2 = 7501x^6 + 27430x^5 + 49933x^4 + 75452x^3 + 37947x^2 + 27430x - 25077$

All ten of these curves have primes of almost good reduction that divide the minimal discriminant of the curve but not the conductor of the Jacobian. These are all (non-quadratic) twists of curves on Visser's list and have Jacobians isogenous to Jacobians of curves on Visser's list, but neither the twists nor the isogenies are easy to discover computationally. We found them simply because their Jacobians happen to be isogenous to Pryms found by our search. In total we found 290 isomorphism classes of genus 2 curves $C/\mathbb{Q}$ whose Jacobians have 2-power conductor; the other 280 already appear in Visser's list.

References

[1] L. Alpöge and B. Lawrence, *Conditional algorithmic Mordell*, arXiv:2408.11653v1, 2024.
[2] M. A. Bennett, A. Gherga and A. Rechnitzer, *Computing elliptic curves over* $\mathbb{Q}$, Math. Comp. **88**:317 (2019), 1341–1390. (MathSciNet: MR3904149)
[3] R. van Bommel, S. Chidambaram, E. Costa, and J. Kieffer, *Computing isogeny classes of typical principally polarized abelian surfaces over the rationals*, LuCaNT: LMFDB, Computation, and Number Theory, Contemp. Math. **796** (2024), 187–214. (MathSciNet: MR4732688)
[4] R. van Bommel, C. Maistret, J. Shi, A.V. Sutherland, *Genus3Covers*, GitHub repository, `https://github.com/AndrewVSutherland/Genus3Covers`.
[5] A.R. Booker and A.V. Sutherland, *A database of genus 2 curves over* $\mathbb{Q}$ *of small conductor*, in preparation.
[6] A. Booker, J. Sijsling, A.V. Sutherland, J. Voight, D. Yasaki, *A database of genus 2 curves over the rational numbers*, Twelfth Algorithmic Number Theory Symposium (ANTS XII), LMS J. Comput. Math. **19** (2016), 235–254. (MathSciNet: MR3540958)
[7] M. Börner, I. Bouw, S. Wewers, *Picard curves with small conductor*, Algorithmic and Experimental Methods in Algebra, Geometry, and Number Theory, pages 97–122, Springer Cham., 2017. (MathSciNet: MR3792722)
[8] I. Bouw, N. Coppola, E. Lorenzo Garcia, and A. Somoza, *On the conductor of Ciani plane quartics*, Matematica **4**:3 (2025), 643–673. (MathSciNet: MR4958726)
[9] I. Bouw, A. Koutsianas, J. Sijsling, S. Wewers, *Conductor and discriminant of Picard curves*, J. Lond. Math. Soc. **102**:1 (2020), 368–404.
[10] W. Bosma, J. J. Cannon, C. Fieker, A. Steel (eds.), *Handbook of Magma functions*, Version 2.29-4 (2025).
[11] G. Boxer, F. Calegari, T. Gee, and V. Pilloni, *Modularity theorems for abelian surfaces*, arXiv:2502.20645v1, 2025.
[12] C. Breuil et al., *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939. (MathSciNet: MR1839918)
[13] A. Brumer and K. Kramer, *The conductor of an abelian variety*, Compositio Math. **92**:2 (1994), 227–248. (MathSciNet: MR1283229)

[14] A. Brumer and K. Kramer, *Paramodular abelian varieties of odd conductor*, Trans. Amer. Math. Soc. **366** (2014), no. 5, 2463–2516. (MathSciNet: MR3165645)

[15] A. Brumer and K. Kramer, *Corrigendum to "Paramodular abelian varieties of odd conductor"*, Trans. Amer. Math. Soc. **372** (2019), no. 3, 2251–2254. (MathSciNet: MR3976591)

[16] E. Costa, D. Harvey, and A.V. Sutherland, *Counting points on smooth plane quartics*, Fifteenth Algorithmic Number Theory Symposium (ANTS XV), Res. Number Theory **9**:1 (2023), 32 pages. (MathSciNet: MR4514545)

[17] J. E. Cremona, *Algorithms for modular elliptic curves*, second edition, Cambridge Univ. Press, Cambridge, 1997. (MathSciNet: MR1628193)

[18] T. Dokchitser, V. Dokchitser, C. Maistret, A. Morgan, *Arithmetic of hyperelliptic curves over local fields*, Math. Ann. **385** (2023), 1213–1322. (MathSciNet: MR4566695)

[19] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern* (German) [Finiteness theorems for abelian varieties over number fields], Invent. Math. **73** (1983), no. 3, 349–366. (MathSciNet: MR0718935)

[20] D. Harvey, *Computing zeta functions of arithmetic schemes*, Proc. Lond. Math. Soc. **111**:6 (2015), 1379–1401. (MathSciNet: MR3447797)

[21] D. Harvey and A.V. Sutherland, *Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time, II*, Frobenius distributions: Lang–Trotter and Sato–Tate conjectures, Contemp. Math. **663** (2016), 127–148. (MathSciNet: MR3502941)

[22] D. Harvey, M. Massierer, and A.V. Sutherland, *Computing L-series of geometrically hyperelliptic curves of genus three*, Twelfth Algorithmic Number Theory Symposium (ANTS XII), LMS J. Comput. Math. **19** (2016), 220–234. (MathSciNet: MR3540957)

[23] B. Huggins, *Fields of moduli and fields of definition of curves*, PhD thesis, University of California, Berkeley, 2005.

[24] F. Johansson, *Arb: efficient arbitrary-precision midpoint-radius interval arithmetic*, IEEE Transactions on Computers **66**:8 (2017), 1281–1292.

[25] I. Kausz, *A discriminant and an upper bound for ω^2 for hyperelliptic arithmetic surfaces*, Compositio Math. **115**:1 (1999), 37–69. (MathSciNet: MR1671741)

[26] K. S. Kedlaya and A. V. Sutherland, *Computing L-series of hyperelliptic curves*, in *Algorithmic number theory*, 312–326, Lecture Notes in Comput. Sci., 5011, Springer, Berlin. MathSciNet: MR2467855

[27] S. Lang, *Introduction to Arakelov theory*, Springer, New York, 1988. (MathSciNet: MR0969124)

[28] R. Lercier and C. Ritzenthaler, *Hyperelliptic curves and their invariants: geometric, arithmetic and algorithmic aspects*, J. Algebra, **372** (2012), 595–636. (MathSciNet: MR2990029)

[29] R. Lercier, C. Ritzenthaler, and J. Sijsling, *Fast computation of isomorphisms of hyperelliptic curves and explicit Galois descent*, Tenth Algorithmic Number Theory Symposium (ANTS X), Open Book Series **1**, pages 463–486, Mathematical Sciences Publishers, 2013. (MathSciNet: MR3207427)

[30] Q. Liu and D. J. Lorenzini, *Models of curves and finite covers*, Compositio Math. **118**:1 (1999), 61–102. (MathSciNet: MR1705977)

[31] The LMFDB Collaboration, *The L-functions and modular forms database*, available online at `https://www.lmfdb.org`; accessed 19 May 2026.

[32] The LMFDB Collaboration, *The L-functions and modular forms database (alpha release)*, available online at `https://alpha.lmfdb.org`; accessed 19 May 2026.

[33] D. Lombardo, E. Lorenzo Garcia, C. Ritzenthaler, and J. Sijsling, *Decomposing Jacobians via Galois covers*, Exp. Math. **32** (2023), 218–240. (MathSciNet: MR4574430)

[34] E. Lupoian and J. Rawson, *Three-torsion subgroups and wild conductor exponents of plane quartics*, Res. Number Theory **11** (2025), paper no. 92, 17 pages. (MathSciNet: MR4967837)

[35] C. Maistret and A.V. Sutherland, *Computing Euler factors of genus 2 curves at odd primes of almost good reduction*, Res. Number Theory **11** (2025), paper no. 37, 21 pages. (MathSciNet: MR4868102)

[36] J.R. Merriman and N.P. Smart, *Curves of genus 2 with good reduction away from 2 with a rational Weierstrass point*, Math. Proc. Cambridge Philos. Soc. **114** (1993), 203–214. (MathSciNet: MR1230127)

[37] B. Poonen, *Computational aspects of curves of genus at least 2*, Second Algorithmic Number Theory Symposium (ANTS II), Lecture Notes Comput. Sci. **1122**, Springer-Verlag, 1996. (MathSciNet: MR1446492)

[38] C. Poor, J. Shurman, and D. Yuen, *Nonlift weight two paramodular eigenform constructions*, J. Korean Math. Soc. **57** (2020), no. 2, 507–522. (MathSciNet: MR4072025)
[39] C. Poor and D. Yuen, *Paramodular cusp forms*, Math. Comp. **84** (2015), no. 293, 1401–1438. (MathSciNet: MR3315514)
[40] C. Poor and D. Yuen, *Antisymmetric paramodular forms of weights 2 and 3*, Int. Math. Res. Not. IMRN 2020, no. 20, 6926–6946.
[41] C. Poor and D. Yuen, *Degree 2 Siegel Paramodular Forms of Weight 2 and Levels up to 1000*; online; accessed 19 May 2026.
[42] C. Ritzenthaler and M. Romagny, *On the Prym variety of genus 3 covers of genus 1 curves*, Épijournal Géom. Algébrique **2** (2018), Art. 2, 8 pp.
[43] J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math. **88** (1968), 492–517. (MathSciNet: MR236190)
[44] J. Shi, *Lifting L-polynomials of genus 2 curves*, J. Théor. Nombres Bordeaux, to appear.
[45] J. Shi, *Lifting L-polynomials of genus 3 curves*, arXiv:2602.00965v1.
[46] T. Shioda, *On the graded ring of invariants of binary octavics*, Amer. J. Math. **89** (1967), 1022–1046. (MathSciNet: MR0220738)
[47] N.P. Smart, *S-unit equations, binary forms and curves of genus 2*, Proc. London Math. Soc. **75** (1997), 217–307. (MathSciNet: MR1455857)
[48] A.V. Sutherland, *A database of nonhyperelliptic genus 3 curves over* $\mathbb{Q}$, Thirteenth Algorithmic Number Theory Symposium (ANTS XIII), The Open Book Series **2**, pages 443–459, Mathematical Sciences Publishers, 2019. (MathSciNet: MR3952027)
[49] A.V. Sutherland, *Counting points on superelliptic curves in average polynomial time*, Fourteenth Algorithmic Number Theory Symposium (ANTS XIV), The Open Book Series **4**, pages 403–422, Mathematical Sciences Publishers, 2020. (MathSciNet: MR4235126)
[50] A.V. Sutherland, *A database of genus 2 curves of small conductor*, slides of talk at Rational Points 2025.
[51] R. Visser, *The effective Shafarevich Conjecture*, PhD Thesis, University of Warwick, 2024.
[52] D. Zywina, *Determining monodromy groups of abelian varieties*, Res. Number Theory **8**:89 (2022). MathSciNet: MR4496693