J. Aust. Math. Soc. **96** (2014), 354–385
doi:10.1017/S1446788714000044

FROM SEPARABLE POLYNOMIALS TO NONEXISTENCE OF RATIONAL POINTS ON CERTAIN HYPERELLIPTIC CURVES

NGUYEN NGOC DONG QUAN

(Received 6 November 2012; accepted 29 October 2013)

Communicated by J. Borwein

Abstract

We give a separability criterion for the polynomials of the form

$$ax^{2n+2} + (bx^{2m} + c)(dx^{2k} + e).$$

Using this separability criterion, we prove a sufficient condition using the Brauer–Manin obstruction under which curves of the form

$$z^2 = ax^{2n+2} + (bx^{2m} + c)(dx^{2k} + e)$$

have no rational points. As an illustration, using the sufficient condition, we study the arithmetic of hyperelliptic curves of the above form and show that there are infinitely many curves of the above form that are counterexamples to the Hasse principle explained by the Brauer–Manin obstruction.

2010 *Mathematics subject classification*: primary 14G05; secondary 11G35, 11G30.

Keywords and phrases: Azumaya algebras, Brauer groups, Brauer–Manin obstruction, Hasse principle, hyperelliptic curves.

1. Introduction

Let $\mathcal{V}$ be a smooth geometrically irreducible variety defined over a global field k. A fundamental problem in arithmetic geometry is to determine what the set of k-rational points on $\mathcal{V}$ is. The problem is widely open even in the case where $\mathcal{V}$ is an algebraic irreducible curve. One of the most celebrated theorems dealing with the understanding of the set of rational points on curves of genus greater than one is Faltings' theorem, or equivalently the Mordell conjecture, which says that an algebraic irreducible curve of genus greater than one over a number field has finitely many rational points. Despite this striking result, there exists no known algorithm that determines what the set of

The author was supported by a postdoctoral fellowship at the Department of Mathematics, University of British Columbia, during the preparation of this paper.

rational points on a curve looks like, or says whether or not an algebraic irreducible curve over a number field possesses a rational point.

Take an algebraic irreducible curve C over $\mathbb{Q}$, and for each prime p including $p = \infty$, let $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ be *the* embedding of $\mathbb{Q}$ into $\mathbb{Q}_p$. Under these embeddings, one can view C as a curve over $\mathbb{Q}_p$ for each prime p, and one can ask what the relationship is between the set of all $\mathbb{Q}$-rational points on C and that of all $\mathbb{Q}_p$-rational points on C for each prime p. It is not difficult to realize that if $C(\mathbb{Q}_p) = \emptyset$ for some prime p, then it follows immediately that C has no $\mathbb{Q}$-rational points. Thus, in an ideal setting and with some skill, this fact provides a *simple* way to show that $C(\mathbb{Q})$ is empty by proving that C has no $\mathbb{Q}_p$-points for some prime p. To add some interest, we assume that $C(\mathbb{Q}_p) \neq \emptyset$ for each prime p including $p = \infty$. The *Hasse principle* expects that C should have a $\mathbb{Q}$-rational point. The Hasse principle fails in general, and even does not hold in the case where C is of genus one; for example, the Lind–Reichardt curve [9, 11] defined by

$$2z^2 = x^4 - 17$$

has points over each $\mathbb{Q}_p$ including $p = \infty$ whereas it possesses no points over $\mathbb{Q}$.

Recall that the *Hasse reciprocity law* [12] states that the sequence of abelian groups

$$0 \to \mathrm{Br}(\mathbb{Q}) \to \bigoplus_p \mathrm{Br}(\mathbb{Q}_p) \to \mathbb{Q}/\mathbb{Z} \to 0$$

is exact, where the third map is the sum of the local invariant maps from local class field theory. For each scheme $\mathcal{X}$, we denote by $\mathrm{Br}(\mathcal{X})$ the Brauer group of $\mathcal{X}$, and for a commutative ring A, define

$$\mathrm{Br}(A) := \mathrm{Br}(\mathrm{Spec}(A)).$$

In 1970, Manin [10], based on the Hasse reciprocity law, introduced the notion of the Brauer–Manin obstruction. Roughly speaking, the Brauer–Manin obstruction measures how badly the Hasse principle for varieties fails. Let $\mathbb{A}_{\mathbb{Q}}$ be the ring of rational adeles, and let $C(\mathbb{A}_{\mathbb{Q}})$ denote the set of adelic points on C. Assume further that C is projective. It is well known [8] that

$$C(\mathbb{A}_{\mathbb{Q}}) = \prod_p C(\mathbb{Q}_p).$$

Manin [10] introduced a subset of $C(\mathbb{A}_{\mathbb{Q}})$, say $C(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}$, such that

$$C(\mathbb{Q}) \subseteq C(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} \subseteq C(\mathbb{A}_{\mathbb{Q}}).$$

Here $C(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}$ is defined to be the *right kernel* of the *adelic Brauer–Manin pairing* (see [12])

$$\begin{aligned} \mathcal{E} : \mathrm{Br}(C) \times C(\mathbb{A}_{\mathbb{Q}}) &\longrightarrow \mathbb{Q}/\mathbb{Z} \\ (\mathcal{A}, (P_p)_p) &\mapsto \sum_p \mathrm{inv}_p(\mathcal{A}(P_p)), \end{aligned} \tag{1.1}$$

https://doi.org/10.1017/S1446788714000044 Published online by Cambridge University Press

where for each prime p, $\mathrm{inv}_p : \mathrm{Br}(\mathbb{Q}_p) \longrightarrow \mathbb{Q}/\mathbb{Z}$ is the invariant map of local class field theory. We will say that C is a *counterexample to the Hasse principle explained by the Brauer–Manin obstruction* if $C(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} = \emptyset$ but $C(\mathbb{A}_{\mathbb{Q}}) = \emptyset$.

In this paper, we are interested in using the Brauer–Manin obstruction to study the arithmetic of curves of the form

$$z^2 = ax^{2n+2} + (bx^{2m} + c)(dx^{2k} + e), \tag{1.2}$$

where (n, m, k) is a triple of positive integers, and a, b, c, d, e are some integers such that $a \neq 0$. For each quintuple (a, b, c, d, e) with $a \neq 0$, we also assume that $n > m + k - 1$ and that the polynomial on the right-hand side of (1.2) is separable. These conditions are equivalent to saying that the affine part is smooth so that the nonsingular projective curve associated to (1.2) is of genus n. To add some interest to the arithmetic of curves of the form (1.2), we require that they are everywhere locally solvable.

Before stating the main problem we are interested in, let us recall the following definition.

Definition 1.1.

(i) Let C_0 be the affine curve defined by the equation $z^2 = F(x)$, where $F(x) \in \mathbb{Q}[x]$ is a polynomial of degree $2n + 2$. Let C_1 be the affine curve defined by the equation $v^2 = u^{2n+2}F(1/u)$. Throughout this paper, by the *smooth projective model* C of the affine curve C_0 we mean that C is the variety obtained by gluing together C_0 and C_1 via $u = 1/x$ and $v = z/x^{n+1}$.

(ii) Let C be the projective smooth model as in (i). A *point at infinity* on C is one of the points on C_1 with $u = 0$.

The main interest of this paper lies in partially answering the following problem.

Problem 1.2. Let (n, m, k) be a triple of positive integers such that $n > m + k - 1$. Describe all the quintuples (a, b, c, d, e) of integers with $a \neq 0$ such that the smooth projective model of the affine curve defined by

$$z^2 = ax^{2n+2} + (bx^{2m} + c)(dx^{2k} + e)$$

is a counterexample to the Hasse principle explained by the Brauer–Manin obstruction.

Some results on Problem 1.2 are known when letting $m = k = 1$. The curves of the form (1.2) with $m = k = 1$ first appeared in the work of Coray and Manoil [3] out of the attempt to construct hyperelliptic curves of arbitrary genus greater than one violating the Hasse principle. To be more precise, letting

$$\begin{cases} a = 605 \times 10^6 \\ b = 18 \\ c = -4400 \\ d = 45 \\ e = -8800, \end{cases} \tag{1.3}$$

https://doi.org/10.1017/S1446788714000044 Published online by Cambridge University Press

Coray and Manoil [3] showed that the family of hyperelliptic curves of varying genus $n \geq 2$ with fixed coefficients defined by

$$z^2 = 605 \times 10^6 x^{2n+2} + (18x^2 - 4400)(45x^2 - 8800) \tag{1.4}$$

for any integer $n \geq 2$ is counterexamples to the Hasse principle explained by the Brauer–Manin obstruction. Thus the quintuple (a, b, c, d, e) given by (1.3) satisfies the conditions in Problem 1.2, where $m = k = 1$ and n is an arbitrary positive integer greater than one. The main idea in the approach of Coray and Manoil is that they define a $\mathbb{Q}$-morphism from the curve given by (1.4) to the threefold in $\mathbb{P}^5$ defined by

$$\begin{cases} u_1^2 - 5v_1^2 = 2xy \\ u_2^2 - 5v_2^2 = 2(x + 20y)(x + 25y), \end{cases}$$

which was first studied by Colliot-Thélène *et al.* [2]. The latter is a counterexample to the Hasse principle explained by the Brauer–Manin obstruction, and hence it follows from functoriality that the curve defined by (1.4) is a counterexample to the Hasse principle explained by the Brauer–Manin obstruction.

Upon directly studying the Brauer–Manin obstruction of curves of the form (1.2) with $m = k = 1$ without relating them to certain threefolds in $\mathbb{P}^5$ in the same spirit as in the approach of Coray and Manoil, the author [4] described infinitely many quintuples (a, b, c, d, e) of integers satisfying the conditions in Problem 1.2, where n is an arbitrary positive integer greater than one and $m = k = 1$. On the other hand, following the approach of Coray and Manoil, the author [5] showed that there are certain rational functions $P_i(t) \in \mathbb{Q}(t)$ for $1 \leq i \leq 5$ such that curves defined by

$$z^2 = P_1(t)x^{2n+2} + (P_2(t)x^2 + P_3(t))(P_4(t)x^2 + P_5(t))$$

for each $t \in \mathbb{Q}$ are counterexamples to the Hasse principle explained by the Brauer–Manin obstruction, where n is a positive integer such that $n > 5$ and $n \not\equiv 0 \bmod 4$. In other words, the author [5] described a one parameter family of quintuples (a, b, c, d, e) satisfying the requirements in Problems 1.2, where $m = k = 1$ and n is a positive integer such that $n > 5$ and $n \not\equiv 0 \bmod 4$.

We are mainly concerned with investigating Problem 1.2 for curves of the form (1.2), where m and k are arbitrary positive integers. Note that when $m + k \geq 3$, it seems that one cannot follow the approach of Coray and Manoil. The reason is that in order to embed curves of the form (1.2) into a certain threefold in $\mathbb{P}^5$ of the same form as that studied by Colliot-Thélène *et al.* [2], we must require that $m + k = 2$ so that the threefold is the intersection of two quadrics.

For the rest of this section, for rational numbers $a, b, c, d, e \in \mathbb{Q}$ with $a \neq 0$, let $F(x) \in \mathbb{Q}[x]$ be the polynomial defined by

$$F(x) := ax^{2n+2} + (bx^{2m} + c)(dx^{2k} + e) \in \mathbb{Q}[x]. \tag{1.5}$$

Now, fix a curve of the form $z^2 = F(x)$ for some $a, b, c, d, e \in \mathbb{Q}$ with $a \neq 0$, and denote it by C. Under mild hypotheses, we will construct an explicit Azumaya algebra on C, say $\mathcal{A}$. The adelic Brauer–Manin pairing $\mathcal{E}$ defined as in (1.1) defines the mapping $\mathcal{E}_{\mathcal{A}} : C(\mathbb{A}_{\mathbb{Q}}) \longrightarrow \mathbb{Q}/\mathbb{Z}$ by sending an adelic point $(P_p)_p \in C(\mathbb{A}_{\mathbb{Q}})$ to $\mathcal{E}(\mathcal{A}, (P_p)_p)$. Under certain conditions, we will show that $\mathcal{E}_{\mathcal{A}}((P_p)_p) = 1/2$ for each $(P_p)_p \in C(\mathbb{A}_{\mathbb{Q}})$, and hence it follows that $C(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} = \emptyset$. This approach follows the same spirit as that of the author in [4]. The main difference between this paper and [4] is that in this paper the quintuples (a, b, c, d, e) run through a *large* infinite subset of $\mathbb{Z}^5$ and n, m, k are arbitrary positive integers such that $n > \min(m + 2k - 1, 2m + k - 1)$, whereas in [4] m and k are equal to one and the choice of the quintuples (a, b, c, d, e) is somehow *restrictive*.

To produce an Azumaya algebra on C, it is crucial that the curve C is smooth of genus n; in other words, the polynomial $F(x)$ defined by (1.5) is separable. Hence, one of the main difficulties we need to solve is to find certain reasonably mild conditions on a, b, c, d, e for which the polynomial $F(x)$ defined by (1.5) is separable. Theorem 2.1 in Section 2 gives a sufficient condition for polynomials of the above form to have distinct roots. This sufficient condition is easy to test, and is of independent interest.

The outline of the paper is as follows. In Section 2, we prove a separability criterion for the polynomials $F(x)$. The separability criterion depends on the lower bound of n, and certain congruences modulo some prime dividing a. This is Theorem 2.1. The conditions in Theorem 2.1 are *mild*, and allow one to produce a *large* class of smooth curves of the form (1.2) of arbitrary genus greater than two that are counterexamples to the Hasse principle in subsequent sections.

In Section 3, using the separability criterion in Section 2, we prove a *sufficient* condition under which curves of the form (1.2) have no rational points. In the last two sections, in order to prove that the sufficient condition in Section 3 can apply to a *large* class of curves of the form (1.2), we construct infinitely many quintuples (a, b, c, d, e) for which the curves of the form (1.2) are counterexamples to the Hasse principle explained by the Brauer–Manin obstruction, where n, m, k are positive integers such that

$$n > \min(m + 2k - 1, 2m + k - 1).$$

The construction of such quintuples (a, b, c, d, e) depends on a theorem of Iwaniec [7], which says that quadratic polynomials in two variables satisfying certain mild conditions represent infinitely many primes.

2. A separability criterion

In this section, we will give a separability criterion for the polynomials defined by

$$ax^{2n+2} + (bx^{2m} + c)(dx^{2k} + e)$$

for some integers a, b, c, d, e and some positive integers n, m, k. The main result in this section is the following theorem, which is a generalization of a lemma in the author's PhD Thesis (see [6, Lemma 4.1.1]).

https://doi.org/10.1017/S1446788714000044 Published online by Cambridge University Press

THEOREM 2.1. *Let n, m, k be positive integers, and let a, b, c, d, e be integers such that $a \neq 0$. Let p be an odd prime such that p divides a. Let $F(x) \in \mathbb{Q}[x]$ be the polynomial defined by*

$$F(x) := ax^{2n+2} + (bx^{2m} + c)(dx^{2k} + e). \tag{2.1}$$

Define

$$\begin{aligned}
n_1 &:= (m+k)(v_p(a) - v_p(bd)) + m + k - 1,\\
n_2 &:= (m+k)(v_p(a) - v_p(b)) + m - 1,\\
n_3 &:= (m+k)(v_p(a) - v_p(d)) + k - 1,\\
n_4 &:= (m+k)v_p(a) - 1,\\
n_5 &:= v_p(a) - v_p(bd) + m + k - 1,
\end{aligned}$$

where v_p denotes the p-adic valuation with the usual convention that $v_p(0) = \infty$. Suppose that the following are true:

(A1) *$n > m + k - 1$ and $n > \max(n_1, n_2, n_3, n_4, n_5)$;*
(A2) *$ce \not\equiv 0 \bmod p$, $km \not\equiv 0 \bmod p$, and $b^k e^m + (-1)^{m+k+1} c^k d^m \not\equiv 0 \bmod p$.*

Then F is separable: that is, it has exactly $2n + 2$ distinct roots in $\mathbb{C}$.

PROOF. Assume the contrary, that is, there exists an element α in $\mathbb{C}$ such that

$$F(\alpha) = \frac{\partial F}{\partial x}(\alpha) = 0,$$

where $\partial F/\partial x$ denotes the formal derivative of F with respect to the variable x. We see that

$$\begin{aligned}
(2n+2)F(\alpha) - \alpha\Big(\frac{\partial F}{\partial x}(\alpha)\Big) &= 2(n-m-k+1)bd\alpha^{2(m+k)} + 2(n-m+1)be\alpha^{2m}\\
&\quad + 2(n-k+1)cd\alpha^{2k} + (2n+2)ce = 0,
\end{aligned}$$

and hence

$$G(\beta) = 0, \tag{2.2}$$

where $G(x)$ is the polynomial in $\mathbb{Q}[x]$ defined by

$$\begin{aligned}
G(x) := (n-m-k+1)&bdx^{m+k} + (n-m+1)bex^m\\
&+ (n-k+1)cdx^k + (n+1)ce
\end{aligned} \tag{2.3}$$

and $\beta = \alpha^2$. Since $F(\alpha) = 0$, we see that

$$a\beta^{n+1} + (b\beta^m + c)(d\beta^k + e) = 0. \tag{2.4}$$

Define $K = \mathbb{Q}(\beta)$, and let $\mathfrak{p}$ be a prime of K above p. Let $K_{\mathfrak{p}}$ be the completion of K at $\mathfrak{p}$. Set $f := v_{\mathfrak{p}}(p)$, where $v_{\mathfrak{p}}$ denotes the extension of the p-adic valuation of $\mathbb{Q}_p$ to $K_{\mathfrak{p}}$. Recall that f is the *ramification index* of $K_{\mathfrak{p}}$ over $\mathbb{Q}_p$, and that for each $\gamma \in \mathbb{Q}$, we have

$$v_{\mathfrak{p}}(\gamma) = f v_p(\gamma).$$

Since the degree of $G(x)$ is at most $m+k$, we see that the degree of $K_{\mathfrak{p}}$ over $\mathbb{Q}_p$ is at most $m+k$. Furthermore, f satisfies

$$1 \leq f \leq m+k. \tag{2.5}$$

We now prove that

$$n > \max(n_1, n_2, n_3, n_4, n_5) \geq \max(m_1, m_2, m_3, m_4), \tag{2.6}$$

where

$$\begin{aligned} m_1 &:= f(v_p(a) - v_p(bd)) + m + k - 1, \\ m_2 &:= f(v_p(a) - v_p(b)) + m - 1, \\ m_3 &:= f(v_p(a) - v_p(d)) + k - 1, \\ m_4 &:= f v_p(a) - 1. \end{aligned}$$

By (A1), it suffices to show that

$$\max(n_1, n_2, n_3, n_4, n_5) \geq \max(m_1, m_2, m_3, m_4).$$

If $v_p(a) - v_p(bd) \geq 0$, we deduce from (2.5) that

$$\begin{aligned} m_1 &= f(v_p(a) - v_p(bd)) + m + k - 1 \\ &\leq (m+k)(v_p(a) - v_p(bd)) + m + k - 1 = n_1. \end{aligned}$$

If $v_p(a) - v_p(bd) < 0$, we see that

$$m_1 = f(v_p(a) - v_p(bd)) + m + k - 1 \leq v_p(a) - v_p(bd) + m + k - 1 = n_5.$$

Thus we deduce that

$$m_1 \leq \max(n_1, n_5) \leq \max(n_1, n_2, n_3, n_4, n_5). \tag{2.7}$$

If $v_p(a) - v_p(b) \geq 0$, we see that

$$m_2 = f(v_p(a) - v_p(b)) + m - 1 \leq (m+k)(v_p(a) - v_p(b)) + m - 1 = n_2.$$

If $v_p(a) - v_p(b) < 0$, we deduce that

$$v_p(b) > v_p(a) \geq 1,$$

and hence it follows that

$$b \equiv 0 \bmod p.$$

It follows from (A2) that

$$(-1)^{m+k+1} c^k d^m \not\equiv 0 \bmod p,$$

and thus $d \not\equiv 0 \bmod p$. Therefore we see that

$$\begin{aligned} n_5 &= v_p(a) - v_p(bd) + m + k - 1 \\ &= v_p(a) - v_p(b) - v_p(d) + m + k - 1 \\ &= v_p(a) - v_p(b) + m + k - 1. \end{aligned}$$

https://doi.org/10.1017/S1446788714000044 Published online by Cambridge University Press

Since $v_p(a) - v_p(b) < 0$, we deduce that

$$\begin{aligned} m_2 &= f(v_p(a) - v_p(b)) + m - 1 \\ &\leq v_p(a) - v_p(b) + m - 1 \\ &< v_p(a) - v_p(b) + m + k - 1 = n_5. \end{aligned}$$

Therefore

$$m_2 \leq \max(n_2, n_5) \leq \max(n_1, n_2, n_3, n_4, n_5). \tag{2.8}$$

We now prove that $m_3 \leq \max(n_1, n_2, n_3, n_4, n_5)$. Indeed, if $v_p(a) - v_p(d) \geq 0$, we see that

$$m_3 = f(v_p(a) - v_p(d)) + k - 1 \leq (m + k)(v_p(a) - v_p(d)) + k - 1 = n_3.$$

If $v_p(a) - v_p(d) < 0$, we deduce that $v_p(d) > v_p(a) \geq 1$, and hence $d \equiv 0 \bmod p$. Using (A2), it follows that $b \not\equiv 0 \bmod p$. Therefore

$$\begin{aligned} n_5 &= v_p(a) - v_p(bd) + m + k - 1 \\ &= v_p(a) - v_p(b) - v_p(d) + m + k - 1 \\ &= v_p(a) - v_p(d) + m + k - 1, \end{aligned}$$

and thus it follows that

$$\begin{aligned} m_3 &= f(v_p(a) - v_p(d)) + k - 1 \\ &\leq v_p(a) - v_p(d) + k - 1 \\ &< v_p(a) - v_p(d) + m + k - 1 = n_5. \end{aligned}$$

Therefore

$$m_3 \leq \max(n_1, n_2, n_3, n_4, n_5). \tag{2.9}$$

Finally we see that

$$m_4 = f v_p(a) - 1 \leq (m + k) v_p(a) - 1 = n_4 \leq \max(n_1, n_2, n_3, n_4, n_5). \tag{2.10}$$

By (2.7)–(2.10), we deduce that

$$n > \max(n_1, n_2, n_3, n_4, n_5) \geq \max(m_1, m_2, m_3, m_4).$$

We prove that β is an integral element of $K_{\mathfrak{p}}$. Assume the contrary, that is, $v_{\mathfrak{p}}(\beta) < 0$. Since $v_{\mathfrak{p}}(\beta)$ is an integer, we see that $v_{\mathfrak{p}}(\beta) \leq -1$. We have that

$$v_{\mathfrak{p}}(a\beta^{n+1}) = f v_p(a) + (n + 1) v_{\mathfrak{p}}(\beta),$$

and it follows from (A2) that

$$\begin{aligned} v_{\mathfrak{p}}((b\beta^m + c)(d\beta^k + e)) &= v_{\mathfrak{p}}(b\beta^m + c) + v_{\mathfrak{p}}(d\beta^k + e) \\ &\geq \min(v_{\mathfrak{p}}(b\beta^m), v_{\mathfrak{p}}(c)) + \min(v_{\mathfrak{p}}(d\beta^k), v_{\mathfrak{p}}(e)) \\ &\geq \min(f v_p(b) + m v_{\mathfrak{p}}(\beta), 0) + \min(f v_p(d) + k v_{\mathfrak{p}}(\beta), 0) \\ &\geq \min(f v_p(bd) + (m + k) v_{\mathfrak{p}}(\beta), f v_p(b) + m v_{\mathfrak{p}}(\beta), f v_p(d) \\ &\qquad + k v_{\mathfrak{p}}(\beta), 0). \end{aligned}$$

By (2.6), we see that

$$-(n-m-k+1)v_{\mathfrak{p}}(\beta) \geq n-m-k+1 > f(v_p(a)-v_p(bd)),$$

and hence

$$v_{\mathfrak{p}}(a\beta^{n+1}) = fv_p(a) + (n+1)v_{\mathfrak{p}}(\beta) < fv_p(bd) + (m+k)v_{\mathfrak{p}}(\beta).$$

Similarly, we can show that

$$\begin{aligned} v_{\mathfrak{p}}(a\beta^{n+1}) &< fv_p(b) + mv_{\mathfrak{p}}(\beta), \\ v_{\mathfrak{p}}(a\beta^{n+1}) &< fv_p(d) + kv_{\mathfrak{p}}(\beta), \\ v_{\mathfrak{p}}(a\beta^{n+1}) &< 0. \end{aligned}$$

Thus we deduce that

$$\begin{aligned} v_{\mathfrak{p}}(a\beta^{n+1}) &< \min(fv_p(bd) + (m+k)v_{\mathfrak{p}}(\beta), fv_p(b) + mv_{\mathfrak{p}}(\beta), fv_p(d) + kv_{\mathfrak{p}}(\beta), 0) \\ &\leq v_{\mathfrak{p}}((b\beta^m + c)(d\beta^k + e)), \end{aligned}$$

and hence it follows from (2.4) that

$$\begin{aligned} +\infty = v_{\mathfrak{p}}(0) &= v_{\mathfrak{p}}(a\beta^{n+1} + (b\beta^m + c)(d\beta^k + e)) \\ &= v_{\mathfrak{p}}(a\beta^{n+1}) = fv_p(a) + (n+1)v_{\mathfrak{p}}(\beta) \leq fv_p(a) - (n+1), \end{aligned}$$

which is a contradiction. Therefore β is an integral element of $K_{\mathfrak{p}}$.

Taking (2.4) modulo $\mathfrak{p}$ and noting that $\mathfrak{p}$ is a prime over p and p divides a, we see that

$$(b\beta^m + c)(d\beta^k + e) \equiv 0 \bmod \mathfrak{p},$$

and hence we deduce that

$$b\beta^m \equiv -c \bmod \mathfrak{p} \tag{2.11}$$

or

$$d\beta^k \equiv -e \bmod \mathfrak{p}. \tag{2.12}$$

Suppose that (2.11) holds. Taking (2.2) modulo $\mathfrak{p}$, we see that

$$\begin{aligned} 0 &= G(\beta) \\ &\equiv -(n-m-k+1)cd\beta^k - (n-m+1)ce + (n-k+1)cd\beta^k + (n+1)ce \\ &\equiv cdm\beta^k + cem \bmod \mathfrak{p}, \end{aligned}$$

and it follows from (A2) that

$$d\beta^k \equiv -e \bmod \mathfrak{p}.$$

Thus we deduce from (2.11) and the last congruence that

$$b^k d^m \beta^{mk} \equiv (-1)^k c^k d^m \equiv (-1)^m b^k e^m \bmod \mathfrak{p},$$

and hence

$$(-1)^m b^k e^m - (-1)^k c^k d^m \equiv 0 \bmod \mathfrak{p}.$$

https://doi.org/10.1017/S1446788714000044 Published online by Cambridge University Press

Therefore we see that

$$b^k e^m + (-1)^{m+k+1} c^k d^m \equiv 0 \bmod \mathfrak{p},$$

which contradicts (A2).

Suppose that (2.12) holds. Taking (2.2) modulo $\mathfrak{p}$, we see that

$$\begin{aligned} 0 &= G(\beta) \\ &\equiv -(n-m-k+1)be\beta^m + (n-m+1)be\beta^m - (n-k+1)ce + (n+1)ce \\ &\equiv kbe\beta^m + cek \bmod \mathfrak{p}, \end{aligned}$$

and hence it follows from (A2) that

$$b\beta^m \equiv -c \bmod \mathfrak{p}.$$

Using the same arguments as above, we deduce that

$$b^k e^m + (-1)^{m+k+1} c^k d^m \equiv 0 \bmod \mathfrak{p},$$

which contradicts (A2).

Therefore we see that F is separable. □

3. Nonexistence of rational points on certain hyperelliptic curves

In this section, using Theorem 2.1, we give a *sufficient* condition under which certain curves C of the form

$$C : z^2 = ax^{2n+2} + (bx^{2m} + c)(dx^{2k} + e)$$

satisfy $C(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} = \emptyset$. We begin by proving the following lemma, which shows how to construct an Azumaya algebra on the curves C of the form as above.

Lemma 3.1. *We maintain the notation and assumptions of Theorem 2.1. Assume (A1) and (A2) in Theorem 2.1. Suppose that the following are true:*

(A3) *$a = a_1 a_2^2$, where a_1, a_2 are relatively prime integers such that a_1 is a positive squarefree integer and $a_1 \equiv 1 \bmod 8$;*
(A4) *$b \neq 0$.*

Let C be the smooth projective model of the affine curve defined by

$$z^2 = F(x), \tag{3.1}$$

where $F(x) \in \mathbb{Q}[x]$ is the polynomial defined by (2.1). Let $\mathcal{A}$ be the class of the quaternion algebra $(a_1, bx^{2m} + c)$ in $\mathrm{Br}(\mathbb{Q}(C))$, where $\mathbb{Q}(C)$ denotes the function field of C. Then the quaternion algebras

$$\mathcal{B} := (a_1, dx^{2k} + e)$$

and

$$\mathcal{E} := \left(a_1, \frac{bx^{2m} + c}{x^{2m}}\right)$$

represent the same class as $\mathcal{A}$ in $\mathrm{Br}(\mathbb{Q}(C))$. Furthermore $\mathcal{A}, \mathcal{B}, \mathcal{E}$ together define an Azumaya algebra on C.

https://doi.org/10.1017/S1446788714000044 Published online by Cambridge University Press

Proof. Throughout the proof, let C_0 and C_1 be the affine curves associated to C as in part (i) of Definition 1.1. Recall that C_0 is given by the equation $z^2 = F(x)$ and C_1 is given by the equation $v^2 = u^{2n+2}F(1/u)$, where $u = 1/x$ and $v = z/x^{n+1}$.

We will prove that there is a Zariski open covering $\{U_i\}$ of C such that $\mathcal{A}$ extends to an element $\mathrm{Br}(U_i)$ for each i. We see that (3.1) can be written in the form

$$(bx^{2m} + c)(dx^{2k} + e) = z^2 - a_1a_2^2x^{2n+2} = \mathrm{Norm}_{\mathbb{Q}(\sqrt{a_1})/\mathbb{Q}}(z - \sqrt{a_1}a_2x^{n+1}). \tag{3.2}$$

Hence it follows that $\mathcal{A} + \mathcal{B} = 0$. Furthermore, since x^{2m} is a square, we have $\mathcal{A} - \mathcal{E} = (a_1, x^{2m}) = 0$. Since $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{E}$ belong to the 2-torsion part of $\mathrm{Br}(\mathbb{Q}(C))$, this implies that $\mathcal{A} = \mathcal{B} = \mathcal{E}$.

Now let U_1 be the *largest* open subvariety of C in which the rational function $F := bx^{2m} + c$ has neither a zero nor a pole, and let U_2 be the *largest* open subvariety of C in which $G := dx^{2k} + e$ has neither a zero nor a pole. Since $\mathcal{A} = \mathcal{B}$, we have that $\mathcal{A}$ is an Azumaya algebra on U_1 and also on U_2. We prove that in the open subset C_0 of C, the locus where both F and G have a zero is empty. Assume the contrary, that is, there is a point (x, z) on C_0 such that

$$bx^{2m} + c = dx^{2k} + e = 0.$$

Hence we deduce that

$$b^kd^mx^{2km} = (-1)^kc^kd^m = (-1)^mb^ke^m,$$

and it follows that

$$(-1)^mb^ke^m - (-1)^kc^kd^m = 0.$$

Thus we see that

$$b^ke^m + (-1)^{m+k+1}c^kd^m = 0,$$

which contradicts (A2). Therefore, in the open subset C_0 of C, the locus where both F and G have a zero is empty.

Let $H := (bx^{2m} + c)/x^{2m}$ be a rational function in $\mathbb{Q}(C)$. Since $u = 1/x$, the rational function H can be written in the form $H = b + cu^{2m}$. Let ∞ be a point at infinity on C. By part (ii) of Definition 1.1 and the equation of C_1, we know that $\infty = (u, v) = (0, \pm\sqrt{a})$. Thus we see that

$$H(\infty) = b \neq 0.$$

Hence H is regular and nonvanishing at the points at infinity on C.

Now let U_3 be the *largest* open subvariety of C in which H has neither a zero nor a pole. Since $\mathcal{A} = \mathcal{E}$, we deduce that $\mathcal{A}$ is an Azumaya algebra on U_3. By what we have shown, we see that $C = U_1 \cup U_2 \cup U_3$ and $\mathcal{A}$ is an Azumaya algebra on each U_i for $i = 1, 2, 3$. Therefore $\mathcal{A}$ is an Azumaya algebra of C. □

Theorem 3.2. *We maintain the notation and assumptions of Lemma 3.1. Assume that $a_1 \neq 1$, and write*

$$a_1 = p_1p_2 \dots p_h,$$

where h is a positive integer and $p_1, p_2, \dots, p_h$ are the distinct primes dividing a_1. Assume (A1)–(A4), and suppose further that the following are true:

(A5) *there are positive integers* h_1, h_2, h_3 *such that* $1 \le h_1 \le h_2 \le h_3 \le h$ *and* $h_1 + h_3 - h_2$ *is odd; furthermore,* $\gcd(c, p_i) = 1$ *for each* $1 \le i \le h_2$, $\gcd(e, p_i) = 1$ *for each* $h_2 + 1 \le i \le h$,

$$\left(\frac{c}{p_i}\right) = \begin{cases} -1 & \text{if } 1 \le i \le h_1, \\ 1 & \text{if } h_1 + 1 \le i \le h_2, \end{cases}$$

and

$$\left(\frac{e}{p_i}\right) = \begin{cases} -1 & \text{if } h_2 + 1 \le i \le h_3, \\ 1 & \text{if } h_3 + 1 \le i \le h, \end{cases}$$

where $(\cdot/\cdot)$ *denotes the Jacobi symbol;*

(A6) *for each odd prime* l *dividing* a_2, a_1 *is a square modulo* l*;*

(A7) *for each odd prime* l *dividing* $b^k e^m + (-1)^{m+k+1} c^k d^m$ *such that* a_1 *and* l *are relatively prime,* l *does not divide* $\gcd(c, e)$ *or* a_1 *is a quadratic residue modulo* l*;*

(A8) $b \equiv 0 \bmod p_i$ *for each* $1 \le i \le h_2$ *and* $d \equiv 0 \bmod p_i$ *for each* $h_2 + 1 \le i \le h$.

Let C *be the smooth projective model as in Lemma 3.1. Then* $C(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} = \emptyset$.

PROOF. We maintain the notation of the proof of Lemma 3.1. Set

$$\mathbf{P} := \{p_1, p_2, \ldots, p_{h_1}\} \cup \{p_{h_2+1}, p_{h_2+2}, \ldots, p_{h_3}\}. \tag{3.3}$$

We will prove that for any $P_l \in C(\mathbb{Q}_l)$,

$$\mathrm{inv}_l(\mathcal{A}(P_l)) = \begin{cases} 0 & \text{if } l \notin \mathbf{P}, \\ \frac{1}{2} & \text{if } l \in \mathbf{P}. \end{cases} \tag{3.4}$$

Since C_0 is smooth and C is the smooth projective model of C_0, we know that $C_0(\mathbb{Q}_l)$ is l-adically dense in $C(\mathbb{Q}_l)$. It is well known [13, Lemma 3.2] that $\mathrm{inv}_l(\mathcal{A}(P_l))$ is a continuous function on $C(\mathbb{Q}_l)$ with the l-adic topology. Hence it suffices to prove (3.4) for $P_l \in C_0(\mathbb{Q}_l)$. We consider the following cases.

Case 1: $l = \infty, 2$ *or* l *is an odd prime such that* $\gcd(a_1, l) = 1$ *and* a_1 *is a square in* $\mathbb{Q}_l^\times$.

We see that the Hilbert symbol $(a_1, t)_l$ is one for any $t \in \mathbb{Q}_l^\times$. Hence $\mathrm{inv}_l(\mathcal{A}(P_l))$ is zero.

Case 2: l *is an odd prime such that* $\gcd(a_1, l) = 1$ *and* a_1 *is not a square in* $\mathbb{Q}_l^\times$.

In this case, we consider the following subcases.

Subcase 2(i): $v_l(x) \ge 0$.

We contend that at least one of $bx^{2m} + c$ and $dx^{2k} + e$ is nonzero modulo l. Assume the contrary, that is,

$$bx^{2m} + c \equiv dx^{2k} + e \equiv 0 \bmod l. \tag{3.5}$$

Hence we see that

$$b^k d^m x^{2mk} \equiv (-1)^k c^k d^m \equiv (-1)^m b^k e^m \bmod l,$$

and hence

$$(-1)^m b^k e^m - (-1)^k c^k d^m \equiv 0 \bmod l.$$

Therefore we see that

$$b^k e^m + (-1)^{m+k+1} c^k d^m \equiv 0 \bmod l.$$

By (A7) and since a_1 is not a square modulo l, we deduce from the congruence above that l does not divide $\gcd(c, e)$.

On the other hand, we see from (3.5) and (3.2) that

$$z^2 \equiv a_1 a_2^2 x^{2n+2} \bmod l.$$

By (A6) and since a_1 is not a square modulo l, we deduce that l does not divide a_2. Since a_1 is a quadratic nonresidue modulo l, it follows from the last congruence that $x \equiv z \equiv 0 \bmod l$. Hence we deduce from (3.5) that $c \equiv e \equiv 0 \bmod l$, and hence l divides $\gcd(c, e)$, which is a contradiction. Thus, at least one of $bx^{2m} + c$ and $dx^{2k} + e$ is nonzero modulo l, say U. Hence the local Hilbert symbol $(a_1, U)_l$ is one. Therefore $\mathrm{inv}_l(\mathcal{A}(P_l))$ is zero.

Subcase 2(ii): $\epsilon := v_l(x) < 0$.

By (A6) and since a_1 is not a square modulo l, we deduce that l does not divide a_2. By (A1) and (3.1), we see that

$$v_l(z) = \frac{v_l(z^2)}{2} = \frac{v_l(a_1 a_2^2 x^{2n+2})}{2} = (n+1)\epsilon.$$

Hence there exist elements $x_0, z_0 \in \mathbb{Z}_l^\times$ such that

$$x = x_0 l^\epsilon,$$
$$z = z_0 l^{(n+1)\epsilon}.$$

Hence we see from (3.1) that

$$z_0^2 l^{2(n+1)\epsilon} = a_1 a_2^2 x_0^{2n+2} l^{(2n+2)\epsilon} + (b x_0^{2m} l^{2m\epsilon} + c)(d x_0^{2k} l^{2k\epsilon} + e),$$

and hence

$$z_0^2 = a_1 a_2^2 x_0^{2n+2} + l^{-2(n-m-k+1)\epsilon}(b x_0^{2m} + c l^{-2m\epsilon})(d x_0^{2k} + e l^{-2k\epsilon}).$$

Taking the above equation modulo l and noting that $n - m - k + 1$ is greater than zero, we deduce that

$$z_0^2 \equiv a_1 a_2^2 x_0^{2n+2} \bmod l.$$

By (A6), we easily see that $a_2 \not\equiv 0 \bmod l$. Thus it follows that

$$a_1 \equiv \left(\frac{z_0}{a_2 x_0^{n+1}}\right)^2 \bmod l,$$

which is a contradiction since a_1 is not a square modulo l. Therefore, in any event, we see that $\mathrm{inv}_l(\mathcal{A}(P_l))$ is zero.

Case 3: l is an odd prime such that l divides a_1.

By assumption, we see that $l = p_i$ for some $1 \le i \le h$. We contend that $v_{p_i}(x) \ge 0$. Assume the contrary, that is, $v_{p_i}(x) < 0$. Set $\epsilon = v_{p_i}(x)$. We see that

$$\begin{aligned} v_{p_i}((bx^{2m} + c)(dx^{2k} + e)) &= v_{p_i}(bx^{2m} + c) + v_{p_i}(dx^{2k} + e) \\ &\ge \min(2m\epsilon + v_{p_i}(b), v_{p_i}(c)) + \min(2k\epsilon + v_{p_i}(d), v_{p_i}(e)) \\ &\ge \min(2m\epsilon, 0) + \min(2k\epsilon, 0) \\ &\ge 2m\epsilon + 2k\epsilon \\ &\ge 2(m + k)\epsilon. \end{aligned}$$

Since $n > m + k - 1$, we deduce that

$$-2(n - m - k + 1)\epsilon \ge 2 > 1,$$

and hence

$$v_{p_i}(ax^{2n+2}) = 1 + 2(n + 1)\epsilon < 2(m + k)\epsilon \le v_{p_i}((bx^{2m} + c)(dx^{2k} + e)).$$

By (3.1), we see that

$$2v_{p_i}(z) = v_{p_i}(z^2) = v_{p_i}(ax^{2n+2}) = 1 + (2n + 2)\epsilon,$$

which is a contradiction since the left-hand side is an even integer whereas the right-hand side is odd. Therefore $v_{p_i}(x) \ge 0$.

We now consider the following subcases.

Subcase 3(i): $1 \le i \le h_1$ or $h_2 + 1 \le i \le h_3$.

If the integer i satisfies $1 \le i \le h_1$, then by (A5) and (A8) we see that $(c/p_i) = -1$ and $b \equiv 0 \bmod p_i$. Thus we deduce that

$$bx^{2m} + c \equiv c \not\equiv 0 \bmod p_i.$$

Since $a_1 = p_i a_1^*$, where a_1^* is an integer such that $\gcd(a_1^*, p_i) = 1$, it follows from [1, Theorem 5.2.7] that the local Hilbert symbol $(a_1, bx^{2m} + c)_{p_i}$ satisfies

$$(a_1, bx^{2m} + c)_{p_i} = \left(\frac{c}{p_i}\right) = -1.$$

Therefore we deduce that $\mathrm{inv}_{p_i}(\mathcal{A}(P_{p_i}))$ is $1/2$.

If the integer i satisfies $h_2 + 1 \le i \le h_3$, then using the same arguments as above, we see from (A5) and (A8) that the local Hilbert symbol $(a_1, dx^{2k} + e)_{p_i}$ satisfies

$$(a_1, dx^{2m} + e)_{p_i} = \left(\frac{e}{p_i}\right) = -1.$$

Since $\mathcal{A}$ and $\mathcal{B}$ represent the same class in $\mathrm{Br}(\mathbb{Q}(C))$, we deduce that

$$\mathrm{inv}_{p_i}(\mathcal{A}(P_{p_i})) = 1/2.$$

https://doi.org/10.1017/S1446788714000044 Published online by Cambridge University Press

Subcase 3(ii): $h_1 + 1 \leq i \leq h_2$ or $h_3 + 1 \leq i \leq h$.

If the integer i satisfies $h_1 + 1 \leq i \leq h_2$, then by (A5) and (A8) we see that $(c/p_i) = 1$ and $b \equiv 0 \bmod p_i$. Thus we deduce that

$$bx^{2m} + c \equiv c \not\equiv 0 \bmod p_i.$$

Since $a_1 = p_i a_1^*$, where a_1^* is an integer such that $\gcd(a_1^*, p_i) = 1$, it follows from [1, Theorem 5.2.7] that the local Hilbert symbol $(a_1, bx^{2m} + c)_{p_i}$ satisfies

$$(a_1, bx^{2m} + c)_{p_i} = \left(\frac{c}{p_i}\right) = 1.$$

Therefore we deduce that

$$\mathrm{inv}_{p_i}(\mathcal{A}(P_{p_i})) = 0.$$

If the integer i satisfies $h_3 + 1 \leq i \leq h$, then using the same arguments as above, we see from (A5) and (A8) that the local Hilbert symbol $(a_1, dx^{2m} + e)_{p_i}$ satisfies

$$(a_1, dx^{2m} + e)_{p_i} = \left(\frac{e}{p_i}\right) = 1.$$

Since $\mathcal{A}$ and $\mathcal{B}$ represent the same class in $\mathrm{Br}(\mathbb{Q}(C))$, we deduce that

$$\mathrm{inv}_{p_i}(\mathcal{A}(P_{p_i})) = 0.$$

By what we have shown and since $h_1 + h_3 - h_2$ is odd, we see that for any $(P_l)_l \in C(\mathbb{A}_{\mathbb{Q}})$, the sum $\sum_l \mathrm{inv}_l \mathcal{A}(P_l)$ satisfies

$$\begin{aligned}\sum_l \mathrm{inv}_l \mathcal{A}(P_l) &= \sum_{1 \leq i \leq h_1} \mathrm{inv}_{p_i} \mathcal{A}(P_{p_i}) + \sum_{h_2+1 \leq i \leq h_3} \mathrm{inv}_{p_i} \mathcal{A}(P_{p_i}) \\ &= \sum_{1 \leq i \leq h_1} \tfrac{1}{2} + \sum_{h_2+1 \leq i \leq h_3} \tfrac{1}{2} \\ &= \tfrac{1}{2} \bmod \mathbb{Z},\end{aligned}$$

which proves that $C(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} = \emptyset$. □

Using Theorem 3.2, we reprove the following result, which is the main assertion of [4, Theorem 1.2].

COROLLARY 3.3 [4, Theorem 1.2]. *Let p be a prime such that $p \equiv 1 \bmod 8$ and let n be a positive integer such that $n \geq 3$. Assume that the following are true:*

(i) *there is an integer d_* such that d_* is a quadratic nonresidue in $\mathbb{F}_p^\times$, d_* is odd and $\gcd(d_*, n) = 1$;*

(ii) *there is a nonzero integer m_* such that m_* is even and $q = d_*^2 + pm_*^2$ is a prime.*

Let $\mathcal{X}$ be the smooth projective model of the affine curve given by

$$\mathcal{X} : z^2 = pq^2x^{2n+2} + (d_*(p + d_*)x^2 - q)(pm_*^2(p + d_*)x^2 - d_*q). \tag{3.6}$$

Then $\mathcal{X}(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} = \emptyset$.

https://doi.org/10.1017/S1446788714000044 Published online by Cambridge University Press

PROOF. Let

$$h_1 = h_2 = h_3 = h = 1,$$

$$\begin{cases} a_1 := p, \\ a_2 := q, \\ a := a_1 a_2^2, \\ b := pm_*^2(p + d_*), \\ c := -d_* q, \\ d := d_*(p + d_*), \\ e := -q, \end{cases}$$

and

$$m = k = 1.$$

By (i) and (ii) in Corollary 3.3, one can verify that the quintuple (a, b, c, d, e) defined as above satisfies (A1)–(A8). Hence Theorem 3.2 implies that $\mathcal{X}(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} = \emptyset$, and thus our contention follows. □

4. Certain hyperelliptic curves violating the Hasse principle

In this section, using Theorem 3.2, we will construct certain hyperelliptic curves of arbitrary genus greater than two having no $\mathbb{Q}$-rational points. To add some interest to these curves, we require that they are everywhere locally solvable, that is, they are counterexamples to the Hasse principle explained by the Brauer–Manin obstruction.

Let h be a positive integer, and let $p_1, p_2, \ldots, p_h$ be distinct odd primes. Define

$$a_1 := p_1 p_2 \ldots p_h. \tag{4.1}$$

Let q_1, q_2, q_3 be nonzero odd integers, and define

$$a_2 := q_1 q_2 q_3. \tag{4.2}$$

Let c_1, e_1 be nonzero integers, and let n, m, k be positive integers. Suppose that the following are true:

(B1) $\gcd(a_2, c_1) = \gcd(a_2, e_1) = \gcd(c_1, e_1) = 1$ and $\gcd(a_2, p_i) = \gcd(c_1, p_i) = \gcd(e_1, p_i) = 1$ for each $1 \leq i \leq h$;

(B2) there exist integers h_1, h_2, h_3 such that $h_1 + h_3 - h_2$ is odd, $1 \leq h_1 \leq h_2 \leq h_3 \leq h$,

$$\left(\frac{c_1}{p_i}\right) = \left(\frac{e_1}{p_i}\right) = \begin{cases} -1 & \text{if } 1 \leq i \leq h_1, \\ 1 & \text{if } h_1 + 1 \leq i \leq h_2, \end{cases}$$

and

$$\left(\frac{c_1}{p_i}\right) = \left(\frac{e_1}{p_i}\right) = \begin{cases} -1 & \text{if } h_2 + 1 \leq i \leq h_3, \\ 1 & \text{if } h_3 + 1 \leq i \leq h; \end{cases}$$

(B3) $p_i \equiv 1 \bmod 4$ for each $1 \leq i \leq h$ and $a_1 \equiv 1 \bmod 8$.

https://doi.org/10.1017/S1446788714000044 Published online by Cambridge University Press

(B4) for each $1 \le i \le h$, the prime p_i is a square modulo l, where l is any odd prime dividing a_2;

(B5) $q_1 = \Delta c_1^2 + \Phi e_1^2$, where

$$\Phi := \prod_{i=1}^{h_2} p_i \tag{4.3}$$

and

$$\Delta := \prod_{i=h_2+1}^{h} p_i; \tag{4.4}$$

(B6) $n - m + 1 \not\equiv 0 \bmod l$ for each odd prime l dividing c_1;

(B7) $n - k + 1 \not\equiv 0 \bmod l$ for each odd prime l dividing e_1;

(B8) there is some integer t with $1 \le t \le h$ such that $km \not\equiv 0 \bmod p_t$;

(B9) let t be the integer in (B8). Then

$$\begin{cases} n > m + 2k - 1 & \text{if } 1 \le t \le h_2, \\ n > 2m + k - 1 & \text{if } h_2 + 1 \le t \le h. \end{cases}$$

Define

$$\begin{cases} a := a_1 a_2^2 \\ b := \Phi(a_1 - c_1 e_1 q_2 q_3) e_1 q_2 \\ c := c_1 q_1 q_2^2 q_3 \\ d := -\Delta(a_1 - c_1 e_1 q_2 q_3) c_1 q_3 \\ e := -e_1 q_1 q_2 q_3^2. \end{cases} \tag{4.5}$$

The following result is the main theorem in this section.

Theorem 4.1. *We maintain the notation and assumptions as above. Assume (B1)–(B9). Let $\mathcal{D}$ be the smooth projective model of the affine curve defined by*

$$\mathcal{D} : z^2 = ax^{2n+2} + (bx^{2m} + c)(dx^{2k} + e). \tag{4.6}$$

Then $\mathcal{D}$ is a counterexample to the Hasse principle explained by the Brauer–Manin obstruction.

For the proof of Theorem 4.1, we need the following lemmas.

Lemma 4.2. *We maintain the notation as in Theorem 4.1, and assume that (B1)–(B9) hold. Then (A1), (A2) in Theorem 3.2 hold, where p is taken to be p_t in (A1).*

Proof. Using (4.5) and noting that $a_1 - c_1 e_1 q_2 q_3 \equiv -c_1 e_1 q_2 q_3 \not\equiv 0 \bmod p_t$, we see that

$$v_{p_t}(a) = 1,$$
$$v_{p_t}(bd) = v_{p_t}(-a_1 c_1 e_1 q_2 q_3 (a_1 - c_1 e_1 q_2 q_3)^2) = v_{p_t}(a_1) = 1.$$

Furthermore, we see that

$$v_{p_t}(b) = \begin{cases} 1 & \text{if } 1 \le t \le h_2, \\ 0 & \text{if } h_2 + 1 \le t \le h, \end{cases}$$

https://doi.org/10.1017/S1446788714000044 Published online by Cambridge University Press

and

$$v_{p_t}(d) = \begin{cases} 0 & \text{if } 1 \leq t \leq h_2, \\ 1 & \text{if } h_2 + 1 \leq t \leq h. \end{cases}$$

Letting n_1, n_2, n_3, n_4, n_5 as in Theorem 2.1 with p replaced by p_t, we note that

$$n_1 = n_4 = n_5 = m + k - 1,$$

$$n_2 = \begin{cases} m - 1 & \text{if } 1 \leq t \leq h_2, \\ 2m + k - 1 & \text{if } h_2 + 1 \leq t \leq h, \end{cases}$$

and

$$n_3 = \begin{cases} m + 2k - 1 & \text{if } 1 \leq t \leq h_2, \\ k - 1 & \text{if } h_2 + 1 \leq t \leq h. \end{cases}$$

Thus we deduce that

$$\max(n_1, n_2, n_3, n_4, n_5) = \begin{cases} m + 2k - 1 & \text{if } 1 \leq t \leq h_2, \\ 2m + k - 1 & \text{if } h_2 + 1 \leq t \leq h. \end{cases}$$

Therefore, we deduce from (B9) that

$$n > \max(n_1, n_2, n_3, n_4, n_5).$$

Furthermore, it follows from (B9) that

$$n > \min(m + 2k - 1, 2m + k - 1) > m + k - 1.$$

Thus (A1) in Theorem 2.1 holds.

We now prove that (A2) is true. We easily see from (4.5) and (B1) that $ce \not\equiv 0 \bmod p_t$. By (B8), it is clear that $km \not\equiv 0 \bmod p_t$. We contend that $b^k e^m + (-1)^{m+k+1} c^k d^m \not\equiv 0 \bmod p_t$. If $1 \leq t \leq h_2$, then it follows from (4.5) that $a_1 \equiv 0 \bmod p_t$ and $b \equiv 0 \bmod p_t$. Hence we deduce from (4.4) and (B1) that

$$\begin{aligned} b^k e^m + (-1)^{m+k+1} c^k d^m &\equiv (-1)^{m+k+1} c^k d^m \\ &\equiv (-1)^{m+k+1} (c_1 q_1 q_2^2 q_3)^k (\Delta c_1^2 e_1 q_2 q_3^2)^m \\ &\not\equiv 0 \bmod p_t. \end{aligned}$$

If $h_2 + 1 \leq t \leq h$, then it follows from (4.5) that $a_1 \equiv 0 \bmod p_t$ and $d \equiv 0 \bmod p_t$. Hence we deduce from (4.3) and (B1) that

$$\begin{aligned} b^k e^m + (-1)^{m+k+1} c^k d^m &\equiv b^k e^m \\ &\equiv (-c_1 e_1^2 q_2^2 q_3 \Phi)^k (-e_1 q_1 q_2 q_3^2)^m \\ &\not\equiv 0 \bmod p_t. \end{aligned}$$

Therefore (A2) in Theorem 3.2 holds. Hence our contention follows. □

LEMMA 4.3. *We maintain the notation in Theorem 4.1, and assume that (B1)–(B9) hold. Let $\mathcal{D}$ be the curve in Theorem 4.1. Then $\mathcal{D}$ is everywhere locally solvable.*

https://doi.org/10.1017/S1446788714000044 Published online by Cambridge University Press

Proof. By Lemma 4.2, we know that (A1), (A2) in Theorem 3.2 hold. Set

$$F(x) = ax^{2n+2} + (bx^{2m} + c)(dx^{2k} + e) \in \mathbb{Q}[x].$$

Let $\mathcal{D}_0, \mathcal{D}_1$ be the affine curves associated to $\mathcal{D}$ as in part (i) of Definition 1.1. Recall that $\mathcal{D}_0$ is given by the equation $z^2 = F(x)$ and $\mathcal{D}_1$ is given by the equation $v^2 = u^{2n+2}F(1/u)$, where $u = 1/x$ and $v = z/x^{n+1}$.

Since (A1), (A2) hold, it follows from Theorem 2.1 that $F(x)$ is separable, and hence $\mathcal{D}$ is smooth of genus n.

We now prove that $\mathcal{D}$ is everywhere locally solvable. For any odd prime l not dividing $a_1c_1e_1q_2q_3$, note that since

$$a_1(-c_1e_1q_2q_3)(-a_1c_1e_1q_2q_3) = (a_1c_1e_1q_2q_3)^2$$

is a square in $\mathbb{Q}_l^\times$, we deduce that at least one of $a_1, -c_1e_1q_2q_3, -a_1c_1e_1q_2q_3$ is a square in $\mathbb{Q}_l^\times$. Hence it suffices to consider the following cases.

Case 1: $l = 2$, $l = \infty$ or l is any odd prime such that $\gcd(l, a_1) = 1$ *and a_1 is a square in $\mathbb{Q}_l^\times$.*

Let ∞ be a point at infinity on $\mathcal{D}$. By part (ii) of Definition 1.1, we see that ∞ is one of the points on $\mathcal{D}_1$ with $u = 0$, that is,

$$\infty = (u, v) = (0, \pm\sqrt{a}) = (0, \pm a_2\sqrt{a_1}).$$

Since $a_1 \equiv 1 \bmod 8$, we know that a_1 is a square in $\mathbb{Q}_2^\times$. Furthermore, we also know that a_1 is a square in $\mathbb{R}$. Thus we see that ∞ belongs to $\mathcal{D}(\mathbb{Q}_l)$. Therefore $\mathcal{D}$ is locally solvable at l.

Case 2: l is any odd prime such that $\gcd(l, c_1e_1q_2q_3) = 1$ *and $-c_1e_1q_2q_3$ is a square in $\mathbb{Q}_l^\times$.*

We see that the point $P_1 = (x, z) = (0, q_1q_2q_3\sqrt{-c_1e_1q_2q_3})$ belongs to $\mathcal{D}(\mathbb{Q}_l)$, which proves that $\mathcal{D}$ is locally solvable at l.

Case 3: l is any odd prime such that $\gcd(l, a_1c_1e_1q_2q_3) = 1$ *and $-a_1c_1e_1q_2q_3$ is a square in $\mathbb{Q}_l^\times$.*

Using (4.5) and (4.1), we see that

$$bd = -a_1c_1e_1q_2q_3(a_1 - c_1e_1q_2q_3)^2.$$

By (4.5), we deduce that

$$\begin{aligned} a + ce + be + cd = {} & a_1q_1^2q_2^2q_3^2 - c_1e_1q_1^2q_2^3q_3^3 - e_1^2q_1q_2^2q_3^2\Phi(a_1 - c_1e_1q_2q_3) \\ & - c_1^2q_1q_2^2q_3^2\Delta(a_1 - c_1e_1q_2q_3), \end{aligned}$$

and hence it follows from (B5) that

$$\begin{aligned} a + ce + be + cd &= q_1^2q_2^2q_3^2(a_1 - c_1e_1q_2q_3) - q_1q_2^2q_3^2(a_1 - c_1e_1q_2q_3)(\Delta c_1^2 + \Phi e_1^2) \\ &= q_1q_2^2q_3^2(a_1 - c_1e_1q_2q_3)[q_1 - (\Delta c_1^2 + \Phi e_1^2)] \\ &= 0. \end{aligned}$$

https://doi.org/10.1017/S1446788714000044 Published online by Cambridge University Press

Thus we deduce that

$$\begin{aligned} a + (b + c)(d + e) &= a + bd + be + cd + ce \\ &= bd + (a + ce + be + cd) \\ &= bd \\ &= -a_1c_1e_1q_2q_3(a_1 - c_1e_1q_2q_3)^2, \end{aligned} \tag{4.7}$$

which proves that the point $P_2 = (x, z) = (1, [a_1 - c_1e_1q_2q_3][-a_1c_1e_1q_2q_3]^{1/2})$ belongs to $\mathcal{D}(\mathbb{Q}_l)$. Therefore $\mathcal{D}$ is locally solvable at l.

Case 4: $l = p_i$ for some $1 \le i \le h$.

By (B2) and (B3), we easily see that

$$\left(\frac{-c_1e_1}{p_i}\right) = \left(\frac{-1}{p_i}\right)\left(\frac{c_1}{p_i}\right)\left(\frac{e_1}{p_i}\right) = 1.$$

We prove that q_2, q_3 are squares modulo p_i. We first show that q_2 is a square modulo p_i. Write

$$q_2 = \delta \prod_{l_*|q_2} l_*^{\nu_{l_*}(q_2)},$$

where the product is taken over all the primes l_* dividing q_2 and δ is either 1 or -1. Note that by (B3) we know that

$$\left(\frac{\delta}{p_i}\right) = 1.$$

By (B3), (B4) and the quadratic reciprocity law, we see that

$$\left(\frac{q_2}{p_i}\right) = \left(\frac{\delta \prod_{l_*|q_2} l_*^{\nu_{l_*}(q_2)}}{p_i}\right) = \left(\frac{\delta}{p_i}\right)\prod_{l_*|q_2}\left(\frac{l_*}{p_i}\right)^{\nu_{l_*}(q_2)} = \prod_{l_*|q_2}\left(\frac{p_i}{l_*}\right)^{\nu_{l_*}(q_2)} = 1,$$

and it thus follows that q_2 is a square modulo p_i. Repeating the same arguments as above, we can show that q_3 is a square modulo p_i. Therefore we deduce that

$$\left(\frac{-c_1e_1q_2q_3}{p_i}\right) = 1,$$

which proves that $-c_1e_1q_2q_3$ is a square in $\mathbb{Q}_{p_i}^\times$. Therefore the point P_1 in *Case 2* belongs to $\mathcal{D}(\mathbb{Q}_{p_i})$. Hence $\mathcal{D}$ is locally solvable at p_i.

Case 5: l is an odd prime such that l divides q_2q_3.

By (B4), we see that p_i is a square modulo l for each $1 \le i \le h$. Hence it follows from (4.5) that

$$\left(\frac{a_1}{l}\right) = \prod_{i=1}^{h}\left(\frac{p_i}{l}\right) = 1,$$

which proves that a_1 is a square in $\mathbb{Q}_l^\times$. Thus we see that the point at infinity ∞ in *Case 1* belongs to $\mathcal{D}(\mathbb{Q}_l)$. Therefore $\mathcal{D}$ is locally solvable at l.

Case 6: l is an odd prime such that l divides c_1.

Recall that $F(x) = ax^{2n+2} + (bx^{2m} + c)(dx^{2k} + e)$ is the polynomial defining the curve $\mathcal{D}$. We consider the following system of equations:

$$\begin{cases} F(x) & \equiv 0 \bmod l \\ \dfrac{\partial F}{\partial x}(x) & \not\equiv 0 \bmod l. \end{cases}$$

Note that

$$\frac{\partial F}{\partial x}(x) = (2n+2)ax^{2n+1} + 2mbx^{2m-1}(dx^{2k} + e) + 2kdx^{2k-1}(bx^{2m} + c).$$

Since $c_1 \equiv 0 \bmod l$, it follows from (4.7) that

$$F(1) = a + (b + c)(d + e) = -a_1c_1e_1q_2q_3(a_1 - c_1e_1q_2q_3)^2 \equiv 0 \bmod l.$$

Using (4.5) and the fact that $c_1 \equiv 0 \bmod l$, we see that

$$\begin{aligned} \frac{\partial F}{\partial x}(1) &\equiv (2n+2)a + 2ma_1e_1q_2\Phi(-e_1q_1q_2q_3^2) \\ &\equiv (2n+2)a_1q_1^2q_2^2q_3^2 - 2ma_1e_1^2q_1q_2^2q_3^2\Phi \\ &\equiv a_1q_1q_2^2q_3^2((2n+2)q_1 - 2m\Phi e_1^2) \bmod l. \end{aligned}$$

Since

$$q_1 = \Delta c_1^2 + \Phi e_1^2 \equiv \Phi e_1^2 \bmod l,$$

we deduce from (4.3), (B1) and (B6) that

$$\begin{aligned} \frac{\partial F}{\partial x}(1) &\equiv a_1q_1q_2^2q_3^2((2n+2)\Phi e_1^2 - 2m\Phi e_1^2) \\ &\equiv 2(n - m + 1)a_1e_1^2q_1q_2^2q_3^2\Phi \\ &\not\equiv 0 \bmod l. \end{aligned}$$

It thus follows from Hensel's lemma that $\mathcal{D}$ is locally solvable at l.

Case 7: l is an odd prime such that l divides e_1.

We maintain the same notation as in *Case 6*. We see that

$$F(1) = a + (b + c)(d + e) = -a_1c_1e_1q_2q_3(a_1 - c_1e_1q_2q_3)^2 \equiv 0 \bmod l.$$

Using (4.5) and the fact that $e_1 \equiv 0 \bmod l$, we see that

$$\begin{aligned} \frac{\partial F}{\partial x}(1) &\equiv (2n+2)a + 2kcd \\ &\equiv (2n+2)a_1q_1^2q_2^2q_3^2 - 2ka_1c_1^2q_1q_2^2q_3^2\Delta \\ &\equiv a_1q_1q_2^2q_3^2((2n+2)q_1 - 2k\Delta c_1^2). \end{aligned}$$

Since

$$q_1 = \Delta c_1^2 + \Phi e_1^2 \equiv \Delta c_1^2 \bmod l,$$

https://doi.org/10.1017/S1446788714000044 Published online by Cambridge University Press

we deduce from (4.4), (B1) and (B7) that

$$\begin{aligned}\frac{\partial F}{\partial x}(1,0) &\equiv a_1q_1q_2^2q_3^2((2n+2)\Delta c_1^2 - 2k\Delta c_1^2)\\ &\equiv 2(n-k+1)a_1c_1^2q_1q_2^2q_3^2\Delta\\ &\not\equiv 0 \bmod l.\end{aligned}$$

Thus it follows from Hensel's lemma that $\mathcal{D}$ is locally solvable at l.

By what we have shown, we deduce that $\mathcal{D}$ is everywhere locally solvable. □

We now prove Theorem 4.1.

Proof of Theorem 4.1. We will use Theorem 3.2 to prove that $\mathcal{D}(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} = \emptyset$. By Lemma 4.2, it suffices to show that conditions (A3)–(A8) in Theorem 3.2 hold. By (4.1), (4.2), (4.5), (B1) and (B3), we see that (A3) holds trivially. We contend that $a_1 - c_1e_1q_2q_3$ is nonzero modulo p_1. Assume the contrary, that is, $a_1 - c_1e_1q_2q_3 \equiv 0 \bmod p_1$, and hence it follows from (4.1) that

$$c_1e_1q_2q_3 \equiv 0 \bmod p_1,$$

which is in contradiction to (B1). Therefore one sees that $a_1 - c_1e_1q_2q_3 \not\equiv 0 \bmod p_1$, and hence $a_1 - c_1e_1q_2q_3 \neq 0$. Thus we see from (4.5) that $b \neq 0$. Thus (A4) holds.

Now we prove that (A5) is true. Indeed, we know from *Case 4* of the proof of Lemma 4.3 that q_2 and q_3 are squares modulo p_i for each $1 \le i \le h$. Using the same arguments as in *Case 4* of the proof of Lemma 4.3, we can show that q_1 is a square modulo p_i for each $1 \le i \le h$. Hence we deduce from (B2) and (B3) that

$$\left(\frac{c}{p_i}\right) = \left(\frac{c_1q_1q_2^2q_3}{p_i}\right) = \left(\frac{c_1}{p_i}\right)\left(\frac{q_1q_2^2q_3}{p_i}\right) = \begin{cases}-1 & \text{if } 1 \le i \le h_1,\\ 1 & \text{if } h_1+1 \le i \le h_2,\end{cases}$$

and

$$\begin{aligned}\left(\frac{e}{p_i}\right) = \left(\frac{-e_1q_1q_2q_3^2}{p_i}\right) &= \left(\frac{-1}{p_i}\right)\left(\frac{e_1}{p_i}\right)\left(\frac{q_1q_2q_3^2}{p_i}\right)\\ &= \begin{cases}-1 & \text{if } h_2+1 \le i \le h_3,\\ 1 & \text{if } h_3+1 \le i \le h.\end{cases}\end{aligned}$$

Therefore (A5) follows.

Let l be any odd prime such that l divides a_2. By (B4), we see that

$$\left(\frac{a_1}{l}\right) = \prod_{i=1}^{h}\left(\frac{p_i}{l}\right) = 1,$$

and hence it follows that a_1 is a square modulo l. Thus (A6) holds. By (4.5), we easily see that (A8) holds trivially.

We now prove that (A7) is true. Let l be an odd prime such that $\gcd(l, a_1) = 1$ and l divides $b^ke^m + (-1)^{m+k+1}c^kd^m$. Assume further that l divides $\gcd(c, e)$. Since c_1, e_1 are

https://doi.org/10.1017/S1446788714000044 Published online by Cambridge University Press

relatively prime, we see that $\gcd(c, e) = q_1q_2q_3 = a_2$. Hence l divides a_2, and thus it follows from (B4) that

$$\left(\frac{a_1}{l}\right) = \prod_{i=1}^{h}\left(\frac{p_i}{l}\right) = 1.$$

Therefore a_1 is a square modulo l, and thus (A7) holds. Applying Theorem 3.2 for the curve $\mathcal{D}$, we deduce that $\mathcal{D}(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} = \emptyset$.

By Lemma 4.3, we know that $\mathcal{D}$ is everywhere locally solvable, and thus $\mathcal{D}$ is a counterexample to the Hasse principle explained by the Brauer–Manin obstruction. Thus our contention follows. □

5. Infinitude of the quintuples (a, b, c, d, e) satisfying (B1)–(B9)

In this section, we will show how to produce families of hyperelliptic curves of arbitrary genus greater than two violating the Hasse principle explained by the Brauer–Manin obstruction. Using Theorem 4.1, it suffices to prove that there are infinitely many quintuples (a, b, c, d, e) satisfying (B1)–(B9). Following [4], we will make use of a theorem of Iwaniec on the representation of primes using quadratic polynomials to show the existence of infinitely many quintuples (a, b, c, d, e) satisfying (B5). The other conditions in Theorem 4.1 will follow immediately. Note that by introducing two more parameters q_2 and q_3 in Theorem 4.1 and imposing *mild* conditions on them, the number of the quintuples (a, b, c, d, e) satisfying (B1)–(B9) is *large*. We begin by recalling the following definition in [7].

Definition 5.1. Let $P(x, y) \in \mathbb{Q}[x, y]$ be a quadratic polynomial in two variables x and y. We say that P *depends essentially on two variables* if $\partial P/\partial x$ and $\partial P/\partial y$ are linearly independent as elements of the $\mathbb{Q}$-vector space $\mathbb{Q}[x, y]$.

Theorem 5.2 (Iwaniec [7, page 435]). *Let $P(x, y) = ax^2 + bxy + cy^2 + ex + fy + g \in \mathbb{Z}[x, y]$ be a quadratic polynomial defined over $\mathbb{Z}$, and assume that the following are true:*

(i) *a, b, c, e, f, g are in $\mathbb{Z}$ and $\gcd(a, b, c, e, f, g) = 1$;*
(ii) *$P(x, y)$ is irreducible in $\mathbb{Q}[x, y]$, represents arbitrarily large odd numbers, and depends essentially on two variables;*
(iii) *$D = af^2 - bef + ce^2 + (b^2 - 4ac)g = 0$ or $\Delta = b^2 - 4ac$ is a perfect square.*

Then

$$N \log^{-1} N \ll \sum_{\substack{p \le N,\, p = P(x,y) \\ p \text{ prime}}} 1.$$

We now prove the main result in this section.

Lemma 5.3. *Let n, m, k be positive integers such that $n > \min(m + 2k - 1, 2m + k - 1)$. Let h be a positive integer, and let h_1, h_2, h_3 be positive integers. Assume that the following are true:*

(H1) $1 \le h_1 \le h_2 \le h_3 \le h$;
(H2) $h_1 + h_3 - h_2$ *is odd; and*
(H3) *if* $h_2 = h$, *then* $n > m + 2k - 1$.

Then there are infinitely many quintuples (a, b, c, d, e) *that satisfy* (B1)–(B9) *in Theorem 4.1.*

Proof. Define

$$t = \begin{cases} 1 & \text{if } \min(m + 2k - 1, 2m + k - 1) = m + 2k - 1, \\ h & \text{if } \min(m + 2k - 1, 2m + k - 1) = 2m + k - 1 \text{ and } m \neq k. \end{cases} \tag{5.1}$$

Set

$$\mathcal{P} := \{l \text{ odd prime} \mid n - m + 1 \equiv 0 \bmod l \quad \text{or} \quad n - k + 1 \equiv 0 \bmod l\}, \tag{5.2}$$

and define

$$\epsilon := \prod_{l \in \mathcal{P}} l. \tag{5.3}$$

Note that since $n > \min(m + 2k - 1, 2m + k - 1)$, it follows that $n - m + 1 \neq 0$ and $n - k + 1 \neq 0$. Hence the set $\mathcal{P}$ is of finite cardinality.

We now define the odd primes $p_1, p_2, \ldots, p_h$. If $h = 1$, we simply choose p_1 to be an odd prime satisfying the following:

(C1*) $p_1 \equiv 1 \bmod 8$, $km \not\equiv 0 \bmod p_1$ and $p_1 \equiv 1 \bmod l$ for each $l \in \mathcal{P}$.

If $h \ge 2$, we let p_1, p_h be odd primes satisfying the following:

(C1) $p_1 \equiv 1 \bmod 4$, $p_h \equiv 1 \bmod 4$, $p_1 p_h \equiv 1 \bmod 8$;
(C2) $km \not\equiv 0 \bmod p_1$ and $km \not\equiv 0 \bmod p_h$;
(C3) $p_1 \equiv 1 \bmod l$ and $p_h \equiv 1 \bmod l$ for each $l \in \mathcal{P}$;
(C4) p_1 is a square modulo p_h.

Such odd primes p_1, p_h exist. Indeed, using the Chinese Remainder Theorem, Dirichlet's theorem on primes in arithmetic progressions, and noting that $\mathcal{P}$ is of finite cardinality, we deduce that there is an odd prime p_h such that $p_h \equiv 1 \bmod 4$, $km \not\equiv 0 \bmod p_h$ and $p_h \equiv 1 \bmod l$ for each $l \in \mathcal{P}$. Similarly, there exists an odd prime p_1 such that p_1 and km are relatively prime, $p_1 \equiv 1 \bmod l$ for each $l \in \mathcal{P}$,

$$p_1 \equiv \begin{cases} 1 \bmod 8 & \text{if } p_h \equiv 1 \bmod 8, \\ 5 \bmod 8 & \text{if } p_h \equiv 5 \bmod 8, \end{cases} \tag{5.4}$$

and p_1 is a quadratic residue modulo p_h. It is easy to see that $p_1 p_h \equiv 1 \bmod 8$, and hence p_1, p_h satisfy (C1)–(C4) above. Using similar arguments, there exist distinct odd primes $p_2, p_3, \ldots, p_{h_2}$ such that the following are true:

(C5) $p_i \equiv 1 \bmod 4$ for each $2 \le i \le h_2$ and

$$\Big(\prod_{\substack{1 \le i \le h_2, \\ i \neq h}} p_i\Big) p_h \equiv 1 \bmod 8;$$

https://doi.org/10.1017/S1446788714000044 Published online by Cambridge University Press

(C6) $p_i \equiv 1 \bmod l$ for each $l \in \mathcal{P}$ and each $2 \le i \le h_2$ with $i \ne h$;
(C7) p_i is a quadratic residue modulo p_h for each $2 \le i \le h_2$ with $i \ne h$.

Similarly, there exist distinct odd primes $p_{h_2+1}, p_{h_2+2}, \dots, p_{h-1}$ such that the following are true:

(C8) $p_i \equiv 1 \bmod 4$ for each $h_2 + 1 \le i \le h - 1$ and $\prod_{i=1}^{h} p_i \equiv 1 \bmod 8$;
(C9) $p_i \equiv 1 \bmod l$ for each $h_2 + 1 \le i \le h - 1$ and each $l \in \mathcal{P}$;
(C10) p_j is a square modulo p_i for each $1 \le i \le h_2$ and each $h_2 + 1 \le j \le h - 1$.

Define

$$a_1 := p_1 p_2 \dots p_h. \tag{5.5}$$

Since t is either 1 or h, it follows from the choice of p_1 and p_h that $km \not\equiv 0 \bmod p_t$, and hence (B8) holds. It is clear that (B3) is true.

We prove that (B9) is true. Indeed, if $h_2 = h$, then it follows from (H3) that $n > m + 2k - 1$. Thus (B9) follows immediately. Assume now that $h_2 < h$. If $t = 1$, then it follows from (5.1) that $n > m + 2k - 1$, and thus (B9) holds. If $t = h$, then it follows from (5.1) that $n > 2m + k - 1$. Since $h_2 < t = h$, we deduce that (B9) is true. Therefore, in any event, (B9) holds.

Since $\mathcal{P} \cap \{p_1, p_2, \dots, p_h\}$ is empty and $\mathcal{P}$ is a finite set of odd primes, we deduce that there are nonzero integers c_1^*, e_1^* such that the following are true:

(C11) c_1^*, e_1^* are odd and $\gcd(c_1^*, e_1^*) = 1$;
(C12) $c_1^* \equiv \frac{1}{4} \bmod l$ and $e_1^* \equiv 1 \bmod l$ for each $l \in \mathcal{P}$, where $\mathcal{P}$ is defined by (5.2);
(C13) $\gcd(c_1^*, p_i) = \gcd(e_1^*, p_i) = 1$ for each $1 \le i \le h$,

$$\left(\frac{c_1^*}{p_i}\right) = \left(\frac{e_1^*}{p_i}\right) = \begin{cases} -1 & \text{if } 1 \le i \le h_1, \\ 1 & \text{if } h_1 + 1 \le i \le h_2, \end{cases}$$

and

$$\left(\frac{c_1^*}{p_i}\right) = \left(\frac{e_1^*}{p_i}\right) = \begin{cases} -1 & \text{if } h_2 + 1 \le i \le h_3, \\ 1 & \text{if } h_3 + 1 \le i \le h. \end{cases}$$

Set

$$\Phi := \prod_{i=1}^{h_2} p_i, \tag{5.6}$$

$$\Delta := \prod_{i=h_2+1}^{h} p_i, \tag{5.7}$$

and define the quadratic polynomial $P(x, y) \in \mathbb{Z}[x, y]$ by

$$P(x, y) := 16\Delta(\epsilon a_1 x + c_1^*)^2 + \Phi(2\epsilon a_1 y + e_1^*)^2,$$

https://doi.org/10.1017/S1446788714000044 Published online by Cambridge University Press

where ϵ is defined as in (5.3). Expanding $P(x, y)$ in the form $Ax^2 + Bxy + Cy^2 + Ex + Fy + G$, we see that

$$\begin{aligned} A &= 16a_1^2\epsilon^2\Delta, \\ B &= 0, \\ C &= 4a_1^2\epsilon^2\Phi, \\ E &= 32a_1c_1^*\epsilon\Delta, \\ F &= 4a_1e_1^*\epsilon\Phi, \\ G &= 16{c_1^*}^2\Delta + {e_1^*}^2\Phi. \end{aligned}$$

We prove that $\gcd(A, B, C, E, F, G) = 1$. Since Δ and Φ are relatively prime, we see that $\gcd(A, C) = 4a_1^2\epsilon^2$. Hence it suffices to prove that $\gcd(4a_1^2\epsilon^2, G) = 1$, that is, $G \not\equiv 0 \bmod 2$, $G \not\equiv 0 \bmod p_i$ for each $1 \le i \le h$ and $G \not\equiv 0 \bmod l$ for each $l \in \mathcal{P}$. Since e_1^* is odd, it is obvious that $G \equiv 1 \bmod 2$. By the definition of Δ and Φ, it follows from (C13) that

$$G = 16{c_1^*}^2\Delta + {e_1^*}^2\Phi \equiv 16{c_1^*}^2\Delta \not\equiv 0 \mod p_i$$

for each $1 \le i \le h_2$, and

$$G = 16{c_1^*}^2\Delta + {e_1^*}^2\Phi \equiv {e_1^*}^2\Phi \not\equiv 0 \mod p_i$$

for each $h_2 + 1 \le i \le h$. Hence it remains to show that $G \not\equiv 0 \bmod l$ for each $l \in \mathcal{P}$. By (C3), (C6), (C9), (C12), (5.6) and (5.7) and since l is odd for each $l \in \mathcal{P}$, we deduce that

$$G = 16{c_1^*}^2\Delta + {e_1^*}^2\Phi \equiv 1 + 1 \equiv 2 \not\equiv 0 \mod l$$

for each $l \in \mathcal{P}$. Thus it follows that $\gcd(4a_1^2\epsilon^2, G) = 1$, and hence $\gcd(A, C, G) = 1$. Therefore $\gcd(A, B, C, E, F, G) = 1$, and thus condition (i) in Theorem 5.2 is true. One can verify that

$$D = AF^2 - BEF + CE^2 + (B^2 - 4AC)G = 0,$$

and hence condition (iii) in Theorem 5.2 holds. Furthermore, since $\Phi(2\epsilon a_1y + e_1^*)^2$ is an odd integer, we see that $P(x, y)$ represents arbitrarily large odd numbers. It is clear that $P(x, y)$ is irreducible in $\mathbb{Q}[x, y]$, and that it depends essentially on two variables. Thus condition (ii) in Theorem 5.2 is true. Hence Theorem 5.2 says that there are infinitely many odd primes q such that $q = P(x, y)$ for some $x, y \in \mathbb{Z}$. Take such integers x, y, and define

$$c_1 := 4(\epsilon a_1x + c_1^*), \tag{5.8}$$

$$e_1 := 2\epsilon a_1y + e_1^*, \tag{5.9}$$

and

$$q_1 := P(x, y) = \Delta c_1^2 + \Phi e_1^2. \tag{5.10}$$

Let $\mathcal{S}$ be the set of odd primes l satisfying the following conditions:

(i) $\gcd(l, c_1) = \gcd(l, e_1) = 1$ and $\gcd(l, p_i) = 1$ for each $1 \le i \le h$;

(ii) l is a square modulo p_i for each $1 \le i \le h$.

https://doi.org/10.1017/S1446788714000044 Published online by Cambridge University Press

We see that the set $\mathcal{S}$ is of *infinite* cardinality. Let I and J be (possibly empty) finite subsets of $\mathcal{S}$. For each $l \in I$, take a positive integer m_l, and for each $l \in J$, take a positive integer n_l. Define

$$q_2 := \prod_{l \in I} l^{m_l}, \tag{5.11}$$

and

$$q_3 := \prod_{l \in J} l^{n_l}. \tag{5.12}$$

We set

$$a_2 := q_1 q_2 q_3, \tag{5.13}$$

where q_1, q_2, q_3 are defined by (5.10)–(5.12), respectively.

Recall that we have shown above that (B3), (B8) and (B9) are true. It remains to prove that (B1), (B2) and (B4)–(B7) are true. By (5.6), (5.7) and (5.10), we see that (B5) holds trivially. By (5.8), (5.9), we see that

$$c_1 = 4(\epsilon a_1 x + c_1^*) \equiv 4c_1^* \not\equiv 0 \bmod p_i$$

and

$$e_1 = 2\epsilon a_1 y + e_1^* \equiv e_1^* \not\equiv 0 \bmod p_i$$

for each $1 \le i \le h$. By (5.10) and since q_1 is an odd prime, we deduce that $\gcd(c_1, q_1) = \gcd(e_1, q_1) = \gcd(c_1, e_1) = 1$. It is easy to see from (5.10) that $\gcd(q_1, p_i) = 1$ for each $1 \le i \le h$. By the definition of $\mathcal{S}$, it is now clear that (B1) holds.

Since $c_1 \equiv 4c_1^* \bmod p_i$ for each $1 \le i \le h$, we see that

$$\left(\frac{c_1}{p_i}\right) = \left(\frac{4c_1^*}{p_i}\right) = \left(\frac{4}{p_i}\right)\left(\frac{c_1^*}{p_i}\right) = \left(\frac{c_1^*}{p_i}\right) = \begin{cases} -1 & \text{if } 1 \le i \le h_1, \\ 1 & \text{if } h_1 + 1 \le i \le h_2. \end{cases}$$

Since $e_1 \equiv e_1^* \bmod p_i$ for each $1 \le i \le h$, using the same arguments as above, we deduce that

$$\left(\frac{e_1}{p_i}\right) = \left(\frac{e_1^*}{p_i}\right) = \begin{cases} -1 & \text{if } 1 \le i \le h_1, \\ 1 & \text{if } h_1 + 1 \le i \le h_2. \end{cases}$$

Similarly, one can show that

$$\left(\frac{c_1}{p_i}\right) = \left(\frac{e_1}{p_i}\right) = \begin{cases} -1 & \text{if } h_2 + 1 \le i \le h_3, \\ 1 & \text{if } h_3 + 1 \le i \le h. \end{cases}$$

Therefore (B2) holds.

We now prove that (B4) is true. Let l be any odd prime dividing a_2. If l divides $q_2 q_3$, then we see that l belongs to the set $\mathcal{S}$. By the definition of $\mathcal{S}$, we deduce that l is a square modulo p_i for each $1 \le i \le h$. By the quadratic reciprocity law and since $p_i \equiv 1 \bmod 4$ for each $1 \le i \le h$, we deduce that p_i is a square modulo l for

https://doi.org/10.1017/S1446788714000044 Published online by Cambridge University Press

each $1 \le i \le h$. If l divides q_1, then it follows that $l = q_1$ since q_1 is an odd prime. By (5.10), we see that

$$q_1 \equiv \begin{cases} \Delta c_1^2 \mod p_i & \text{if } 1 \le i \le h_2, \\ \Phi e_1^2 \mod p_i & \text{if } h_2 + 1 \le i \le h. \end{cases}$$

We contend that Δ is a square modulo p_i for each $1 \le i \le h_2$ and Φ is a square modulo p_i for each $h_2 + 1 \le i \le h$. Indeed, by (C4), (C7) and the quadratic reciprocity law, we know that p_h is a square modulo p_i for each $1 \le i \le h_2$. Thus it follows from (C10) that p_j is a square modulo p_i for each $1 \le i \le h_2$ and $h_2 + 1 \le j \le h$. Using the quadratic reciprocity law and noting that $p_i \equiv 1 \bmod 4$ for each $1 \le i \le h$, we deduce that p_i is a square modulo p_j k for each $1 \le i \le h_2$ and $h_2 + 1 \le j \le h$. Thus it follows from (5.6), (5.7) that Δ is a square modulo p_i for each $1 \le i \le h_2$ and Φ is a square modulo p_i for each $h_2 + 1 \le i \le h$. Therefore we deduce that

$$\left(\frac{q_1}{p_i}\right) = \left(\frac{\Delta c_1^2}{p_i}\right) = \left(\frac{\Delta}{p_i}\right) = 1$$

for each $1 \le i \le h_2$, and that

$$\left(\frac{q_1}{p_i}\right) = \left(\frac{\Phi e_1^2}{p_i}\right) = \left(\frac{\Phi}{p_i}\right) = 1$$

for each $h_2 + 1 \le i \le h$. Thus, in any case, q_1 is a quadratic residue modulo p_i for each $1 \le i \le h$, and hence it follows from the quadratic reciprocity law that p_i is a square modulo q_1 for each $1 \le i \le h$. Therefore (B4) holds.

We prove that (B6) is true. Assume the contrary, that is, there is an odd prime l dividing c_1 such that $n - m + 1 \equiv 0 \bmod l$. It follows that l belongs to $\mathcal{P}$, where $\mathcal{P}$ is defined by (5.2). Hence it follows from (5.3) that $\epsilon \equiv 0 \bmod l$. By (5.8) and (C12), we see that

$$c_1 = 4(\epsilon a_1 x + c_1^*) \equiv 4c_1^* \equiv 1 \mod l,$$

which is a contradiction since $c_1 \equiv 0 \bmod l$. Thus $n - m + 1 \not\equiv 0 \bmod l$, and therefore (B6) holds.

We now show that (B7) holds. Assume the contrary, that is, there is an odd prime l dividing e_1 such that $n - k + 1 \equiv 0 \bmod l$. It follows that l belongs to $\mathcal{P}$, and hence $\epsilon \equiv 0 \bmod l$. By (5.9) and (C12), we deduce that

$$e_1 = 2\epsilon a_1 y + e_1^* \equiv e_1^* \equiv 1 \mod l,$$

which is a contradiction since $e_1 \equiv 0 \bmod l$. Thus $n - k + 1 \not\equiv 0 \bmod l$, and therefore (B7) holds.

Now let (a, b, c, d, e) be the quintuple defined as in (4.5). By what we have shown, we see that the quintuple (a, b, c, d, e) satisfies (B1)–(B9) in Theorem 4.1, which proves our contention. □

https://doi.org/10.1017/S1446788714000044 Published online by Cambridge University Press

COROLLARY 5.4. *Let k, m, n be positive integers such that*

$$n > \min(2m + k - 1, m + 2k - 1).$$

Then there exist infinitely many quintuples (a, b, c, d, e) of integers such that the smooth projective model $\mathcal{D}^{(n,m,k)}_{(a,b,c,d,e)}$ of the affine curve defined by

$$\mathcal{D}^{(n,m,k)}_{(a,b,c,d,e)} : z^2 = ax^{2n+2} + (bx^{2m} + c)(dx^{2k} + e)$$

is of genus n and a counterexample to the Hasse principle explained by the Brauer–Manin obstruction.

PROOF. Let h be any positive integer, and let h_1, h_2, h_3 be positive integers satisfying (H1), (H2), (H3) in Lemma 5.3. Using Lemma 5.3 and Theorem 4.1, our contention follows immediately. □

REMARK 5.5. For positive integers k, m, n with

$$n > \min(2m + k - 1, m + 2k - 1),$$

Corollary 5.4 says that there are infinitely many hyperelliptic curves of genus n that are counterexamples to the Hasse principle explained by the Brauer–Manin obstruction. The construction of such hyperelliptic curves are *explicit*, and the proof of Lemma 5.3 can be viewed as an algorithm for producing hyperelliptic curves of arbitrary genus greater than two violating the Hasse principle explained by the Brauer–Manin obstruction. We will use the proof of Lemma 5.3 to produce families of hyperelliptic curves of arbitrary genus greater than two with fixed coefficients in the example below.

EXAMPLE 5.6. Let $h = 2$, and let $(h_1, h_2, h_3) = (1, 2, 2)$. Let $p_1 = 17$ and $p_2 = 89$. Let $c_1 = 44, e_1 = 5$, and let $q_1 = 39\,761$. We see that

$$q_1 = 39\,761 = 44^2 + 17 \times 89 \times 5^2 = c_1^2 + p_1 p_2 e_1^2.$$

Following the proof of Lemma 5.3, let $\mathcal{S}$ be the set of odd primes l satisfying the following conditions:

(i) $l \not\equiv 0 \bmod 5$, $l \not\equiv 0 \bmod 11$, $l \not\equiv 0 \bmod 17$ and $l \not\equiv 0 \bmod 89$;
(ii) l is a quadratic residue modulo 17;
(iii) l is a quadratic residue modulo 89.

Note that $\mathcal{S}$ is of infinite cardinality. For example, the set consisting of the primes 47, 53, 67, 157, 179, 223, 251, 257, 263, 271, 307, 331, 373, 409, 443, 461, 463, 467 is a subset of $\mathcal{S}$ consisting of the primes in $\mathcal{S}$ that are less than 500.

Let I and J be (possible empty) finite subsets of $\mathcal{S}$. For each $l \in I$, choose a positive integer m_l, and for each $l \in J$, take a positive integer n_l. We define

$$q_2 := \prod_{l \in I} l^{m_l} \tag{5.14}$$

and

$$q_3 := \prod_{l \in J} l^{n_l}. \tag{5.15}$$

We set

$$a_1 := p_1 p_2 = 1513$$

and

$$a_2 := q_1 q_2 q_3 = 39\,761\Big(\prod_{l \in I} l^{m_l}\Big)\Big(\prod_{l \in J} l^{n_l}\Big).$$

Following (4.5) and the proof of Lemma 5.3, we define

$$\begin{cases} a := a_1 a_2^2 = 2\,391\,957\,864\,073 q_2^2 q_3^2 \\ b := p_1 p_2 (a_1 - c_1 e_1 q_2 q_3) e_1 q_2 = 7565 q_2 (1513 - 220 q_2 q_3) \\ c := c_1 q_1 q_2^2 q_3 = 1\,749\,484 q_2^2 q_3 \\ d := -(a_1 - c_1 e_1 q_2 q_3) c_1 q_3 = -44 q_3 (1513 - 220 q_2 q_3) \\ e := -e_1 q_1 q_2 q_3^2 = -198\,805 q_2 q_3^2. \end{cases} \tag{5.16}$$

Let $\mathcal{Z}$ be the set of triples (n, m, k) of positive integers satisfying the following four conditions:

(i) $n - m + 1 \not\equiv 0 \bmod 11$;
(ii) $n - k + 1 \not\equiv 0 \bmod 5$;
(iii) $km \not\equiv 0 \bmod 17$ and $km \not\equiv 0 \bmod 89$;
(iv) $n > m + 2k - 1$.

By condition (iv) above, we see that conditions (H1), (H2), (H3) in Lemma 5.3 are true. As shown in the proof of Lemma 5.3, we see that the quintuple (a, b, c, d, e) defined by (5.16) satisfies (B1)–(B9) in Theorem 4.1.

Let $(n, m, k) \in \mathcal{Z}$, and let $\mathcal{D}^{(n,m,k)}_{(a,b,c,d,e)}$ be the smooth projective model of the affine curve defined by

$$\mathcal{D}^{(n,m,k)}_{(a,b,c,d,e)} : z^2 = a x^{2n+2} + (b x^{2m} + c)(d x^{2k} + e).$$

Then it follows from Theorem 4.1 that $\mathcal{D}^{(n,m,k)}_{(a,b,c,d,e)}$ is a counterexample to the Hasse principle explained by the Brauer–Manin obstruction.

In Table 1, we list the curves $\mathcal{D}^{(n,m,k)}_{(a,b,c,d,e)}$ for a few special values of (a, b, c, d, e), where (n, m, k) is an arbitrary triple in $\mathcal{Z}$.

Remark 5.7. We contend that for a positive integer $n \geq 3$, there exists a pair (m, k) of positive integers such that the triple (n, m, k) belongs to the set $\mathcal{Z}$ in Example 5.6. Indeed, if $n \not\equiv 0 \bmod 11$ and $n \not\equiv 0 \bmod 5$, then letting $k = m = 1$, one can verify that the triple (n, m, k) satisfies conditions (i)–(iv) of the set $\mathcal{Z}$. Hence (n, m, k) belongs to $\mathcal{Z}$. It remains to consider the case when $n \equiv 0 \bmod 11$ or $n \equiv 0 \bmod 5$. Assume first that $n \equiv 0 \bmod 11$. We see that $n \geq 11$. Let k be a positive integer such that $1 \leq k \leq 4$ and $k \not\equiv n + 1 \bmod 5$, and let $m = 2$. We see that

$$m + 2k - 1 = 2 + 2k - 1 = 2k + 1 \leq 9 < n.$$

TABLE 1. Certain hyperelliptic curves $\mathcal{D}^{(n,m,k)}_{(a,b,c,d,e)}$ with $(n, m, k) \in \mathcal{Z}$ violating the Hasse principle.

q_2	q_3	$\mathcal{D}^{(n,m,k)}_{(a,b,c,d,e)}$
1	1	$z^2 = 239\,195\,786\,4073x^{2n+2}$ $-(9\,781\,545x^{2m} + 1\,749\,484)(56\,892x^{2k} + 198\,805)$
1	47	$z^2 = 5\,283\,834\,921\,737\,257x^{2n+2}$ $-(66\,776\,255x^{2m} - 82\,225\,748)(18\,254\,236x^{2k} - 439\,160\,245)$
53	1	$z^2 = 6\,719\,009\,640\,181\,057x^{2n+2}$ $-(4\,068\,388\,915x^{2m} - 4\,914\,300\,556)(446\,468x^{2k} - 10\,536\,665)$

Hence the triple (n, m, k) satisfies condition (iv) of the set $\mathcal{Z}$. One can show that (n, m, k) satisfies conditions (i)–(iii) of $\mathcal{Z}$, and thus $(n, m, k) \in \mathcal{Z}$.

Assume now that $n \equiv 0 \bmod 5$ and $n \not\equiv 0 \bmod 11$. We see that $n \geq 5$. Letting $m = 1$ and $k = 2$, we deduce that

$$m + 2k - 1 = 4 < n.$$

Thus the triple (n, m, k) satisfies condition (iv) of $\mathcal{Z}$. It is not difficult to see that (n, m, k) satisfies conditions (i)–(iii) of $\mathcal{Z}$, and thus $(n, m, k) \in \mathcal{Z}$.

REMARK 5.8. Remark 5.7 says that for a given positive integer $n \geq 3$ there is a pair (m, k) of positive integers such that the triple (n, m, k) belongs to $\mathcal{Z}$. Hence the genus of the curves in Example 5.6 ranges over the set of positive integers greater than 2. Thus Example 5.6 produces families of hyperelliptic curves of arbitrary genus greater than 2 that are counterexamples to the Hasse principle explained by the Brauer–Manin obstruction.

Acknowledgements

I would like to thank Romyar Sharifi for useful comments on Lemma 4.1.1 in my PhD Thesis, which is a special case of Theorem 2.1. I am grateful to the referee for a very careful reading and making many extremely useful comments and suggestions that greatly improved the paper. I also thank the referee for pointing out some errors in an earlier version of this paper.

References

[1] H. Cohen, *Number Theory, Volume I: Tools and Diophantine Equations*, Graduate Texts in Mathematics, 239 (Springer, New York, 2007).

[2] J. -L. Colliot-Thélène, D. F. Coray and J. -J. Sansuc, 'Descente et principe de Hasse pour certaines variétés rationnalles', *J. reine angew. Math* **320** (1980), 150–191.

[3] D. Coray and C. Manoil, 'On large Picard groups and the Hasse principle for curves and $K3$ surfaces', *Acta. Arith.* **76** (1996), 165–189.

[4] N. N. Dong Quan, 'The Hasse principle for certain hyperelliptic curves and forms', *Q. J. Math.* **64** (2013), 253–268.

[5] N. N. Dong Quan, 'Algebraic families of hyperelliptic curves violating the Hasse principle', 2013. Available at http://www.math.ubc.ca/~dongquan/JTNB-algebraic-families.pdf.

[6] N. N. Dong Quan, 'Nonexistence of rational points on certain varieties', PhD Thesis, University of Arizona, 2012.

https://doi.org/10.1017/S1446788714000044 Published online by Cambridge University Press

[7] H. Iwaniec, 'Primes represented by quadratic polynomials in two variables', *Acta Arith.* **24** (1974), 435–459.
[8] J. Jahnel, 'Brauer groups, Tamagawa measures, and rational points on algebraic varieties', Habilitationsschrift, Georg-August-Universität Göttingen, 2008.
[9] C. E. Lind, 'Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Eins', Thesis, University of Uppasala, 1940.
[10] Yu. I. Manin, 'Le groupe de Brauer-Grothendieck en géométrie Diophantienne', *Actes, Congres. Intern. Math.* **1** (1970), 401–411.
[11] H. Reichardt, 'Einige im Kleinen überall lösbre, im Grossen unlösbare diophantische Gleichungen', *J. reine angew. Math.* **184** (1942), 12–18.
[12] A. N. Skorobogatov, *Torsors and Rational Points*, Cambridge Tracts in Mathematics, 144 (Cambridge University Press, Cambridge, 2001).
[13] B. Viray, 'Failure of the Hasse principle for Châtelet surfaces in characteristic 2', *J. Théor. Nombres Bordeaux* **24** (2012), 231–236.

NGUYEN NGOC DONG QUAN, Department of Mathematics,
University of British Columbia, Vancouver, British Columbia, V6T 1Z2, Canada
e-mail: dongquan.ngoc.nguyen@gmail.com

https://doi.org/10.1017/S1446788714000044 Published online by Cambridge University Press