TORSION SUBGROUPS OF ELLIPTIC CURVES
IN SHORT WEIERSTRASS FORM

MICHAEL A. BENNETT AND PATRICK INGRAM

ABSTRACT. In a recent paper by M. Wieczorek, a claim is made regarding the possible rational torsion subgroups of elliptic curves $E/\mathbb{Q}$ in short Weierstrass form, subject to certain inequalities for their coefficients. We provide a series of counterexamples to this claim and explore a number of related results. In particular, we show that, for any $\varepsilon > 0$, all but finitely many curves

$$E_{A,B} \; : \; y^2 = x^3 + Ax + B,$$

where A and B are integers satisfying $A > |B|^{1+\varepsilon} > 0$, have rational torsion subgroups of order either one or three. If we modify our demands upon the coefficients to $|A| > |B|^{2+\varepsilon} > 0$, then the $E_{A,B}$ now have trivial rational torsion, with at most finitely many exceptions, at least under the assumption of the abc-conjecture of Masser and Oesterlé.

1. INTRODUCTION

In a recent paper of Wieczorek [9], the claim is made that any elliptic curve of the form

$$E_{A,B} \; : \; y^2 = x^3 + Ax + B,$$

where A and B are integers satisfying the inequality

$$(1) \qquad\qquad A \geqslant |B| > 0,$$

must have rational torsion subgroup isomorphic to either the trivial group, $\mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/9\mathbb{Z}$, with the final case conjectured impossible. Unfortunately, this is rather over-optimistic. Indeed, one can verify easily that

$$(2) \qquad y^2 = x^3 + 1213612539482606085x - 844976094618678570$$

is an elliptic curve satisfying inequality (1) but with a point of order five (for example, $(x, y) = (1884166899, 94739648709888)$), providing a counterexample to the claim. As we shall observe, there are, in all likelihood, infinitely many such counterexamples—the curve (2) provides the "smallest". The main difficulty is that the results of [9] rely heavily upon those of [2] (regarding which the authors feel they can scarcely improve upon the eloquent Math Review of Bremner, MR2001F : 11085). There are, however, variants of the claims of [9] which turn out to be true.

Our first result is

Theorem 1. *Let $\varepsilon > 0$. Then there exist at most finitely many integers A and B satisfying*

$$A > |B|^{1+\varepsilon} > 0$$

for which $E_{A,B}(\mathbb{Q})_{\mathrm{Tors}}$ is nontrivial and not isomorphic to $\mathbb{Z}/3\mathbb{Z}$.

The proof of this result depends, perhaps somewhat surprisingly, upon Roth's Theorem on rational approximation to algebraic numbers. With slightly stronger restrictions upon A and B, under an additional hypothesis, we may in fact rule out the existence of any rational torsion point on $E_{A,B}$ (at least with finitely many exceptions):

Theorem 2. *Let $\varepsilon > 0$ and suppose that the abc-conjecture of Masser and Oesterlé holds. Then there are only finitely many integers A and B satisfying*

$$(3) \qquad\qquad |A| > |B|^{2+\varepsilon} > 0$$

for which $E_{A,B}$ has nontrivial rational torsion.

Recall that the abc-conjecture asserts, if a, b and c are positive integers with $a + b = c$, that, given $\varepsilon > 0$, we have

$$c \ll_{\varepsilon} \prod_{p | abc} p^{1+\varepsilon}.$$

It is worth noting, before we proceed with our proofs, that these are not general facts about integer points on elliptic curves. If we set $B = 1$, $A = t^2 - 2$ for $t \geqslant 2$ integral, then $E_{A,B}(\mathbb{Q})$ always contains the point $(1, t)$, while $A > |B|^{\delta}$ for all positive δ.

The outline of this paper is as follows. In Section 1, we describe the basic structure of our argument and prove a more precise version of Theorem 1. In Section 2, we produce families of examples to demonstrate that our results are sharp and subsequently indicate a number of counterexamples to the claims of [9]. Section 3 is devoted to the proof of Theorem 2 and a corresponding result (Proposition 6) which guarantees that this theorem is essentially best possible. Finally, in Section 4, we address the problem of finding effective and unconditional versions of Theorems 1 and 2.

We will restrict A and B to nonzero integers, and only consider the group of $\mathbb{Q}$-rational points on any given curve. Our first result is trivial.

Lemma 1. *If A and B satisfy $A \geqslant |B| > 0$, then the curve $E_{A,B}$ has no rational point of order two.*

Proof. It is elementary to show that if the above curve has a rational point of order two, then $x^3 + Ax + B$ must have an integral root. But if $x \geqslant 1$ we have $-B \leqslant A \leqslant Ax$, whence $Ax + B \geqslant 0$, and so $x^3 + Ax + B \geqslant 1$. The case $x \leqslant -1$ is similar and, as $B \neq 0$, we obtain the desired result. $\square$

From this and work of Mazur [5], classifying possible rational torsion subgroups, it follows, if $E_{A,B}(\mathbb{Q})_{\mathrm{Tors}}$ is nontrivial, that

$$E_{A,B}(\mathbb{Q})_{\mathrm{Tors}} \cong \mathbb{Z}/3\mathbb{Z}, \ \mathbb{Z}/5\mathbb{Z}, \ \mathbb{Z}/7\mathbb{Z} \text{ or } \mathbb{Z}/9\mathbb{Z}.$$

Theorem 1 is thus an immediate consequence of the following

Proposition 3. *Let $\varepsilon > 0$. Then there are at most finitely many integers A and B for which*

(i) $|A| > |B|^{1+\varepsilon}$ *and $E_{A,B}$ has a rational point of order 5;*
(ii) $|A| > |B|^{4/5+\varepsilon}$ *and $E_{A,B}$ has a rational point of order 7;*
(iii) $|A| > |B|^{3/4+\varepsilon}$ *and $E_{A,B}$ has a rational point of order 9.*

Our proof of this proposition relies upon the well-known rational parametrizations for $X_1(N)$ with $N \in \{5, 7, 9\}$ (see e.g. Kubert [4]). Specifically, we use these to show that there is a finite collection of algebraic numbers $\theta_1, \ldots, \theta_k$ such that, given $\varepsilon > 0$, there exists an $\varepsilon' > 0$ for which a curve $E_{A,B}$, with (A, B) satisfying (i), (ii) or (iii) above, necessarily corresponds to a rational p/q with

$$\left| \theta_i - \frac{p}{q} \right| < \frac{1}{q^{2+\varepsilon'}},$$

for some $i \in \{1, \ldots, k\}$. By Roth's theorem [6], there can be only finitely many such p/q.

It is known (see e.g. [4]) that the set of elliptic curves with torsion group $\mathbb{Z}/N\mathbb{Z}$ may be written in Tate normal form as

$$y^2 + (1 - c)xy - by = x^3 - bx^2,$$

where $b = c = t$, in case $N = 5$, $b = t^3 - t^2$ and $c = t^2 - t$, in case $N = 7$, and $b = t^2(t-1)(t^2 - t + 1)$ and $c = t^2(t-1)$, if $N = 9$. Here, t is a nonzero rational. It is easy to show (see [7]) that the elliptic curves in short Weierstrass form, birational to $E_{A,B}$, are exactly those of the form E_{Aq^4, Bq^6}, with q a nonzero rational. If A and B are nonzero integers such that there is no prime l with $l^4 \mid A$ and $l^6 \mid B$, then every curve with integer coefficients, birational to $E_{A,B}$, is of the form E_{Ak^4, Bk^6} for some nonzero integer k. We call such an (A, B) a *minimal pair*. If a minimal pair (A, B) fails to satisfy $|A| > |B|^\delta$ (for $\delta > 2/3$), then so does (Ak^4, Bk^6) for any nonzero integer k, whereby any birationally equivalent curve with integer coefficients also fails. If, on the other hand, (A, B) does satisfy such an inequality, then there are only finitely many integers k for which the same is true of (Ak^4, Bk^6), and hence only finitely many birational images of the given elliptic curve (with integer coefficients) satisfy $|A| > |B|^\delta$. It therefore suffices to prove Proposition 3 for minimal pairs (A, B).

1.1. **Short Weierstrass form.** We begin by finding curves in short Weierstrass form, birational to the above Tate normal forms. It is a routine exercise to verify that an elliptic curve $E/\mathbb{Q}$ with a rational point of order N is birational to

$$E_{A,B} \; : \; y^2 = x^3 + A_N(t)x + B_N(t),$$

where $A_N(t) = -27A_N^*(t)$ and $B_N(t) = 54B_N^*(t)$, for

$$A_N^*(t) = \begin{cases} t^4 - 12t^3 + 14t^2 + 12t + 1, & \text{if } N = 5, \\[2mm] t^8 - 12t^7 + 42t^6 - 56t^5 + 35t^4 - 14t^2 + 4t + 1, & \text{if } N = 7, \\[2mm] \begin{aligned} &\left(t^3 - 3t^2 + 1\right)\left(t^9 - 9t^8 + 27t^7 - 48t^6\right. \\ &\quad \left. + 54t^5 - 45t^4 + 27t^3 - 9t^2 + 1\right), \end{aligned} & \text{if } N = 9, \end{cases}$$

and

$$B_N^*(t) = \begin{cases} (t^2+1)(t^4 - 18t^3 + 74t^2 + 18t + 1), & \text{if } N = 5, \\ \\ \begin{aligned} & t^{12} - 18t^{11} + 117t^{10} - 354t^9 + 570t^8 - 486t^7 \\ & +273t^6 - 222t^5 + 174t^4 - 46t^3 - 15t^2 + 6t + 1, \end{aligned} & \text{if } N = 7, \\ \\ \begin{aligned} & t^{18} - 18t^{17} + 135t^{16} - 570t^{15} + 1557t^{14} - 2970t^{13} \\ & +4128t^{12} - 4230t^{11} + 3240t^{10} - 2032t^9 + 1359t^8 \\ & -1080t^7 + 735t^6 - 306t^5 + 27t^4 + 42t^3 - 18t^2 + 1, \end{aligned} & \text{if } N = 9. \end{cases}$$

Here, t is a nonzero rational number. It is straightforward to check that the polynomials $B_N(t)$ have either 4 real roots (if $N = 5$) or 6 real roots (if $N = 7$ or 9). For future use, we will refer to these roots as $\theta_{N,i}$, where $1 \leqslant i \leqslant 4$ (if $N = 5$) or $1 \leqslant i \leqslant 6$ (otherwise), and where we always assume

$$\theta_{N,i} < \theta_{N,i+1}.$$

The following result characterizes minimal pairs (A, B) for elliptic curves $E_{A,B}$ with a rational N-torsion point, $N \in \{5, 7, 9\}$.

Lemma 2. *If $N \in \{5, 7, 9\}$, the minimal pair corresponding to*

$$(A_N(p/q), B_N(p/q)),$$

where p and q are coprime integers with $q > 0$, is either

$$\left(q^{2N-6} A_N(p/q), q^{3N-9} B_N(p/q)\right)$$

or

$$\left(3^{-4} q^{2N-6} A_N(p/q), 3^{-6} q^{3N-9} B_N(p/q)\right).$$

The latter case occurs precisely when $N \in \{7, 9\}$ and $p \equiv -q \mod 3$.

Proof. To find possible common factors of the two integers $q^{2N-6} A_N(p/q)$ and $q^{3N-9} B_N(p/q)$, we calculate the resultant of $A_N^*(t)$ and $B_N^*(t)$. These turn out to be

$$2^{12} \cdot 3^6 \cdot 5, \quad -2^{24} \cdot 3^{12} \cdot 7 \quad \text{and} \quad -2^{36} \cdot 3^{27},$$

for $N = 5, 7$ and 9, respectively, and so it follows that

$$(4) \qquad \gcd\left(q^{2N-6} A_N(p/q), q^{3N-9} B_N(p/q)\right)$$

is not divisible by l^4 for any prime $l > 3$. Further, if either p or q is even, then $q^{3N-9} B_N^*(p/q)$ is odd, while, if both p and q are odd,

$$q^6 B_5^*(p/q) \equiv (p^2 + q^2)((p^2 - pq - q^2)^2 + 3p^2 q^2) \equiv 8 \mod 16,$$

$$q^8 A_7^*(p/q) \equiv (p^4 + p^2 q^2 + q^4)^2 \equiv 1 \mod 2$$

and

$$q^{12} A_9^*(p/q) \equiv p^{12} + p^8 q^4 + q^{12} \equiv 1 \mod 2.$$

We may thus conclude that either 16 fails to divide $q^{2N-6} A_N(p/q)$ or 64 does not divide $q^{3N-9} B_N(p/q)$.

It remains, then, to consider the powers of 3 dividing the quantity (4). In case $N = 5$, we have

$$q^4 A_5^*(p/q) \equiv \left(p^2 + q^2\right)^2 \equiv 1 \mod 3$$

and so 3^4 fails to divide $q^4 A_5(p/q)$. If $N = 7$ or 9, then

$$q^{2N-6} A_N^*(p/q) \equiv (p+q)^2 \mod 3$$

and hence to have $3^4 \mid q^{2N-6} A_N(p/q)$, necessarily $p \equiv -q \mod 3$. Conversely, if $p \equiv -q \mod 3$, it follows that

$$q^{3N-9} B_N^*(p/q) \equiv 0 \mod 27$$

and thus $3^{-4} q^{2N-6} A_N(p/q)$ and $3^{-6} q^{3N-9} B_N(p/q)$ are integers. Assuming that $p \equiv -q \mod 3$, however, implies the congruences

$$q^8 A_7^*(p/q) \equiv 3q^8 \mod 9$$

and

$$q^{12} A_9^*(p/q) \equiv 9q^{12} \mod 27.$$

Since p and q are coprime and $p \equiv -q \mod 3$ (so that q is not a multiple of 3), we can thus never have $q^{2N-6} A_N(p/q)$ divisible by 3^8. This completes our proof. $\square$

Let us note at this stage, if $N \in \{5, 7, 9\}$ and A, B are integral such that the curve $E_{A,B}$ has a rational N-torsion point, then Lemma 2 ensures that B is necessarily even. In particular, this precludes the possibility that $B = \pm 1$. It follows that Theorem 1 implies the existence of a constant $\kappa > 0$ such that if $A > |B|^\kappa$, then either $E_{A,B}(\mathbb{Q})_{\text{Tors}}$ is trivial or

$$E_{A,B}(\mathbb{Q})_{\text{Tors}} \cong \mathbb{Z}/3\mathbb{Z}.$$

We will explore this further in Section 4.

1.2. Connections to Diophantine approximation. Given Lemma 2, we now show that a minimal pair (A, B) with $|A|$ suitably larger than $|B|$ necessarily corresponds to a good rational approximation to one of the roots of the polynomials $B_N(t)$. To be precise, we have:

Proposition 4. *Let ε be a nonnegative real number, $N \in \{5, 7, 9\}$ and set*

$$\varepsilon_N = \frac{(3N - 11)^2 \varepsilon}{2N - 6 + (3N - 11)\varepsilon}.$$

Further, define constants $C_{N,i}$ via

	i odd	i even
$C_{5,i}$	22.91	157.07
$C_{7,i}$	12.73	118.33
$C_{9,i}$	11.06	110.63

If A and B are nonzero integers for which $E_{A,B}$ has a rational point of order N, where

$$|A| > |B|^{\frac{2N-6}{3N-11}+\varepsilon},$$

then there exist integers k, p, q and i, with k and q nonzero, such that either

$$A = (k/3)^4 q^{2N-6} A_N(p/q), \ \ B = (k/3)^6 q^{3N-9} B_N(p/q),$$

in case $N \in \{7, 9\}$ and $p \equiv -q \mod 3$, or

$$A = k^4 q^{2N-6} A_N(p/q), \ \ B = k^6 q^{3N-9} B_N(p/q),$$

otherwise. Further, we have that either

$$A = 10992742853 \ \text{ and } \ B = -1657321950314$$

or

$$\left| \theta_{N,i} - \frac{p}{q} \right| < \frac{1}{C_{N,i}^* q^{2+\varepsilon_N}}.$$

Here,

$$C_{N,i}^* = \begin{cases} 3^{-1} \cdot C_{N,i} & \text{if } N = 7 \text{ and } p \equiv -q \mod 3, \\ 3^{-2/3} \cdot C_{N,i} & \text{if } N = 9 \text{ and } p \equiv -q \mod 3, \\ C_{N,i} & \text{otherwise.} \end{cases}$$

Proof. We begin by considering the case $N = 5$. From our prior remarks, it suffices to treat minimal pairs (A, B). In this situation, the assumption that

$$\left| q^4 A_5(p/q) \right| > \left| q^6 B_5(p/q) \right|^{1+\varepsilon}$$

implies the inequality

$$(5) \qquad |B_5(p/q)| < |A_5(p/q)|^{\frac{1}{1+\varepsilon}} \cdot q^{-2-\varepsilon_5}.$$

In particular, for any $\varepsilon \geqslant 0$, we have

$$(6) \qquad |B_5(p/q)| < \max\left\{1, |A_5(p/q)|\right\} \cdot q^{-2}.$$

For fixed q, since the degree of the polynomial $A_5(t)$ is less than that of $B_5(t)$, there are at most finitely many integers p for which p/q satisfies (6). We easily compute, via Maple VII, that there are, in fact, no such p/q with $1 \leqslant q \leqslant 1000$. We may thus assume that $q > 1000$, whereby, from (6),

$$|B_5(p/q)| < 10^{-6} \max\left\{1, |A_5(p/q)|\right\}.$$

This inequality implies, after a short calculation, that

$$(7) \qquad \left| \theta_{5,i} - \frac{p}{q} \right| < 5 \times 10^{-8}$$

for one of $i \in \{1, 2, 3, 4\}$.

Next note that, via the Mean Value Theorem,

$$|B_5(p/q)| = \left| \theta_{5,i} - \frac{p}{q} \right| \cdot |B_5'(\zeta)|$$

for some ζ between $\theta_{5,i}$ and p/q. From (5) and the fact that $|A_5(p/q)| > 1$ on the intervals defined by (7), we thus have

$$(8) \qquad \left| \theta_{5,i} - \frac{p}{q} \right| < |A_5(p/q)| \cdot |B_5'(\zeta)|^{-1} \cdot q^{-2-\varepsilon_5}.$$

From (7), it is an exercise in calculus to verify that, for ζ between p/q and $\theta_{5,i}$, we have

$$|B_5'(\zeta)| > \begin{cases} 251.720151, & \text{if } i = 1, \\ 245.275862, & \text{if } i = 2, \\ 573453.818, & \text{if } i = 3, \\ 4033780.05, & \text{if } i = 4. \end{cases}$$

Similarly,

$$|A_5(p/q)| < \begin{cases} 10.98357, & \text{if } i = 1, \\ 1.561466, & \text{if } i = 2, \\ 25022.03, & \text{if } i = 3, \\ 25679.46, & \text{if } i = 4. \end{cases}$$

From (8), then, it follows that

$$(9) \qquad \left| \theta_{5,i} - \frac{p}{q} \right| < \frac{1}{C_{5,i} \, q^{2+\varepsilon_5}},$$

as claimed.

If $N \in \{7, 9\}$, we argue similarly, with a few minor complications. Here the analogues of inequality (5) are

$$|B_7(p/q)| < 3^\delta \cdot |A_7(p/q)|^{5/4} \cdot \left(3^\delta \cdot |A_7(p/q)|^{-1/4}\right)^{\frac{25\varepsilon}{4+5\varepsilon}} \cdot q^{-2-\varepsilon_7}$$

and

$$|B_9(p/q)| < 3^{2\delta/3} \cdot |A_9(p/q)|^{4/3} \cdot \left(3^\delta \cdot |A_9(p/q)|^{-1/4}\right)^{\frac{64\varepsilon}{9+12\varepsilon}} \cdot q^{-2-\varepsilon_9}.$$

In each case, we have $\delta = 1$ if $p \equiv -q \mod 3$ and $\delta = 0$ otherwise. Again, we first search for nonzero p/q satisfying one of these inequalities with $1 \leqslant q \leqslant 1000$. We find such rationals only if $N = 7$ and

$$p/q \in \{28/5, -5/23, 23/28\}.$$

Each of these three values leads to

$$A = 10992742853, \quad B = -1657321950314.$$

Otherwise, we may assume that $q > 1000$, $|A_N(p/q)| > 81$ and so

$$|B_N(p/q)| < 3^{\frac{(N-5)\delta}{2N-12}} \cdot |A_N(p/q)|^{\frac{3N-11}{2N-6}} \cdot q^{-2} < 3 \cdot 10^{-6} \cdot |A_N(p/q)|^{\frac{3N-11}{2N-6}}.$$

After some computation, we find, in each case, that

$$\left|\theta_{N,i} - \frac{p}{q}\right| < 3 \times 10^{-7}$$

for some $1 \leqslant i \leqslant 6$ and that

$$\left|\theta_{N,i} - \frac{p}{q}\right| < 3^{\frac{(N-5)\delta}{2N-12}} \cdot |A_N(p/q)|^{\frac{3N-11}{2N-6}} \cdot |B_N'(\zeta)|^{-1} \cdot q^{-2-\varepsilon_N}.$$

Arguing as previously leads to the desired result. $\qquad\square$

Let us note that

$$|B_5'(\theta_{5,i})| \cdot |A_5(\theta_{5,i})|^{-1} = \begin{cases} 22.91796\ldots & \text{if } i \in \{1,3\}, \\ 157.0820\ldots & \text{if } i \in \{2,4\}, \end{cases}$$

$$|B_7'(\theta_{7,i})| \cdot |A_7(\theta_{7,i})|^{-5/4} = \begin{cases} 12.73690\ldots & \text{if } i \in \{1,3,5\}, \\ 118.3370\ldots & \text{if } i \in \{2,4,6\} \end{cases}$$

and

$$|B_9'(\theta_{9,i})| \cdot |A_9(\theta_{9,i})|^{-4/3} = \begin{cases} 11.06719\ldots & \text{if } i \in \{1,3,5\}, \\ 110.6379\ldots & \text{if } i \in \{2,4,6\}. \end{cases}$$

These represent, therefore, optimal values for $C_{N,i}$ which we may approach with additional computation.

2. EXAMPLES AND COUNTEREXAMPLES

To find examples of curves $E_{A,B}$ with a rational 5-, 7- or 9-torsion point and $|A|$ suitably large relative to $|B|$, we appeal to the following, a straightforward consequence of Proposition 4.

Proposition 5. *Let $N \in \{5, 7, 9\}$. If A and B are integers such that $E_{A,B}$ has rational N-torsion and*

$$|A| > |B|^{\frac{2N-6}{3N-11}}, \tag{10}$$

then, in the sense of Proposition 4, the pair (A, B) corresponds to a rational number p/q such that $p/q = p_j/q_j$ is the jth convergent in the continued fraction expansion to $\theta_{N,i}$ for some i. If we write $\theta = \theta_{N,i}$ and denote the partial quotients of θ by

$$\theta = [a_0, a_1, a_2, \ldots],$$

then, necessarily,

$$a_{j+1} \geqslant [C^*_{N,i}] - 1.$$

Conversely, if

$$a_{j+1} \geqslant [C^*_{N,i}] + 1,$$

for the corresponding convergent p_j/q_j, define

$$A = 3^{-4\delta} q_j^{2N-6} A_N(p_j/q_j), \quad B = 3^{-6\delta} q_j^{3N-9} B_N(p_j/q_j),$$

where $\delta = 1$, if $N \in \{7, 9\}$ and $p_j \equiv -q_j \mod 3$, and $\delta = 0$, otherwise. Then we have both (10) and

$$E_{A,B}(\mathbb{Q})_{\mathrm{Tors}} \cong \mathbb{Z}/N\mathbb{Z}.$$

Proof. If A and B are integers for which $E_{A,B}$ has a rational N-torsion point ($N \in \{5, 7, 9\}$) and satisfies (10), then applying Proposition 4 with $\varepsilon = 0$, there exist integers p, q and i ($q \neq 0$) for which

$$\left| \theta_{N,i} - \frac{p}{q} \right| < \frac{1}{C^*_{N,i} q^2}.$$

Since $C^*_{N,i} > 2$ in all cases, we conclude that $p/q = p_j/q_j$, the jth convergent in the simple continued fraction expansion to $\theta_{N,i}$, for some j. From the well-known inequalities

$$\frac{1}{(a_{j+1} + 2)q_j^2} < \left| \theta_{N,i} - \frac{p_j}{q_j} \right| < \frac{1}{a_{j+1} q_j^2} \tag{11}$$

(see e.g. Khinchin [3]; here a_{j+1} is the $(j+1)$st partial quotient in the simple continued fraction expansion to $\theta_{N,i}$), it follows that $C^*_{N,i} < a_{j+1} + 2$ and so $[C^*_{N,i}] \leqslant a_{j+1} + 1$.

If, on the other hand, p_j/q_j is a convergent to one of the $\theta_{N,i}$, with corresponding partial quotient $a_{j+1} \geqslant [C^*_{N,i}] + 1$, then, from (11),

$$\left| \theta_{N,i} - \frac{p_j}{q_j} \right| < \frac{1}{\left([C^*_{N,i}] + 1 \right) q_j^2}.$$

A short calculation ensures that either $q_j > 1000$ or, as previously, $N = 7$,

$$p_j/q_j \in \{28/5, -5/23, 23/28\}$$

and

$$A = 10992742853, \quad B = -1657321950314$$

(so that $E_{A,B}(\mathbb{Q})_{\mathrm{Tors}} \cong \mathbb{Z}/7\mathbb{Z}$). We may thus assume that $q_j > 1000$ and so, using the fact that $[C^*_{N,i}] + 1 \geqslant C^*_{N,i} + 0.09$ and tracing our way back through the proof

of Proposition 4, we find that

$$\left|3^{-4\delta}q^{2N-6}A_N(p_j/q_j)\right| > \left|3^{-6\delta}q^{3N-9}B_N(p_j/q_j)\right|^{\frac{2N-6}{3N-11}}$$

as desired. □

Computing the continued fraction expansions of $\theta_{5,i}$, we find that

$$\theta_{5,1} = [-1, 1, 5, \alpha_5], \quad \theta_{5,2} = [-1, 1, 10, \beta_5], \quad \theta_{5,3} = [6, \alpha_5] \quad \text{and} \quad \theta_{5,4} = [11, \beta_5],$$

where

$$\alpha_5 = [1, 9, 1, 19, 12, 32, 1, 5, 1090, 10, \ldots] \quad \text{and} \quad \beta_5 = [3, 12, 14, 1, 8, 1, 8, 4, 4, 1, 6, \ldots].$$

Note that

$$\theta_{5,1} \cdot \theta_{5,3} = \theta_{5,2} \cdot \theta_{5,4} = -1.$$

From Proposition 5, it follows that counterexamples to the main theorem of [9], i.e. curves $E_{A,B}$ with $A > |B| > 0$ and $E_{A,B}(\mathbb{Q})_{\text{Tors}} \cong \mathbb{Z}/5\mathbb{Z}$, correspond to partial quotients a_i to α_5 with $a_i = 21$ or 22 (possibly) or $a_i \geq 23$ (definitely). The first two such counterexamples are the curve (2) and that given by

$$y^2 = x^3 + 1846418414860182412922978853\, x + 38812921993228946179376502.$$

We expect, of course, that $a_i \geqslant 23$ infinitely often. Computations in this case agree with the well-known general heuristics, which indicate that roughly 6% of the a_i should be at least this large.

Similarly, examples of pairs (A, B) with $-A > |B| > 0$ and $E_{A,B}(\mathbb{Q})_{\text{Tors}} \cong \mathbb{Z}/5\mathbb{Z}$ correspond to convergents to β_5 with suitably large partial quotients (the first such yields a curve with coefficients in excess of 250 decimal digits). For $N \in \{7, 9\}$, we have

$$\theta_{7,1} = [-1, 1, 3, \alpha_7], \; \theta_{7,3} = [0, 1, 4, \alpha_7], \; \theta_{7,5} = [5, \alpha_7],$$
$$\theta_{7,2} = [-1, 1, 5, \beta_7], \; \theta_{7,4} = [0, 1, 6, \beta_7], \; \theta_{7,6} = [7, \beta_7],$$

where

$$\alpha_7 = [1, 1, 2, 8, 1, 2, 1, 2, 1, 1, 1, 27, \ldots] \text{ and } \beta_7 = [2, 1, 1, 1, 1, 15, 1, 1, 1, 4, 2, 2, 53, \ldots],$$

and

$$\theta_{9,1} = [-1, 1, 2, \alpha_9], \; \theta_{9,3} = [0, 1, 3, \alpha_9], \; \theta_{9,5} = [4, \alpha_9],$$
$$\theta_{9,2} = [-1, 1, 3, \beta_9], \; \theta_{9,4} = [0, 1, 4, \beta_9], \; \theta_{9,6} = [5, \beta_9],$$

where

$$\alpha_9 = [2, 10, 1, 2, 7, 5, 1, 1, 6, 2, 56, \ldots] \quad \text{and} \quad \beta_9 = [2, 5, 2, 14, 1, 4, 1, 1, 1, 2, 1, 6, \ldots].$$

Here, in both cases,

$$\theta_{N,1} \cdot \theta_{N,3} \cdot \theta_{N,5} = \theta_{N,2} \cdot \theta_{N,4} \cdot \theta_{N,6} = -1.$$

Thus to obtain curves $E_{A,B}$ with a rational point of order seven which satisfy $|A| > |B|^{4/5}$ or one of order nine, with $|A| > |B|^{3/4}$, we merely need search the continued fraction expansions to α_7, β_7, α_9 and β_9 for "large" partial quotients. The curve of lowest height satisfying either of these inequalities is one we encountered during the proof of Proposition 4, namely

$$y^2 = x^3 + 10992742853x - 1657321950314.$$

The next smallest example has a value of A with 65 decimal digits!

3. Proof of Theorem 2

We will now proceed with the proof of Theorem 2. From Proposition 3, it suffices to consider curves with a rational 2-torsion or 3-torsion point, for which the pair (A, B) satisfies (3) with A and B suitably large. In the case where $E_{A,B}$ has a rational point of order two, it follows that $x^3 + Ax + B$ has a linear factor in $\mathbb{Z}[x]$ and hence there exist integers α and β such that $A = \beta - \alpha^2$ and $B = -\alpha\beta$. Since we assume $B \neq 0$, we have

$$\frac{|A|}{B^2} = \frac{|\beta - \alpha^2|}{\alpha^2 \beta^2} \leqslant \frac{|\beta| + |\alpha|^2}{\alpha^2 \beta^2} \leqslant 1$$

unless $\beta = \pm 1$. If $\beta = 1$, then $A = 1 - \alpha^2$ and $B = -\alpha$, in which case $|A| < B^2$ (or $B = 0$). If, however, $\beta = -1$, we obtain a family of curves given by $A = -(1 + \alpha^2)$ and $B = \alpha$, for α integral. In any case,

$$\limsup_{|B| \to \infty} |A|/B^2 \leqslant 1$$

and so, given $\varepsilon > 0$, with at most finitely many exceptions, we contradict inequality (3).

Suppose next that $E_{A,B}$ has a rational point (x, y) of order three (so that, via the theorem of Nagell-Lutz (see e.g. [7]), x and y are integers). Using the duplication formula for points on $E_{A,B}$, we see that both

$$\left(\frac{3x^2 + A}{2y}\right)^2 = 3x \ \text{ and } \ 3x^4 + 6Ax^2 + 12Bx = A^2.$$

The first of these equations implies $x = 3s^2$ for some positive integer s, while the second gives that A is divisible by 3, say $A = 3A_0$, and that $x^3 + 6A_0 x + 4B = t^2$, where $A_0 = st$. Solving the quadratic in t, we have

$$t = 9s^3 \pm 2\sqrt{27s^6 + B},$$

whereby $27s^6 + B$ is a perfect square. Let $\theta = B/s^6$. If $|\theta| \geqslant 1$, then

$$|A| \cdot |B|^{-2/3} = |27 \pm 6\sqrt{27 + \theta}| \cdot |\theta|^{-2/3} \leqslant 27 + 6\sqrt{28},$$

and so

$$|A| \leqslant \left(27 + 6\sqrt{28}\right) |B|^{2/3}.$$

Now suppose that $|\theta| < 1$ and let

$$M^2 = 27s^6 + B = s^6(27 + \theta)$$

(so that $|M| < 2\sqrt{7}\, s^3$). Given $\varepsilon > 0$, let $\varepsilon_1 = \varepsilon/(2\varepsilon + 12)$. Then, applying the abc-conjecture to the equation $M^2 - B = 27s^6$, we have

$$s^6 \ll (s|BM|)^{1+\varepsilon_1} \ll \left(s^4|B|\right)^{1+\varepsilon_1},$$

where the implicit constants depend only upon ε. It follows that

$$|B| \gg s^{4/(2+\varepsilon/2)}$$

and so, since $|A| \ll s^4$, we have $|A| \ll |B|^{2+\varepsilon/2}$. For sufficiently large $|B|$, this contradicts (3), completing the proof of Theorem 2.

One may construct examples to demonstrate that the exponent 2 above cannot be reduced:

Proposition 6. *There exist infinitely many pairs of integers (A, B) for which both*

$$A > B^2 > 0$$

and

$$E_{A,B}(\mathbb{Q})_{\mathrm{Tors}} \cong \mathbb{Z}/3\mathbb{Z}.$$

Proof. Let s and u be positive integral solutions to the Pell equation $4u^2 - 3s^2 = 1$, and set

$$B = 1 - 3u^2, \quad A = 27s^4 + 6s(8u^3 - 3u).$$

One easily checks that $E_{A,B}$ has a rational point of order three (with x-coordinate $3s^2$). On the other hand,

$$\lim_{u,s \to \infty} \frac{A}{B^2} = \frac{48 + 32\sqrt{3}}{9} = 11.49173 \ldots.$$

$\square$

Whether or not this value corresponds to the $\limsup |A|/B^2$ (where this is taken over nonzero integers A, B for which $E_{A,B}(\mathbb{Q})_{\mathrm{Tors}} \cong \mathbb{Z}/3\mathbb{Z}$) is an open question.

4. EFFECTIVE, UNCONDITIONAL RESULTS

In this section, we will concentrate on effective results along the lines of Theorem 1 (i.e. ones which do not rely upon Roth's theorem) and on an unconditional version of Theorem 2. To deduce these, we will need to assume much more restrictive bounds upon A, relative to $|B|$. In the case of rational 5-torsion, the fact that $B_5(t)$ is a reducible polynomial leads to a reasonably clean result:

Proposition 7. *If A and B are integers, there are no elliptic curves $E_{A,B}$ with a rational point of order five satisfying*

$$|A| \geqslant B^2 > 0.$$

Proof. With $A_5(t), B_5(t)$ defined as previously, write $B_5(t) = 54(t^2 + 1)f(t)$. Then, from Proposition 4 with $\varepsilon = 1$, if p/q corresponds to a curve $E_{A,B}$ with rational five torsion and $|A| \geqslant B^2 > 0$, we have

$$(12) \qquad \left| \theta_{5,i} - \frac{p}{q} \right| < \frac{1}{C_{5,i}\, q^4}$$

for one of $i \in \{1, 2, 3, 4\}$. On the other hand, since each $\theta_{5,i}$ is a root of $f(t)$, we may apply the Mean Value Theorem (in this context, Liouville's Theorem) to conclude that

$$(13) \qquad \left| \theta_{5,i} - \frac{p}{q} \right| = \left| \frac{f(p/q)}{f'(\xi)} \right|$$

for some ξ between $\theta_{5,i}$ and p/q. Consideration of the continued fraction expansions of the $\theta_{5,i}$ shows that inequality (12) has no solutions with $1 \leqslant q \leqslant 10^6$, say, and hence we necessarily have

$$|f'(\xi)| < \begin{cases} 4.6, & \text{if } i = 1, \\ 4.6, & \text{if } i = 2, \\ 218, & \text{if } i = 3, \\ 578, & \text{if } i = 4. \end{cases}$$

From this, (12) and (13), it follows that

$$|q^4 f(p/q)| = |p^4 - 18p^3 q + 74p^2 q^2 + 18pq^3 + q^4| \leqslant 9.$$

It is nowadays a relatively routine matter to solve such a Thue inequality for p and q, via, e.g., Pari. We find that necessarily either $p = 0$ or $q = 0$, contradicting the fact that p/q is a nonzero rational. $\square$

For $N \in \{7, 9\}$, the polynomial $B_N^*(t)$ is irreducible. As a result, we cannot obtain an analogous result to Proposition 7 from a straightforward application of Liouville's theorem. In each case, however, we may apply effective improvements upon Liouville's theorem (of Baker-Fel'dman type), say those of Bugeaud and Győry [1], to conclude, if

$$|A| > B^{10^{390}},$$

that $E_{A,B}(\mathbb{Q})$ may contain a rational point of order seven or nine, only if $E_{A,B}$ corresponds to a parameter p/q with $q < e^{10^{15}}$. We suppress the details.

Returning for a last time to the claims of [9], it is worth noting that, although the condition $A \geqslant |B| > 0$ does not prevent $E_{A,B}(\mathbb{Q})$ from containing a point of order five, it probably rules out the possibility of rational points of order seven or nine (and hence the conjecture in [9] is likely true). To prove this, we would require a strong effective improvement on Liouville's Theorem for $\theta_{9,1}$, of the form

$$\left| \theta_{9,1} - \frac{p}{q} \right| > \frac{c}{q^6},$$

where c is a suitable absolute positive constant. This seems to be out of reach of current methods in Diophantine approximation.

If, instead of Theorem 2, we desire an unconditional criterion to guarantee trivial rational torsion, we may derive the following:

Proposition 8. *Let $\varepsilon > 0$ be given. Then there exists a constant c_ε such that if A and B are nonzero integers for which the curve $E_{A,B}$ has a nontrivial rational torsion point, then*

$$\log |A| < c_\varepsilon |B|^{1+\varepsilon}.$$

Proof. By our preceding results, we may assume that $E_{A,B}$ has a rational point of order 3. Let s and M be as earlier in this section, so that

$$M^2 = (s^2)^3 + B.$$

By a theorem of Stark [8], we have

$$(14) \qquad\qquad \log \max(|M|, s^2) \ll |B|^{1+\varepsilon},$$

where the implied constant depends only on ε. Recalling that $A = 27s^4 + 6sM$, if $s^2 \leqslant |M|$, then $|A| \leqslant 33M^2$. Similarly, if $|M| \leqslant s^2$, then $|A| \leqslant 33s^4$. In either case, there is an absolute constant κ such that

$$\log |A| < \kappa \log \max(|M|, s^2),$$

whence the desired inequality is obtained from (14). $\square$

5. Concluding remarks

Theorem 2 and (admittedly rather naive) computation lead us to close our paper by asking the following:

Question. *Are the only curves $E_{A,B}$ with a nontrivial rational torsion point for which*

$$|A| > |B|^{5/2} > 0,$$

where A and B are integers, those with

$$(A, B) = (-2, \pm 1), (57, -2), (381699, 37) \text{ and } (4156357129881, 93886)?$$

One finds the last three of these pairs by searching for integer values of s for which the quantity $3\sqrt{3}\,s^3$ is close to an integer (at least, relative to s). Here, as previously, $A = 3st$, $t = 9s^3 \pm 2\sqrt{27s^6 + B}$, and hence the condition that $3\sqrt{3}\,s^3$ is well approximated by an integer enables us to find "reasonably small" B.

References

[1] Y. Bugeaud and K. Győry, Bounds for the solutions of Thue-Mahler equations and norm form equations, *Acta Arith.* 74 (1996), 273–292. MR1373714 (97b:11046)

[2] A. Dąbrowski and M. Wieczorek, Families of elliptic curves with trivial Mordell-Weil group, *Bull. Austral. Math. Soc.* 62 (2000), 303–306. MR1786212 (2001f:11085)

[3] A.Y. Khinchin, Continued Fractions, Dover Publications, New York, 1964. MR1451873 (98c:11008)

[4] D. Kubert, Universal bounds on the torsion of elliptic curves, *Proc. London Math. Soc.* 33 (1976), 193–237. MR0434947 (55:7910)

[5] B. Mazur, Modular curves and the Eisenstein ideal, *Inst. Hautes Études Sci. Publ. Math.* 47 (1977), 33–186. MR0488287 (80c:14015)

[6] K. Roth, Rational approximations to algebraic numbers, *Mathematika* 2 (1955), 1–20. MR0072182 (17:242d)

[7] J. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics 106, Springer-Verlag, New York 1986. MR0817210 (87g:11070)

[8] H. Stark, Effective estimates of solutions of some Diophantine equations, *Acta Arith.* 24 (1973), 251–259. MR0340175 (49:4931)

[9] M. Wieczorek, Torsion points on certain families of elliptic curves, *Canad. Math. Bull.* 46 (2003), 157–160. MR1955623 (2004b:11081)

Department of Mathematics, University of British Columbia, Vancouver, British Columbia, Canada V6T 1Z4

Department of Mathematics, University of British Columbia, Vancouver, British Columbia, Canada V6T 1Z4