

ON THE HASSE PRINCIPLE FOR CERTAIN QUARTIC HYPERSURFACES

NGUYEN NGOC DONG QUAN

(Communicated by Ken Ono)

Dedicated to my parents

ABSTRACT. We prove that there are infinitely many non-isomorphic quartic curves which are counter-examples to the Hasse principle explained by the Brauer-Manin obstruction. Further, these quartic curves have no points defined over number fields of odd degree. As a consequence, we show that there are infinitely many quartic hypersurfaces of arbitrary dimension violating the Hasse principle.

1. INTRODUCTION

Let k be a global field and \mathbb{A}_k be the adèle ring of k . Let \mathcal{V} be a smooth geometrically irreducible variety defined over k and let $\text{Br}(\mathcal{V})$ be the Brauer group of \mathcal{V} , that is, the group of equivalence classes of Azumaya algebras on \mathcal{V} . In 1970, Manin (see [12]) introduced a set $\mathcal{V}(\mathbb{A}_k)^{\text{Br}}$ given by

$$\mathcal{V}(\mathbb{A}_k)^{\text{Br}} = \left\{ (P_v) \in \mathcal{V}(\mathbb{A}_k) \text{ such that } \sum_v \text{inv}_v \mathcal{A}(P_v) = 0 \text{ for all } \mathcal{A} \in \text{Br}(\mathcal{V}) \right\},$$

where for each valuation v and each Azumaya algebra $\text{Br}(\mathcal{V})$, $\text{inv}_v : \text{Br}(k_v) \rightarrow \mathbb{Q}/\mathbb{Z}$ is the local invariant map from class field theory and $\mathcal{A}(P_v)$ is defined as follows. A point $P_v \in \mathcal{V}(k_v)$ gives a map $\text{Spec}(k_v) \rightarrow \mathcal{V}$ and hence induces a pullback map $\text{Br}(\mathcal{V}) \rightarrow \text{Br}(k_v)$. We write $\mathcal{A}(P_v)$ for the image of \mathcal{A} under this map.

It is well-known that

$$\mathcal{V}(k) \subseteq \mathcal{V}(\mathbb{A}_k)^{\text{Br}} \subseteq \mathcal{V}(\mathbb{A}_k).$$

We say that \mathcal{V} satisfies *the Hasse principle* if the following is true:

$$\mathcal{V}(k) \neq \emptyset \Leftrightarrow \mathcal{V}(k_v) \neq \emptyset \forall v.$$

If $\mathcal{V}(k) = \emptyset$ and $\mathcal{V}(\mathbb{A}_k) \neq \emptyset$, we say that \mathcal{V} is *a counter-example to the Hasse principle*. Further, if we also have $\mathcal{V}(\mathbb{A}_k)^{\text{Br}} = \emptyset$, we say that \mathcal{V} is *a counter-example to the Hasse principle explained by the Brauer-Manin obstruction*.

Received by the editors November 14, 2009 and, in revised form, July 5, 2010 and October 26, 2010.

2010 *Mathematics Subject Classification*. Primary 14G05, 11G35, 11G30.

Key words and phrases. Azumaya algebras, Brauer groups, Brauer-Manin obstruction, Hasse principle, quartic hypersurfaces.

In 1921, Hasse proved that smooth quadric hypersurfaces of arbitrary dimension satisfy the Hasse principle. The first counter-examples of genus one curves to the Hasse principle were discovered by Lind ([11]) in 1940 and independently by Reichardt ([17]).

The purpose of this paper is to construct infinitely many absolutely irreducible non-isomorphic quartic curves which (i) violate the Hasse principle, (ii) have no points defined over arbitrary number fields of odd degree over \mathbb{Q} and (iii) are counter-examples to the Hasse principle explained by the Brauer-Manin obstruction. As a consequence, we prove that there are infinitely many quartic hypersurfaces of arbitrary dimension violating the Hasse principle. More precisely, we shall prove the following.

Theorem 1.1. *Let p be a prime such that $p \equiv 1 \pmod{16}$. Assume the following is true:*

- (A1) *There are integers d , m and a prime q for which $d^2 = pm^2 + q$.*
- (A2) *d is a quadratic non-residue in \mathbb{F}_p^\times and $d \equiv 0, \pm 3 \pmod{5}$.*
- (A3) *$m \equiv 0, \pm 3 \pmod{5}$, $m \equiv \pm 3 \pmod{13}$, $m \equiv \pm 3, \pm 6, \pm 8, \pm 10 \pmod{17}$, $m \equiv 0, \pm 1, \pm 2, \pm 3, \pm 7, \pm 15, \pm 16, \pm 20 \pmod{29}$, m is odd and $d - m \not\equiv 0 \pmod{5}$.*

Let $\mathcal{X} \subseteq \mathbb{P}_{\mathbb{Q}}^2$ be the curve defined by

$$\mathcal{X} : x^4 - py^4 = q(y^2 + qz^2)^2.$$

Then, \mathcal{X} has points everywhere locally and is a counter-example to the Hasse principle explained by the Brauer-Manin obstruction. Furthermore, $\mathcal{X}(L) = \emptyset$ for any number field L of odd degree over \mathbb{Q} .

Remark 1.2. Conditions (A1), (A2) and (A3) guarantee local solubility of \mathcal{X} . In Section 4, we shall prove that there are infinitely many quadruples (p, q, d, m) satisfying (A1), (A2) and (A3).

Theorem 1.1 will be proved in Section 3. In Section 4 and Section 5, we shall prove the following.

Theorem 1.3. *There are infinitely many quadruples of integers (p, q, d, m) satisfying the conditions (A1), (A2) and (A3) above. A subset of these pairs gives rise to infinitely many pairwise non-isomorphic curves that satisfy the conclusions of Theorem 1.1.*

Corollary 1.4. *There exist infinitely many quartic hypersurfaces in $\mathbb{P}_{\mathbb{Q}}^{n-1}$ defined by*

$$x_1^4 - px_2^4 - q(x_3^2 + q(x_4^2 + \cdots + x_n^2))^2 = 0,$$

which violate the Hasse principle and have no points defined over arbitrary number fields of odd degree.

The infinite family of quartic curves described in Theorem 1.1 is *arithmetic* in nature. So, it is natural to ask whether there exists an *algebraic family of quartic curves* satisfying the conclusions of Theorem 1.1. This is known for genus one curves; more precisely, Poonen ([13]) constructed an algebraic family of genus one curves

$$5x^3 + 9y^3 + 10z^3 + 12 \left(\frac{t^2 + 82}{t^2 + 22} \right)^3 (x + y + z)^3 = 0, \quad t \in \mathbb{Q},$$

violating the Hasse principle.

2. THE HASSE PRINCIPLE ON ABSOLUTELY IRREDUCIBLE QUARTIC HYPERSURFACES

In this section, we shall prove the main lemmas which play a central role in the proof of Theorem 1.1.

For the proof of Lemma 2.2, we need the following.

Lemma 2.1. *Let p be a prime such that $p \equiv 1 \pmod{16}$ and assume (A1), (A2), (A3). Then, the polynomial $f(x, y, z) = x^4 - py^4 - q(y^2 + qz^2)^2$ is irreducible in every field of characteristic different from 2, p and q .*

Proof. Let k be a field of characteristic different from 2, p and q . It suffices to prove that $f(x, y, z)$ is irreducible as a polynomial in x over $k(y, z)$. Assume the contrary. Then, we see that $f(x, y, z) = x^4 - ((p + q)y^4 + 2q^2y^2z^2 + q^3z^4)$, and hence by Capelli’s theorem (see [16], Satz 428) we have that $\pm[(p + q)y^4 + 2q^2y^2z^2 + q^3z^4]$ is a square in $k(y, z)$. It follows from this that $4q^4 - 4(p + q)q^3$ must be zero, which is possible only if $\text{char} k = 2, p$, or q , proving our contention. \square

Now we prove that there exist certain quartic curves having points everywhere locally.

Lemma 2.2. *Let p be a prime such that $p \equiv 1 \pmod{16}$. Assume (A1), (A2), (A3) and let \mathcal{X} be the curve given by*

$$\mathcal{X} : x^4 - py^4 = q(y^2 + qz^2)^2.$$

Then, \mathcal{X} has points everywhere locally.

Proof. The defining equation of \mathcal{X} can be rewritten in the form

$$f(x, y, z) = x^4 - (p + q)y^4 - 2q^2y^2z^2 - q^3z^4 = 0.$$

We shall show that $f(x, y, z)$ represents 0 in every l -adic field \mathbb{Q}_l , including $\mathbb{Q}_\infty = \mathbb{R}$.

For the real field \mathbb{R} , we see that $P = (x, y, z) = (\sqrt[4]{p + q}, 1, 0)$ clearly lies on \mathcal{X} .

Suppose that $l \geq 37$ is a prime for which \mathcal{X} is smooth and geometrically irreducible. Then it follows that the genus of \mathcal{X} is 3, and hence Weil’s inequality mandates an l -adic point on \mathcal{X} .

Now, consider the following systems of equations when l is in $\{3, 5, 7, 11, 13, 17, 19, 23, 29, 31\}$:

- (1) $f(x, y, z) \equiv 0 \pmod{l}, \frac{\partial f}{\partial x}(x, y, z) \not\equiv 0 \pmod{l},$
- (2) $f(x, y, z) \equiv 0 \pmod{l}, \frac{\partial f}{\partial y}(x, y, z) \not\equiv 0 \pmod{l},$
- (3) $f(x, y, z) \equiv 0 \pmod{l}, \frac{\partial f}{\partial z}(x, y, z) \not\equiv 0 \pmod{l}.$

It is not difficult to show that systems (1), (2) and (3) have no solutions if and only if l, p and q take values given in Table 1.

It is not hard to check that the values of (p, q, l) given in Table 1 contradict assumptions (A1), (A2) and (A3). For example, assume that $(p \pmod{5}, q \pmod{5})$ are (1, 2), (1, 3), and (3, 4), respectively. Then, it follows from $pm^2 + q = d^2$ and $d \equiv 0, \pm 3 \pmod{5}$ that $m^2 \equiv 1, 2, 3 \pmod{5}$. However, 2, 3 are non-squares in \mathbb{F}_5 and $m \equiv 0, \pm 3 \pmod{5}$; this is a contradiction.

TABLE 1. Values of (p, q, l) do not satisfy (1), (2) and (3)

l	5	5	5	13	13	13	13	13	13	
$p \bmod l$	1	1	3	4	7	8	10	11	12	
$q \bmod l$	2	3	4	11	10	4	8	12	7	
l	17	17	17	29	29	29	29	29	29	29
$p \bmod l$	6	7	10	1	7	16	20	23	24	25
$q \bmod l$	2	8	9	17	3	11	21	14	2	19

Hence, in any event, we know that there are points on \mathcal{X} in \mathbb{Q}_l , where l is in the set $\{3, 5, 7, 11, 13, 17, 19, 23, 29, 31\}$.

Suppose that $l = 2$. By assumption, we know that $p \equiv 1 \pmod{4}$ and m is odd. Hence, by the fact that $q = d^2 - pm^2$ and q is prime, we know that $q \equiv 3 \pmod{4}$. Thus, $q \equiv 3, 7, 11, 15, 19, 23, 27, 31 \pmod{32}$. Furthermore, it is not hard to see that $p \equiv 1, 17 \pmod{32}$. Table 2 shows triples (x, y, z) of integers such that $f(x, y, z) \equiv 0 \pmod{2^5}$ and $\frac{\partial f}{\partial x} = 4x^3 \not\equiv 0 \pmod{2^3}$.

TABLE 2. 2-adic points on \mathcal{X}

p	q	(x, y, z)	p	q	(x, y, z)
1	3	(1, 3, 1)	17	3	(1, 1, 1)
1	7	(1, 1, 1)	17	7	(1, 3, 1)
1	11	(1, 3, 1)	17	11	(1, 1, 1)
1	15	(1, 1, 1)	17	15	(1, 3, 1)
1	19	(1, 3, 1)	17	19	(1, 1, 1)
1	23	(1, 1, 1)	17	23	(1, 3, 1)
1	27	(1, 3, 1)	17	27	(1, 1, 1)
1	31	(1, 1, 1)	17	31	(1, 3, 1)

It follows from Table 2 and Hensel’s lemma that \mathcal{X} is locally solvable in \mathbb{Q}_2 .

Now suppose that $l = q$. The equation of \mathcal{X} modulo q is of the form $x^4 - py^4 = 0$. Since $p \equiv (d/m)^2 \pmod{q}$ and $q \equiv 3 \pmod{4}$, p must be a quadratic, hence quartic, residue modulo q . Therefore, $p = u^4$ for some $u \in \mathbb{F}_q^\times$, and thus

$$f(u, 1, 1) = u^4 - p \equiv 0 \pmod{q} \quad \text{and} \quad \frac{\partial f}{\partial x}(u, 1, 1) = 4u^3 \not\equiv 0 \pmod{q}.$$

So, we know by Hensel’s lemma that there is a point on \mathcal{X} , defined over \mathbb{Q}_q .

Suppose that $l = p$. Then the equation of \mathcal{X} modulo p is of the form

$$x^4 - q(y^2 + qz^2)^2 = 0.$$

We know that $q \equiv d^2 \pmod{p}$; thus q is a square in \mathbb{Q}_p , that is, $q = u^2$ with $u \in \mathbb{Q}_p^\times$. Hence, the equation of \mathcal{X} can be rewritten in the form

$$(x^2 - u(y^2 + qz^2))(x^2 + u(y^2 + qz^2)) = 0$$

in \mathbb{Q}_p . Both quadratic forms $[x^2 \pm u(y^2 + qz^2)]$ have p -adic units as their coefficients. Thus, there are non-trivial points on both quadratic forms, defined over \mathbb{Q}_p . It therefore follows from Hensel’s lemma that there are points on \mathcal{X} , defined over \mathbb{Q}_p .

Suppose that l is a prime for which \mathcal{X} is singular at l . Then, using the Jacobian criterion, one sees that $l|(p+q)$. With no loss of generality, we can assume $l \geq 37$ and $l \neq p, q$. In the finite field \mathbb{F}_l , \mathcal{X} is of the form $x^4 - 2q^2y^2z^2 - q^3z^4$. We know that an affine model of \mathcal{X} is

$$\mathcal{X}_a : x^4 - 2q^2y^2 - q^3 = 0.$$

Since $l \neq q$, it follows that over \mathbb{F}_l , \mathcal{X}_a is birationally isomorphic to the curve given by

$$\mathcal{X}_q : Y^2 = 2X^4 - 2q^3.$$

The discriminant of \mathcal{X}_q is $-2^{18}q^9$, which is non-zero in \mathbb{F}_l . Thus, \mathcal{X}_q is of genus 1 over \mathbb{F}_l , and it follows immediately from this that the curve \mathcal{X} is of genus 1 over \mathbb{F}_l as well. We know by Weil's inequality that there are points on \mathcal{X} defined over \mathbb{F}_l if l is greater than 11, which is the case since $l \geq 37$. Thus, it follows from Hensel's lemma that \mathcal{X} contains points defined over \mathbb{Q}_l , where $l|(p+q)$ and $l \neq p, q$.

Hence, it follows from Lemma 2.1 that \mathcal{X} is everywhere locally solvable. \square

Lemma 2.3. *Let p be a prime such that $p \equiv 1 \pmod{16}$. Assume (A1), (A2), (A3).*

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

$$(4) \quad qz^2 = x^4 - p.$$

Let $\mathbb{Q}(\mathcal{D})$ be the function field of \mathcal{D} and let \mathcal{A} be the class of the quaternion algebra $(p, qz + dx^2 + pm)$. Then \mathcal{A} is an Azumaya algebra of \mathcal{D} ; that is, \mathcal{A} belongs to the subgroup $Br(\mathcal{D})$ of $Br(\mathbb{Q}(\mathcal{D}))$. Further, the quaternion algebras \mathcal{A} , $\mathcal{B} = (p, qz - dx^2 - pm)$, $\mathcal{E} = (p, qz - dx^2 + pm)$ and $\mathcal{F} = \left(p, \frac{qz + dx^2 + pm}{x^2}\right)$ all represent the same class in $Br(\mathbb{Q}(\mathcal{D}))$.

Proof. The main ideas of the proof below were provided by Poonen to the author (personal communication).

We shall prove that \mathcal{A} has no residue along any integral divisor on \mathcal{D} . Hence, it suffices to show that there is a Zariski open covering $\{U_i\}$ of \mathcal{D} such that \mathcal{A} extends to an element of $Br(U_i)$ for each i .

Equation (4) can be rewritten in the form

$$(5) \quad (qz + dx^2 + pm)(qz - dx^2 - pm) = -p(mx^2 + d)^2 = \text{Norm}_{\mathbb{Q}(\sqrt{p})/\mathbb{Q}}(\sqrt{p}(mx^2 + d))$$

and

$$(6) \quad (qz + dx^2 + pm)(qz - dx^2 + pm) = -pq(1 - mz)^2.$$

Since $q = d^2 - pm^2 = \text{Norm}_{\mathbb{Q}(\sqrt{p})/\mathbb{Q}}(d + \sqrt{p}m)$, it follows from (6) that

$$(qz + dx^2 + pm)(qz - dx^2 + pm) = \text{Norm}_{\mathbb{Q}(\sqrt{p})/\mathbb{Q}}(\sqrt{p}(1 - mz)) \text{Norm}_{\mathbb{Q}(\sqrt{p})/\mathbb{Q}}(d + \sqrt{p}m).$$

Hence, we deduce that $\mathcal{A} + \mathcal{E} = 0$, and also, it follows from (5) that $\mathcal{A} + \mathcal{B} = 0$. Further, we have that $\mathcal{A} - \mathcal{F} = (p, x^2) = 0$ since x^2 is a square. Since \mathcal{A} , \mathcal{B} , \mathcal{E} and \mathcal{F} belong to $Br(\mathbb{Q}(\mathcal{D}))$ [2], this implies that $\mathcal{A} = \mathcal{B} = \mathcal{E} = \mathcal{F}$.

Now let U_1 be an open subvariety of \mathcal{D} in which the rational function $f := qz + dx^2 + pm$ has neither a zero nor a pole, and let U_2 be an open subvariety of \mathcal{D} in which $g := qz - dx^2 - pm$ has neither a zero nor a pole. Then, since $\mathcal{A} = \mathcal{B}$, \mathcal{A} is an Azumaya algebra on U_1 and also on U_2 .

Now, we prove that in the affine part of \mathcal{D} , the locus where both f and g have a zero is empty. Indeed, assume (X, Z) is a zero of f and g . Then it follows that $qZ = 0$; hence, $Z = 0$. Thus, $dX^2 + pm = 0$, and so $X^2 = -\frac{pm}{d}$. Further, by equation (5), we know that $X^2 = -\frac{d}{m}$. Therefore, $\frac{pm}{d} = \frac{d}{m}$, and hence $d^2 = pm^2$, which implies that $q = 0$, a contradiction.

Let $h := \frac{qz + dx^2 + pm}{x^2}$ and denote by $\infty = (X_\infty : Y_\infty : Z_\infty)$ a point at infinity on \mathcal{D} . We know that $Y_\infty = 0$, and it follows from equation (4) that $\frac{Z_\infty}{X_\infty^2} = \pm \frac{1}{\sqrt{q}}$. Hence, $h(\infty) = q\frac{Z_\infty}{X_\infty^2} + d + pm\frac{Y_\infty^2}{X_\infty^2} = \pm\sqrt{q} + d$, which is non-zero. Thus, h is regular and non-vanishing at points at infinity on \mathcal{D} .

Now let U_3 be an open subvariety of \mathcal{D} in which h has neither a zero nor a pole. Then, since $\mathcal{A} = \mathcal{F}$, we deduce that \mathcal{A} is an Azumaya algebra on U_3 .

By what we have shown, it follows that $\mathcal{D} = U_1 \cup U_2 \cup U_3$, and since \mathcal{A} is an Azumaya algebra on each U_i for $i = 1, 2, 3$, we deduce that \mathcal{A} belongs to $\text{Br}(\mathcal{D})$, proving our contention. \square

Remark 2.4. Following the suggestion of the referee, we can give another proof of Lemma 2.3 as follows. Let Γ be a divisor defined over \mathbb{Q} and lying on \mathcal{D} defined by

$$\Gamma : f = qz + dx^2 + pm = 0 \quad \text{and} \quad mx^2 + d = 0,$$

and let σ be a generator of the Galois group $\text{Gal}(\mathbb{Q}(\sqrt{p})/\mathbb{Q})$. Then, by equation (5), one easily checks that $\text{div}(f) = 2\Gamma = \Gamma + \sigma\Gamma$ since $\sigma\Gamma = \Gamma$. Hence, by Proposition 2.2.3 in Patrick Corn’s Ph.D. thesis (see [8, p. 41]), we deduce that \mathcal{A} is in the image of $\text{Br}(\mathcal{D}) \rightarrow \text{Br}(\mathbb{Q}(\mathcal{D}))$.

Lemma 2.5. *Suppose the same assumptions as in Lemma 2.3 and let \mathcal{D} be the smooth projective model as in Lemma 2.3. Then \mathcal{D} is a counter-example to the Hasse principle explained by a Brauer-Manin obstruction.*

Proof. First we prove that \mathcal{D} is locally solvable for each l -adic local field \mathbb{Q}_l and over the reals \mathbb{R} . We know that the discriminant of \mathcal{D} is $-2^8 p^3 q^6$. Hence, \mathcal{D} is singular only at the primes 2, p and q , so the Weil inequality mandates an l -adic point on \mathcal{D} for $l \geq 5$ and $l \neq p, q$. Hence, it suffices to verify that \mathcal{D} is locally solvable in \mathbb{Q}_l with $l = 2, 3, p, q$. The cases when $l = 2, p, q$ were already considered in Lemma 2.2.

Therefore, we need only exhibit a smooth 3-adic point on \mathcal{D} .

TABLE 3. 3-adic points on \mathcal{D}

$p \bmod 3$	1	1	2	2
$q \bmod 3$	1	2	1	2
(x, z)	(1, 0)	(0, 1)	(0, 1)	(1, 1)

Let $P(x, z) = x^4 - p - qz^2$ be the defining equation of \mathcal{D} . We consider the following systems of equations for $l = 3$:

$$(7) \quad P(x, z) \equiv 0 \pmod{3}, \quad \frac{\partial P}{\partial x} \not\equiv 0 \pmod{3}$$

and

$$(8) \quad P(x, z) \equiv 0 \pmod{3}, \frac{\partial P}{\partial z} \not\equiv 0 \pmod{3}.$$

It follows from Table 3 and Hensel’s lemma that we can exhibit a smooth 3-adic point on \mathcal{D} . Hence, \mathcal{D} is locally solvable for each l -adic local field \mathbb{Q}_l .

Finally, we see that $P = (\sqrt[4]{p}, 0)$ lies on \mathcal{D} . So, \mathcal{D} has points defined over the reals \mathbb{R} .

Now we prove that $\mathcal{D}(\mathbb{A}_{\mathbb{Q}})^{\text{Br}} = \emptyset$.

Let $\mathbb{Q}(\mathcal{D})$ be the function field of \mathcal{D} . Let \mathcal{A} be the class of quaternion algebra $(p, qz + dx^2 + pm)$. It follows from Lemma 2.3 that the element \mathcal{A} is an Azumaya algebra of \mathcal{D} and \mathcal{A} equals the class of the quaternion algebras \mathcal{B} , \mathcal{E} and \mathcal{F} , where \mathcal{B} , \mathcal{E} and \mathcal{F} are the same as in Lemma 2.3.

We shall prove that for any $P_l \in \mathcal{D}(\mathbb{Q}_l)$,

$$(9) \quad \text{inv}_l(\mathcal{A}(P_l)) = \begin{cases} 0 & \text{if } l \neq p, \\ 1/2 & \text{if } l = p. \end{cases}$$

Since \mathcal{D} is smooth, we know that $\mathcal{D}_0(\mathbb{Q}_l)$ is l -adically dense in $\mathcal{D}(\mathbb{Q}_l)$, where \mathcal{D}_0 is the affine curve given by $x^4 - p = qz^2$. Since $\text{inv}(\mathcal{A}(P_l))$ is a continuous function on $\mathcal{D}(\mathbb{Q}_l)$ with the l -adic topology, it suffices to prove (9) for $P_l \in \mathcal{D}_0(\mathbb{Q}_l)$.

Suppose that $l = \infty$, $l = 2$ or $l = q$. Then $p \in \mathbb{Q}_l^{\times 2}$, whence for any $t \in \mathbb{Q}_l^{\times}$, the Hilbert symbol $(p, t)_l$ is 1. Hence, $\text{inv}_l(\mathcal{A}(P_l)) = 0$.

Suppose that l is an odd prime such that $l \neq p, q$ and p is a square in \mathbb{Q}_l^{\times} . Then, repeating in the same manner as above, we deduce that $\text{inv}_l(\mathcal{A}(P_l)) = 0$.

Suppose that l is an odd prime such that $l \neq p, q$ and p is not a square in \mathbb{Q}_l . Assume $(qz + dx^2 + pm)$, $(qz - dx^2 + pm)$ and $(qz - dx^2 - pm)$ are zero modulo l at P_l . Then we get $2qz \equiv 0 \pmod{l}$, and hence $z \equiv 0 \pmod{l}$; thus, $x^4 \equiv p \pmod{l}$. Since p is not a square in \mathbb{Q}_l , x is 0 modulo l . Therefore, l divides p , a contradiction. Hence, at least one of the $(qz + dx^2 + pm)$, $(qz - dx^2 + pm)$ and $(qz - dx^2 - pm)$ is an l -unit in \mathbb{Z}_l^{\times} , say U . Thus, the Hilbert symbol $(p, U)_l = 1$. Since $\mathcal{A} = \mathcal{B} = \mathcal{E}$, we imply that $\text{inv}_l \mathcal{A}(P_l) = 0$.

Finally, suppose that $l = p$. It follows from equation (4) and $q \equiv d^2 \pmod{p}$ that $x^4 - d^2 z^2 \equiv 0 \pmod{p}$ at P_p . Assume $x = 0$ modulo p at P_p . Then $z = 0$ modulo p at P_p . Modulo p^2 from equation (4), we see that $-p \equiv 0 \pmod{p^2}$, a contradiction. Hence, $x \not\equiv 0 \pmod{p}$ and $z \not\equiv 0 \pmod{p}$ at P_p . Thus, we see that $\mathcal{D}_0(\mathbb{Q}_p) = U \cup V$, where $U = \{(x, z) \in \mathcal{D}_0(\mathbb{Q}_p) \text{ such that } x, z \in \mathbb{Z}_p^{\times} \text{ and } x^2 + dz \equiv 0 \pmod{p}\}$ and $V = \{(x, z) \in \mathcal{D}_0(\mathbb{Q}_p) \text{ such that } x, z \in \mathbb{Z}_p^{\times} \text{ and } x^2 - dz \equiv 0 \pmod{p}\}$.

Suppose that $P_p \in U$ and $x \equiv a \pmod{p}$ with $a \in \mathbb{F}_p^{\times}$ at P_p . Then, $z = -a^2/d$ modulo p . Hence, $(qz - dx^2 + pm) \equiv (d^2(-a^2/d) - da^2) \equiv (-2a^2)d \pmod{p}$, and hence, $(qz - dx^2 + pm) \in \mathbb{Z}_p^{\times}$. Using Theorem 5.2.7 in [5], we deduce that the local

Hilbert symbol $(p, qz - dx^2 + pm)_p = \left(\frac{(-2a^2)d}{p}\right) = -1$ since d is non-square in \mathbb{F}_p . Hence, $\text{inv}_p \mathcal{A}(P_p) = 1/2$.

Now, suppose that $P_p \in V$ and $x \equiv a \pmod{p}$ with $a \in \mathbb{F}_p^{\times}$ at P_p . Then $z = a^2/d$ modulo p . Then $(qz + dx^2 + pm) \equiv (d^2(a^2/d) + da^2) \equiv (2a^2)d \pmod{p}$. Hence, we deduce that the Hilbert symbol $(p, (qz + dx^2 + pm))_p = \left(\frac{(2a^2)d}{p}\right) = -1$.

Therefore, $\text{inv}_p \mathcal{A}(P_p) = \frac{1}{2}$. In either case, $\text{inv}_p \mathcal{A}(P_p) = \frac{1}{2}$.

Therefore, $\sum_l \text{inv}_l \mathcal{A}(P_l) = 1/2$ for any $(P_l)_l \in \mathcal{D}(\mathbb{A}_{\mathbb{Q}})$, and hence, $\mathcal{D}(\mathbb{A}_{\mathbb{Q}})^{\text{Br}} = \emptyset$, proving our contention. \square

3. PROOF OF THEOREM 1.1

We state a theorem due to Coray as well as a well-known result that we need in the proof of Theorem 1.1.

Theorem 3.1 (Coray; see [6, Corollary 6.5]). *Let Γ be an absolutely irreducible plane curve of degree 4, defined over a number field k . Suppose Γ contains a k -rational set of d points with d odd. Then Γ also contains a k -rational set of 3 points.*

Lemma 3.2 (See [7, Lemma 4.8]). *Let k be a number field and let \mathcal{V}_1 and \mathcal{V}_2 be (proper) k -varieties. Assume that there is a k -morphism $\alpha : \mathcal{V}_1 \rightarrow \mathcal{V}_2$. Then if the Brauer-Manin obstruction to the Hasse principle holds for \mathcal{V}_2 , it also holds for \mathcal{V}_1 .*

3.1. Proof of Theorem 1.1. We know from Lemma 2.2 that \mathcal{X} has points everywhere locally.

We see that the Jacobian of \mathcal{X} is isogenous to the product of the following three curves

$$\mathcal{D}_1 : x^2 - py^4 - q(y^2 + qz^2)^2 = 0, \mathcal{D}_2 : x^4 - py^2 - q(y + qz^2)^2 = 0,$$

and

$$\mathcal{D}_3 : x^4 - py^4 - q(y^2 + qz)^2 = 0$$

with obvious maps

$$\mu_i : \mathcal{X} \rightarrow \mathcal{D}_i, i = 1, 2, 3.$$

Let \mathcal{D} be the smooth projective model in Lemma 2.5. Then we know that there is a \mathbb{Q} -morphism α given by

$$\alpha : \mathcal{D}_3 \rightarrow \mathcal{D}, (x : y : z) \mapsto (X : Y : Z) = (x : y : y^2 + qz).$$

Hence, we have a sequence of \mathbb{Q} -morphisms

$$\mathcal{X} \xrightarrow{\mu_3} \mathcal{D}_3 \xrightarrow{\alpha} \mathcal{D}.$$

We know from Lemma 2.5 that $\mathcal{D}(\mathbb{A}_{\mathbb{Q}})^{\text{Br}} = \emptyset$. Hence, using Lemma 3.2, we deduce that $\mathcal{D}_3(\mathbb{A}_{\mathbb{Q}})^{\text{Br}} = \emptyset$ and whence $\mathcal{X}(\mathbb{A}_{\mathbb{Q}})^{\text{Br}} = \emptyset$, proving that \mathcal{X} is a counterexample to the Hasse principle explained by the Brauer-Manin obstruction.

For the last contention, we shall use the argument, due to Cassels (see [4]), to show that there are no points on \mathcal{X} , defined over any number field of odd degree. By Theorem 3.1, it suffices to show that \mathcal{X} has no point defined over any number field of degree 3 over the rationals.

Assume the contrary; that is, there exists an effective \mathbb{Q} -rational divisor T on \mathcal{X} of degree 3. We know that there are $a, b, c \in \mathbb{Q}$, depending on T , such that the conic

$$x^2 = ay^2 + bz^2 + cyz$$

passes through the points of T . It meets \mathcal{D}_3 in the three points $\mu_3(T)$ and a fourth point, which must be rational. Thus, there exists a rational point on \mathcal{D}_3 , a contradiction. Hence, there are no points on \mathcal{X} , defined over any number field of degree 3, whence over any number field of odd degree. \square

Corollary 3.3. *Assume (A1), (A2) and (A3) and let $\mathcal{H}_{p,q}$ be the quartic hypersurface given by*

$$\mathcal{H}_{p,q} : x_1^4 - px_2^4 - q(x_3^2 + q(x_4^2 + \dots + x_n^2))^2 = 0$$

with $n \geq 4$. Then $\mathcal{H}_{p,q}$ is absolutely irreducible and there are points on $\mathcal{H}_{p,q}$, defined over each l -adic field \mathbb{Q}_l , but no points defined over each number field of odd degree.

Proof. It is clear from Lemma 2.1 that $\mathcal{H}_{p,q}$ is absolutely irreducible and there are points on $\mathcal{H}_{p,q}$, defined over each l -adic field \mathbb{Q}_l . Assume $\mathcal{H}_{p,q}$ contains a point $P = (a_1, a_2, \dots, a_n)$ defined over some number field, say K , of odd degree over the rationals. We consider the quadratic polynomial $F(X) = X^2 - (a_4^2 + \dots + a_n^2)$ in K . If F is reducible, there exists an element $A \in K$ such that $A^2 = a_4^2 + \dots + a_n^2$. Hence, the quartic curve defined by $x_1^4 - px_2^4 - q(x_3^2 + qx_4^2)^2$ contains a point $Q = (a_1, a_2, a_3, A)$, a contradiction to Theorem 1.1.

Assume F is irreducible and let α be a root of F in the algebraic closure of K . Then the number field $K(\alpha)$ is of odd degree over the rationals, and the quartic curve defined by $x_1^4 - px_2^4 - q(x_3^2 + qx_4^2)^2$ contains a point $R = (a_1, a_2, a_3, \alpha)$, a contradiction to Theorem 1.1. Thus, $\mathcal{H}_{p,q}$ contains no points defined over each number field of odd degree. □

4. INFINITUDE OF QUADRUPLES (p, q, d, m)

In this section, we show that there are infinitely many distinct pairs (p, q) of primes satisfying assumptions (A1), (A2) and (A3).

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

Theorem 4.1 (Iwaniec; see [10, p. 443]). *Let $P(x, y) = ax^2 + bxy + cy^2 + ex + fy + g$ be a quadratic polynomial defined over \mathbb{Q} and assume the following:*

- (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

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

Now we prove the main lemma in this section.

Lemma 4.2. *There exist infinitely many distinct pairs (p, q) of primes with $p \equiv 1 \pmod{16}$, satisfying (A1), (A2) and (A3).*

Proof. Let p be a prime such that $p \equiv 1 \pmod{16}$. By the Chinese Remainder Theorem, we know that there are integers d_0, m_0 satisfying (A2), (A3) such that $d_0 - m_0 \not\equiv 0 \pmod{5}$ and at least one of the d_0 and m_0 is zero modulo 5. Hence, if m is of the form $(Ly + m_0)$ where $L = 2 \cdot 5 \cdot 13 \cdot 17 \cdot 29$ and $y \in \mathbb{Z}$, then m satisfies (A3).

Let $P(x, y)$ be the quadratic polynomial in two variables, x and y , given by

$$P(x, y) = (5px + d_0)^2 - p(Ly + m_0)^2.$$

It is obvious that $P(x, y)$ is irreducible in $\mathbb{Q}[x, y]$. One easily checks that P depends essentially on two variables.

Now, expanding $P(x, y)$ in the form of $ax^2 + bxy + cy^2 + ex + fy + g$, we get by comparing the coefficients of $P(x, y)$ that

$$a = 25p^2, b = 0, c = -pL^2, e = 10pd_0, f = -2pLm_0, g = d_0^2 - pm_0^2.$$

Since $\gcd(a, g) = 1$, we see that $\gcd(a, b, c, e, f, g) = 1$. Now $-p(Ly + m_0)^2$ is odd for every integer y . Therefore, when d_0 is odd, we can let x be odd arbitrarily, whence $P(x, y) = (5px + d_0)^2 - p(Ly + m_0)^2$ represents arbitrarily large odd numbers. When d_0 is even, we let x range over the set of even integers. Then $P(x, y) = (5px + d_0)^2 - p(Ly + m_0)^2$ represents arbitrarily large odd numbers. In any event, $P(x, y)$ represents arbitrarily large odd numbers. Furthermore, by computation, we see that $D = af^2 - bef + ce^2 + (b^2 - 4ac)g = 0$. Thus, $P(x, y)$ satisfies all of the conditions in Theorem 4.1. Therefore, there are infinitely many primes q such that $P(x, y) = q$ for some integers x, y . When this is the case, the pairs (p, q) satisfy assumptions (A1), (A2) and (A3) as desired with $d = 5px + d_0$ and $m = Ly + m_0$. \square

Example 4.3. Let $p = 17$ and let $(q, d, m) = (67447, 260, 3)$. Then we see that the quadruple (p, q, d, m) satisfies (A1), (A2) and (A3) with $260^2 = 17 \cdot 3^2 + 67447$. Then it follows from Theorem 1.1 that the quartic curve \mathcal{X}_{17} given by

$$x^4 - 17y^4 = 67447(y^2 + 67447z^2)^2$$

violates the Hasse principle explained by the Brauer-Manin obstruction.

5. INFINITUDE OF NON-ISOMORPHIC QUARTIC CURVES VIOLATING THE HASSE PRINCIPLE

We state a theorem due to Howe in [9] that we need in the proof of Theorem 1.3.

For every triple (a, b, c) of complex numbers, let $Q(a, b, c)$ denote the plane quartic curve defined by

$$Q(a, b, c) : x^4 + y^4 + z^4 + ax^2y^2 + bx^2z^2 + cy^2z^2 = 0.$$

Assume $Q(a, b, c)$ is non-singular; that is, $a^2 + b^2 + c^2 - abc - 4$ is non-zero and none of a^2 , b^2 , and c^2 are equal to 4. An isomorphism $\phi : Q(a, b, c) \rightarrow Q(a', b', c')$ is said to be *strict* if ϕ can be represented by the product of a permutation matrix and a diagonal matrix.

We have the following:

Theorem 5.1 (Howe; see [9, section 2]). *An isomorphism class of non-singular quartics of the form $Q(a', b', c')$ is equal to one of the following:*

(i) *the strict isomorphism class of the curve $Q(a, b, c)$ for some a, b , and c such that a^2, b^2 , and c^2 are pairwise unequal;*

(ii) *the union of the strict isomorphism classes of the curves $Q(a, b, b)$ and $Q(-2 + 16/(a + 2), 2b/d, 2b/d)$ for some a and b with $b \neq 0$, where $d^2 = a + 2$;*

or

(iii) *the union of the strict isomorphism classes of the curves $Q(a, 0, 0)$, $Q(-2 + 16/(a + 2), 0, 0)$, and $Q(-2 + 16/(-a + 2), 0, 0)$, for some a .*

5.1. **Proof of Theorem 1.3 and Corollary 1.4.** Corollary 1.4 easily follows from Lemma 4.2 and Corollary 3.3. So, it remains to prove Theorem 1.3.

The infinitude of the pairs (p, q) satisfying the conditions in Theorem 1.1 is clear from Lemma 4.2. Thus, it suffices to prove that two of the quartic curves arising from that family are not isomorphic to each other.

For a given p , denote by q_1, q_2 distinct primes with

$$pm_i^2 + d_i^2 = q_i, i = 1, 2 \text{ and } q_1, q_2 \neq 2,$$

where m_i are integers and d_i are quadratic non-residues in \mathbb{F}_p such that the quadruples (p, q_i, d_i, m_i) satisfy the conditions in Theorem 1.1.

Let \mathcal{C}_{q_i} be the quartic curves given by

$$\mathcal{C}_{q_i} : x^4 - py^4 - q_i(y^2 + q_iz^2)^2 = 0, i = 1, 2,$$

and assume \mathcal{C}_{q_1} is isomorphic to \mathcal{C}_{q_2} . Denote by ϕ be the isomorphism between them. It is clear that we can consider $\mathcal{C}_{q_1}, \mathcal{C}_{q_2}$ as algebraic curves defined over the complex field and ϕ as an isomorphism between them, defined over the complex field. Further, $\mathcal{C}_{q_1}, \mathcal{C}_{q_2}$ are isomorphic to Q_1, Q_2 , respectively, over the complex field, where Q_1, Q_2 are given by

$$Q_i : X^4 + Y^4 + Z^4 - \frac{2q_i^2}{[-(p + q_i)]^{1/2}[-q_i^3]^{1/2}} Y^2 Z^2 = 0, i = 1, 2,$$

with the maps

$$\mu_i : (x, y, z) \mapsto (X, Y, Z) = \left(x, -(p + q_i)^{1/4}y, (-q_i^3)^{1/4}z\right), i = 1, 2,$$

where we denote by $(\cdot)^{1/4}$ and $(\cdot)^{1/2}$ the principal branches of the fourth root function and the square root function in \mathbb{C} , respectively.

By assumption, Q_1 is isomorphic to Q_2 . Furthermore, by Theorem 5.1 we know that Q_2 is in the union of the strict isomorphism classes of the curves Q_1, Q_3 and Q_4 , where Q_3, Q_4 are defined by

$$Q_i : X^4 + Y^4 + Z^4 + c_i Y^2 Z^2 = 0, i = 3, 4,$$

where $c_3 = -2 + \frac{16}{\frac{-2q_1^2}{[-(p + q_1)]^{1/2}[-q_1^3]^{1/2}} + 2}$ and $c_4 = -2 + \frac{16}{\frac{2q_1^2}{[-(p + q_1)]^{1/2}[-q_1^3]^{1/2}} + 2}$.

Assume Q_2 is in the strict isomorphism class of the curve Q_1 . Then, using Theorem 5.1, we deduce that Q_2 is the image of the strict isomorphism of the form $(x, y, z) \mapsto (Ax, By, Cz)$, where the triple A, B, C are complex numbers satisfying $A^4 = B^4 = C^4 = 1$ and

$$\frac{2q_2^2}{[-(p + q_2)]^{1/2}[-q_2^3]^{1/2}} = \frac{2q_1^2}{[-(p + q_1)]^{1/2}[-q_1^3]^{1/2}} B^2 C^2.$$

Squaring the latter identity, we get $q_1 = q_2$, a contradiction.

Assume now that Q_2 is in the strict isomorphism class of the curve Q_4 . Then, repeating in the same manner as above, we know that there is a triple (A, B, C) of complex numbers satisfying $A^4 = B^4 = C^4 = 1$ and

$$(10) \quad \frac{-2q_2^2}{[-(p + q_2)]^{1/2}[-q_2^3]^{1/2}} = \left(-2 + \frac{16}{\frac{2q_1^2}{[-(p + q_1)]^{1/2}[-q_1^3]^{1/2}} + 2}\right) B^2 C^2.$$

Squaring (10), simplifying and moving the term $[-(p + q_1)]^{1/2}[-q_1^3]^{1/2}$ to one side and then squaring both sides again, we get

$$(9p^2q_1^3 + 10pq_1^4 + 8p^3q_1^2 + 8q_1^4q_2)^2 = 2q_1^2(3p + 4q_2)^2(p + q_1)(q_1^3).$$

Modulo 2 the last identity, we deduce that

$$81p^4q_1^6 \equiv 0 \pmod{2},$$

which is impossible since p, q_1 are distinct from 2.

Repeating in the same manner, we can show that Q_2 is not in the strict isomorphism class of the curve Q_3 .

Hence, we conclude that C_{q_1} is not isomorphic to C_{q_2} .

Thus, the conclusions in Theorem 1.3 follow immediately from Theorem 1.1 and Lemma 4.2. \square

ACKNOWLEDGEMENTS

The author would like to thank his parents, Nguyen Ngoc Quang and Phan Thi Thien Huong, for their constant encouragement and support. He is grateful to Andrew Bremner for teaching him many topics in Diophantine equations and for reading and giving many helpful comments on an earlier version of the article. The author is indebted to Bjorn Poonen for the main ideas of the proof of Lemma 2.3 and for his papers and notes ([14] and [15]), from which the author has learned a lot. He also thanks Dinesh Thakur for his useful comments on the presentation of the article. The author would like to thank the referee for a careful reading, suggesting many good references and making many thoughtful suggestions that greatly improved the paper and for pointing out mistakes in the original version of the article.

REFERENCES

- [1] A. Bremner, D.J. Lewis and P. Morton, *Some varieties with points only in a field extension*, Arch. Math. 43 (1984), pp. 344–350. MR802310 (87a:11023)
- [2] W. Bosma, J. Cannon and C. Playoust, *The magma algebra system. I. The user language*, J. Symbolic Comput. 24 (1997), pp. 235–265. MR1484478
- [3] M. Bright, *Brauer groups of diagonal quartic surfaces*, J. Symbolic Comput. 41 (2006), no. 5, pp. 544–558. MR2209163 (2007h:14022)
- [4] J.W.S. Cassels, *The arithmetic of certain quartic curves*, Proc. Roy. Soc. Edinburgh Sect. A 100A (1985), pp. 201–218. MR807702 (86m:11017)
- [5] H. Cohen, *Number Theory, Volume I: Tools and Diophantine equations*, Graduate Texts in Math., 239, Springer-Verlag, 2007. MR2312337 (2008e:11001)
- [6] D. Coray, *Algebraic points on cubic hypersurfaces*, Acta. Arith. 30 (1976), pp. 267–296. MR0429731 (55:2742)
- [7] D. Coray, C. Manoil, *On large Picard groups and the Hasse principle for curves and K3 surfaces*, Acta. Arith. 76 (1996), pp. 165–189. MR1393513 (97j:14038)
- [8] P. Corn, *Del Pezzo surfaces and the Brauer-Manin obstruction*, Ph.D. thesis, University of California, Berkeley, 2005; ProQuest LLC, Ann Arbor, MI, 2005. MR2707740
- [9] E. Howe, *Plane quartics with Jacobians isomorphic to a hyperelliptic Jacobian*, Proc. Amer. Math. Soc. 129 (2001), pp. 1647–1657. MR1814093 (2002a:14028)
- [10] H. Iwaniec, *Primes represented by quadratic polynomials in two variables*, Acta. Arith. 24 (1974), pp. 435–459. MR0342464 (49:7210)
- [11] C.E. Lind, *Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Eins*, Thesis, University of Uppasala, 1940. MR0022563 (9:225c)
- [12] Yu.I. Manin, *Le groupe de Brauer-Grothendieck en géométrie diophantienne*, Actes du Congrès International des Mathématiciens, Nice (1970), Gauthier-Villars, Paris, 1971, pp. 401–411. MR0427322 (55:356)

- [13] B. Poonen, *An explicit family of genus-one curves violating the Hasse principle*, J. Théor. Nombres Bordeaux 13 (2001), no. 1, 263–274. MR1838086 (2002e:14036)
- [14] B. Poonen, *Existence of rational points on smooth projective varieties*, J. Eur. Math. Soc. (JEMS) 11 (2009), no. 3, 529–543. MR2505440 (2010c:14019)
- [15] B. Poonen, *Rational points*, 2003. Available at <http://www-math.mit.edu/~poonen/papers/Qpoints.pdf>.
- [16] L. Rédei, *Algebra I*, Leipzig, 1959. MR0106151
- [17] H. Reichardt, *Einige im Kleinen überall lösbar, im Grossen unlösbar diophantische Gleichungen*, J. Reine Angew. Math. 184 (1942), pp. 12–18. MR0009381 (5:141c)
- [18] V. Scharaschkin, *Local global problems and the Brauer-Manin obstruction*, Ph.D. Thesis, University of Michigan; ProQuest LLC, Ann Arbor, MI, 1999. MR2700328
- [19] A. Schinzel, *Hasse's principle for systems of ternary quadratic forms and one biquadratic form*, Studia Math. 77 (1983), pp. 103–109. MR743067 (85h:11018)
- [20] E.S. Selmer, *The Diophantine equation $ax^3 + by^3 + cz^3 = 0$* , Acta. Math. 85 (1951), pp. 203–362. MR0041871 (13:13i)
- [21] A.N. Skorobogatov, *Torsors and rational points*, Cambridge Tracts in Math, 144. Cambridge Univ. Press, 2001. MR1845760 (2002d:14032)
- [22] H.P.F. Swinnerton-Dyer, *Brauer-Manin obstructions on some Del Pezzo surfaces*, Math. Proc. Cam. Phil. Soc. 125 (1999), pp. 193–198. MR1643855 (99h:11071)

DEPARTMENT OF MATHEMATICS, THE UNIVERSITY OF ARIZONA, TUCSON, ARIZONA 85721
E-mail address: dongquan@math.arizona.edu