J. Aust. Math. Soc. **100** (2016), 42–64
doi:10.1017/S1446788715000348

CERTAIN GENERALIZED MORDELL CURVES OVER THE RATIONAL NUMBERS ARE POINTLESS

NGUYEN NGOC DONG QUAN

(Received 25 September 2014; accepted 26 July 2015; first published online 28 October 2015)

Communicated by W. Zudilin

Abstract

A conjecture of Scharaschkin and Skorobogatov states that there is a Brauer–Manin obstruction to the existence of rational points on a smooth geometrically irreducible curve over a number field. In this paper, we verify the Scharaschkin–Skorobogatov conjecture for explicit families of generalized Mordell curves. Our approach uses standard techniques from the Brauer–Manin obstruction and the arithmetic of certain threefolds.

2010 *Mathematics subject classification*: primary 14G25, secondary 11G35, 14G05, 14H45.

Keywords and phrases: Brauer–Manin obstruction, rational points, generalized curves.

1. Introduction

Faltings' theorem, née the Mordell conjecture, states that a smooth geometrically irreducible curve over a number field has only finitely many rational points. Despite this celebrated result, the following open problem remains widely open: for a family of smooth geometrically irreducible curves C over $\mathbb{Q}$, determine the sets $C(\mathbb{Q})$ of all rational points on the curves C. This problem remains open even in the case where we assume further that the family of curves under consideration are of special type such as *generalized Mordell curves* that we will shortly define. In fact, we will mainly study generalized Mordell curves in this paper.

For a positive integer $n \geq 3$, a *generalized Mordell curve of degree n* over $\mathbb{Q}$ is the smooth projective model of the affine curve of the form $Az^2 = Bx^n + C$, where A, B, C are nonzero integers. Although the defining equations of generalized Mordell curves are deceptively simple looking, the problem of finding all rational points on an arbitrary generalized Mordell curve remains widely open.

In this paper, we are concerned with studying nonexistence of rational points on certain generalized Mordell curves of degree n divisible by 12. Since we only deal with curves with no rational points, it is natural to ask what obstructs the existence of rational points on such curves. We will prove that the *Brauer–Manin obstruction*

explains the absence of rational points on the generalized Mordell curves that we study in this paper.

For a smooth geometrically irreducible curve C over $\mathbb{Q}$, a conjecture of Scharaschkin and Skorobogatov [5, 8] states that there is a Brauer–Manin obstruction to the existence of rational points on C. More precisely, the Scharaschkin–Skorobogatov conjecture states that if $C(\mathbb{Q})$ is empty, then the set $C(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}$ is empty. (For the definition of $C(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}$ as well as a basic introduction to the Brauer–Manin obstruction, see [3, 4] or [8].) Hence, the generalized Mordell curves in this paper provide new examples for which the conjecture of Scharaschkin and Skorobogatov holds.

In [1], Bhargava proved that for each $n \geq 1$, a positive proportion of hyperelliptic curves $z^2 = F(x)$ of genus n over $\mathbb{Q}$ fails the Hasse principle, and the failure can be explained by the Brauer–Manin obstruction. In particular, this implies that the conjecture of Scharaschkin and Skorobogatov holds for a positive proportion of hyperelliptic curves of genus n for each $n \geq 1$. Despite this beautiful result, there is no known method for determining whether an *arbitrary explicit* hyperelliptic curve satisfies the Scharaschkin–Skorobogatov conjecture. The main goal of this paper is to verify the conjecture of Scharaschkin and Skorobogatov for explicit families of hyperelliptic curves over $\mathbb{Q}$.

We now begin to describe the main results in this paper. Let p be a prime such that $p \equiv 1 \bmod 8$. Here and elsewhere we denote by $\mathcal{X}_p$ the threefold in $\mathbb{P}^6_{\mathbb{Q}}$ defined by

$$\mathcal{X}_p\colon \begin{cases} b^2 - c^2 + 2pef = 0, \\ 2ab - 2cd + pf^2 = 0, \\ a^2 - d^2 + pg^2 = 0. \end{cases} \tag{1.1}$$

We describe certain rational points on $\mathcal{X}_p$ that are of great interest in this paper.

Definition 1.1. Let p be a prime such that $p \equiv 1 \bmod 8$. Let n be a positive integer such that $n \geq 1$. Let $(A, B, C, D, E, F, G) \in \mathbb{Z}^7$ be a septuple of integers such that at least one of them is nonzero. We say that (A, B, C, D, E, F, G) *satisfies GMC with respect to the couple* (p, n) if the following are true:

(A1) the point $\mathcal{P} := (a : b : c : d : e : f : g) = (A : B : C : D : E : F : G)$ belongs to $\mathcal{X}_p(\mathbb{Q})$;

(A2) let l be any odd prime such that $\gcd(l, 3) = \gcd(l, p) = 1$ and l divides E. Then p is a square in $\mathbb{Q}_l^{\times}$ or $v_l(E) - v_l(G) < 6n$;

(A3) $\gcd(A, D, G) = 1$, $E \not\equiv 0 \bmod p$, and $G \not\equiv 0 \bmod p$;

(A4) let l be any odd prime such that $\gcd(l, 3) = \gcd(l, p) = 1$ and

$$\gcd(AC - BD, DE - CF, AE - BF) \equiv 0 \bmod l.$$

Then p is a square in $\mathbb{Q}_l^{\times}$;

(A5) there exists an integer H such that $G - EH^6 \equiv 0 \bmod p$ and $A + \zeta BH^4$ is a quadratic nonresidue in $\mathbb{F}_p^{\times}$ for any cube root of unity ζ in $\mathbb{F}_p^{\times}$.

https://doi.org/10.1017/S1446788715000348 Published online by Cambridge University Press

Moreover, if 3 is a quadratic nonresidue in $\mathbb{F}_p^\times$, we further assume that the following are true:

(A6) $v_3(E) - v_3(G) < 6n$;
(A7) $A + B \not\equiv 0 \bmod 3$ and $G \equiv 0 \bmod 3$.

Remark 1.2. Since $p \equiv 1 \bmod 8$, it follows from the quadratic reciprocity law that -3 is not a square in $\mathbb{F}_p^\times$ if and only if p is not a square in $\mathbb{F}_3^\times$ or, equivalently, $p \equiv 2 \bmod 3$. Hence, if $p \equiv 2 \bmod 3$, then the group of all cube roots of unity in $\mathbb{F}_p^\times$ is trivial. Thus, (A5) is tantamount to the condition that there exists an integer H such that $G - EH^6 \equiv 0 \bmod p$ and $A + BH^4$ is a quadratic nonresidue in $\mathbb{F}_p^\times$.

Remark 1.3. Note that if (A, B, C, D, E, F, G) satisfies GMC with respect to (p, n), then A, D, E, and G are nonzero. Indeed, by (A3), we know that $E, G \not\equiv 0 \bmod p$ and hence E, G are nonzero. Assume that $A = 0$. Then, by (A1) and the third equation of (1.1), we see that $D^2 = pG^2$. Hence, $p = (D/G)^2$, which is a contradiction since p is a prime. Hence, $A \neq 0$. Assume that $D = 0$. Then, by (A1) and the third equation of (1.1), we deduce that $A^2 + pG^2 = 0$, which is a contradiction since $A^2 + pG^2 > 0$. Hence, $D \neq 0$.

We are now ready to sketch the main ideas how to construct generalized Mordell curves for which the Scharaschkin–Skorobogatov conjecture holds. For a prime $p \equiv 1 \bmod 8$, a positive integer n, and each septuple (A, B, C, D, E, F, G) satisfying GMC with respect to (p, n), we will construct an Azumaya algebra $\mathcal{A}$ on the generalized Mordell curve C of the shape $pz^2 = E^2x^{12n} - G^2$. The construction of the Azumaya algebra $\mathcal{A}$ mainly relies on the equations of the threefold $\mathcal{X}_p$. Using conditions (A1)–(A7), we will show that $\mathcal{A}$ satisfies

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

for any $P_l \in C(\mathbb{Q}_l)$. From these invariants of the Azumaya algebra $\mathcal{A}$, it follows that $C(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}} = \emptyset$ and thus C satisfies the Scharaschkin–Skorobogatov conjecture. In particular, this implies that C has no rational points over $\mathbb{Q}$. More precisely, we obtain the following result.

Theorem 1.4 (see Theorem 2.2). *Let p be a prime such that $p \equiv 1 \bmod 8$ and let n be a positive integer. Let (A, B, C, D, E, F, G) be a septuple of integers satisfying* GMC *with respect to (p, n). Then the generalized Mordell curve C defined by*

$$C : pz^2 = E^2x^{12n} - G^2$$

satisfies $C(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}} = \emptyset$.

We will prove Theorem 1.4 in Section 2. In the first part of Section 3, we will describe a subset of $\mathcal{X}_p(\mathbb{Q})$ for each prime p. Using this subset and Theorem 1.4, we prove that for each prime p with $p \equiv 1 \bmod 8$ and $p \equiv 2 \bmod 3$, there exist infinitely many couples (E, G) such that for each (E, G), there is a constant $n_{E,G}$ depending only on E, G for which the curve C in Theorem 1.4 satisfies $C(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}} = \emptyset$ for any $n > n_{E,G}$. This is Corollary 3.3.

https://doi.org/10.1017/S1446788715000348 Published online by Cambridge University Press

In the last part of Section 3, we prove conditionally under the assumption of Schinzel's hypothesis H that for each positive integer k divisible by 12, there are infinitely many generalized Mordell curves of degree k that satisfy the Scharaschkin–Skorobogatov conjecture.

2. Nonexistence of rational points on certain generalized Mordell curves

In this section, we describe a relationship between rational points on $\mathcal{X}_p$ that satisfy GMC and certain generalized Mordell curves with no rational points. More precisely, we show that for each prime $p \equiv 1 \bmod 8$ and a positive integer n, the existence of a septuple (A, B, C, D, E, F, G) satisfying GMC with respect to (p, n) implies nonexistence of rational points on the generalized Mordell curve of the shape $pz^2 = E^2x^{12n} - G^2$. Furthermore, there is a Brauer–Manin obstruction to the existence of rational points on such curves. We begin by proving the main lemma in this section.

Lemma 2.1. *Let p be a prime such that $p \equiv 1 \bmod 8$ and let n be a positive integer. Assume that $(A, B, C, D, E, F, G) \in \mathbb{Z}^7$ is a septuple of integers satisfying* GMC *with respect to the couple (p, n). Let C be the generalized Mordell curve defined by*

$$C : pz^2 = E^2x^{12n} - G^2. \tag{2.1}$$

Let $\mathbb{Q}(C)$ be the function field of C, and let $\mathcal{A}$ be the class of the quaternion algebra $(p, A + Bx^{4n} + pz)$ in $\mathrm{Br}(\mathbb{Q}(C))$. Then $\mathcal{A}$ is an Azumaya algebra of C. Furthermore, $\mathcal{B} := (p, A + Bx^{4n} - pz)$ and $\mathcal{E} := (p, (A + Bx^{4n} + pz/x^{6n}))$ represent the same class as $\mathcal{A}$ in $\mathrm{Br}(\mathbb{Q}(C))$.

Proof. We will prove that there is a Zariski open covering $(U_i)_i$ of C such that $\mathcal{A}$ extends to an element of $\mathrm{Br}(U_i)$ for each i.

By (A1), we see that (2.1) can be written in the form

$$\begin{aligned}(A + Bx^{4n} + pz)(A + Bx^{4n} - pz) &= (Cx^{4n} + D)^2 - px^{4n}(Ex^{4n} + F)^2 \\ &= \mathrm{Norm}_{\mathbb{Q}(\sqrt{p})/\mathbb{Q}}((Cx^{4n} + D) - \sqrt{p}x^{2n}(Ex^{4n} + F)).\end{aligned} \tag{2.2}$$

It follows from the identity above that $\mathcal{A} + \mathcal{B} = 0$. Furthermore, we see that $\mathcal{A} - \mathcal{E} = (p, x^{6n}) = 0$. Since $\mathcal{A}, \mathcal{B}$, and $\mathcal{E}$ belong to the 2-torsion part of $\mathrm{Br}(\mathbb{Q}(C))$, we deduce that $\mathcal{A} = \mathcal{B} = \mathcal{E}$.

Let U_1 be the *largest* open subvariety of C in which the rational function $R_1 := A + Bx^{4n} + pz$ has neither a zero nor a pole. Let U_2 be the *largest* open subvariety of C in which $R_2 := A + Bx^{4n} - pz$ has neither a zero nor a pole. Since $\mathcal{A} = \mathcal{B}$, $\mathcal{A}$ is an Azumaya algebra on U_1 and also on U_2. We prove that in the affine part of C, the locus where both R_1 and R_2 have a zero is empty. Assume the contrary, and let (X, Z) be a common zero of R_1 and R_2. We see that

$$A + BX^{4n} = R_1 + R_2 = 0$$

and

$$Z = \frac{R_1 - R_2}{2p} = 0.$$

https://doi.org/10.1017/S1446788715000348 Published online by Cambridge University Press

This implies that $B \neq 0$; otherwise, we deduce that $A = 0$, which is a contradiction to Remark 1.3. Hence, $B \neq 0$ and thus it follows that $X^{4n} = -A/B$. By (2.1),

$$X^{12n} = \frac{G^2}{E^2} = \left(-\frac{A}{B}\right)^3.$$

Hence,

$$(-A)^3 = \frac{B^3G^2}{E^2}. \tag{2.3}$$

Let H be an integer satisfying (A5) in Definition 1.1. Since $E \not\equiv 0 \bmod p$, it follows from (A5) and (2.3) that

$$(-A)^3 = \frac{B^3G^2}{E^2} \equiv (BH^4)^3 \bmod p.$$

Hence, $-A \equiv \zeta BH^4 \bmod p$ for some cube root of unity ζ in $\mathbb{F}_p^\times$. Thus, $A + \zeta BH^4 \equiv 0 \bmod p$, which is a contradiction to (A5). Therefore, in the affine part of C, the locus where both R_1 and R_2 have a zero is empty.

Let $R_3 := (A + Bx^{4n} + pz/x^{6n})$, and let $\infty = (X_\infty : Y_\infty : Z_\infty)$ be a point at infinity on C. We know that $Y_\infty = 0$ and

$$\frac{Z_\infty}{X_\infty^{6n}} = \pm\frac{E}{\sqrt{p}}.$$

It follows that

$$R_3(\infty) = \frac{AY_\infty^{6n} + BX_\infty^{4n}Y_\infty^{2n} + pZ_\infty}{X_\infty^{6n}} = \frac{pZ_\infty}{X_\infty^{6n}} = \pm\sqrt{p}E.$$

By Remark 1.3, we know that E is nonzero. Hence, $R_3 \neq 0$ and thus R_3 is regular and nonvanishing at the points at infinity on C.

Let U_3 be the *largest* open subvariety of C in which the rational function R_3 has neither a zero nor a pole. Then, since $\mathcal{A} = \mathcal{E}$, we deduce that $\mathcal{A}$ is an Azumaya algebra on U_3. By what we have shown, it follows that $C = U_1 \cup U_2 \cup U_3$. Since $\mathcal{A}$ is an Azumaya algebra on each U_i for $1 \leq i \leq 3$, we deduce that $\mathcal{A}$ belongs to $\mathrm{Br}(C)$, proving our contention. □

We now prove the main theorem in this section, which relates rational points on $\mathcal{X}_p$ satisfying GMC with respect to a given couple (p, n) to nonexistence of rational points on certain generalized Mordell curves.

THEOREM 2.2. *Let p be a prime such that $p \equiv 1 \bmod 8$ and let n be a positive integer. Let $(A, B, C, D, E, F, G) \in \mathbb{Z}^7$ be a septuple of integers satisfying* GMC *with respect to (p, n). Let C be the generalized Mordell curve defined by (2.1) in Lemma 2.1. Then $C(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}} = \emptyset$.*

PROOF. We maintain the notation of Lemma 2.1. We will prove that for any $P_l \in C(\mathbb{Q}_l)$,

$$\mathrm{inv}_l(\mathcal{A}(P_l)) = \begin{cases} 0 & \text{if } l \neq p, \\ 1/2 & \text{if } l = p. \end{cases} \tag{2.4}$$

https://doi.org/10.1017/S1446788715000348 Published online by Cambridge University Press

Since C is smooth, we know that $C^*(\mathbb{Q}_l)$ is l-adically dense in $C(\mathbb{Q}_l)$, where C^* is the affine curve given by $pz^2 = E^2x^{12n} - G^2$. Since $\mathrm{inv}_l(\mathcal{A}(P_l))$ is a continuous function on $C(\mathbb{Q}_l)$ with respect to the l-adic topology, it suffices to prove (2.4) for any $P_l \in C^*(\mathbb{Q}_l)$.

Suppose that $l = 2, \infty$, or l is an odd prime such that $l \neq p$ and p is a square in $\mathbb{Q}_l^\times$. Then, for any $t \in \mathbb{Q}_l^\times$, the local Hilbert symbol $(p, t)_l$ is 1. Thus, $\mathrm{inv}_l(\mathcal{A}(P_l))$ is 0.

Suppose that $l = 3$. If 3 is a square in $\mathbb{F}_p^\times$, then, by the quadratic reciprocity law, we know that p is a square in $\mathbb{F}_3^\times$. Hence, using the same arguments as above, we deduce that $\mathrm{inv}_3(\mathcal{A}(P_3)) = 0$. If 3 is a quadratic nonresidue in $\mathbb{F}_p^\times$, then we contend that $v_3(x) \geq 0$. Assume the contrary, that is, $v_3(x) = \epsilon < 0$. Since $\epsilon = v_3(x) \in \mathbb{Z}$, we see that $\epsilon \leq -1$. Hence, by (A6),

$$v_3(E^2x^{12n}) = 2v_3(E) + 12n\epsilon \leq 2v_3(E) - 12n < 2v_3(G) = v_3(G^2).$$

It then follows that

$$2v_3(z) = v_3(pz^2) = \min(v_3(E^2x^{12n}), v_3(G^2)) = v_3(E^2x^{12n}) = 2v_3(E) + 12n\epsilon$$

and hence $v_3(z) = v_3(E) + 6n\epsilon$. Therefore, there exist elements $x_0, z_0, E_0 \in \mathbb{Z}_3^\times$ such that

$$\begin{aligned} x &= 3^{\epsilon}x_0, \\ z &= 3^{v_3(E)+6n\epsilon}z_0, \\ E &= 3^{v_3(E)}E_0. \end{aligned}$$

By (2.1),

$$p3^{2v_3(E)+12n\epsilon}z_0^2 = 3^{2v_3(E)+12n\epsilon}E_0^2x_0^{12n} - G^2.$$

Multiplying both sides of the above equation by $3^{-2v_3(E)-12n\epsilon}$,

$$pz_0^2 = E_0^2x_0^{12n} - 3^{-2v_3(E)-12n\epsilon}G^2. \tag{2.5}$$

We see that

$$\begin{aligned} v_3(3^{-2v_3(E)-12n\epsilon}G^2) &= 2v_3(G) - 2v_3(E) - 12n\epsilon > -12n - 12n\epsilon \quad \text{(by (A6))} \\ &= 12n(-\epsilon - 1) \geq 0. \end{aligned}$$

Hence, $v_3(3^{-2v_3(E)-12n\epsilon}G^2) > 0$. Since $v_3(3^{-2v_3(E)-12n\epsilon}G^2)$ is an integer,

$$v_3(3^{-2v_3(E)-12n\epsilon}G^2) \geq 1$$

and thus $3^{-2v_3(E)-12n\epsilon}G^2 \in 3\mathbb{Z}_3$. Reducing Equation (2.5) modulo 3,

$$p \equiv \left(\frac{E_0x_0^{6n}}{z_0}\right)^2 \bmod 3,$$

which is a contradiction since p is not a square in $\mathbb{F}_3^\times$. This contradiction implies that $v_3(x) \geq 0$. By (2.1), we see that $v_3(z) \geq 0$.

By (A7) and (2.1),

$$pz^2 = E^2x^{12n} - G^2 \equiv E^2x^{12n} \bmod 3.$$

https://doi.org/10.1017/S1446788715000348 Published online by Cambridge University Press

Since p is not a square in $\mathbb{F}_3^\times$, it follows that $z \equiv Ex \equiv 0 \bmod 3$. Assume that $A + Bx^{4n} + pz \equiv 0 \bmod 3$. Since $z \equiv 0 \bmod 3$, it follows that $A + Bx^{4n} \equiv 0 \bmod 3$. We see from (2.2) that

$$(Cx^{4n} + D)^2 - px^{4n}(Ex^{4n} + F)^2 \equiv 0 \bmod 3.$$

Since p is not a square in $\mathbb{F}_3^\times$,

$$Cx^{4n} + D \equiv x(Ex^{4n} + F) \equiv 0 \bmod 3.$$

Thus, we deduce that $A + Bx^{4n} \equiv Cx^{4n} + D \equiv 0 \bmod 3$. We contend that $x \not\equiv 0 \bmod 3$; otherwise, $A \equiv D \equiv 0 \bmod 3$ and hence it follows from (A7) that 3 divides $\gcd(A, D, G)$, which is a contradiction to (A3). Thus, $x \not\equiv 0 \bmod 3$ and hence we deduce that $x^2 \equiv 1 \bmod 3$. By (A7),

$$0 \equiv A + Bx^{4n} \equiv A + B \not\equiv 0 \bmod 3,$$

which is a contradiction. Hence, $A + Bx^{4n} + pz \not\equiv 0 \bmod 3$ and thus we deduce that the local Hilbert symbol $(p, A + Bx^{4n} + pz)_3$ is 1. Therefore, $\mathrm{inv}_3(\mathcal{A}(P_3))$ is 0.

Suppose that l is an odd prime such that $\gcd(l, 3) = \gcd(l, p) = 1$ and p is not a square in $\mathbb{Q}_l^\times$. We consider the following two cases.

⋆ *Case 1.* $v_l(x) \geq 0$.

Assume that

$$\begin{cases} A + Bx^{4n} + pz \equiv 0 \bmod l, \\ A + Bx^{4n} - pz \equiv 0 \bmod l. \end{cases} \tag{2.6}$$

By (2.2),

$$(Cx^{4n} + D)^2 - px^{4n}(Ex^{4n} + F)^2 \equiv 0 \bmod l.$$

Since p is not a square in $\mathbb{Q}_l^\times$,

$$\begin{cases} Cx^{4n} + D \equiv 0 \bmod l, \\ x(Ex^{4n} + F) \equiv 0 \bmod l. \end{cases} \tag{2.7}$$

Adding both of the equations of (2.6),

$$A + Bx^{4n} \equiv 0 \bmod l. \tag{2.8}$$

If $x \equiv 0 \bmod l$, then it follows from (2.8) and the first equation of (2.7) that $A \equiv D \equiv 0 \bmod l$. By (A1), we deduce that $pG^2 = D^2 - A^2 \equiv 0 \bmod l$. Since $p \neq l$, we deduce that l divides G and hence l divides $\gcd(A, D, G)$, which is a contradiction to (A3). If $x \not\equiv 0 \bmod l$, then it follows from the second equation of (2.7) that

$$Ex^{4n} + F \equiv 0 \bmod l. \tag{2.9}$$

Hence, it follows from (2.8), (2.9), and the first equation of (2.7) that

$$\begin{cases} BCx^{4n} \equiv -AC \equiv -BD \bmod l, \\ BEx^{4n} \equiv -AE \equiv -BF \bmod l, \\ CEx^{4n} \equiv -DE \equiv -CF \bmod l. \end{cases}$$

https://doi.org/10.1017/S1446788715000348 Published online by Cambridge University Press

Thus,

$$\begin{cases} AC - BD \equiv 0 \bmod l, \\ AE - BF \equiv 0 \bmod l, \\ DE - CF \equiv 0 \bmod l \end{cases}$$

and hence l divides $\gcd(AC - BD, DE - CF, AE - BF)$. Thus, it follows from (A4) that p is a square in $\mathbb{Q}_l^\times$, which is a contradiction. Therefore, at least one of $A + Bx^{4n} + pz$ and $A + Bx^{4n} - pz$ is nonzero modulo l, say U. Since $\mathcal{A}$ and $\mathcal{B}$ represent the same class in $\mathrm{Br}(\mathbb{Q}(C))$, we deduce that the local Hilbert symbol $(p, U)_l$ is 1. Hence, $\mathrm{inv}_l(\mathcal{A}(P_l))$ is 0.

$\star$ *Case 2.* $v_l(x) = \epsilon < 0$.

Since $\epsilon = v_l(x) \in \mathbb{Z}$, we deduce that $\epsilon \leq -1$. If $v_l(E) = 0$, then

$$v_l(E^2 x^{12n}) = 12n\epsilon \leq -12n < v_l(G^2).$$

If $v_l(E) > 0$, then l divides E. Since p is not a square in $\mathbb{Q}_l^\times$, it follows from (A2) that

$$v_l(E) - v_l(G) < 6n.$$

Hence,

$$v_l(E^2 x^{12n}) = 2v_l(E) + 12n\epsilon \leq 2v_l(E) - 12n < 2v_l(G) = v_l(G^2).$$

Thus, in any event, we see that $v_l(E^2 x^{6n}) < v_l(G^2)$. Hence, it follows from (2.1) that

$$v_l(z) = \frac{v_l(pz^2)}{2} = \frac{\min(v_l(E^2 x^{12n}), v_l(G^2))}{2} = v_l(E) + 6n\epsilon.$$

Hence, there are elements $x_0, z_0, E_0 \in \mathbb{Z}_l^\times$ such that

$$\begin{aligned} x &= l^\epsilon x_0, \\ z &= l^{v_l(E)+6n\epsilon} z_0, \\ E &= l^{v_l(E)} E_0. \end{aligned}$$

Hence, it follows from (2.1) that

$$pl^{2v_l(E)+12n\epsilon} z_0^2 = l^{2v_l(E)+12n\epsilon} E_0^2 x_0^{12n} - G^2.$$

Multiplying both sides of the above equation by $l^{-2v_l(E)-12n\epsilon}$,

$$pz_0^2 = E_0^2 x_0^{12n} - G^2 l^{-2v_l(E)-12n\epsilon}. \tag{2.10}$$

If $v_l(E) = 0$, then

$$\begin{aligned} v_l(G^2 l^{-2v_l(E)-12n\epsilon}) &= 2v_l(G) - 2v_l(E) - 12n\epsilon \\ &= 2v_l(G) - 12n\epsilon \\ &\geq 2v_l(G) + 12n \geq 12n \geq 12. \end{aligned}$$

If $v_l(E) > 0$, then we know that l divides E. Since p is not a square in $\mathbb{Q}_l^\times$, we deduce from (A2) that

$$v_l(E) - v_l(G) < 6n$$

https://doi.org/10.1017/S1446788715000348 Published online by Cambridge University Press

and hence

$$\begin{aligned} v_l(G^2 l^{-2v_l(E)-12n\epsilon}) &= 2v_l(G) - 2v_l(E) - 12n\epsilon \\ &> -12n - 12n\epsilon = 12n(-\epsilon - 1) \geq 0. \end{aligned}$$

Thus, in any event,

$$v_l(G^2 l^{-2v_l(E)-12n\epsilon}) > 0.$$

Since $v_l(G^2 l^{-2v_l(E)-12n\epsilon})$ is an integer,

$$v_l(G^2 l^{-2v_l(E)-12n\epsilon}) \geq 1$$

and hence

$$G^2 l^{-2v_l(E)-12n\epsilon} \in l\mathbb{Z}_l.$$

Reducing Equation (2.10) modulo l,

$$p \equiv \left(\frac{E_0 x_0^{6n}}{z_0}\right)^2 \bmod l,$$

which is a contradiction since p is not a square in $\mathbb{Q}_l^\times$.

Thus, in any event, if l is an odd prime such that $\gcd(l, 3) = \gcd(l, p) = 1$ and p is not a square in $\mathbb{Q}_l^\times$, then $\mathrm{inv}_l(\mathcal{A}(P_l))$ is 0.

Suppose that $l = p$. If $v_p(x) = \epsilon < 0$, then we know from (A3) that $E \not\equiv 0 \bmod p$. Hence,

$$v_p(E^2 x^{12n}) = 12n\epsilon < 0 \leq v_p(G^2).$$

It then follows from the above inequality and (2.1) that

$$1 + 2v_p(z) = v_p(pz^2) = v_p(E^2 x^{12n}) = 12n\epsilon,$$

which is a contradiction since the left-hand side is an odd integer whereas the right-hand side is an even integer.

If $v_p(x) \geq 0$, then it follows from (2.1) that

$$1 + 2v_p(z) = v_p(pz^2) = v_p(E^2 x^{12n} - G^2) \geq 0.$$

Hence, it follows that $v_p(z) \geq -\frac{1}{2}$. Since $v_p(z) \in \mathbb{Z}$, we deduce that $v_p(z) \geq 0$ and hence $z \in \mathbb{Z}_p$. We contend that $x \in \mathbb{Z}_p^\times$. Assume the contrary, that is, $x \equiv 0 \bmod p$. By (2.1),

$$G^2 = E^2 x^{12n} - pz^2 \equiv 0 \bmod p,$$

which is a contradiction to (A3). Hence, we deduce that $x \in \mathbb{Z}_p^\times$. Reducing Equation (2.1) modulo p,

$$E^2 x^{12n} - G^2 \equiv 0 \bmod p. \tag{2.11}$$

Let H be an integer satisfying (A5) in Definition 1.1. By (2.11), (A3), and (A5),

$$x^{12n} \equiv \left(\frac{G}{E}\right)^2 \equiv H^{12} \bmod p$$

https://doi.org/10.1017/S1446788715000348 Published online by Cambridge University Press

and hence $x^{4n} \equiv \zeta H^4 \bmod p$ for some cube root of unity ζ in $\mathbb{F}_p^\times$. Thus, it follows from (A5) that

$$A + Bx^{4n} + pz \equiv A + \zeta BH^4 \not\equiv 0 \bmod p.$$

Using [2, Theorem 5.2.7], we deduce from (A5) that the local Hilbert symbol $(p, A + Bx^{4n} + pz)_p$ satisfies

$$(p, A + Bx^{4n} + pz)_p = \left(\frac{A + \zeta BH^4}{p}\right) = -1,$$

which proves that $\mathrm{inv}_p(\mathcal{A}(P_p)) = 1/2$.

Therefore, in any event,

$$\sum_l \mathrm{inv}_l \mathcal{A}(P_l) = 1/2$$

for any $(P_l)_l \in C(\mathbb{A}_\mathbb{Q})$ and hence $C(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}} = \emptyset$. Hence, our contention follows. □

3. A subset of the set of all rational points on $\mathcal{X}_p$

In this section, we describe a subset of $\mathcal{X}_p(\mathbb{Q})$ for each prime p. Using this subset and Theorem 2.2, we will show that there exist infinitely many generalized Mordell curves of arbitrarily high degree that have no rational points. Furthermore, there is a Brauer–Manin obstruction to the existence of rational points on these curves.

Let p be an odd prime such that $p \neq 3$. Let λ and γ be nonzero *odd integers* such that

$$\gcd(\lambda, 3\gamma) = \gcd(p, 3\gamma) = \gcd(p, \lambda) = 1.$$

Since $\gcd(p\lambda^2, 9\gamma^2) = 1$, there exist nonzero integers ϵ_0 and δ_0 such that

$$p\lambda^2\epsilon_0 + 9\gamma^2\delta_0 = 1.$$

For integers $\mu, t_0, F_0 \in \mathbb{Z}$, we define

$$\begin{cases} A := \dfrac{p\lambda^2 - 9\gamma^2}{2}, \\ B := 2pF_0^2(\delta_0 - \epsilon_0 - \mu(p\lambda^2 + 9\gamma^2)) + (p\lambda^2 + 9\gamma^2)t_0F_0, \\ C := 2pF_0^2(\delta_0 + \epsilon_0 - \mu(p\lambda^2 - 9\gamma^2)) + (p\lambda^2 - 9\gamma^2)t_0F_0, \\ D = \dfrac{p\lambda^2 + 9\gamma^2}{2}, \\ E := F_0(2pF_0(\epsilon_0 + 9\mu\gamma^2) - 9\gamma^2t_0)(2F_0(\delta_0 - p\mu\lambda^2) + \lambda^2t_0), \\ F := 2F_0, \\ G = 3\lambda\gamma. \end{cases} \tag{3.1}$$

Note that B and C can be written in the following form:

$$\begin{cases} B := 2pF_0^2(\delta_0 - \epsilon_0 - 2\mu D) + 2Dt_0F_0, \\ C := 2pF_0^2(\delta_0 + \epsilon_0 - 2\mu A) + 2At_0F_0. \end{cases} \tag{3.2}$$

https://doi.org/10.1017/S1446788715000348 Published online by Cambridge University Press

It is not difficult to verify that the point $\mathcal{P} := (a : b : c : d : e : f : g) = (A : B : C : D : E : F : G)$ belongs to $\mathcal{X}_p(\mathbb{Q})$; hence, the septuple (A, B, C, D, E, F, G) satisfies (A1) in Definition 1.1. We see that (3.1) defines a parametrization of a subset of $\mathcal{X}_p(\mathbb{Q})$ by parameters $\lambda, \gamma, \mu, t_0$, and F_0. Using this parametrization, we will show that there are infinitely many septuples (A, B, C, D, E, F, G) satisfying GMC with respect to the couples (p, n), where n is a sufficiently large integer. The following lemma is the main result in this section.

LEMMA 3.1. *Let p be a prime such that $p \equiv 1 \bmod 8$ and $p \equiv 2 \bmod 3$. Then there exist infinitely many septuples $(A, B, C, D, E, F, G) \in \mathbb{Z}^7$ such that they satisfy (3.1) and (A1), (A3)–(A5), and (A7) in Definition 1.1 and such that for any integer $n \geq 1$, they satisfy (A6) in Definition 1.1 with respect to the couple (p, n).*

PROOF. Let λ and γ be odd integers such that

$$\gcd(\lambda, 3\gamma) = \gcd(p, 3\gamma) = \gcd(p, \lambda) = 1. \tag{3.3}$$

Since $\gcd(p\lambda^2, 9\gamma^2) = 1$, there exist nonzero integers ϵ^* and δ^* such that

$$p\lambda^2\epsilon^* + 9\gamma^2\delta^* = 1.$$

We see that $\epsilon_0 = \epsilon^* + 9\gamma^2 s^*$ and $\delta_0 = \delta^* - p\lambda^2 s^*$ satisfy the following equation:

$$p\lambda^2\epsilon_0 + 9\gamma^2\delta_0 = 1, \tag{3.4}$$

where s^* is an arbitrary integer. For our purpose, we choose s^* such that $\delta^* + s^* \equiv 2 \bmod 3$. Since $\lambda \not\equiv 0 \bmod 3$ and $p \equiv 2 \bmod 3$,

$$\delta_0 = \delta^* - p\lambda^2 s^* \equiv \delta^* - 2s^* \equiv \delta^* + s^* \equiv 2 \bmod 3. \tag{3.5}$$

Let (A, B, C, D, E, F, G) be the septuple of integers defined by (3.1), where μ, t_0, and F_0 will be determined later. It is not difficult to prove that (A, B, C, D, E, F, G) belongs to $\mathcal{X}_p(\mathbb{Q})$, where $\mathcal{X}_p$ is the threefold defined by (1.1), and hence it satisfies (A1) in Definition 1.1. By (3.1) and (3.2),

$$\begin{aligned}
AC - BD &= A(2pF_0^2(\delta_0 + \epsilon_0 - 2\mu A) + 2At_0F_0) \\
&\quad - D(2pF_0^2(\delta_0 - \epsilon_0 - 2\mu D) + 2Dt_0F_0) \\
&= 4pF_0^2(D^2 - A^2)\mu + 2pF_0^2(A(\delta_0 + \epsilon_0) - D(\delta_0 - \epsilon_0)) + 2t_0F_0(A^2 - D^2) \\
&= 4p^2F_0^2G^2\mu + 2pF_0^2(\epsilon_0(A + D) + \delta_0(A - D)) - 2pt_0F_0G^2 \\
&\quad \text{(since } A^2 - D^2 + pG^2 = 0\text{)} \\
&= 2pF_0(2pF_0G^2\mu + F_0(\epsilon_0(A + D) + \delta_0(A - D)) - t_0G^2) \\
&= 2pF_0Q^*,
\end{aligned} \tag{3.6}$$

where

$$Q^* = 2pF_0G^2\mu + F_0(\epsilon_0(A + D) + \delta_0(A - D)) - t_0G^2.$$

https://doi.org/10.1017/S1446788715000348 Published online by Cambridge University Press

By (3.1),

$$A + D = p\lambda^2,$$
$$A - D = -9\gamma^2.$$

By the above identities, (3.4), and since $G = 3\lambda\gamma$,

$$\begin{aligned} Q^* &= 2pF_0G^2\mu + F_0(p\lambda^2\epsilon_0 - 9\gamma^2\delta_0) - t_0G^2 \\ &= 2pF_0G^2\mu + F_0(2p\lambda^2\epsilon_0 - 1) - t_0G^2 \\ &= (18p\lambda^2\gamma^2F_0)\mu + F_0(2p\lambda^2\epsilon_0 - 1) - 9\lambda^2\gamma^2t_0. \end{aligned} \tag{3.7}$$

⋆ *Step 1.* Choosing t_0.

We define

$$t_0 := -3\lambda\gamma F_0 t_1, \tag{3.8}$$

where t_1 is an integer which will be chosen below in this step, and F_0 will be chosen in Step 2. By (3.7), one can write Q^* in the form

$$Q^* = F_0((18p\lambda^2\gamma^2)\mu + 2p\lambda^2\epsilon_0 - 1 + 27\lambda^3\gamma^3t_1) = F_0(P_1^*\mu + R_1^*), \tag{3.9}$$

where

$$\begin{cases} P_1^* := 18p\lambda^2\gamma^2, \\ R_1^* := 2p\lambda^2\epsilon_0 - 1 + 27\lambda^3\gamma^3t_1. \end{cases} \tag{3.10}$$

Since $\gcd(27\lambda^3\gamma^3, p) = 1$, there exist nonzero integers t_2 and t_3 such that

$$27\lambda^3\gamma^3t_2 - pt_3 = 1. \tag{3.11}$$

Take any nonzero integer π such that π is a *quadratic residue* in $\mathbb{F}_p^\times$, and let t_5 be any nonzero integer such that

$$\begin{cases} t_5 \equiv \dfrac{\pi - 2\lambda^2\epsilon_0 - t_3}{27\lambda^3\gamma^3} \bmod p, \\ t_5 \equiv 1 - t_3 \bmod 2. \end{cases} \tag{3.12}$$

Note that there are infinitely many such integers π and t_5. Define

$$t_1 := t_2 + pt_5 \tag{3.13}$$

and

$$t_4 := t_3 + 27\lambda^3\gamma^3t_5. \tag{3.14}$$

By (3.11), (3.13), and (3.14),

$$27\lambda^3\gamma^3t_1 - pt_4 = 1. \tag{3.15}$$

In summary, by (3.8) and (3.13), t_0 is of the form

$$t_0 = -3\lambda\gamma F_0(t_2 + pt_5), \tag{3.16}$$

where t_2 is an integer satisfying (3.11) and t_5 is any nonzero integer satisfying (3.12).

https://doi.org/10.1017/S1446788715000348 Published online by Cambridge University Press

⋆ *Step 2*. Choosing F_0.

Define

$$u := \begin{cases} 1 & \text{if } \lambda\gamma \text{ is a quadratic residue modulo } p, \\ 0 & \text{if } \lambda\gamma \text{ is a quadratic nonresidue modulo } p. \end{cases} \tag{3.17}$$

We take F_0 to be any nonzero integer such that the following are true:

(F1) $F_0 = 3^u F_1$, where F_1 is an integer such that $\gcd(F_1, 3) = \gcd(F_1, p) = 1$;
(F2) p is a square in $\mathbb{Q}_l^\times$ for each odd prime l dividing F_1.

⋆ *Step 3*. Defining H.

We prove that $(3\lambda\gamma)/F_0$ is a quadratic residue in $\mathbb{F}_p^\times$. Assume first that $\lambda\gamma$ is a quadratic residue in $\mathbb{F}_p^\times$. By (3.17) in Step 2, we know that $u = 1$. By (F1) in Step 2,

$$\frac{3\lambda\gamma}{F_0} = \frac{3\lambda\gamma}{3^u F_1} = \frac{\lambda\gamma}{F_1}.$$

Hence, in order to prove that $(3\lambda\gamma)/F_0$ is a quadratic residue in $\mathbb{F}_p^\times$, it suffices to prove that F_1 is a square in $\mathbb{F}_p^\times$. Write F_1 in the form

$$F_1 = \pm 2^{v_2(F_1)} \prod_{l|F_1} l^{v_l(F_1)},$$

where the product is taken over all odd primes l dividing F_1. Since $p \equiv 1 \bmod 8$, we know that -1 and 2 are quadratic residues in $\mathbb{F}_p^\times$. Hence, it follows from (F2) in Step 2 and the quadratic reciprocity law that

$$\begin{aligned} \left(\frac{F_1}{p}\right) &= \left(\frac{\pm 2^{v_2(F_1)} \prod_{l|F_1} l^{v_l(F_1)}}{p}\right) \\ &= \left(\frac{\pm 1}{p}\right)\left(\frac{2^{v_2(F_1)}}{p}\right) \prod_{l|F_1} \left(\frac{l^{v_l(F_1)}}{p}\right) \\ &= \left(\frac{2}{p}\right)^{v_2(F_1)} \prod_{l|F_1} \left(\frac{p}{l}\right)^{v_l(F_1)} \\ &= 1. \end{aligned}$$

Thus, F_1 is a quadratic residue in $\mathbb{F}_p^\times$ and hence $(3\lambda\gamma)/F_0$ is a quadratic residue in $\mathbb{F}_p^\times$.

Assume now that $\lambda\gamma$ is a quadratic nonresidue in $\mathbb{F}_p^\times$. By (3.17) in Step 2, we know that $u = 0$. Hence, $3^u = 1$ and hence $F_0 = 3^u F_1 = F_1$. As was shown above, F_1 is a square in $\mathbb{F}_p^\times$ and thus F_0 is a square in $\mathbb{F}_p^\times$. Since $p \equiv 2 \bmod 3$, we deduce that p is a quadratic nonresidue in $\mathbb{F}_3^\times$. By the quadratic reciprocity law, we deduce that 3 is a quadratic nonresidue in $\mathbb{F}_p^\times$. Thus, $3\lambda\gamma$ is a square in $\mathbb{F}_p^\times$ and therefore it follows that $(3\lambda\gamma)/F_0$ is a quadratic residue in $\mathbb{F}_p^\times$.

Therefore, in any event, $(3\lambda\gamma)/F_0$ is a square in $\mathbb{F}_p^\times$. We now define H to be any nonzero integer such that

$$H \equiv \left(\frac{3\lambda\gamma}{F_0}\right)^{1/2} \bmod p. \tag{3.18}$$

https://doi.org/10.1017/S1446788715000348 Published online by Cambridge University Press

⋆ *Step 4.* Defining μ.

By (3.10) and (3.15), R_1^* can be written in the form

$$R_1^* = 2p\lambda^2\epsilon_0 - 1 + 27\lambda^3\gamma^3 t_1 = 2p\lambda^2\epsilon_0 + pt_4 = pR_2^*,$$

where

$$R_2^* := 2\lambda^2\epsilon_0 + t_4. \tag{3.19}$$

By (3.9) and (3.10), we can write Q^* in the form

$$Q^* = F_0(P_1^*\mu + R_1^*) = pF_0(P_2^*\mu + R_2^*) = pF_0Q_1^*, \tag{3.20}$$

where

$$Q_1^* = P_2^*\mu + R_2^* \tag{3.21}$$

and

$$P_2^* = 18\lambda^2\gamma^2.$$

We contend that $\gcd(3pP_2^*, R_2^*) = 1$. Since λ and γ is odd, it follows from (3.12), (3.14), and (3.19) that

$$R_2^* \equiv t_4 \equiv t_3 + 27\lambda^3\gamma^3 t_5 \equiv t_3 + t_5 \equiv 1 \bmod 2. \tag{3.22}$$

Since $\gcd(p, \lambda) = 1$, it follows from (3.15) and (3.19) that

$$R_2^* \equiv t_4 \equiv -\frac{1}{p} \not\equiv 0 \bmod l \tag{3.23}$$

for each odd prime l dividing λ and hence $\gcd(R_2^*, \lambda) = 1$. Since $\gcd(p, 3\gamma) = 1$, it follows from (3.4)–(3.19) that

$$R_2^* = 2\lambda^2\epsilon_0 + t_4 \equiv \frac{2}{p} + t_4 \equiv \frac{2}{p} - \frac{1}{p} \equiv \frac{1}{p} \not\equiv 0 \bmod l \tag{3.24}$$

for each odd prime l dividing 3γ and hence $\gcd(R_2^*, 3\gamma) = 1$. By (3.12), (3.14), and (3.19),

$$R_2^* = 2\lambda^2\epsilon_0 + t_4 = 2\lambda^2\epsilon_0 + t_3 + 27\lambda^3\gamma^3 t_5 \equiv \pi \not\equiv 0 \bmod p \tag{3.25}$$

and hence $\gcd(R_2^*, p) = 1$. Since $P_2^* = 18\lambda^2\gamma^2$, it follows from (3.22)–(3.25) that

$$\gcd(3pP_2^*, R_2^*) = 1.$$

We now define μ. Since $\gcd(3pP_2^*, R_2^*) = 1$, it follows from Dirichlet's theorem on arithmetic progressions that there are infinitely many integers μ_1 such that $3pP_2^*\mu_1 + R_2^*$ is an odd prime. Take such an integer μ_1 and define

$$\mu = 3p\mu_1. \tag{3.26}$$

By (3.21), the choice of μ_1, and the definition of μ, we see that Q_1^* is an odd prime.

https://doi.org/10.1017/S1446788715000348 Published online by Cambridge University Press

⋆ *Step 5.* Verifying (A3).

By (3.1) and (3.3), we see that $\gcd(A, D, G) = 1$ and $G \not\equiv 0 \bmod p$. Hence, it remains to verify that $E \not\equiv 0 \bmod p$. We see that

$$\begin{aligned} E &= F_0(2pF_0(\epsilon_0 + 9\mu\gamma^2) - 9\gamma^2 t_0)(2F_0(\delta_0 - p\mu\lambda^2) + \lambda^2 t_0) \quad \text{(by (3.1))} \\ &\equiv -9\gamma^2 F_0 t_0(\lambda^2 t_0 + 2\delta_0 F_0) \\ &\equiv 27\lambda\gamma^3 F_0^2 t_2(-3\lambda^3\gamma F_0 t_2 + 2\delta_0 F_0) \quad \text{(by (3.16))} \\ &\equiv -27\lambda\gamma^3 F_0^3 t_2\left(3\lambda^3\gamma t_2 - \frac{2}{9\gamma^2}\right) \quad \text{(by (3.4))} \\ &\equiv -\frac{F_0^3}{\lambda^2}\left(\frac{1}{9\gamma^2} - \frac{2}{9\gamma^2}\right) \quad \text{(by (3.11))} \\ &\equiv \frac{F_0^3}{9\lambda^2\gamma^2} \not\equiv 0 \bmod p. \end{aligned} \tag{3.27}$$

Hence, (A3) holds.

⋆ *Step 6.* Verifying (A4).

Let l be any odd prime such that $\gcd(l, 3) = \gcd(l, p) = 1$ and l divides $AC - BD$. We will prove that p is a square in $\mathbb{Q}_l^\times$. Indeed, by (3.6) and (3.20), we can write $AC - BD$ in the form

$$AC - BD = 2pF_0Q^* = 2p^2F_0^2Q_1^*, \tag{3.28}$$

where Q_1^* is given by (3.21). Recall that by the choice of μ in Step 4, Q_1^* is an odd prime. If l divides F_0, then it follows from (F1) in Step 2 that l divides F_1. Hence, it follows from (F2) in Step 2 that p is a square in $\mathbb{Q}_l^\times$. If $\gcd(l, F_0) = 1$, we see that since Q_1^* is an odd prime, l divides $AC - BD$, and $\gcd(l, 2pF_0) = 1$, it follows from (3.28) that $l = Q_1^*$. Hence, it suffices to show that p is a square in $\mathbb{Q}_{Q_1^*}^\times$, where $\mathbb{Q}_{Q_1^*}$ denotes the Q_1^*-adic field.

By (3.21), (3.25), and (3.26),

$$Q_1^* = P_2^*\mu + R_2^* = 3pP_2^*\mu_1 + R_2^* \equiv R_2^* \equiv \pi \bmod p.$$

By the choice of π in Step 1, we know that π is a quadratic residue in $\mathbb{F}_p^\times$. Hence, it follows from the last congruence that $(Q_1^*/p) = 1$, where $(\cdot/\cdot)$ denotes the Jacobi symbol. By the quadratic reciprocity law,

$$\left(\frac{p}{Q_1^*}\right) = \left(\frac{Q_1^*}{p}\right) = 1$$

and thus p is a square in $\mathbb{Q}_{Q_1^*}^\times$. Hence, (A4) holds.

⋆ *Step 7.* Verifying (A5).

Since $p \equiv 2 \bmod 3$, p is a quadratic nonresidue in $\mathbb{F}_3^\times$. By the quadratic reciprocity law, we deduce that 3 is a quadratic nonresidue in $\mathbb{F}_p^\times$ and hence -3 is not a square in $\mathbb{F}_p^\times$. Thus, the group of all cube roots of unity in $\mathbb{F}_p^\times$ is trivial. We will prove that

https://doi.org/10.1017/S1446788715000348 Published online by Cambridge University Press

H satisfies (A5), where H is defined in Step 3. Note that since the group of all cube roots of unity in $\mathbb{F}_p^\times$ is trivial, the second condition in (A5) is tantamount to saying that $A + BH^4$ is a quadratic nonresidue in $\mathbb{F}_p^\times$.

By (3.1), (3.18), and (3.27),

$$\begin{aligned} G - EH^6 &\equiv 3\lambda\gamma - \left(\frac{F_0^3}{9\lambda^2\gamma^2}\right)\left(\frac{27\lambda^3\gamma^3}{F_0^3}\right) \\ &\equiv 3\lambda\gamma - 3\lambda\gamma \equiv 0 \bmod p. \end{aligned}$$

We see that

$$\begin{aligned} A + BH^4 &\equiv -\frac{9\gamma^2}{2} + 9\gamma^2 t_0 F_0\left(\frac{9\lambda^2\gamma^2}{F_0^2}\right) \quad \text{(by (3.1) and (3.18))} \\ &\equiv -\frac{9\gamma^2}{2} + 9\gamma^2(-3\lambda\gamma F_0(t_2 + pt_5))F_0\left(\frac{9\lambda^2\gamma^2}{F_0^2}\right) \quad \text{(by (3.16))} \\ &\equiv -\frac{9\gamma^2}{2} - 27\lambda\gamma^3 F_0^2 t_2\left(\frac{9\lambda^2\gamma^2}{F_0^2}\right) \\ &\equiv -\frac{9\gamma^2}{2} - (27\lambda^3\gamma^3 t_2)9\gamma^2 \\ &\equiv -\frac{9\gamma^2}{2} - 9\gamma^2 \quad \text{(by (3.11))} \\ &\equiv 3\left(\frac{-1}{2}\right)(3\gamma)^2 \bmod p. \end{aligned}$$

Since -1 and 2 are quadratic residues in $\mathbb{F}_p^\times$ and 3 is a quadratic nonresidue in $\mathbb{F}_p^\times$, we deduce that $3(\frac{-1}{2})(3\gamma)^2$ is a quadratic nonresidue in $\mathbb{F}_p^\times$. Hence, $A + BH^4$ is a quadratic nonresidue in $\mathbb{F}_p^\times$ and thus (A5) holds.

$\star$ *Step 8.* Verifying (A6).

Since $\lambda \not\equiv 0 \bmod 3$ and $p \equiv 2 \bmod 3$, it follows from (3.4) that

$$\epsilon_0 \equiv \frac{1}{p\lambda^2} \equiv \frac{1}{2} \equiv 2 \bmod 3. \tag{3.29}$$

By (3.1) and (3.16),

$$\begin{aligned} E &= F_0(2pF_0(\epsilon_0 + 9\mu\gamma^2) - 9\gamma^2 t_0)(2F_0(\delta_0 - p\mu\lambda^2) + \lambda^2 t_0) \\ &= F_0(2pF_0(\epsilon_0 + 9\mu\gamma^2) - 9\gamma^2(-3\lambda\gamma F_0(t_2 + pt_5))) \\ &\qquad \times (2F_0(\delta_0 - p\mu\lambda^2) + \lambda^2(-3\lambda\gamma F_0(t_2 + pt_5))) \quad \text{(by (3.16))} \\ &= F_0^3(2p(\epsilon_0 + 9\mu\gamma^2) + 27\lambda\gamma^3(t_2 + pt_5))(2(\delta_0 - p\mu\lambda^2) - 3\lambda^3\gamma(t_2 + pt_5)). \end{aligned}$$

Hence,

$$\begin{aligned} v_3(E) = v_3(F_0^3) &+ v_3(2p(\epsilon_0 + 9\mu\gamma^2) + 27\lambda\gamma^3(t_2 + pt_5)) \\ &+ v_3(2(\delta_0 - p\mu\lambda^2) - 3\lambda^3\gamma(t_2 + pt_5)). \end{aligned} \tag{3.30}$$

https://doi.org/10.1017/S1446788715000348 Published online by Cambridge University Press

By (F1) in Step 2,

$$v_3(F_0^3) = 3v_3(F_0) = 3v_3(3^u F_1) = 3v_3(3^u) + 3v_3(F_1) = 3u. \tag{3.31}$$

By (3.29) and since $p \equiv 2 \bmod 3$,

$$2p(\epsilon_0 + 9\mu\gamma^2) + 27\lambda\gamma^3(t_2 + pt_5) \equiv 2p\epsilon_0 \equiv 8 \equiv 2 \bmod 3$$

and hence

$$v_3(2p(\epsilon_0 + 9\mu\gamma^2) + 27\lambda\gamma^3(t_2 + pt_5)) = 0. \tag{3.32}$$

By (3.26),

$$\mu = 3p\mu_1 \equiv 0 \bmod 3$$

and hence it follows from (3.5) that

$$2(\delta_0 - p\mu\lambda^2) - 3\lambda^3\gamma(t_2 + pt_5) \equiv 2\delta_0 \equiv 4 \equiv 1 \bmod 3.$$

Thus,

$$v_3(2(\delta_0 - p\mu\lambda^2) - 3\lambda^3\gamma(t_2 + pt_5)) = 0. \tag{3.33}$$

Hence, it follows from (3.30)–(3.33) that

$$v_3(E) = 3u$$

and thus we deduce from (3.1), (3.3), and (3.17) that

$$v_3(E) - v_3(G) = 3u - v_3(3\lambda\gamma) = 3u - 1 \leq 3 - 1 = 2 < 3n$$

for any integer $n \geq 1$. Therefore, (A6) holds.

$\star$ *Step 9.* Verifying (A7).

By (3.16), we know that

$$t_0 = -3\lambda\gamma F_0(t_2 + pt_5) \equiv 0 \bmod 3.$$

Since $p \equiv 2 \bmod 3$, $\lambda \not\equiv 0 \bmod 3$, and $\mu = 3p\mu_1 \equiv 0 \bmod 3$, it follows from (3.1), (3.3), (3.5), and (3.29) that

$$\begin{aligned} A + B &\equiv \frac{p\lambda^2}{2} + 2pF_0^2(\delta_0 - \epsilon_0) \\ &\equiv 1 + 4F_0^2(2 - 2) \equiv 1 \not\equiv 0 \bmod 3. \end{aligned}$$

By (3.1), we know that

$$G = 3\lambda\gamma \equiv 0 \bmod 3.$$

Hence, (A7) holds.

By what we have shown above, our contention follows. □

Remark 3.2. Lemma 3.1 shows that for a prime p with $p \equiv 1 \bmod 8$ and $p \equiv 2 \bmod 3$, and an integer $n \geq 1$, there are infinitely many septuples (A, B, C, D, E, F, G) defined by (3.1) that satisfy (A1) and (A3)–(A7) with respect to the couple (p, n). It is not difficult to choose n sufficiently large so that the septuples (A, B, C, D, E, F, G) in Lemma 3.1 satisfy GMC with respect to (p, n). Such septuples produce infinitely many generalized

https://doi.org/10.1017/S1446788715000348 Published online by Cambridge University Press

Mordell curves of degree $12n$ that have no rational points, and there is a Brauer–Manin obstruction to the existence of rational points on these curves. This remark is summarized in the following corollary.

COROLLARY 3.3. *Let p be a prime such that $p \equiv 1 \bmod 8$ and $p \equiv 2 \bmod 3$. There exists an infinite set $\mathfrak{C}_p \subseteq \mathbb{Z}^7$ consisting of the septuples $(A, B, C, D, E, F, G) \in \mathbb{Z}^7$ defined by (3.1) that satisfy (A1), (A3)–(A5), and (A7) in Definition 1.1. Furthermore, for each septuple $\mathcal{T} = (A, B, C, D, E, F, G) \in \mathfrak{C}_p$, there exists a positive real number $n_{E,G} \geq 1$ that depends only on E and G such that for any integer $n > n_{E,G}$, the septuple $\mathcal{T}$ satisfies* GMC *with respect to (p, n), and the smooth projective model $C_{n,\mathcal{T}}$ of the affine curve defined by*

$$C_{n,\mathcal{T}} : pz^2 = E^2 x^{12n} - G^2$$

satisfies $C_{n,\mathcal{T}}(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} = \emptyset$.

PROOF. Let $\mathfrak{C}_p$ be the set of the septuples $(A, B, C, D, E, F, G) \in \mathbb{Z}^7$ satisfying the following two conditions:

(i) (A, B, C, D, E, F, G) satisfies (3.1), and (A1), (A3)–(A5), and (A7) in Definition 1.1; and
(ii) for any $n \geq 1$, (A, B, C, D, E, F, G) satisfies $(A6)$ in Definition 1.1 with respect to the couple (p, n).

By Lemma 3.1, we know that $\mathfrak{C}_p$ is of infinite cardinality.

Take any septuple $\mathcal{T} = (A, B, C, D, E, F, G) \in \mathfrak{C}_p$, and let $\mathcal{S}_{E,G}$ be the set of odd primes l such that $\gcd(l, 3p) = 1$, l divides E, and p is not a square in $\mathbb{Q}_l^{\times}$. Set

$$n^*_{E,G} := \begin{cases} \max\limits_{l \in \mathcal{S}_{E,G}} \left(\dfrac{v_l(E) - v_l(G)}{6} \right) & \text{if } \mathcal{S}_{E,G} \neq \emptyset, \\ 1 & \text{if } \mathcal{S}_{E,G} = \emptyset \end{cases}$$

and define

$$n_{E,G} := \max(1, n^*_{E,G}).$$

Let n be any integer such that $n > n_{E,G}$. Let l be any odd prime such that $\gcd(l, 3p) = 1$ and l divides E. If p is not a square in $\mathbb{Q}_l^{\times}$, then l belongs to $\mathcal{S}_{E,G}$. Hence, by definition of $n_{E,G}$,

$$6n > 6n_{E,G} \geq 6n^*_{E,G} \geq v_l(E) - v_l(G),$$

which proves that the septuple $\mathcal{T}$ satisfies (A2) with respect to (p, n) and thus it satisfies GMC with respect to the couple (p, n). The last assertion follows immediately from Theorem 2.2. □

REMARK 3.4. Corollary 3.3 only produces generalized Mordell curves of degree $12n$ with n sufficiently large that have no rational points such that there is a Brauer–Manin obstruction to the existence of rational points on these curves. For *each* $n \geq 1$, we are interested in looking for infinitely many generalized Mordell curves of degree $12n$ that have no rational points and satisfy the Scharaschkin–Skorobogatov conjecture.

https://doi.org/10.1017/S1446788715000348 Published online by Cambridge University Press

In order to do that, it suffices to show that for any $n \geq 1$, there are infinitely many septuples (A, B, C, D, E, F, G) from Lemma 3.1 satisfying (A2) with respect to (p, n), that is,

$$v_l(E) - v_l(G) < 6n,$$

where l is any odd prime such that $\gcd(l, 3p) = 1$, l divides E, and p is not a square in $\mathbb{Q}_l^\times$. This can be proved conditionally under the assumption of *Schinzel's hypothesis H*. The rest of the paper is devoted to proving this result.

We begin by recalling the statement of Schinzel's hypothesis H [6, 7].

Conjecture 3.5 (Schinzel's hypothesis H). Let $F_1(x), F_2(x), \ldots, F_n(x)$ be nonconstant polynomials in $\mathbb{Z}[x]$ such that the polynomials $F_1(x), \ldots, F_n(x)$ have positive leading coefficients and are irreducible over $\mathbb{Q}$. Assume that the polynomial

$$F(x) := \prod_{i=1}^{n} F_i(x) \in \mathbb{Z}[x]$$

has no fixed prime divisor, that is, there is no prime q dividing $F(m)$ for all integers m. Then there are infinitely many arbitrarily large positive integers x such that $F_1(x), F_2(x), \ldots, F_n(x)$ are simultaneously primes.

Corollary 3.6. *Let p be a prime such that $p \equiv 1 \bmod 8$ and $p \equiv 2 \bmod 3$. Let $\mathfrak{C}_p$ be the set defined in Corollary 3.3. Assume Schinzel's hypothesis H. Let n be a positive integer. Then there exist infinitely many septuples (A, B, C, D, E, F, G) in $\mathfrak{C}_p$ that satisfy* GMC *with respect to the couple (p, n).*

Proof. We maintain the same notation as in the proof of Lemma 3.1. Using exactly the same words and repeating the same arguments from the beginning of the proof of Lemma 3.1 to the end of Step 3 in the proof of Lemma 3.1, we let $\lambda, \gamma, \epsilon_0, \delta_0$ as in the proof of Lemma 3.1, and define t_0, F_0, and H as in Steps 1–3 in the proof of Lemma 3.1. Let (A, B, C, D, E, F, G) be the septuple of integers defined by (3.1), where μ will be determined shortly.

By (3.8),

$$\begin{aligned} E &= F_0(2pF_0(\epsilon_0 + 9\mu\gamma^2) - 9\gamma^2 t_0)(2F_0(\delta_0 - p\mu\lambda^2) + \lambda^2 t_0) \\ &= F_0(2pF_0(\epsilon_0 + 9\mu\gamma^2) - 9\gamma^2(-3\lambda\gamma F_0 t_1))(2F_0(\delta_0 - p\mu\lambda^2) + \lambda^2(-3\lambda\gamma F_0 t_1)) \\ &= F_0^3(2p(\epsilon_0 + 9\mu\gamma^2) + 27\lambda\gamma^3 t_1)(2(\delta_0 - p\mu\lambda^2) - 3\lambda^3\gamma t_1) \\ &= -F_0^3((18p\gamma^2)\mu + 2p\epsilon_0 + 27\lambda\gamma^3 t_1)((2p\lambda^2)\mu - 2\delta_0 + 3\lambda^3\gamma t_1) \end{aligned}$$

and hence

$$E = -F_0^3 E_1^* E_2^*, \tag{3.34}$$

where

$$E_1^* := (18p\gamma^2)\mu + 2p\epsilon_0 + 27\lambda\gamma^3 t_1$$

and

$$E_2^* := (2p\lambda^2)\mu - 2\delta_0 + 3\lambda^3\gamma t_1.$$

https://doi.org/10.1017/S1446788715000348 Published online by Cambridge University Press

Let

$$\mu := 3p\mu_1, \tag{3.35}$$

where μ_1 will be determined below. We see that

$$E_1^* := (54p^2\gamma^2)\mu_1 + 2p\epsilon_0 + 27\lambda\gamma^3 t_1$$

and

$$E_2^* := (6p^2\lambda^2)\mu_1 - 2\delta_0 + 3\lambda^3\gamma t_1.$$

Write $t_1 = 2^v t_1^*$, where v is a nonnegative integer and t_1^* is an odd integer. We contend that t_1 is an even integer, that is, $v \geq 1$. By (3.12), (3.14), (3.15), and since λ and γ are odd,

$$\begin{aligned} 1 = 27\lambda^3\gamma^3 t_1 - pt_4 &\equiv t_1 + t_4 \\ &\equiv t_1 + t_3 + 27\lambda^3\gamma^3 t_5 \\ &\equiv t_1 + t_3 + t_5 \equiv t_1 + 1 \bmod 2 \end{aligned}$$

and hence

$$t_1 \equiv 0 \bmod 2.$$

Thus, t_1 is an even integer and therefore $v \geq 1$.

We see that

$$E_1^* = 2E_1 \tag{3.36}$$

and

$$E_2^* = 2E_2, \tag{3.37}$$

where

$$E_1 := (27p^2\gamma^2)\mu_1 + p\epsilon_0 + 27\lambda\gamma^3 2^{v-1} t_1^*$$

and

$$E_2 := (3p^2\lambda^2)\mu_1 - \delta_0 + 3\lambda^3\gamma 2^{v-1} t_1^*.$$

Let Q_1^* be the integer defined by (3.21) in Step 4 in the proof of Lemma 3.1. We can write Q_1^* in the form

$$Q_1^* = P_2^*\mu + R_2^* = 3pP_2^*\mu_1 + R_2^*,$$

where we recall from Step 4 in the proof of Lemma 3.1 that

$$P_2^* = 18\lambda^2\gamma^2$$

and

$$R_2^* = 2\lambda^2\epsilon_0 + t_4.$$

Viewing μ_1 as a variable, we see that E_1, E_2 and Q_1^* are polynomials with integral coefficients in the variable μ_1, that is, E_1, E_2, and Q_1^* belong to $\mathbb{Z}[\mu_1]$. Upon assuming Schinzel's hypothesis H, we will show that there should be infinitely many arbitrarily large positive integers μ_1 such that E_1, E_2, and Q_1^* are simultaneously primes. In order

https://doi.org/10.1017/S1446788715000348 Published online by Cambridge University Press

to apply Schinzel's hypothesis H, we need to prove that the polynomial $\Psi(\mu_1) \in \mathbb{Z}[\mu_1]$ defined by

$$\Psi(\mu_1) := E_1 E_2 Q_1^* \tag{3.38}$$

has no fixed divisors, that is, there is no prime q dividing $\Psi(m)$ for every integer m. To prove the latter, it suffices to show that

$$\gcd(27p^2\gamma^2, p\epsilon_0 + 27\lambda\gamma^3 2^{\nu-1} t_1^*) = 1,$$
$$\gcd(3p^2\lambda^2, -\delta_0 + 3\lambda^3\gamma 2^{\nu-1} t_1^*) = 1,$$

and

$$\gcd(3pP_2^*, R_2^*) = 1.$$

Using the same arguments as in Step 4 in the proof of Lemma 3.1,

$$\gcd(3pP_2^*, R_2^*) = 1. \tag{3.39}$$

We now prove that

$$\gcd(27p^2\gamma^2, p\epsilon_0 + 27\lambda\gamma^3 2^{\nu-1} t_1^*) = 1.$$

Indeed, by (3.15),

$$2^{\nu-1} t_1^* = \frac{t_1}{2} \equiv \frac{1}{54\lambda^3\gamma^3} \not\equiv 0 \bmod p.$$

Since $\gcd(p, \lambda) = \gcd(p, \gamma) = \gcd(p, 3) = 1$,

$$p\epsilon_0 + 27\lambda\gamma^3 2^{\nu-1} t_1^* \equiv 27\lambda\gamma^3 2^{\nu-1} t_1^* \not\equiv 0 \bmod p.$$

Since $\gcd(\lambda, 3\gamma) = 1$, we see that if l is any prime dividing 3γ, then it follows from (3.4) that

$$p\epsilon_0 \equiv \frac{1}{\lambda^2} \not\equiv 0 \bmod l$$

and hence

$$p\epsilon_0 + 27\lambda\gamma^3 2^{\nu-1} t_1^* \equiv p\epsilon_0 \not\equiv 0 \bmod l.$$

Thus,

$$\gcd(27p^2\gamma^2, p\epsilon_0 + 27\lambda\gamma^3 2^{\nu-1} t_1^*) = 1. \tag{3.40}$$

We prove that

$$\gcd(3p^2\lambda^2, -\delta_0 + 3\lambda^3\gamma 2^{\nu-1} t_1^*) = 1.$$

Indeed, by (3.4) and (3.15),

$$\begin{aligned} -\delta_0 + 3\lambda^3\gamma 2^{\nu-1} t_1^* = -\delta_0 + 3\lambda^3\gamma\left(\frac{t_1}{2}\right) &\equiv -\frac{1}{9\gamma^2} + 3\lambda^3\gamma\left(\frac{1}{54\lambda^3\gamma^3}\right) \\ &\equiv -\frac{1}{9\gamma^2} + \frac{1}{18\gamma^2} \\ &\equiv -\frac{1}{18\gamma^2} \not\equiv 0 \bmod p. \end{aligned}$$

https://doi.org/10.1017/S1446788715000348 Published online by Cambridge University Press

By (3.5),

$$-\delta_0 + 3\lambda^3\gamma 2^{\nu-1}t_1^* \equiv -\delta_0 \equiv -2 \equiv 1 \bmod 3.$$

By (3.4) and since $\gcd(\lambda, 3\gamma) = 1$, we see that if l is any prime dividing λ, then

$$-\delta_0 + 3\lambda^3\gamma 2^{\nu-1}t_1^* \equiv -\delta_0 \equiv -\frac{1}{9\gamma^2} \not\equiv 0 \bmod l.$$

Therefore,

$$\gcd(3p^2\lambda^2, -\delta_0 + 3\lambda^3\gamma 2^{\nu-1}t_1^*) = 1. \tag{3.41}$$

By (3.39)–(3.41), we see that the polynomial Ψ defined by (3.38) has no fixed prime divisor. On the other hand, E_1, E_2, and Q_1^* have positive leading coefficients and are irreducible over $\mathbb{Q}$. Hence, Schinzel's hypothesis H expects that there should be infinitely many arbitrarily large positive integers μ_1 such that E_1, E_2, and Q_1^* are simultaneously primes. Take such a positive integer μ_1 and define μ by (3.35). We see that the choice of μ here is compatible with that of μ in Step 4 in the proof of Lemma 3.1. More precisely, in Step 4 in the proof of Lemma 3.1, we chose μ so that $\mu = 3p\mu_1$ and $Q_1^* = 3pP_2^*\mu_1 + R_2^*$ is an odd prime for some integer μ_1, and it is not difficult to realize that the choice of μ here satisfies these conditions. Repeating the same arguments as in Steps 5–9 in the proof of Lemma 3.1, we deduce that the septuple (A, B, C, D, E, F, G) satisfies (A1) and (A3)–(A7) with respect to the couple (p, n). It remains to prove that (A, B, C, D, E, F, G) satisfies (A2) with respect to the couple (p, n).

By (3.34), (3.36), and (3.37),

$$E = -4F_0^3E_1E_2.$$

Let l be any odd prime such that $\gcd(l, 3) = \gcd(l, p) = 1$ and l divides E. Then either l divides F_0, or $\gcd(l, F_0) = 1$ and l divides E_1E_2. If l divides F_0, then it follows from (F1) and (F2) in Step 3 in the proof of Lemma 3.1 that p is a square in $\mathbb{Q}_l^\times$. If l does not divide F_0 and l divides E_1E_2, then, since E_1, E_2 are odd primes, it follows that

$$v_l(E) = v_l(-4F_0^3E_1E_2) = v_l(E_1E_2) \le 2.$$

Thus,

$$v_l(E) - v_l(G) \le 2 + 0 = 2 < 6n.$$

Thus, (A, B, C, D, E, F, G) satisfies (A2) with respect to the couple (p, n). Since (A, B, C, D, E, F, G) is defined by (3.1), it follows that (A, B, C, D, E, F, G) belongs to $\mathfrak{C}_p$ and satisfies GMC with respect to the couple (p, n). Hence, our contention follows. □

Acknowledgement

I would like to thank the referee for useful comments and pointing out some typos in an earlier version of this paper.

https://doi.org/10.1017/S1446788715000348 Published online by Cambridge University Press

References

[1] M. Bhargava, 'Most hyperelliptic curves over $\mathbb{Q}$ have no rational points', Preprint, 2013. Available at http://arxiv.org/pdf/1308.0395.pdf.
[2] H. Cohen, *Number Theory, Vol. I: Tools and Diophantine Equations*, Graduate Texts in Mathematics, 239 (Springer, New York, 2007).
[3] J. Jahnel, *Brauer Groups, Tamagawa Measures, and Rational Points on Algebraic Varieties*, Mathematical Surveys and Monographs, 198 (American Mathematical Society, Providence, RI, 2014).
[4] B. Poonen, 'Rational points on varieties', 2008. Available at http://www-math.mit.edu/~poonen/papers/Qpoints.pdf.
[5] V. Scharasckin, 'Local–global problems and the Brauer–Manin obstruction', PhD Thesis, University of Michigan, 1999.
[6] A. Schinzel, 'Remarks on the paper 'Sur certaines hypothèses concernant les nombres premiers'', *Acta Arith.* **7** (1961–1962), 1–8.
[7] A. Schinzel and W. Sierpiński, 'Sur certaines hypothèses concernant les nombres premiers', *Acta Arith.* **4** (1958), 185–208; corrigendum *Acta Arith.* **5** (1958), 259.
[8] A. N. Skorobogatov, *Torsors and Rational Points*, Cambridge Tracts in Mathematics, 144 (Cambridge University Press, Cambridge, 2001).

NGUYEN NGOC DONG QUAN, Department of Mathematics,
The University of Texas at Austin,
Austin, TX 78712, USA
e-mail: dongquan.ngoc.nguyen@gmail.com

https://doi.org/10.1017/S1446788715000348 Published online by Cambridge University Press