MATHEMATICS OF COMPUTATION
Volume 88, Number 318, July 2019, Pages 1913–1927
https://doi.org/10.1090/mcom/3387
Article electronically published on November 14, 2018

3-TORSION AND CONDUCTOR OF GENUS 2 CURVES

TIM DOKCHITSER AND CHRISTOPHER DORIS

Abstract. We give an algorithm to compute the conductor for curves of genus 2. It is based on the analysis of 3-torsion of the Jacobian for genus 2 curves over 2-adic fields.

1. Introduction

One of the main arithmetic invariants of a curve $C/\mathbb{Q}$ (or over a number field) is its *conductor*. It is a representation-theoretic quantity measuring the arithmetic complexity of C, and it is particularly important in the considerations that involve Galois representations or L-functions of curves.

In practice, the conductor is difficult to compute. It is defined as a product $N = \prod_p p^{n_p}$ over primes p, so the problem is computing the local *conductor exponents* n_p; these are functions of $C/\mathbb{Q}_p$. For elliptic curves (genus 1), the problem of computing n_p is solved with Tate's algorithm [31] and Ogg-Saito's formula [25, 28]. In genus 2 and $p \neq 2$ there is an algorithm of Liu [22] via the Namikawa–Ueno classification [24], and for hyperelliptic curves of arbitrary genus there is a formula for the conductor [9], again for $p \neq 2$.

As the global conductor N requires the knowledge of n_p for *all* primes p, including $p = 2$, it is currently only provably computable for elliptic curves and for quotients of modular curves using modular methods (see, e.g., [14]). In practice, one can guess N from the functional equation of the L-function (see, e.g., [1, 6]), but this approach is conditional on the conjectural analytic continuation of the L-function, and is basically restricted to reasonably small N.

In this paper, we propose an (unconditional) algorithm to compute the conductor for curves of genus 2. The case to consider is $p = 2$, so from now on C will be a non-singular projective curve of genus 2, defined over a finite extension K of $\mathbb{Q}_2$. Recall that the conductor exponent is the sum of the *tame* and *wild* parts (see §2),

$$n_2 = n = n_{\text{tame}} + n_{\text{wild}}.$$

The difficult one is the wild part, which is the Swan conductor of the l-adic Tate module of the Jacobian J/K of C/K for any $l \neq 2$. We will take $l = 3$ and use that n_{wild} can be computed from the action of $\mathrm{Gal}(\bar{K}/K)$ on the 3-torsion $J[3]$. The equations defining $J[3]$ as a scheme are well known in genus 2 (see §4.1 or [3]),

Received by the editor July 6, 2017, and, in revised form, February 14, 2018, and April 25, 2018.

2010 *Mathematics Subject Classification.* Primary 11G20; Secondary 14D10, 11F80, 11G30.

Key words and phrases. Conductor, hyperelliptic curves, 3-torsion, local fields.

This research was partially supported by an EPSRC grant EP/M016838/1 "Arithmetic of hyperelliptic curves" and by GCHQ.

and we use Gröbner basis machinery to convert them essentially to a univariate equation of degree $80 = |J[3] \setminus \{0\}|$. The problem then becomes to compute the Galois group of this polynomial and enough information about the inertia action on the roots to reconstruct the conductor. This is the core of the paper (§4). In particular, we discuss how to guarantee that the results are provably correct (§4.3).

As for the tame part, it can be computed from the regular model of C/K, which is in principle accessible: take any model of C over the ring of integers of K, and perform repeated blowups until it becomes regular.[1] However, the algorithm to compute a regular model is currently only partially implemented in Magma [2], and so we complement our algorithm with a result that determines n_{tame} from elementary invariants, in the majority of the cases (Theorem 3.2).

An alternative approach to getting the conductor would be to find a Galois extension F/K where C acquires semistable reduction and a semistable model over F, and analyse the action of inertia of F/K on the model. From this one can determine the l-adic representation $V_l J$; in particular, the conductor exponent (see, e.g., [8, §6]). Moreover, there are more compact polynomials defining such an F in the case of genus 2, $p = 2$ than the degree 80 3-torsion polynomial. For example, there is the monodromy polynomial of Lehr-Matignon in the potentially good reduction case, of degree 16 [20, §3]. However, the splitting field of any such polynomial would have ramification degree no less than that of $K(J[3])/K$, by the Serre-Tate theorem [30, Cor. 2]. So such a field (and the model of C over it) would still be prohibitively large to compute, and our algorithm avoids this.

We end by noting that the core of the paper is a special test case of a general algorithm (in progress) to find Galois groups over local fields [11]. Regarding Gröbner bases, the algorithm would be accelerated by an algorithm to solve multivariate systems of equations p-adically (see Remark 5.1). This is also work in progress. Finally, it should be possible to extend the algorithm to compute the conductor to function fields of characteristic 2 as well, by modifying the equations of the curve and its 3-torsion in §4.1 appropriately.

This algorithm has been implemented as a Magma package [13], and has been used to verify most of the genus 2 curves in the LMFDB (§6).

2. Notation

Throughout the paper, we use the following notation:

$K, L, \ldots$	local fields, of residue characteristic p
$\mathcal{K}, \mathcal{L}, \ldots$	global fields
G_K	$= \mathrm{Gal}(\bar{K}/K)$, the absolute Galois group of K
$I_K < G_K$	its inertia group
T	$\mathbb{Z}_l$-module with an action of G_K, with $l \neq p$
V	the associated l-adic representation $T \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$
$\bar{V}$	the reduction $T \otimes_{\mathbb{Z}_l} \mathbb{F}_l$
G^u	upper numbering of ramification groups
G_v	lower numbering of ramification groups
$n = n_{\text{tame}} + n_{\text{wild}}$	conductor exponent

[1] Then $n_{\text{tame}} = 4 - 2d_a - d_t$, where d_a ("abelian part") is the sum of genera of reduced components of the special fibre of the model, and d_t ("toric part") is the number of loops.

We are interested in the situation that J/K is an abelian variety, $T = T_l J$ is its l-adic Tate module, $V = V_l J$ and $\bar{V} = J[l]$ is its l-torsion. Recall that the conductor exponent of such a representation is given by (see, e.g., [32])

$$n(V) = \int_{-1}^{\infty} \operatorname{codim} V^{G_K^u} du,$$

with

$$n_{\text{tame}}(V) = \int_{-1}^{0} \qquad \text{and} \qquad n_{\text{wild}}(V) = \int_{0}^{\infty}.$$

For $u > 0$, G_K^u is pro-p, and [32, §6]

$$\operatorname{codim} V^{G_K^u} = \operatorname{codim} \bar{V}^{G_K^u}.$$

Our approach is that we will compute $n_{\text{tame}}(V)$ as the codimension of inertia invariants V^{I_K} and the wild conductor exponent as

$$n_{\text{wild}}(V) = \int_{0}^{\infty} \operatorname{codim} J[l]^{G_K^u} du,$$

and replace G_K by $\operatorname{Gal}(K(J[l])/K)$.

3. Tame conductor exponent

Let K be any non-Archimedean local field, J/K a g-dimensional abelian variety, and l a prime different from the residue characteristic of K. Write $T = T_l J$ for the l-adic Tate module of J/K and $V = V_l J = T_l J \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$, both viewed as representations of the inertia group $I_K < G_K$.

Recall[2] that there is a canonical filtration on T coming from the toric part and the abelian part of J over a field where it acquires semistable reduction. See, e.g., [4], §2.10, for details. With respect to this filtration, I_K acts on T as

$$\begin{pmatrix} \chi & * & N \\ 0 & \rho & * \\ 0 & 0 & \hat{\chi} \end{pmatrix} \tag{3.1}$$

with $\chi : I_K \to \mathrm{GL}_t(\mathbb{Z}_l)$, $\rho : I_K \to \mathrm{GL}_{2a}(\mathbb{Z}_l)$ continuous with finite image ($t =$ "toric", $a =$ "abelian", $2t + 2a = \operatorname{rk}_{\mathbb{Z}_l} T = 2g$), and $\hat{\chi}$ the dual of χ. The "monodromy matrix" N has $\mathbb{Z}$-coefficients, and χ factors through $\mathrm{GL}_t(\mathbb{Z})$ as well. In particular, $\chi \otimes \mathbb{Q}_l$ is self-dual with determinant of order 1 or 2. Consequently, the same holds for $\rho \otimes \mathbb{Q}_l$, as $\det(3.1) = 1$ by the Weil pairing.

Now, we specialise to the case when $J = \operatorname{Jac} C$ is the Jacobian of a genus 2 curve and $l = 3$. We will explain in §4 how to compute the image I of I_K in $\operatorname{Aut} J[3]$ and the dimension of inertia invariants $\dim J[3]^I$.

We can also compute t and a using a theorem of Liu [21, Thm. 1] that determines the stable type of C/K from the Igusa invariants of the curve. There are seven possible stable types in genus 2; in other words, possibilities for stable reduction. (For elliptic curves there are two types of stable reduction—good and multiplicative.) They are listed as cases I, II, ..., VII in Liu's theorem, and in the notation of [7]

[2] These are "standard" facts that we found a little hard to locate in the literature, but they are summarised in [4], §2.10: for the existence of a $\operatorname{Gal}(\bar{K}/K)$-stable filtration that forces the Galois group action to be upper-triangular see [4, p. 13, 2nd half]; for the fact that the representations on the graded pieces χ and ρ are independent of l see [4, p.13, bottom], and for the maps between them and the monodromy pairing see [4, pp. 30,32]. See also the forthcoming paper [10].

they are denoted $2, 1_n, I_{n,m}, U_{n,m,r}, 1\times 1, 1\times I_n, I_n\times I_m$. The special fibres are as shown in Figure 1, with numbers above the components indicating geometric genus.

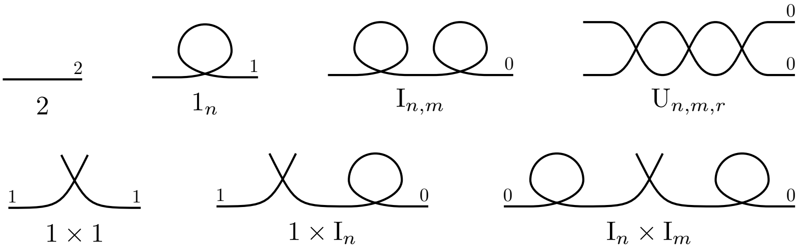

FIGURE 1. The seven stable reduction types for genus 2.

Of these, types 2 and 1×1 have $t=0, a=2$ (potentially good reduction of J), types 1_n and $1\times I_n$ have $t=a=1$ (mixed), and $I_{n,m}$, $U_{n,m,r}$, and $I_n\times I_m$ have $t=2, a=0$ (potentially totally toric reduction).

The main result of this section recovers the tame conductor exponent of J/K from the invariants I, $\dim J[3]^I$, and t, when this is possible.

Theorem 3.2. *Let K be a non-Archimedean local field of residue characteristic $\neq 3$ and C/K a genus 2 curve with Jacobian J/K. Write*

$$\begin{aligned} I &= \textit{image of inertia } I_K < G_K \textit{ in } \operatorname{Aut} J[3] \textit{ (so } I<\mathrm{Sp}_4(\mathbb{F}_3)\textit{)},\\ d &= \dim(V_3J)^I \textit{ (so } 0\le d\le 4\textit{)},\\ \bar d &= \dim J[3]^I \textit{ (so } 0\le \bar d\le 4\textit{)},\\ t &= \textit{potential toric dimension of } J \textit{ (so } 0\le t\le 2\textit{)},\\ f &= 4-d = n_{\mathrm{tame}}(V_3J) = n_{\mathrm{tame}}(J/K) \textit{ (so } 0\le f\le 4\textit{)}.\end{aligned}$$

Then $\bar d\ge d$ and so $f\ge 4-\bar d$. Moreover,

(1) *If $\bar d=0$, then $f=4$.*
(2) *If $\bar d=4$, then $d=4-t$ and $f=t$.*
(3) *Suppose J has potentially good reduction ($t=0$). If $|I|=3$ and $\bar d=2$, then $f=4$; in all other cases, f is the smallest even integer $\ge 4-\bar d$.*
(4) *If $(t,|I|)\in\{(1,3),(2,3),(1,2),(1,6)\}$, then f is not uniquely determined as a function of t, I, and $\bar d$.*
(5) *If $(t,|I|)=(2,9)$, then $f=4$; in all other cases not covered, $f=3$.*

Proof. Write $T=T_3J$, $V=V_3J$. Note that after tensoring (3.1) with $\mathbb{Q}_3$ and a suitable change of basis, both $*$'s can be made 0 and N can be a $t\times t$ identity matrix. In particular,

$$V^{I_K}=\chi^I\oplus\rho^I,\qquad f=4-\dim\chi^I-\dim\rho^I. \tag{3.3}$$

If V has an I_K-invariant subspace of dimension d, its intersection with T gives a rank d saturated sublattice of T, whose reduction contributes at least dimension d to $J[3]^I$. This shows that $\bar d\ge d$, and implies (1).

(2) By Raynaud's semistability criterion [16, Prop. 4.7], J is semistable if $J[m]$ is unramified for some $m\ge 3$ coprime to the residue characteristic. Here I_K acts trivially on $J[3]$, and so J is semistable. In other words, $f=t$ and $d=4-t$.

For the remainder of the proof, we assume $\bar d\in\{1,2,3\}$.

(3) By Serre-Tate's theorem [30, Cor. 2], J has good reduction over $K(J[3])$; that is, I_K acts on V_3J through I. By Poincaré duality, this representation has

even-dimensional inertia invariants; in other words, d is even. As $d \le \bar{d} \in \{1,2,3\}$, the only possibility for $f = 4-d$ not to be the smallest even integer $\ge 4-\bar{d}$ is when $d=0$ and $\bar{d} \in \{2,3\}$. Suppose we are in that case.

Consider the possibilities for $I < \mathrm{Sp}_4(\mathbb{F}_3)$. Note that 3 divides $|I|$, for otherwise the classical representation theory of I agrees with its modular representation over $\mathbb{F}_3$, implying $d = \bar{d}$. Also note that $C_3 \times C_3$ is not a quotient of I, as the residue characteristic of K is not 3, and tame inertia is cyclic. Computing in Magma [2], we find that $\mathrm{Sp}_4(\mathbb{F}_3)$ has 162 conjugacy classes of subgroups, of which five satisfy the three properties (a) order multiple of 3, (b) no $C_3 \times C_3$-quotient, and (c) $\bar{d} \in \{2,3\}$. Call them $H_1, H_2, H_3 \cong C_3$, $H_4 \cong C_6$, and $H_5 \cong \mathrm{SL}_2(\mathbb{F}_3)$.

By the classification of integral C_p-lattices [5, 27], there are two indecomposable $\mathbb{Z}_3[C_3]$-lattices, up to isomorphism: the trivial lattice of rank 1, and a lattice Λ of rank 2 on which the generator of C_3 acts as $\left(\begin{smallmatrix}-1 & 1\\ -1 & 0\end{smallmatrix}\right)$; every finite rank $\mathbb{Z}_3[C_3]$-lattice is a direct sum of these. If $I \cong C_3$, then, as $d=0$, we must have $T \cong \Lambda \oplus \Lambda$, and it has $\bar{d} = 2$ as claimed.

It remains to show that $I \in \{H_4, H_5\}$ with $d = 0$ is impossible. Suppose we are in this case, and let $z \in I$ be the unique central element of order 2. As above, the classical representation theory of the group $\langle z \rangle \cong C_2$ agrees with its modular representation over $\mathbb{F}_3$. In both H_4 and H_5 the action of z on $\bar{V} = J[3]$ has two $+1$ and two -1 eigenvalues. The same is therefore true for V; moreover, $V = V^+ \oplus V^-$ and $T = T^+ \oplus T^-$ decompose into the two 2-dimensional eigenspaces for z and this decomposition induces the one on $J[3]$.

The group $\mathrm{SL}_2(\mathbb{F}_3)$ has three 1-dimensional complex representations factoring through $\mathrm{SL}_2(\mathbb{F}_3)/Q_8 \cong C_3$, three faithful 2-dimensional ones in which z acts as -1, and a 3-dimensional one with z acting as $+1$. Thus, when I is H_4 and H_5, the space T^+ must be a representation of the unique C_3 quotient of I. It has no trivial subrepresentations (as $d=0$), so $T^+ \cong \Lambda$ as a $\mathbb{Z}_3[C_3]$-module. But then

$$\bar{d} = \dim(\Lambda \otimes \mathbb{F}_3)^{C_3} + \dim(T^- \otimes \mathbb{F}_3)^I = 1 + 0,$$

contradicting the assumption $\bar{d} \in \{2,3\}$.

(4) The following curves give examples over $\mathbb{Q}_2$ that prove that f is not a function of t, I, and $\bar{d}$, as claimed. (In each case, f can be determined by computing the regular model.)

t	I	$\bar{d}$	f	$C/\mathbb{Q}_2$
1	C_3	3	1	$y^2 = x^6 + 4x^4 + 2x^3 + 4x^2 + 1$
1	C_3	3	3	$y^2 = 4x^6 - 20x^4 - 8x^3 + 21x^2 + 22x + 13$
2	C_3	2	2	$y^2 = x^6 + 6x^4 - 7x^2 + 16$
2	C_3	2	4	$y^2 = 5x^6 + 4x^3 - 12$
1	C_2	2	2	$y^2 = -x^6 + 6x^4 - x^2 - 8$
1	C_2	2	3	$y^2 = x^6 - 6x^4 + x^2 + 8$
1	C_6	1	3	$y^2 = x^6 - 6x^4 + 5x^2 + 8$
1	C_6	1	4	$y^2 = x^6 - 31x^4 - 25x^2 - 32$

(5) To deal with all the remaining cases, first suppose that J has totally toric reduction over $K(J[3])$; in other words, $t = 2$. In the notation of (3.1), we have a homomorphism

$$\chi : I \longrightarrow \mathrm{GL}_2(\mathbb{Z}) \quad (\hookrightarrow \mathrm{GL}_2(\mathbb{Z}_3))$$

whose image we denote by $\bar{I}$ and whose kernel is C_1 or C_3. Finite subgroups of $\mathrm{GL}_2(\mathbb{Z})$ are contained in D_4 or D_6. Of those, D_3, D_6 only occur as inertia groups in residue characteristic 3, and C_2^2, C_4, C_6, D_4 have an element acting as -1, forcing $\bar{d} = 0$ (case (1)). The remaining possibilities are

$$\bar{I} \in \{C_1, C_2, C_3\}, \qquad I \in \{C_1, C_2, C_3, C_6, C_9\}.$$

We have excluded $I = C_1$ (case (1)) and $I = C_3$ (case (4)). When $I = C_9$, its image $\bar{I} \cong C_3$ has no invariants, and so $f = 4$ (proving the case $(t, |I|) = (2, 9)$). The only remaining case is $\bar{I} = C_2$, acting with eigenvalues $+1, -1$ (otherwise $\bar{d} \in \{0, 4\}$ again). In this case, the full action on T is of the form

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

in some basis, with non-zero $*$'s. This has 1-dimensional invariants, and so $f = 3$, as claimed.

Finally suppose $t = 1$, so that I_K acts on T as

$$\begin{pmatrix} \chi & * & * & \neq 0 \\ 0 & a & b & * \\ 0 & c & d & * \\ 0 & 0 & 0 & \chi \end{pmatrix}$$

As before, write ρ for the representation $I_K \to \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Because I is not one of the already excluded groups C_1, C_2, C_3, C_6, the image of I_K under $\bar{\rho} = \rho \mod 3$ is not C_1 or C_2. But any other subgroup of $\mathrm{GL}_2(\mathbb{Z}_3)$ of finite order is either D_3, which cannot be a local Galois group, or $\bar{\rho}(I)$, which has no invariants on $\mathbb{F}_3^2$. Hence $\bar{\rho}^{I_K} = 0$, and $J[3]^{I_K} = \chi^{I_K}$ has either dimension 0 (case (1)) or dimension 1 with $f = 3$, as claimed. □

4. Wild conductor exponent

Recall that we wish to compute

$$n_{\mathrm{wild}} = \int_0^\infty \operatorname{codim} J[3]^{G^u}\, du,$$

where $G = G_K$. Note, however, that G_K acts on $J[3]$ through its finite quotient $\mathrm{Gal}(K(J[3])/K)$ so we may equally well take $G = \mathrm{Gal}(K(J[3])/K)$ or any quotient in between.

The integrand here is decreasing, non-negative, integral, and left-constant, so if we denote by $u_1 = 0, u_2, \ldots, u_t$ the jump points in the integrand, then we get

$$n_{\mathrm{wild}} = \sum_{i=2}^{t} (u_i - u_{i-1}) \operatorname{codim} J[3]^{G^{u_i}}.$$

Let $Z \in J[3]$ be a 3-torsion point and let $L = K(Z)$ be the extension it generates. Then Z is fixed by G^u if and only if L is fixed by G^u. Since $G^u \lhd G$, this occurs if and only if any K-conjugate of Z is fixed by G^u. If $\hat{u} = \hat{u}(L/K) = \inf\{u : L \text{ fixed by } G^u\}$ denotes the highest upper ramification break of L/K, then this occurs if and only if $\hat{u} \leq u$.

Hence, if $Z_1, \dots, Z_m$ are representatives of the K-conjugacy classes of $J[3]$, generating extensions L_i/K with highest upper ramification break $\hat{u}_i$, then letting $u_0 = -1 < u_1 = 0 < \cdots < u_t$ be the sorted elements of $\{-1, 0, \hat{u}_1, \dots, \hat{u}_m\}$ we deduce

$$n_{\text{wild}} = \sum_{i=2}^{t} (u_i - u_{i-1}) \left(2g - \log_3 \sum_{j : \hat{u}_j \le u_i} (L_j : K) \right)$$

since $2g = \dim V$ and $(L_j : K)$ is the number of K-conjugates of Z_j.

We proceed by finding the extensions L_i/K explicitly, from which we compute n_{wild} via this equation.

4.1. **Equation for 3-torsion of genus 2 curves.** As before, let C/K be a curve of genus 2, with Jacobian J. The linear system for the canonical divisor on C yields a standard model

$$C : y^2 = f(x), \qquad \deg f = 5 \text{ or } 6.$$

The following statement is well known (see, e.g., [3], proof of Lemma 3); in fact, it works over any field of characteristic $\neq 2, 3$.

Proposition 4.1. *Non-zero elements of* $J[3]$ *are in* 1-1 *correspondence with ways of expressing* f *in the form*

$$(*) \qquad f = (z_4x^3 + z_3x^2 + z_2x + z_1)^2 - z_7(x^2 + z_6x + z_5)^3, \qquad z_i \in \bar{K},$$

and this correspondence preserves the action of G_K.

Explicitly, suppose D is a divisor on C,

$$D = (P_1) + (P_2) - (\infty_1) - (\infty_2), \qquad P_i = (X_i, Y_i),$$

for which $3D$ is principal, say $3D = \operatorname{div} g$. Then $g \in \langle 1, x, x^2, x^3, y \rangle$. After a (unique) rescaling, say

$$g = y + b_3x^3 + b_2x^2 + b_1x + b_0,$$

the norm

$$\begin{aligned} \mathrm{Norm}_{K(C)/K(x)}(g) &= (b_3x^3 + b_2x^2 + b_1x + b_0 - y)(b_3x^3 + b_2x^2 + b_1x + b_0 + y) \\ &= (b_3x^3 + b_2x^2 + b_1x + b_0)^2 - f \end{aligned}$$

is a function on $\mathbb{P}^1$ whose divisor $3(X_1) + 3(X_2) - 6(\infty)$ is a cube, and so

$$(b_3x^3 + b_2x^2 + b_1x + b_0)^2 - f = c_2(x^2 + c_1x + c_0)^3,$$

as stated. In this form,

$$X_{1,2} = \text{ roots of } x^2 + c_1x + c_0 = 0, \qquad Y_i = -b_3X_i^3 - b_2X_i^2 - b_1X_i - b_0.$$

We view $(*)$ as giving a system of seven equations in the seven variables z_i.

4.2. **Finding the 3-torsion fields.** Our goal, then, is to find the (K-isomorphism classes of) fields L/K generated by the (K-conjugacy classes of) solutions Z to the system of equations $(*)$.

A general tool used to solve systems of polynomial equations such as this is to compute a Gröbner basis for the polynomial ideal generated by the polynomials. Generically, a reduced sorted minimal Gröbner basis with respect to the lexicographic ordering on variables will be a finite sequence of polynomials such that the first is univariate, the second is a polynomial in two variables, and so on. Then to solve the system, we first find a root of the first polynomial; then we substitute this value into the second polynomial, yielding a polynomial in one variable, and we find a root of this; we repeat this procedure. In the end, this will produce a sequence of roots which together are a solution to the system.

For our system in particular, the 80 roots come in pairs of the form

$$(Z_1, Z_2, Z_3, Z_4, Z_5, Z_6, Z_7), \quad (-Z_1, -Z_2, -Z_3, -Z_4, Z_5, Z_6, Z_7),$$

and so generically there are 40 distinct values for Z_7, for each of these there is a unique value for Z_6 and Z_5 and two distinct values for Z_4, and for each of these there is a unique value for Z_3, Z_2, and Z_1.

In this generic case, the Gröbner basis described above will be a sequence of seven polynomials $B_1, \ldots, B_7 \in K[z_1, \ldots, z_7]$ such that $B_i \in K[z_i, \ldots, z_7]$, $\deg_{z_i} B_i = d_i$, where $d = (1, 1, 1, 2, 1, 1, 40)$.

Following the above discussion on solving systems using Gröbner bases, we first factorize $B_7 \in K[z_7]$ (of degree 40), let g be one of its irreducible factors, let M/K be the extension it defines, and let $Z_7 \in M$ be a root of g. Substituting this into $B_6 \in K[z_6, z_7]$ we get $B_6(z_6, Z_7) \in M[z_6]$, which is linear, and let Z_6 be its root. Similarly we let Z_5 be the root of $B_5(z_5, Z_6, Z_7) \in M[z_5]$. Next, $B_4(z_4, Z_5, Z_6, Z_7) \in M[z_4]$ is quadratic, so we factorize it, let h be one of its factors, let L/M be the extension it defines, and let $Z_4 \in L$ be a root of h. Continuing, we find unique Z_3, Z_2, and Z_1 which together produces a solution $Z = (Z_1, \ldots, Z_7)$. Repeating this for all factors g and h we find all solutions Z of the system (up to conjugacy) and the extensions L/K which they define.

If we are not in this generic case, then the Gröbner basis is not of this form and there is some coincidence in the coordinates of some solutions of the seven equations. If we apply a random Möbius transformation $x \mapsto \frac{ax+b}{cx+d}$ to the defining polynomial $f(x)$, then the curve it defines is isomorphic to the original but the solutions Z have moved, probably to the generic case. In practice, a small number of Möbius transformations is ever necessary to put the solutions into the generic case.

Remark 4.2. An algorithm of this sort would work with any ordering on $\{z_1, \ldots, z_7\}$. This ordering was chosen because it allows us to factor a degree-40 polynomial followed by a quadratic, which is somewhat faster than just factoring a degree-80 polynomial required for other orderings.

4.3. **Provability.** In practice, however, computing a Gröebner basis of this sort is difficult. Gröebner basis algorithms require exact fields, so in practice we represent K as a completion of a number field $\mathcal{K}$ at some place $\mathfrak{p} \mid 2$, and $f(x) \in \mathcal{K}[x]$.

The best known algorithm over number fields (and indeed the only algorithm which appears to run in feasible time on our problem) computes the basis modulo many primes and finds the global basis via the Chinese remainder theorem. The problem here is that a priori we cannot determine the size of the coefficients, and so a heuristic is used to decide if we have used enough primes to get the answer. The result is that the algorithm does not yield provable results. Nevertheless, it is possible to prove the output of the previous algorithm as follows.

Assuming the Gröebner basis algorithm was correct, then any $Z = (Z_1, \ldots, Z_7)$ should be a solution to the original system of seven equations $(*)$ over K. With the following version of Hensel's lemma, we can show that Z is indeed very close to a unique genuine solution, and we can say how close.

The following version of Hensel's lemma is standard (see, e.g., [19], Thm. 23, with $t = \det J_f(b)$, $s = vf(b)$, and $vJ_f^*(b)f(b) \geq s$).

Theorem 4.3 (Hensel's lemma for multivariate systems)**.** *Suppose K is a local field, $F = (F_1, \ldots, F_m) \in \mathcal{O}_K[z_1, \ldots, z_m]$ is a system of m equations in m variables over $\mathcal{O}_K$, and $Z = (Z_1, \ldots, Z_m) \in \mathcal{O}_K^m$. Let $s = \min_i v_K(F_i(Z))$ and let $t = v_K J(F)(Z)$, where $J(F)$ denotes the Jacobian determinant of F (the determinant of the $m \times m$ matrix whose (i,j)th entry is $\frac{\partial F_i}{\partial z_j}$). If $s > 2t$, then there is a unique $Z' \in \mathcal{O}_K^m$ such that $F(Z') = 0$ and $\min_i v_K(Z'_i - Z_i) \geq s - t$.*

Since evaluating resultants, Jacobians, and polynomials is just basic arithmetic, these operations can be performed provably, and hence applying Hensel's lemma we prove that each Z is indeed close to a unique solution Z' of the system of equations. Furthermore, Hensel's lemma gives us a method to compute Z' to any prescribed precision. We expect that $Z = Z'$ but we do not prove so.

It remains to check that these solutions Z' generate the fields L and that they are distinct up to K-conjugacy.

Recall that we have $L/M/K$ with $M = K(Z_7)$, $g(x) \in K[x]$ the minimal polynomial for Z_7, and $L = M(Z_4)$, $h(x) \in M[x]$ the minimal polynomial for Z_4. We also have $Z'_7, Z'_4 \in L$ and want to prove that $L = K(Z'_7, Z'_4)$. Since we expect that $Z'_7 = Z_7$, then we expect Z'_7 is closer to Z_7 than any other root of g, and so by Krasner's lemma we conclude that $M = K(Z_7) \subset K(Z'_7)$. Another application of Krasner's lemma on h and Z'_4 implies that $L = M(Z_4) \subset M(Z'_4)$. Combining these, we deduce $L = M(Z_4) \subset M(Z'_4) \subset K(Z'_4, Z'_7) \subset L$ and hence $L = K(Z'_4, Z'_7) = K(Z')$.

To check Krasner's lemma on a polynomial $h \in K[x]$ and some $Z \in \bar{K}$, note that it is equivalent to check that there is a root of $h(x + Z)$ of higher valuation than all others. It is well known that the Newton polygon of a polynomial measures the valuations of its roots, and therefore Krasner's lemma is applicable if and only if the Newton polygon of $h(x + Z)$ has a vertex with abscissa 1. This condition is explicitly checkable.

Finally, if Z_7 is a root of a factor g of B_7 and Y_7 is a root of a different factor of B_7, then $g(Z_7) = 0 \neq g(Y_7)$, so if we check that $v(g(Z'_7)) > v(g(Y'_7))$, then we have proven that $Z'_7 \neq Y'_7$. Performing a similar check on pairs of Z'_4 determines that they are different. Together, this will prove that each pair of solutions is distinct.

By performing all these checks with large enough precision, we can determine whether or not the Z are a genuine set of distinct solutions generating the right fields. If any of these checks fails, then the Gröebner basis algorithm was incorrect, and we should try the algorithm again with a lower heuristic chance of failure.

Remark 4.4. There is a conceptually simpler method for provability. Letting $I \lhd \mathcal{K}[z_1, \ldots, z_7]$ be the ideal generated by the original system $(*)$, and letting J be the ideal generated by the Gröbner basis, then we wish to prove that $I = J$. Since J is generated by a Gröbner basis, there is a normal form for reduction modulo J, and hence we can check that each generator of I is zero mod J and so deduce $I \lhd J$. Additionally we know a priori that I has precisely 80 solutions, and from the structure of the Gröbner basis that J has precisely 80 solutions. Combined, this implies $I = J$.

We call this the *global proof method* to distinguish it from the *local proof method* above. In practice, unless the coefficients of $f(x)$ are very small, the global method takes much longer than the local method. Over $\mathbb{Q}$, with small coefficients, the global method is typically around twice as quick, but this benefit quickly diminishes as the field degree increases.

4.4. **Tame conductor exponent revisited.** In order to compute the tame conductor exponent using Theorem 3.2, we require $\bar{d} = \dim J[3]^{G_0}$ and $|I|$. In previous sections we have already seen an algorithm to compute $\dim J[3]^{G^u}$ for any u having already computed L_j/K, so this is easy as a side-effect of previous work.

For $|I|$, consider $e = \mathrm{LCM}_j\, e(L_j/K)$, which again is easy to compute from L_j/K. Clearly it is a divisor of $|I|$. The following lemma shows that e is a good enough guess at $|I|$ in the sense that the statement of Theorem 3.2 depends only on t, e, and $\bar{d}$.

Lemma 4.5. *Let $S = \{1,2,3,4,5,6,9,10,12,18\}$. If $e \in S$ or $|I| \in S$, then $|I| = e$. If $e = 80$, then $|I| = 160$. If $e \in \{8,24\}$, then $|I| \in \{8,24\}$. Otherwise $e \in \{16,32,48,64\}$ and $|I| \in \{16,32,48,64,96,128,192,384\}$.*

Proof. Properties of the Weil pairing imply that $I < \mathrm{Sp}_4(\mathbb{F}_3)$. Letting W be the 2-Sylow subgroup of I, ramification theory implies $W \lhd I$ and I/W cyclic. The lemma is proven by checking all groups I consistent with these facts. □

5. The algorithm

We use the following algorithm to compute the highest upper ramification break $\hat{u}(L/K)$. It takes as input the extension L/K and returns the sequence $(u_i, v_i, s_i)_{i=0}^t$, where $v_0 = -1 < v_1 < \cdots < v_t$ are the breaks in the ramification filtration of L/K in the lower numbering, u_i are the corresponding breaks in the upper numbering, and $s_i = |\Gamma_{v_i}|$ are the sizes of the corresponding ramification subsets of the Galois set Γ of K-embeddings $L \to \bar{K}$. In particular, $\hat{u}(L/K) = u_t$.

See, e.g., [15, §§4–5] or [26, §3] for the definition of the ramification polynomial (the coefficients of which have valuation r_i in the algorithm), the ramification polygon P, and its connection to the ramification filtration of L/K. See, e.g., [18] for the connection of this filtration to the upper and lower ramification breaks and the Galois set Γ.

```
(Compute the ramification polygon of $L/U$)
$U \leftarrow$ the maximal unramified subextension of $L/K$
$e \leftarrow (L:U)$
$E \leftarrow$ a defining Eisenstein polynomial for $L/U$
$r_i \leftarrow \min_{j=i}^{e-1} v(E_j\binom{j}{i}) + \frac{j}{e}$ for $i = 1, \dots, e$
$P \leftarrow$ the lower convex hull of the points $(i, r_i)$ for $1 \le i \le e$

(Compute $u_i$, $v_i$, and $s_i = |\Gamma_{v_i}|$)
$u_0 \leftarrow -1$
$v_0 \leftarrow -1$
$s_0 \leftarrow (L:K)$
$t \leftarrow$ the number of faces of $P$
for all $i = 1, \dots, t$ do
    $F \leftarrow$ the $i$th face of $P$ from the right
    $v_i \leftarrow$ the negative of the gradient of $F$
    $s_i \leftarrow$ the abscissa of the right-hand vertex of $F$
    $u_i \leftarrow u_{i-1} + \frac{s_{i-1}}{s_0}(v_i - v_{i-1})$
```

```
end for
return $((u_i, v_i, s_i))_{i=0}^{t}$
```

Now we present the final algorithm, which takes a polynomial $f(x) \in \mathcal{K}[x]$ of degree 5 or 6 over a number field $\mathcal{K}$ defining a hyperelliptic curve $y^2 = f(x)$, and a prime ideal $\mathfrak{p}$ of $\mathcal{K}$ dividing 2, and returns the conductor exponent $n_{\mathfrak{p}}$ of the curve at $\mathfrak{p}$.

```
(Apply Möbius transformations to $f(x)$ until its 3-torsion points are in general position)
repeat
    choose $a, b, c, d \in \mathbb{Z}$ so that $ad - bc \neq 0$
    $\tilde{f} \leftarrow f(\frac{ax+b}{cx+d})(cx+d)^6$
    $F = (F_i)_{i=1}^{7} \leftarrow$ coefficients of

        $(z_1 + z_2x + z_3x^2 + z_4x^3)^2 + z_7(z_5 + z_6x + x^2)^3 - \tilde{f}(x)$

    $B = (B_i)_i \leftarrow$ Gröbner basis of $F$
until $B$ is in generic form

(Find the fields defined by each $Z_7$)
$K \leftarrow \mathcal{K}_{\mathfrak{p}}$
$S \leftarrow$ empty sequence
$C \leftarrow$ empty sequence
$(g_i)_i \leftarrow$ irreducible factorization of $B_7(x)$ over $K$
for all $g_i$ do
    $M \leftarrow$ the extension of $K$ defined by $g_i$
    $Z_7 \leftarrow$ a root of $g_i$ in $M$
    $Z_6 \leftarrow$ the root of linear $B_6(x, Z_7)$ over $M$
    $Z_5 \leftarrow$ the root of linear $B_5(x, Z_6, Z_7)$ over $M$

    (Find the fields defined by each $Z_4$)
    $(h_i)_i \leftarrow$ irreducible factorization of $B_4(x, Z_5, Z_6, Z_7)$ over $M$
    for all $h_i$ do
        $L \leftarrow$ the extension of $M$ defined by $h_i$
        $Z_4 \leftarrow$ a root of $h_i$ in $L$
        $Z_3 \leftarrow$ the root of linear $B_3(x, Z_4, Z_5, Z_6, Z_7)$ over $L$
        $Z_2 \leftarrow$ the root of linear $B_2(x, Z_3, Z_4, Z_5, Z_6, Z_7)$ over $L$
        $Z_1 \leftarrow$ the root of linear $B_1(x, Z_2, Z_3, Z_4, Z_5, Z_6, Z_7)$ over $L$

        (Check the solutions are valid with Hensel's lemma)
        assert $Z$ is Hensel liftable to a solution of $F$
        $Z' \leftarrow$ the Hensel-lifted solution (we expect $Z' = Z$)

        (Check the solutions generate the right fields with Krasner's lemma)
        assert the Newton polygon of $g_i(x + Z'_7)$ has a vertex above 1
        assert the Newton polygon of $h_j(x + Z'_4)$ has a vertex above 1

        (Check the solutions are distinct)
        for $(Y'_7, Y'_4) \in C$ do
            assert $v_K(g_i(Z'_7)) > v_K(g_i(Y'_7))$ or $v_K(h_i(Z'_4)) > v_K(h_i(Y'_4))$
        end for
        append $(Z'_7, Z'_4)$ to $C$
```

```
37:         (Save $L$)
38:         append $L$ to $S$
39:     end for
40: end for

41: (Compute the tame and wild exponents from $S$)
42: $\bar{d} \leftarrow$ the function $u \mapsto \log_3(1 + \sum_{L \in S : \hat{u}(L/K) \leq u} (L : K))$ $(= \dim \bar{V}^{G^u})$
43: $e \leftarrow \mathrm{LCM}_{L \in S}\, e(L/K)$
44: $t \leftarrow$ potential toric dimension of $J$
45: if $\bar{d}(0) = 0$ then
46:     $n_{\mathrm{tame}} \leftarrow 4$
47: else if $\bar{d}(0) = 4$ then
48:     $n_{\mathrm{tame}} \leftarrow t$
49: else if $t = 0$ then
50:     if $e = 3$ and $\bar{d}(0) = 2$ then
51:         $n_{\mathrm{tame}} \leftarrow 4$
52:     else
53:         $n_{\mathrm{tame}} \leftarrow$ smallest even integer $\geq 4 - \bar{d}(0)$
54:     end if
55: else if $(t, e) \in \{(1,3), (2,3), (1,2), (1,6)\}$ then
56:     $n_{\mathrm{tame}} \leftarrow$ the tame exponent, computed from a regular model
57: else if $(t, e) = (2, 9)$ then
58:     $n_{\mathrm{tame}} \leftarrow 4$
59: else
60:     $n_{\mathrm{tame}} \leftarrow 3$
61: end if
62: $u_0, \ldots, u_t \leftarrow$ the sorted elements of $\{\hat{u}(L/K) : L \in S\} \cup \{-1, 0\}$
63: $n_{\mathrm{wild}} \leftarrow \sum_{i=2}^{t} (u_i - u_{i-1})(4 - \bar{d}(u_i))$
64: return $n_{\mathrm{wild}} + n_{\mathrm{tame}}$
```

Remark 5.1. Note that the approach to solving the system of seven equations in seven variables is to compute a Gröbner basis globally, and then solve this system locally. This is the only global aspect of the algorithm, and becomes the bottleneck when the global coefficients become large. An alternative approach is to solve the system of equations directly locally, perhaps using a Montes-type algorithm similar to univariate factorization algorithms which split the system into several smaller systems. This is the subject of ongoing research [11].

Remark 5.2. Recalling Remark 4.4, if we wish to use the global proof method instead, then we can skip over lines 22–36 and instead insert after line 7 a check that each element of F reduces to 0 modulo B.

6. Implementation

The algorithms described in this paper have been implemented [13] in the Magma computer algebra system [2] using a customized implementation of p-adics which removes most p-adic precision considerations from the user [12]. The implementation, modulo bugs, produces provable results at every step.

The LMFDB [23] contains the 66,158 genus 2 hyperelliptic curves defined over $\mathbb{Q}$ computed by Booker et al. [1]. Of these, all but 1,113 have discriminant of 2-valuation less than 12 and therefore their conductor exponent at 2 is computable via

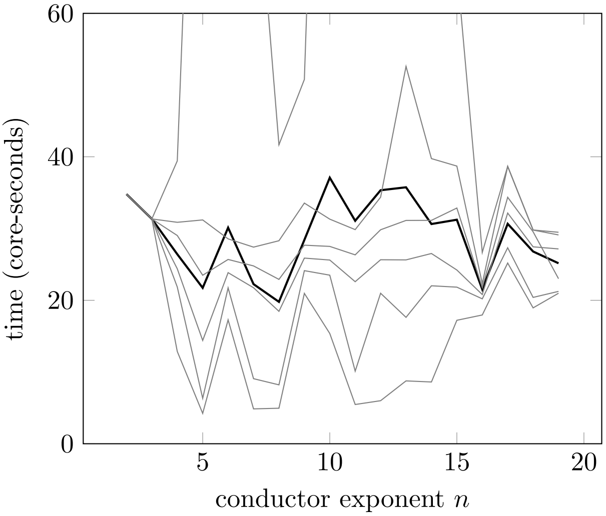

FIGURE 2. Mean (black) and 20-percentiles (gray) of run-time with LMFDB curves by conductor exponent.

Ogg's formula. Our algorithm has been run on the 1,113 remaining curves, using the global proof method (see Remark 4.4). The computation took 9.4 core-hours in total on a 2.7GHz Intel Xeon, averaging 30 core-seconds per curve. For all but six of these curves, the fast tame conductor algorithm of §3 succeeds, and so we compute an entire conductor exponent at 2. For four of the remaining six curves, a regular model was quickly computed by Magma (taking at most 10 seconds) and therefore the tame exponent was deduced this way. For the remaining two curves (labelled `3616.b.462848.1` and `18816.d.602112.1` in the LMFDB) a regular model was computed by hand. In all of these cases, the exponent agrees with the unproven results of [1] and therefore we have proven the conductors for all curves in the LMFDB.

The run-time of the algorithm is usually dominated by the factorization of the degree-40 polynomial over K, at least when the defining polynomial $f(x)$ has fairly small coefficients. When these coefficients grow, the (global) Gröbner basis algorithm dominates the run-time.

This gives some impetus towards developing a fully local algorithm as suggested in Remark 5.1, since this will be independent of global coefficient sizes.

The implementation has also been tested on some curves defined over quadratic number fields. These results were confirmed by Schembri [29] by finding a corresponding Bianchi modular form whose level squared equals the conductor and proving the expected relationship between their L-functions using Faltings-Serre.

The run-time does not appear to grow much with the conductor exponent, as evidenced by the graph in Figure 2 summarizing the run-times of the algorithm on the LMFDB curves.

ACKNOWLEDGMENTS

We would like to thank David Roberts for helpful discussions and the referees for their suggestions.

References

[1] Andrew R. Booker, Jeroen Sijsling, Andrew V. Sutherland, John Voight, and Dan Yasaki, *A database of genus-2 curves over the rational numbers*, LMS J. Comput. Math. **19** (2016), no. suppl. A, 235–254, DOI 10.1112/S146115701600019X. MR3540958

[2] 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, DOI 10.1006/jsco.1996.0125. Computational algebra and number theory (London, 1993). MR1484478

[3] Nils Bruin, E. Victor Flynn, and Damiano Testa, *Descent via* $(3,3)$*-isogeny on Jacobians of genus 2 curves*, Acta Arith. **165** (2014), no. 3, 201–223, DOI 10.4064/aa165-3-1. MR3263947

[4] John Coates, Takako Fukaya, Kazuya Kato, and Ramdorai Sujatha, *Root numbers, Selmer groups, and non-commutative Iwasawa theory*, J. Algebraic Geom. **19** (2010), no. 1, 19–97, DOI 10.1090/S1056-3911-09-00504-9. MR2551757

[5] Fritz-Erdmann Diederichsen, *Über die Ausreduktion ganzzahliger Gruppendarstellungen bei arithmetischer Äquivalenz* (German), Abh. Math. Sem. Hansischen Univ. **13** (1940), 357–412. MR0002133

[6] Tim Dokchitser, *Computing special values of motivic L-functions*, Experiment. Math. **13** (2004), no. 2, 137–149. MR2068888

[7] T. Dokchitser, V. Dokchitser, C. Maistret, and A. Morgan, *Semistable types of hyperelliptic curves*, arXiv:1704.08338 (2017), to appear in Contemporary Mathematics.

[8] Tim Dokchitser and Vladimir Dokchitser, *Quotients of hyperelliptic curves and Étale cohomology*, Q. J. Math. **69** (2018), no. 2, 747–768, DOI 10.1093/qmath/hax053. MR3815163

[9] T. Dokchitser, V. Dokchitser, C. Maistret, and A. Morgan, *Arithmetic of hyperelliptic curves over local fields*, arXiv:1808.02936 (2018).

[10] T. Dokchitser, V. Dokchitser, and A. Morgan, *Tate module and bad reduction*, arXiv:1809.10208 (2018).

[11] C. Doris, PhD thesis, in preparation.

[12] C. Doris, `ExactpAdics`:*An exact representation of p-adic numbers*, arXiv:1805.09794 (2018).

[13] C. Doris, *Genus2Conductor: A package for computing the conductor exponent of curves of genus 2*, https://cjdoris.github.io/Genus2Conductor.

[14] E. Victor Flynn, Franck Leprévost, Edward F. Schaefer, William A. Stein, Michael Stoll, and Joseph L. Wetherell, *Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves*, Math. Comp. **70** (2001), no. 236, 1675–1697, DOI 10.1090/S0025-5718-01-01320-5. MR1836926

[15] Christian Greve and Sebastian Pauli, *Ramification polygons, splitting fields, and Galois groups of Eisenstein polynomials*, Int. J. Number Theory **8** (2012), no. 6, 1401–1424, DOI 10.1142/S1793042112500832. MR2965757

[16] A. Grothendieck, *Modèles de Néron et monodromie*, in Groupes de monodromie en géometrie algébrique, SGA7 I, A. Grothendieck, ed., Lecture Notes in MMath., vol. 288, Springer, Berlin-Heidelberg-New York, 1972, pp. 313–523.

[17] Jordi Guàrdia, Enric Nart, and Sebastian Pauli, *Single-factor lifting and factorization of polynomials over local fields*, J. Symbolic Comput. **47** (2012), no. 11, 1318–1346, DOI 10.1016/j.jsc.2012.03.001. MR2927133

[18] Charles Helou, *Non-Galois ramification theory of local fields*, Algebra Berichte [Algebra Reports], vol. 64, Verlag Reinhard Fischer, Munich, 1990. MR1076620

[19] Franz-Viktor Kuhlmann, *Maps on ultrametric spaces, Hensel's lemma, and differential equations over valued fields*, Comm. Algebra **39** (2011), no. 5, 1730–1776, DOI 10.1080/00927871003789157. MR2821504

[20] Claus Lehr and Michel Matignon, *Wild monodromy and automorphisms of curves*, Duke Math. J. **135** (2006), no. 3, 569–586, DOI 10.1215/S0012-7094-06-13535-4. MR2272976

[21] Qing Liu, *Courbes stables de genre 2 et leur schéma de modules* (French), Math. Ann. **295** (1993), no. 2, 201–222, DOI 10.1007/BF01444884. MR1202389

[22] Qing Liu, *Modèles minimaux des courbes de genre deux* (French), J. Reine Angew. Math. **453** (1994), 137–164, DOI 10.1515/crll.1994.453.137. MR1285783

[23] LMFDB, *L-functions and modular forms database*, www.lmfdb.org.

[24] Yukihiko Namikawa and Kenji Ueno, *The complete classification of fibres in pencils of curves of genus two*, Manuscripta Math. **9** (1973), 143–186, DOI 10.1007/BF01297652. MR0369362

[25] A. P. Ogg, *Elliptic curves and wild ramification*, Amer. J. Math. **89** (1967), 1–21, DOI 10.2307/2373092. MR0207694

[26] Sebastian Pauli and Brian Sinclair, *Enumerating extensions of* (π)*-adic fields with given invariants*, Int. J. Number Theory **13** (2017), no. 8, 2007–2038, DOI 10.1142/S1793042117501081. MR3681687

[27] Irving Reiner, *Integral representations of cyclic groups of prime order*, Proc. Amer. Math. Soc. **8** (1957), 142–146, DOI 10.2307/2032829. MR0083493

[28] Takeshi Saito, *Conductor, discriminant, and the Noether formula of arithmetic surfaces*, Duke Math. J. **57** (1988), no. 1, 151–173, DOI 10.1215/S0012-7094-88-05706-7. MR952229

[29] C. Schembri, *Examples of genuine false elliptic curves which are modular*, arXiv: 1804.07225 (2018), to appear.

[30] Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517, DOI 10.2307/1970722. MR0236190

[31] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Lecture Notes in Math., vol. 476, Springer, Berlin, 1975, pp. 33–52. MR0393039

[32] Douglas Ulmer, *Conductors of* ℓ*-adic representations*, Proc. Amer. Math. Soc. **144** (2016), no. 6, 2291–2299, DOI 10.1090/proc/12880. MR3477046

Department of Mathematics, University of Bristol, Bristol BS8 1TW, United Kingdom

Email address: `tim.dokchitser@bristol.ac.uk`

Department of Mathematics, University of Bristol, Bristol BS8 1TW, United Kingdom

Email address: `christopher.doris@bristol.ac.uk`