A NOTE ON HYPERELLIPTIC CURVES WITH ORDINARY REDUCTION OVER 2-ADIC FIELDS

VLADIMIR DOKCHITSER AND ADAM MORGAN

Abstract. We study a class of semistable ordinary hyperelliptic curves over 2-adic fields and the special fibre of their minimal regular model. We show that these curves can be controlled using 'cluster pictures', similarly to the case of odd residue characteristic.

1. Introduction

Let K be a finite extension of $\mathbb{Q}_p$ and $C/K : y^2 = f(x)$ be a hyperelliptic curve of genus $g \geq 2$. If p is odd then the reduction of C can often be described explicitly in terms of the p-adic distances between the roots of $f(x)$ (see e.g. [6, 10, 4, 11, 20] and the references therein). By contrast, when $p = 2$ these results, which all exploit the fact that the 'x-coordinate' morphism $C \to \mathbb{P}^1_K$ has degree coprime to p, no longer apply. More naively, one can already see that extra difficulties must arise upon noting that no short form Weierstrass equation ever defines a smooth curve over a field of characteristic 2; at the very least one must instead work with Weierstrass equations of the shape $y^2 + Q(x)y = P(x)$ to have a hope of giving explicit equations for components of the reduction.

In spite of the above, for applications to global problems it is often desirable to represent a hyperelliptic curve over $\mathbb{Q}$ (or some other number field) by a short form Weierstrass equation and say something about its reduction at all primes p. This is the situation in [7], for example, in which the 2-parity conjecture is proven for a broad class of Jacobians of genus 2 curves, ultimately via a comparison of their local invariants. The principal aim of the present article is to produce a reasonable stock of examples for which such local comparisons may readily be carried out at $p = 2$. As we shall see, this includes in particular all curves having good ordinary reduction.

1.1. **Weierstrass equations of ordinary curves.**

In what follows, K denotes a finite extension of $\mathbb{Q}_2$ with residue field k and ring of integers $\mathcal{O}_K$. We denote by K^{nr} the maximal unramified extension of K, and denote by $\bar{K}$ the algebraic closure of K. Denote by $v : K^\times \twoheadrightarrow \mathbb{Z}$ the normalised valuation on K. We denote by v also the extension of this to $\bar{K}^\times$.

Let C/K be a hyperelliptic curve of genus $g \geq 2$ and consider the following property:

2010 *Mathematics Subject Classification.* 11G20 (14D10, 14H25, 14H45).

Notation 1.1 (Property $(\star)$)**.** We say a Weierstrass equation $y^2 = cf(x)$ for C satisfies $(\star)$ if: $c \equiv 1 \pmod 4$, $f(x) \in \mathcal{O}_K[x]$ is monic of degree $2g+2$ and squarefree, and the roots of $f(x)$ can be put into pairs $\{\alpha_1, \beta_1\}$, ..., $\{\alpha_{g+1}, \beta_{g+1}\}$ satisfying

- $(x-\alpha_i)(x-\beta_i) \in K^{nr}[x]$ for all i,
- $v(\alpha_i-\beta_i) = v(4)$ for all i,
- $v(\alpha_i-\alpha_j) = v(\beta_i-\beta_j) = v(\alpha_i-\beta_j) = 0$ for all $i \neq j$.

Our first result is then as follows:

Theorem 1.2. *If C can be represented by a Weierstrass equation satisfying $(\star)$ then C has good ordinary reduction. Conversely, if $|k| \geq g+1$ and C has good ordinary reduction, then it can be represented by a Weierstrass equation satisfying $(\star)$.*

We will prove Theorem 1.2 as part of a more general statement. To describe this we introduce the following additional properties:

Notation 1.3 (Properties $(\star\star)$ and $(\dagger)$)**.** We say that a Weierstrass equation $y^2 = cf(x)$ for C satisfies $(\star\star)$ if it satisfies the property $(\star)$ above but with the second bullet point replaced by the weaker condition

- $v(\alpha_i - \beta_i) \geq v(4)$ for all i.

We say that C has reduction type $(\dagger)$ if C/K has semistable reduction and the geometric special fibre of its stable model is either:

- irreducible with normalisation an ordinary curve, or
- a union of 2 rational curves intersecting transverally at $g+1$ points.

We then have the following result relating properties $(\star\star)$ and $(\dagger)$:

Theorem 1.4. *If C can be represented by a Weierstrass equation satisfying $(\star\star)$ then C has reduction type $(\dagger)$. Conversely, if $|k| \geq g+1$ and C has reduction type $(\dagger)$, then it can be represented by a Weierstrass equation satisfying $(\star\star)$.*

1.2. **Special fibre of the stable and minimal regular models.**

When the conditions of Theorem 1.4 are satisfied, one can moreover read off the precise structure of the stable and minimal regular models of C in a straightforward fashion.

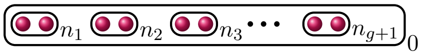
Proposition 1.5. *Suppose that C is given by a Weierstrass equation satisfying $(\star\star)$. Let $\mathcal{C}/\mathcal{O}_K$ denote the stable model of C, and let $\mathcal{C}' = \mathcal{C} \times_{\mathcal{O}_K} \mathcal{O}_{K^{nr}}$. Then the special fibre of $\mathcal{C}'$ has one ordinary double point P_i for each pair $\{\alpha_i, \beta_i\}$ with $v(\alpha_i - \beta_i) > v(4)$, and no others. Such a point P_i has thickness $2(v(\alpha_i - \beta_i) - v(4))$ in $\mathcal{C}'$.*

Remark 1.6. See e.g. [14, Definition 10.3.23] for the definition of the thickness of an ordinary double point. The minimal proper regular model of C over $\mathcal{O}_{K^{nr}}$ is obtained from the stable model by replacing each ordinary double point of thickness n by a chain of $n-1$ rational curves intersecting transversally. (To see this, arguing as in the final paragraph of the proof of [14, Theorem 10.3.34], we see that the minimal proper regular model of C over $\mathcal{O}_{K^{nr}}$ is the minimal desingularisation of the stable model. We may then conclude by [14, Corollary 10.3.25].)

We remark also that in the context of the above proposition, the geometric special fibre of the stable model is a union of 2 rational curves intersecting transversally if and only if there are precisely $g+1$ pairs or roots $\{\alpha_i, \beta_i\}$ with $v(\alpha_i - \beta_i) > v(4)$.

Note that Theorem 1.2 follows immediately from Theorem 1.4 and Proposition 1.5.

Remark 1.7. Property $(\star\star)$ can be rephrased in the language of cluster pictures [6]. Specifically, let $y^2 = cf(x)$ be a Weierstrass equation for C with $c \equiv 1 \pmod 4$ and $f(x) \in \mathcal{O}_K[x]$ monic. Then this equation satisfies $(\star\star)$ if and only if $f(x)$ has cluster picture



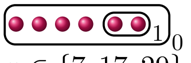
with each $n_i \geq v(4)$ and with the inertia group of K acting trivially on all proper clusters. Informally, Proposition 1.5 then says that a qualitative description of the geometric special fibre of the minimal regular model can be obtained from such a cluster picture by subtracting $v(4)$ from each n_i, and then proceeding as one would in odd residue characteristic (i.e. as described in [1, 6], say).

It seems plausible that a similarly straightforward 'cluster picture' description of the reduction of C holds (at least) whenever C is semistable and the special fibre of its stable model has normalisation a disjoint union of ordinary curves. Beyond that the situation is more delicate; see [16, 12] for a discussion of the case where $f(x)$ has 2-adically equidistant roots (i.e. when there is a single proper cluster). For an explicit description of the potential semistable reduction of an elliptic curve in terms of analagous data, see work of Yelton [21].

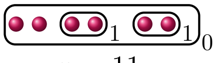
Example 1.8. Consider the genus 2 hyperelliptic curve

$$C/\mathbb{Q} : y^2 = (x-2)(x+2)(x^2+7x-1)(x^2-9x+7). \tag{1.9}$$

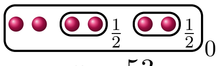
We will determine its reduction over $\mathbb{Q}_p$ for all primes p. Denote by $f(x)$ the right hand side of (1.9). Computing the discriminant of $f(x)$ we see that C has good reduction away from $\{2, 7, 11, 17, 29, 53\}$. For odd primes in this set $f(x)$ has the following cluster picture (see [6, Definition 1.1]):



$p \in \{7, 17, 29\}$



$p = 11$

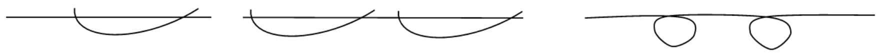


$p = 53$

Here each ● represents a root of $f(x)$. With $p = 7$, for example, the picture indicates that there are two roots whose difference has 7-adic valuation 1 — these roots form a 'cluster' of size 2 — whilst for any other pair of roots r, r' of $f(x)$ we have $\mathrm{ord}_7(r - r') = 0$. To see this is the case note that

$f(x) \pmod 7$ splits completely and has a single double root at $x = 2$. This double root accounts for the cluster of size 2, consisting of $x = 2$ and the unique root of $x^2 - 9x + 7$ congruent to $2 \pmod 7$. The valuation of the difference of these roots is 1 since $\mathrm{ord}_7(2^2 - 9 \cdot 2 + 7) = 1$.

It follows e.g. from [6, Theorem 1.11] that the geometric special fibres of the corresponding minimal regular models take the following form:



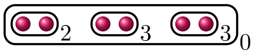
$p \in \{7, 17, 29\}$ $p = 11$ $p = 53$

That is, C has Namikawa–Ueno type (as set out in [17]): I_{2-0-0} when $p \in \{7, 17, 29\}$, I_{2-2-0} when $p = 11$, and I_{1-1-0} when $p = 53$.

To determine the reduction at $p = 2$ where the results of [6] no longer apply, note that we can rewrite $f(x)$ as

$$f(x) = \left(x^2 - 4\right)\left((x - \varphi_+)^2 - 16\right)\left((x - \varphi_-)^2 - 16\right)$$

where $\varphi_\pm = \frac{1}{2}(1 \pm \sqrt{53})$. With the roots paired as in the quadratic factors above we see that the given Weierstrass equation for C satisfies ($\star\star$) over $\mathbb{Q}_2$. From Theorem 1.4 and Proposition 1.5 we see that C has reduction type (†) over $\mathbb{Q}_2$, and that the geometric special fibre of the minimal regular model has the same form as depicted for $p = 11$ above, thus C has Namikawa–Ueno type I_{2-2-0} at $p = 2$. In fact, one sees similarly that $f(x)$ has cluster picture



so the above is consistent with Remark 1.7: substracting $\mathrm{ord}_2(4) = 2$ from the depths of the 3 clusters of size 2 yields the same cluster picture as for $p = 11$.

1.3. **Frobenius action on the special fibre.** Suppose C is given by a Weierstrass equation $y^2 = cf(x)$ satisfying ($\star\star$). One can then complement Proposition 1.5 with an explicit description of the $\mathrm{Gal}(\bar{k}/k)$-action on the dual graph of the geometric special fibres of the stable and minimal regular models. This additional information is what is needed to determine local invariants of the Jacobian of C such as its Tamagawa number and root number (see e.g. [6, Theorem 2.20, Lemma 2.22] for a recipe for computing these invariants from this data).

Recall from Proposition 1.5 that to each pair of roots $\{\alpha_i, \beta_i\}$ of $f(x)$ with $v(\alpha_i - \beta_i) > 4$, there corresponds an ordinary double point P_i on the geometric special fibre of the stable model of C. In Proposition 1.11 below we describe the $\mathrm{Gal}(\bar{k}/k)$-action on the points P_i, and give an explicit characterisation of when such a point is a *split* ordinary double point in the sense of [14, Definition 10.3.8]. This data is sufficient to determine the $\mathrm{Gal}(\bar{k}/k)$-action on the dual graph of stable model, as explained in e.g. [6, Section 2.1]. To obtain the corresponding action for the minimal regular model, one can then use Remark 1.6.

Notation 1.10. In what follows, for $w \in \mathcal{O}_{K^{nr}}$ we denote by $\overline{w}$ the reduction of w to the residue field $\bar{k}$. With the roots $\{\alpha_1, \beta_1\}$, ..., $\{\alpha_{g+1}, \beta_{g+1}\}$ paired as in Notation 1.3, define

$$\gamma_i = \frac{\alpha_i + \beta_i}{2} \quad \text{and} \quad \eta_i = \Big(\frac{\alpha_i - \beta_i}{4}\Big)^2 \qquad (1 \le i \le g+1).$$

By assumption we have $\eta_i \in \mathcal{O}_{K^{nr}}$, and since $\alpha_i + \beta_i \equiv \alpha_i - \beta_i \equiv 0 \bmod 2$ we have $\gamma_i \in \mathcal{O}_{K^{nr}}$ also. Further, define

$$a = \frac{1}{4}(c-1) \in \mathcal{O}_K \quad \text{and} \quad r_i = \overline{\gamma_i} \in \bar{k}.$$

We then have the following:

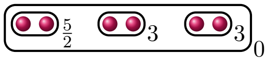
Proposition 1.11. *In the notation above, the correspondence* $\{\alpha_i, \beta_i\} \mapsto P_i$ *is equivariant for the action of* $\mathrm{Gal}(K^{nr}/K) = \mathrm{Gal}(\bar{k}/k)$*. Further,* P_i *is a split ordinary double point over* $k(P_i) = k(r_i)$ *if and only if*

$$\mathrm{Trace}_{k(r_i)/\mathbb{F}_2}\Big(\overline{a} + \sum_{j \neq i} \overline{\eta_j}(r_i - r_j)^{-2}\Big) = 0. \tag{1.12}$$

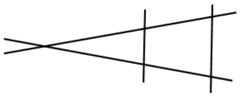
Example 1.13. Consider the genus 2 hyperelliptic curve

$$C/\mathbb{Q}_2 : y^2 = 5(x^2 - 8)(x^2 - 7x + 13)(x^2 + 9x + 21).$$

This has roots $\{\pm 2\sqrt{2}, \zeta_3 \pm 4, \zeta_3^2 \pm 4\}$ where ζ_3 is a primitive 3rd root of unity, and cluster picture



We see from Proposition 1.5 (cf. also Remark 1.7) that C is semistable and that the minimal proper regular model of C over $\mathbb{Z}_2^{nr}$ has special fibre



where each irreducible component is a rational curve.

We can use Proposition 1.11 to determine the Frobenius action on this special fibre. With the roots ordered as written, in the terminology of Notation 1.10 we have $a = 1$,

$$\gamma_1 = 0, \quad \gamma_2 = \zeta_3, \quad \gamma_3 = \zeta_3^2, \quad \eta_1 = 2, \quad \eta_2 = \eta_3 = 4.$$

Since γ_2 and γ_3 are swapped by Frobenius, so are the two components drawn vertically. Further, since $\overline{\eta_i} = 0$ for each i whilst $\overline{a} = 1$, we see from (1.12) that the pair of roots $\{\pm 2\sqrt{2}\}$ corresponds to a non-split ordinary double point. Thus Frobenius swaps the two components drawn horizontally also.

We remark that in fact, as one can show using Remark 3.5, the special fibre of the stable model of C over $\mathbb{Z}_2$ is given explicitly by the equation

$$\big(y + \zeta_3(x^3 + x^2 + x)\big)\,\big(y + \zeta_3^2(x^3 + x^2 + x)\big) = 0,$$

whose two (geometric) components are visibly swapped by Frobenius.

Remark 1.14. In the above example we conclude that $C(\mathbb{Q}_2) = \emptyset$, since each irreducible component of the special fibre has an even-sized $\mathrm{Gal}(\bar{\mathbb{F}}_2/\mathbb{F}_2)$-orbit. In fact, arguing similarly, we have $C(K) = \emptyset$ for every odd degree extension $K/\mathbb{Q}_2$. Thus C is *deficient* in the sense of [18, Section 8].

1.4. **Reduction map on 2-torsion.** Suppose that C is given by a Weierstrass equation satisfying ($\star$), hence has good ordinary reduction by Theorem 1.2. Then the Néron model $\mathcal{J}/\mathcal{O}_K$ of the Jacobian J/K of C is an abelian scheme, and we have an associated reduction map $J[2] \to \overline{J}(\bar{k})[2]$ on 2-torsion points. Here $\overline{J}$ denotes the special fibre of $\mathcal{J}$. Motivated by applications to the parity conjecture (see [7, Theorem A.1], for example) we record an explicit description of the kernel of this reduction map in terms of the roots of $f(x)$, the set of which we denote $\mathcal{R}$.

Recall that $J[2]$ can be identified with the collection of even-sized subsets $S \subseteq \mathcal{R}$, with addition corresponding to symmetric difference, and along with the relations identifying S with $\mathcal{R} \setminus S$ for each such S. This correspondence is realised explicitly by sending $S \subseteq \mathcal{R}$ to the class of the divisor

$$D_S = \sum_{r \in S} P_r - \frac{|S|}{2}(\infty^+ + \infty^-), \tag{1.15}$$

where $P_r = (r, 0)$. For a proof see e.g. [8, Section 5.2.2]. The result is now the following:

Proposition 1.16. *With the notation above, and with the roots of $f(x)$ paired as in Notation 1.1, the kernel of the reduction map $J[2] \to \overline{J}(\bar{k})[2]$ is generated by the subsets $\{\alpha_i, \beta_i\}$ for $1 \leq i \leq g+1$.*

Remark 1.17. For an elliptic curve E/K presented in short Weierstrass form (and with arbitrary reduction type), a similarly explicit description of the reduction map on 2-torsion points is given in the work of Yelton [21, Corollary 6, Remark 7].

1.5. **Layout.** In Section 2 we review some properties of Weierstrass equations over fields of characteristic 2 which will be used later. Section 3 then proves all results mentioned above, beginning with Theorem 1.4 and Proposition 1.5. For explicit equations defining the special fibre of the stable model when C is given by a Weierstrass equation satisfying ($\star\star$), see Remark 3.5.

1.6. **Notation and conventions.** The following notation and conventions will be used throughout the the paper.

By a *hyperelliptic curve* over a field F we mean a smooth proper geometrically connected curve C/F equipped with a finite separable k-morphism $C \to \mathbb{P}^1_F$ of degree 2. We say that C is ordinary if its Jacobian is (however 'good' in Theorem 1.2 refers to good reduction of the curve rather than the weaker property of good reduction of its Jacobian).

Let R be a commutative ring. By a *Weierstrass equation* over R we mean an equation

$$y^2 + Q(x)y = P(x) \tag{1.18}$$

where $P(x), Q(x) \in R[x]$ are polynomials with $\max\{2\deg Q, \deg P\} \in \{2g+1, 2g+2\}$ for some $g \geq 2$. By the scheme X defined by this Weierstrass equation we mean the R-scheme given by gluing the affine charts (1.18) and

$$z^2 + t^{g+1}Q(1/t)z = t^{2g+2}P(1/t) \tag{1.19}$$

via the change of variables $x = 1/t$ and $t^{g+1}y = z$.

For a nonarchimedean local field K, ring of integers $\mathcal{O}_K$ and residue field k, given $w \in \mathcal{O}_K$ we denote by $\overline{w}$ the reduction of w to k. For a polynomial $Q(x) \in \mathcal{O}_K[x]$ we denote by $\overline{Q}(x) \in k[x]$ the reduced polynomial.

2. Weierstrass equations in characteristic 2

Let F be an algebraically closed field of characteristic 2. Let $g \geq 2$ and let C be the curve defined by a Weierstrass equation (1.18) over F with $\deg Q = g + 1$. Denote by $\mathcal{R}$ the set of roots of $Q(x)$ in F. The map $(x, y) \mapsto x$ defines a finite separable morphism $C \to \mathbb{P}^1_F$ of degree 2 which ramifies precisely at the points $P_r = (r, \sqrt{P(r)})$ for $r \in \mathcal{R}$. There are 2 points lying over the point at infinity on $\mathbb{P}^1_F$; we denote these $\infty^{\pm}$.

2.1. **Smooth Weierstrass equations.**

Suppose the curve C is smooth (this can, for example, be detected by the discriminant of the Weierstrass equation; see e.g. [15] or [13, Section 2]). Then C is a genus g hyperelliptic curve over F. Conversely, any hyperelliptic curve X/F of genus $g \geq 2$ can be given by a Weierstrass equation of the form (1.18) with $\deg Q = g + 1$ (cf. [14, Proposition 7.4.24]). Denote by J the Jacobian of C.

Lemma 2.1. *The group $J(F)[2]$ can be identified with the collection of even-sized subsets $S \subseteq \mathcal{R}$, with addition corresponding to symmetric difference. Explicitly, $S \subseteq \mathcal{R}$ corresponds to the class of the divisor*

$$D_S = \sum_{r \in S} P_r - \frac{|S|}{2}(\infty^+ + \infty^-).$$

Proof. This is well known; see, for example, the proof of [5, Theorem 23] (cf. also work of Elkin–Pries [9]). □

Remark 2.2. By Lemma 2.1 we have $\dim J(F)[2] = |\mathcal{R}| - 1$. In particular, C is ordinary if and only if $Q(x)$ is separable. Whilst we have a running assumption that $g \geq 2$, we note that this equivalence also holds when $g = 1$, i.e. for Weierstrass equations $y^2 + Q(x)y = P(x)$ where $\deg Q = 2$ and $\deg P \leq 4$.

2.2. **Semistable Weierstrass equations.**

We continue to suppose that C is given by a Weierstrass equation (1.18), but do not assume that C is smooth.

Lemma 2.3. *The curve C is semistable with normalisation a disjoint union of ordinary curves if and only if $Q(x)$ is separable.*

Proof. From the Jacobian criterion one sees that C is smooth away from the points P_r for $r \in \mathcal{R}$, and that such a point is smooth if and only if $P'(r)^2 + P(r)Q'(r)^2 \neq 0$. Moreover, when $P'(r)^2 + P(r)Q'(r)^2 = 0$ the point P_r is an ordinary double point if and only if r is a simple root of $Q(x)$. For such a point P_r, consider the curve C_1 with Weierstrass equation

$$w^2 + \frac{Q(x)}{x-r}w = \frac{P(x) + P(r) + Q(x)\sqrt{P(r)}}{(x-r)^2}$$

(our assumptions force each side of this equation to lie in $F[x,w]$). The morphism $C' \to C$ defined by

$$(x,w) \longmapsto \Big(x, (x-r)w + \sqrt{P(r)}\Big) \tag{2.4}$$

realises C' as the partial normalisation of C at the point P_r.

Suppose that C has t ordinary double points in total, corresponding to distinct roots $r_1, ..., r_t$ of $Q(x)$, say. We conclude from the above that the normalisation of C is given by a Weierstrass equation of the form

$$y^2 + \widetilde{Q}(x)y = \widetilde{P}(x)$$

where $\widetilde{Q}(x) = Q(x)\prod_{i=1}^{t}(x-r_i)^{-1}$ and $\widetilde{P}(x)$ is a polynomial of degree at most $2(g-t)+2$. By Remark 2.2 such a curve is ordinary if and only if $\widetilde{Q}(x)$ is separable, from which the result follows. □

3. Proofs of the main results

Let K be a finite extension of $\mathbb{Q}_2$, $\mathcal{O}_K$ and k its ring of integers and residue field respectively, and v its normalised valuation.

3.1. Proofs of Theorem 1.4 and Proposition 1.5.

Lemma 3.1. *Suppose $|k| \geq g+1$ and that C has reduction type (†). Then C can be represented by a Weierstrass equation satisfying ($\star\star$).*

Proof. Let $\mathcal{C}/\mathcal{O}_K$ denote the stable model of C and let ι denote the extension of the hyperelliptic involution to $\mathcal{C}$. By [19, Appendice], the quotient $\mathcal{C}/\iota$ is a semistable model of $\mathbb{P}^1_K$ whose special fibre, by assumption, consists of a single geometrically irreducible component (if the geometric special fibre of $\mathcal{C}$ is a union of 2 rational curves intersecting transversally then these are necessarily be swapped by ι). We conclude that the special fibre of $\mathcal{C}/\iota$ is isomorphic to $\mathbb{P}^1_k$. Thus $\mathcal{C}$ is a *Weierstrass model* for C in the sense of [13, Definition 6], so can be represented by a Weierstrass equation (1.18) over $\mathcal{O}_K$ (cf. [13, Section 4.3]). Since $|k| \geq g+1$ we can moreover assume that the reduction $\overline{Q}(x)$ has degree $g+1$, and then that $Q(x)$ is monic. Applying Lemma 2.3 to the reduced Weierstrass equation we see that $\overline{Q}(x)$ is separable.

Completing the square in (1.18) and scaling y by 2 shows that C can be represented by the Weierstrass equation $y^2 = Q(x)^2 + 4P(x)$. Write $Q(x)^2 + 4P(x) = cf(x)$ for $f(x)$ monic of degree $2g+2$, noting that $c \equiv$

1 mod 4 and that $f(x)$ is in $\mathcal{O}_K[x]$. Write $\gamma_1, \ldots, \gamma_{g+1}$ for the roots of $Q(x)$, all of which lie in in K^{nr} since $\overline{Q}(x)$ is separable. Since $f(x) \equiv Q(x)^2$ mod 4, by Hensel's lemma for lifting coprime factorisations (see [3, III.4.3 Theorem 1]) we can factor $f(x)$ over K^{nr} as

$$f(x) = \prod_{i=1}^{g+1} f_i(x)$$

with each $f_i(x) \in \mathcal{O}_{K^{nr}}[x]$ monic quadratic satisfying $f_i(x) \equiv (x-\gamma_i)^2$ mod 4. Since $f_i(x+\gamma_i) \equiv x^2$ mod 4 the discriminant of $f_i(x)$ is congruent to 0 modulo 16, so factoring $f_i(x) = (x-\alpha_i)(x-\beta_i)$ over $\bar{K}$ we find $v(\alpha_i - \beta_i) \geq v(4)$. Finally, since $\overline{f_i}(x) = (x - \overline{\gamma_i})^2$ we have $\overline{\alpha_i} = \overline{\gamma_i} = \overline{\beta_i}$ for each i, hence separability of $\overline{Q}(x)$ gives $v(\alpha_i - \alpha_j) = v(\beta_i - \beta_j) = v(\alpha_i - \beta_j) = 0$ for $i \neq j$. Thus $y^2 = cf(x)$ is a Weierstrass equation for C of the desired form. □

To complete the proof of Theorem 1.4 it remains to study hyperelliptic curves C given by a Weierstrass equation satisfying ($\star\star$). It will be convenient to introduce the following notation.

Notation 3.2 (cf. Notation 1.10)**.** Suppose that C is given by a Weierstrass equation satisfying ($\star\star$). Define

$$f_i(x) = (x-\alpha_i)(x-\beta_i), \quad \gamma_i = \frac{\alpha_i + \beta_i}{2}, \quad \eta_i = \big(\frac{\alpha_i - \beta_i}{4}\big)^2.$$

As explained in Notation 1.10 we have $\eta_i, \gamma_i \in \mathcal{O}_{K^{nr}}$. Further, we have

$$f(x) = \prod_{i=1}^{g+1} f_i(x) \quad \text{and} \quad f_i(x) = (x-\gamma_i)^2 - 4\eta_i. \tag{3.3}$$

Next, set

$$Q(x) = \prod_{i=1}^{g+1} (x - \gamma_i) \quad \text{and } P(x) = \frac{1}{4}(cf(x) - Q(x)^2).$$

By (3.3) we have $f(x) \equiv Q(x)^2 \pmod 4$ so, since $c \equiv 1 \pmod 4$, we have $P(x) \in \mathcal{O}_K[x]$. Finally, write

$$a = \frac{1}{4}(c-1) \in \mathcal{O}_K \quad \text{and} \quad r_i = \overline{\gamma_i} \in \bar{k}.$$

Note that $\alpha_i - \gamma_i = \frac{\beta_i - \alpha_i}{2} \equiv 0$ mod 2 so that $\gamma_i \equiv \alpha_i$ mod 2. In particular, the r_i are all distinct, and $\overline{Q}(x)$ is separable.

Lemma 3.4. *Suppose that C is given by a Weierstrass equation satisfying ($\star\star$). Then C has semistable reduction and, with $P(x)$ and $Q(x)$ as defined in Notation 3.2, the stable model of C is the $\mathcal{O}_K$-scheme defined by the Weierstrass equation $y^2 + Q(x)y = P(x)$. Moreover, C satisfies (†).*

Proof. Reversing the change of variables described in the proof of Lemma 3.1 we see that C/K is represented by the integral Weierstrass equation $y^2{+}Q(x)y = P(x)$. As explained in Notation 3.2 above, $\overline{Q}(x)$ has degree $g{+}1$ and is separable. Denote by $\mathcal{C}/\mathcal{O}_K$ the scheme defined by the Weierstrass equation $y^2 + Q(x)y = P(x)$. By Lemma 2.3 this is a semistable model of C.

Suppose first that the geometric special fibre of $\mathcal{C}$ is irreducible. Then $\mathcal{C}$ is necessarily the stable model of C. Further, since the normalisation of the special fibre of $\mathcal{C}$ is ordinary by Lemma 2.3, we conclude that C satisfies (†).

It remains to consider the case where the geometric special fibre of $\mathcal{C}$ is reducible. Under this assumption, we can find polynomials $\lambda(x), \mu(x)$ in $\bar{\mathbb{F}}_2[x]$ so that

$$y^2 + \overline{Q}(x)y + \overline{P}(x) = (y + \lambda(x))\,(y + \mu(x))\,.$$

We thus see that the geometric special fibre of $\mathcal{C}$ consists of two rational curves intersecting at the $g+1$ roots of $\lambda(x) + \mu(x) = \overline{Q}(x)$. Since $\mathcal{C}$ is semistable, each of these intersections is necessarily transversal. Thus again we conclude that $\mathcal{C}$ is the stable model of C, and that C satisfies (†). □

Theorem 1.4 now follows from combining Lemma 3.1 and Lemma 3.4.

Proof of Proposition 1.5. Let C be given by a Weierstrass equation satisfying ($\star\star$). See Notation 3.2 for the quantities appearing below. As in Lemma 3.4, the stable model $\mathcal{C}/\mathcal{O}_K$ of C is given by the Weierstrass equation $y^2 + Q(x)y = P(x)$. Denote by $\mathcal{C}' = \mathcal{C} \times_{\mathcal{O}_K} \mathcal{O}_{K^{nr}}$ the base-change of $\mathcal{C}$ to $\mathcal{O}_{K^{nr}}$. Then (as in the proof of Lemma 2.3) $\mathcal{C}'$ is smooth away from the points $P_i = (r_i, \sqrt{P(r_i)})$ $(1 \leq i \leq g+1)$ on its the special fibre.

For each i we now compute the completed local ring $\widehat{\mathcal{O}}_{\mathcal{C}',P_i}$ of $\mathcal{C}'$ at P_i. Reordering the roots and translating x we suppose $i = 1$ and $\gamma_i = 0$. Write $Q(x) = x\widetilde{Q}(x)$. Further, write $f(x) = f_1(x)\widetilde{f}(x)$ where $\widetilde{f}(x) = \prod_{j=2}^{g+1} f_j(x)$. As in (3.3) we have $f_1(x) = x^2 - 4\eta_1$, whilst $\widetilde{f}(x) \equiv \widetilde{Q}(x)^2 \pmod 4$.

Claim. There is $G(x) \in \mathcal{O}_{K^{nr}}[[x]]^\times$ with

$$G(x) \equiv \widetilde{Q}(x) \pmod 2 \qquad \text{and} \qquad G(x)^2 = c\widetilde{f}(x).$$

Proof of claim. Let $R = \mathcal{O}_{K^{nr}}[[x]]$, write $c\widetilde{f}(x) = \widetilde{Q}(x)^2 + 4\widetilde{P}(x)$ for some $\widetilde{P}(x) \in \mathcal{O}_{K^{nr}}[x]$, and define $h(t) = t^2 - t\widetilde{Q} - \widetilde{P} \in R[t]$. Since R is Henselian and $\widetilde{Q}(0)$ is a unit in $\mathcal{O}_{K^{nr}}$, there is $G_0 \in R$ with $h(G_0) = 0$. Then $G = 2G_0 - \widetilde{Q}$ has the required properties. □

With $G(x)$ as in the claim, set $u = G(x)^{-1}\big(y + x \cdot \frac{\widetilde{Q}(x) - G(x)}{2}\big)$. A straightforward computation gives

$$y^2 + Q(x)y - P(x) = G(x)^2(u^2 + ux + \eta_1).$$

It follows that $\widehat{\mathcal{O}}_{\mathcal{C}',P_{r_1}}$ is isomorphic to the completed local ring of the scheme

$$u^2 + ux + \eta_1 = 0 \subseteq \mathbb{A}^2_{\mathcal{O}_{K^{nr}}}$$

at the closed point $x = 0$, $u = \sqrt{\overline{\eta_1}}$ on its special fibre. If $v(\alpha_1 - \beta_1) = v(4)$ then $\overline{\eta_1} \neq 0$ and this scheme is smooth. On the other hand, if $v(\alpha_1 - \beta_1) > v(4)$ then $\overline{\eta_1} = 0$ and, setting $v = u + x$, we see that the sought completed local ring is isomorphic to

$$\widehat{\mathcal{O}_{K^{nr}}}[[u, v]]/\big(uv+\eta_1\big).$$

We thus see that P_1 has thickness $v(\eta_1) = 2(v(\alpha_1 - \beta_1) - v(4))$ in $\mathcal{C}'$. □

Remark 3.5. Suppose that C is given by a Weierstrass equation satisfying $(\star\star)$. By Lemma 3.4 the special fibre of the stable model of C is given by the Weierstrass equation $y^2 + \overline{Q}(x)y = \overline{P}(x)$. With the quantities as in Notation 3.2 we have $\overline{Q}(x) = \prod_{i=1}^{g+1}(x - r_i)$. The polynomial $\overline{P}(x)$ is given explicitly by the formula

$$\overline{P}(x) = \overline{a}\overline{Q}(x)^2 + \sum_{i=1}^{g+1} \overline{\eta_i} \prod_{j \neq i} (x - r_j)^2. \tag{3.6}$$

To see this note that from (3.3) we have

$$cf(x) = (1 + 4a) \prod_{i=1}^{g+1} \big((x - \gamma_i)^2 - 4\eta_i\big).$$

Expanding out the righthand side, using the definition of $P(x)$, and reducing to the residue field recovers (3.6).

In particular we see from (3.6) that if $i \in \{1, ..., g + 1\}$ is such that $v(\alpha_i - \beta_i) > v(4)$, hence $\overline{\eta_i} = 0$, then we have

$$\overline{P}(r_i) = 0. \tag{3.7}$$

3.2. **Frobenius action on the special fibre.** It follows readily from the explicit equations for the special fibre of the stable model given in Remark 3.5 that the Frobenius action takes the form asserted in Proposition 1.11.

Proof of Proposition 1.11. As in the statement of the proposition we assume that C is given by a Weierstrass equation of the shape $(\star\star)$. Let $\mathcal{C}/\mathcal{O}_K$ denote its stable model, as described explicitly in Remark 3.5. From the proof of Proposition 1.5 we see that the bijection between ordinary double points on $\mathcal{C}_{\bar{k}}$ and pairs $\{\alpha_i, \beta_i\}$ of roots of $f(x)$ with $v(\alpha_i - \beta_i) > v(4)$ sends a pair $\{\alpha_i, \beta_i\}$ to the point $P_i = (r_i, 0)$ on the special fibre $y^2 + \overline{Q}(x)y = \overline{P}(x)$ of $\mathcal{C}$. The $\mathrm{Gal}(\bar{k}/k)$-equivariance of the map $\{\alpha_i, \beta_i\} \mapsto P_i$ is clear, and we note also that $k(P_i) = k(r_i)$. From the explicit normalisation map (2.4) we see that P_i is a split ordinary double point over $k(P_i)$ if and only if the quadratic equation

$$\begin{aligned} w^2+\overline{Q}'(r_i)w &= \left.\frac{\overline{P}(x)+\overline{P}(r_i)+\overline{Q}(x)\sqrt{\overline{P}(r_i)}}{(x-r_i)^2}\right|_{x=r_i} \\ &\overset{(3.7)}{=} \left.\frac{\overline{P}(x)}{(x-r_i)^2}\right|_{x=r_i} \\ &\overset{(3.6)}{=} \overline{a}\overline{Q}'(r_i)^2+\sum_{j\neq i}\overline{\eta_j}\prod_{s\neq i,j}(r_i-r_s)^2 \end{aligned}$$

is soluble over $k(r_i)$. This latter condition is equivalent to (1.12), as can be seen by replacing w by $\overline{Q}'(r_i)w$ and considering the trace to $\mathbb{F}_2$ of the resulting equation. □

3.3. **Reduction map on 2-torsion.** Now suppose that C is given by a Weierstrass equation $y^2=cf(x)$ satisfying $(\star)$. As in Section 1.4 we denote by $\mathcal{R}$ the set of roots of $f(x)$ in $\bar{K}$. For each even sized subset $S\subseteq\mathcal{R}$ we let D_S denote the divisor defined in (1.15), whose class defines a 2-torsion point on the Jacobian J of C.

Proof of Proposition 1.16. Let $P(x)$ and $Q(x)$ be as in Notation 3.2. By Lemma 3.4 the $\mathcal{O}_K$-scheme $\mathcal{C}$ defined by the integral Weierstrass equation $y^2+Q(x)y=P(x)$ realises the good reduction of C. In particular, by [2, Theorem 9.5.1] the Néron model of J agrees with the identity component of the relative Picard functor $\mathrm{Pic}^0_{\mathcal{C}/\mathcal{O}_K}$. For $S\subseteq\mathcal{R}$ with $|S|$ even it follows that the reduction map $J(\bar{K})\to\overline{J}(\bar{k})$ sends (the class of) the divisor D_S to the (class of the) divisor $\sum_{r\in S}P_{\bar{r}}-\frac{|S|}{2}(\infty^++\infty^-)$ on $\mathcal{C}_{\bar{k}}$, where here $P_{\bar{r}}=(\bar{r},\sqrt{P(\bar{r})})$. The result now follows from Lemma 2.1. □

Acknowledgments. The first author is supported by a Royal Society Research Fellowship. The second author is supported by the Engineering and Physical Sciences Research Council (EPSRC) grant EP/V006541/1 'Selmer groups, Arithmetic Statistics and Parity Conjectures'.

References

[1] A. J. Best, L. A. Betts, M. Bisatt, R. van Bommel, V. Dokchitser, O. Faraggi, S. Kunzweiler, C. Maistret, A. Morgan, S. Muselli, and S. Nowell. A user's guide to the local arithmetic of hyperelliptic curves. *To appear in Bulletin of the London Mathematical Society.*

[2] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models*, volume 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1990.

[3] Nicolas Bourbaki. *Éléments de mathématique.* Masson, Paris, 1985. Algèbre commutative. Chapitres 1 à 4. [Commutative algebra. Chapters 1–4], Reprint.

[4] Irene I. Bouw and Stefan Wewers. Computing L-functions and semistable reduction of superelliptic curves. *Glasg. Math. J.*, 59(1):77–108, 2017.

[5] Wouter Castryck, Marco Streng, and Damiano Testa. Curves in characteristic 2 with non-trivial 2-torsion. *Adv. Math. Commun.*, 8(4):479–495, 2014.

[6] Tim Dokchitser, Vladimir Dokchitser, Céline Maistret, and Adam Morgan. Arithmetic of hyperelliptic curves over local fields. *To appear in Mathematische Annalen.*

[7] Vladimir Dokchitser and Celine Maistret. Parity conjecture for abelian surfaces. *Preprint*, arxiv: 1911.04626, 2019.

[8] Igor V. Dolgachev. *Classical algebraic geometry: a modern view.* Cambridge University Press, Cambridge, 2012.

[9] Arsen Elkin and Rachel Pries. Ekedahl-Oort strata of hyperelliptic curves in characteristic 2. *Algebra and Number Theory*, 7(3):507–532, 2013.

[10] Omri Faraggi and Sarah Nowell. Models of hyperelliptic curves with tame potentially semistable reduction. *Trans. London Math. Soc.*, 7(1):49–95, 2020.

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

[12] Claus Lehr and Michel Matignon. Wild monodromy and automorphisms of curves. *Duke Math. J.*, 135(3):569–586, 2006.

[13] Qing Liu. Modèles entiers des courbes hyperelliptiques sur un corps de valuation discrète. *Trans. Amer. Math. Soc.*, 348(11):4577–4610, 1996.

[14] Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics.* Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.

[15] Paul Lockhart. On the discriminant of a hyperelliptic curve. *Trans. Amer. Math. Soc.*, 342(2):729–752, 1994.

[16] Michel Matignon. Vers un algorithme pour la réduction stable des revêtements p-cycliques de la droite projective sur un corps p-adique. *Math. Ann.*, 325(2):323–354, 2003.

[17] Yukihiko Namikawa and Kenji Ueno. The complete classification of fibres in pencils of curves of genus two. *Manuscripta Math.*, 9:143–186, 1973.

[18] Bjorn Poonen and Michael Stoll. The Cassels-Tate pairing on polarized abelian varieties. *Ann. of Math. (2)*, 150(3):1109–1149, 1999.

[19] Michel Raynaud. p-groupes et réduction semi-stable des courbes. In *The Grothendieck Festschrift, Vol. III*, volume 88 of *Progr. Math.*, pages 179–197. Birkhäuser Boston, Boston, MA, 1990.

[20] Padmavathi Srinivasan. Conductors and minimal discriminants of hyperelliptic curves: A comparison in the tame case. *Preprint*, arXiv:1910.08228, 2019.

[21] Jeffrey Yelton. Semistable models of elliptic curves over residue characteristic 2. *Canad. Math. Bull.*, 64(1):154–162, 2021.

University College London, London WC1H 0AY, UK
Email address: v.dokchitser@ucl.ac.uk

University of Glasgow, Glasgow, G12 8QQ.
Email address: adam.morgan@glasgow.ac.uk