# Contributions to the arithmetic of elliptic curves

by

Patrick M. Ingram

B.Sc., Simon Fraser University, 1999
M.Sc., The University of British Columbia, 2002

A THESIS SUBMITTED IN PARTIAL FULFILMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

Doctor of Philosophy

in

The Faculty of Graduate Studies

(Mathematics)

The University Of British Columbia

April 2006

# Abstract

We present various published and unpublished results on elliptic curves. In particular, we focus on the torsion structures of elliptic curves, and how this is influenced by the relative sizes of the coefficients. We see in the final chapter that these results are special cases of a more general result on approximating rational numbers by $j$-invariants of elliptic curves with certain structures. Various other results regarding the divisibility properties (and consequently integrality) of rational points on elliptic curves are also discussed.

# Contents

# Preface

This thesis follows the 'manuscript style' in the terminology of the Faculty of Graduate Studies at UBC. That is to say, it is primarily a compilation of works that have been accepted for publication by, or at least submitted for publication to, academic journals. This differs from a more traditional thesis in at least two ways. First of all, the reader might notice a slight lack of cohesion in the thesis as a whole. None of the chapters, save the first and last, were meant to appear in the current format, and so no effort has been made to tie them together other than here. The author has resisted the temptation to provide more natural segues in the interests of presenting the material exactly as published. Secondly, as per the style in most academic journals, the text is short on exposition. Given the wealth of good expositions on much of the background material, I have maintained this terseness in the introduction.

In the first chapter we provide a brief overview of the mathematics used in the various papers. It is by no means our goal to provide here anything more than a listing of prerequisite knowledge. References containing more background information are given.

In Chapter 2, the author and Michael Bennett explore the claims of [5], which turn out to be false. In constructing our counterexamples, we found that the claims of [5], while based on deeply flawed arguments, represent a remarkably good approximation of the truth. In particular, we demonstrate that, for any $\varepsilon > 0$, there are at most finitely many pairs of integers $A$ and $B$ satisfying $|A| > |B|^{2+\varepsilon} > 0$ such that the elliptic curve

$$E : y^2 = x^3 + Ax + B$$

has a $\mathbb{Q}$-rational point of finite order not dividing 3. In Chapter 3 the author continues in this vein to consider the restrictions imposed on the torsion in $E(\mathbb{Q})$ by inequalities of the form $|B| > |A|^{\kappa}$ for various $\kappa$, leading to similar results. As noted in Chapter 6, Chapter 2 (respectively Chapter 3) essentially asks the question "If $E/\mathbb{Q}$ is an elliptic curve with $E(\mathbb{Q})_{\text{Tors}}$ of a

certain form, how well can $j(E)$ approximate 0?" (respectively "...1728?"). In the concluding remarks, we briefly take up the problem of approximating an arbitrary rational number by the $j$-invariants of elliptic curves with various torsion structures (the subject of upcoming joint work with Joseph Silverman).

In Chapter 4 we examine another problem in the interface between diophantine approximation and the arithmetic of elliptic curves. In particular, we tackle the problem of primitive divisors in elliptic divisibility sequences. In a paper of Everest, Mclaren, and Ward [3] some partial bounds are obtained on the index of the last term in an elliptic divisibility sequence to fail to have a primitive divisor. In our work we lower these bounds, in the cases in which they apply, and give examples to demonstrate that they cannot, in general, be lowered further. It is interesting to note that Silverman [4] has obtained uniform bounds in these cases for the *number* of terms in such a sequence that fail to have a primitive divisor.

Finally, in Chapter 5 we provide an example of how transcendence may be used more directly to study elliptic curves. Using methods of David [2] we find all integral points on a given elliptic curve. Note that this problem is not unrelated to the material in Chapter 4. Certainly, the terms in an elliptic divisibility sequences corresponding to multiples of the base point which have integral co-ordinates can have no primitive divisors (as denominators of integers have, in general, no prime divisors whatsoever). Tangentially, we prove that a certain family of Diophantine equations each admit only finitely many solutions.

As mentioned above, Chapters 2 through 5 have been published or submitted for publication. Chapter 2, co-authored with Michael Bennett, has appeared in the Transactions of the American Mathematical Society [1]. Chapter 3 will appear in a forthcoming volume of the Proceedings of the London Mathematical Society, and Chapter 5 in the Comptes rendus mathématiques de l'Académie des sciences. Chapter 4 has been submitted to the Journal of Number Theory, and the material in the concluding remarks is currently being refined for eventual publication. All published works are reprinted with permission of the publishers.

# Bibliography

[1] M. A. Bennett and P. Ingram. Torsion subgroups of elliptic curves in short Weierstrass form. *Trans. Amer. Math. Soc.*, 357(8):3325–3337, 2005.

[2] S. David. Minorations de formes linéaires de logarithmes elliptiques. *Mém. Soc. Math. France (N.S.)*, 62, 1995.

[3] G. Everest, G. Mclaren, and T. Ward. Primitive divisors of elliptic divisibility sequences (preprint), 2005.

[4] J. Silverman (unpublished work)

[5] M. Wieczorek. Torsion points on certain families of elliptic curves. *Canad. Math. Bull.*, 46(1):157-160, 2003.

# Acknowledgements

The list of names of those who have contributed positively, in some way or other, to my time as a doctoral student is far too long to reproduce, and so I will highlight only the five without whom I might not have gotten to this point. First and foremost, without the academic and financial support of my supervisor Michael Bennett it is unclear that any of this would have been even remotely possible. Similarly, Nike Vatsal has provided funding and clear answers to questions about algebraic number theory on numerous occasions. It is also quite clear that, without the tireless efforts of the department's graduate secretaries, Lee Yupitan and Marija Zimonja, I would have been consumed by the university's daedalian bureaucratic quagmire a dozen times over. Finally I would like to thank Elissa Ross, whose emotional support during the writing of this thesis was invaluable.

# Chapter 1

# Introduction

We provide here most of the necessary background for the results presented in the various chapters. Those chapters, all of which have appeared or are intended to appear in academic journals, are appropriately terse. In keeping with this, the introductory chapter will reproduce no proofs of well-known results. Results on elliptic curves can be found in [17], while results on diophantine approximation are, unless otherwise noted, in [15] or [16].

## 1.1 Elliptic curves

An elliptic curve $E$ over a field $K$ is a genus one algebraic curve defined over $K$ with a $K$-rational point. Such a curve may always be written in Weierstrass form,

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with $a_i \in K$. When the characteristic of $K$ is not 2 or 3 (indeed, we restrict ourselves throughout to characteristic 0), we may write such a curve in 'short Weierstrass form', as

$$y^2 = x^3 + Ax + B.$$

We define, for such a curve, the discriminant and $j$-invariant in the usual way :

$$\Delta(E) = -16(4A^3 + 27B^2), \quad j(E) = \frac{-1728(4A)^3}{\Delta(E)},$$

where $\Delta(E) \neq 0$ by the non-singularity of $E$. In some cases it makes sense to consider equations such as the above with $\Delta = 0$, but such objects are not elliptic curves. The $j$-invariant classifies $E$ up to isomorphism over an algebraic closure of $K$. It is simple enough to show (see [17]) that two curves in short Weierstrass form, $y^2 = x^3 + Ax + B$ and $y^2 = x^3 + A'x + B'$, are isomorphic over an extension field $L \supseteq K$ just in case there is some $\xi \in L$ such that $A = \xi^4 A'$ and $B = \xi^6 B'$. Note that the condition $A, B, A', B' \in K$

ensures $\xi^2 \in K$, unless $B = 0$ or $A = 0$, in which case we may conclude at most $\xi^4 \in K$ or $\xi^6 \in K$ respectively. Two elliptic curves over $K$ which are isomorphic over $\overline{K}$ are said to be twists of one another.

We denote by $E(K) = (E(K), +, \mathcal{O})$ the group of $K$-rational (projective) points on $E$, where $\mathcal{O}$ is the unique point on $E$ at infinity, and addition is defined by

$$P_1 + P_2 + P_3 = \mathcal{O}$$

just in case $P_1$, $P_2$, and $P_3$ are co-linear on $E$ with multiplicity. This defines an abelian group which, by the theorem of Mordell-Weil, is finitely generated. Note that the isomorphisms discussed above are also group isomorphisms. We denote by $E[n]$ the set of points (in some algebraic closure $\overline{K}$ of $K$) of order (dividing) $n$. As we will see in Section 1.4, if $E/K$ is an elliptic curve, $K \subseteq \mathbb{C}$, then there is an analytic group isomorphism

$$\psi : E(\mathbb{C}) \to \mathbb{C}/\Lambda,$$

for some lattice $\Lambda \subseteq \mathbb{C}$. In particular, we have that $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$, although, in general, $E(K)[n]$ is much smaller. By the Mordell-Weil Theorem, in fact, $\cup_{n \geqslant 1} E(K)[n]$ will always be finite, and it is a straightforward exercise to show that it takes the form $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/nm\mathbb{Z}$ for some $n, m \in \mathbb{Z}$. There are somewhat stronger results known for specific fields :

**Theorem 1.1 (Mazur [12]).** *Let $E/\mathbb{Q}$ be an elliptic curve. Then the subgroup of points in $E(\mathbb{Q})$ of finite order, $E(\mathbb{Q})_{\text{Tors}}$, is isomorphic to one of the following groups :*

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z}, &\quad n \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}, &\quad n \in \{1, 2, 3, 4\}. \end{aligned}$$

Note, apropos of Chapter 2, that the only primes that may divide the order of $E(\mathbb{Q})_{\text{Tors}}$ are 2, 3, 5, and 7. We will also, in Chapter 3, require a similar itemization of possible torsion structures over quadratic fields.

**Theorem 1.2 (Kamienny [10]).** *Let $K/\mathbb{Q}$ be a quadratic extension, and $E/K$ an elliptic curve. Then $E(K)_{\text{Tors}}$ is isomorphic to one of the following groups :*

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z}, &\quad n \in \{1, 2, \ldots, 16, 18\} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}, &\quad n \in \{1, 2, 3, 4, 5, 6\} \\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3n\mathbb{Z}, &\quad n \in \{1, 2\} \\ (\mathbb{Z}/4\mathbb{Z})^2. & \end{aligned}$$

Note that while all of the above groups occur as torsion groups of elliptic curves over quadratic fields, not all groups occur over all quadratic fields. One can show, for example, that if $P, Q \in E(K)$ generate $E[n]$, then the Weil pairing of $P$ and $Q$, an element of $K$, must in fact be a primitive $n$th root of unity. Thus the torsion group $(\mathbb{Z}/4\mathbb{Z})^2$ occurs only over (extensions of) $\mathbb{Q}(i)$, while the groups $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3n\mathbb{Z}$, $n \in \{1, 2\}$, occur only over (extensions of) $\mathbb{Q}(\sqrt{-3})$.

Slightly more generally, we will say that the curve $E/K$ admits an isogeny of degree $n$ if there is a subgroup $\Gamma \subseteq E(\overline{K})$ of order $n$ which is fixed, setwise, by the action of the Galois group $\mathrm{Gal}(\overline{K}/K)$. This is equivalent to the condition that there be a $K$-rational homomorphism from $E$ to another elliptic curve over $K$, with degree $n$. In fact, Mazur's result above is really a result restricting the possible degrees of isogenies on elliptic curves over $\mathbb{Q}$ (see page 39).

## 1.2 Height functions

For a point $P = [x_0 : \cdots : x_N]$ in $N$-dimensional projective space over $K$ we define the absolute logarithmic height of $P$ to be

$$h(P) = \sum_{v \in M_K} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log \max\{|x_0|_v, \ldots, |x_N|_v\},$$

where $M_K$ is a maximal set of normalized, pairwise non-equivalent absolute values on $K$, and $K_v$ denotes the completion of $K$ at $v$ (we will let the reader check, for example in [17], that this is independent of the choice of co-ordinates). For a given number field $K$, one maximal set of valuations on $K$ is given by the set of archimedean valuations

$$|x|_\sigma = |\sigma(x)|$$

for each embedding $\sigma : K \to \mathbb{C}$, along with the non-archimedean '$\mathfrak{p}$-adic' valuations defined by the primes $\mathfrak{p}$ of $K$ by

$$|\mathfrak{p}^\alpha \beta|_\mathfrak{p} = e^{-\alpha}$$

for all $\alpha \in \mathbb{Z}$ and all $\beta \in K$ which do not contain $\mathfrak{p}$ in their factorization.

For a number $\alpha \in K$, we set $h(\alpha) = h([\alpha : 1])$, and for a point $P \in E(K)$ we set

$$h(P) = h(x(P)),$$

where $P = [x(P) : y(P) : 1]$. Occasionally we shall refer to non-logarithmic height, $H(x) = e^{h(x)}$, defined the same way in all of the above settings.

While the definition of height above is useful in a general context, over $\mathbb{Q}$ it represents a complete obfuscation of the more elementary definition of height. Let $p/q \in \mathbb{Q}$ be written such that $(p, q) = 1$. Then at least one of $|p|_\ell$, $|q|_\ell$ is 1 for each $\ell$-adic absolute value, as $p$ and $q$ are integers not both divisible by any given prime. Thus, if $P = [\frac{p}{q} : 1] = [p : q]$,

$$h\left(\frac{p}{q}\right) = h(P) = \log \max\{|p|, |q|\},$$

where $|\cdot|$ denotes the usual, archimedean, absolute value (note that if we set $\log 0 = -\infty$, and treat this as smaller than any real number, the above is defined and real). Similarly, it might be worth noting (see [17, p. 211]) that, if $\alpha \in \overline{\mathbb{Q}}$ of degree $d$ has minimal polynomial $f(x) = a_d x^d + \cdots + a_1 x + a_0$, where $a_i \in \mathbb{Z}$ are pairwise coprime, then

$$\left| h(\alpha) - \frac{1}{d} \log \max\{|a_d|, \ldots, |a_0|\} \right| \leqslant \log 2.$$

One might note, also, from the above listing of absolute values, that $h(P) = h(P^\sigma)$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$.

The height above interacts relatively well with the arithmetic structure of an elliptic curve, but it behooves us to uniformize it somewhat. The canonical height of a point $P \in E(K)$ is defined as

$$\hat{h}(P) = \lim_{n \to \infty} \frac{1}{4^n} h(2^n P).$$

The fact that this limit exists will not be proved here, but is a ready consequence of a careful examination of multiplication by 2 on an elliptic curve. We note, however, that this new height function has properties more amenable to the study of elliptic curves, for example

$$\hat{h}(P + Q) + \hat{h}(P - Q) = 2\hat{h}(P) + 2\hat{h}(Q)$$
$$\hat{h}(mP) = m^2 \hat{h}(P), \text{ for all } m \in \mathbb{Z},$$

and consequently

$$\hat{h}(P) = 0 \text{ if and only if } P \in E(K)_{\mathrm{Tors}},$$

while still retaining a close connection to the 'naïve' height defined above : there exist effective constants $c_1$ and $c_2$ (depending on $E$ and $K$) such that

$$-c_1 \leqslant \hat{h}(P) - h(P) \leqslant c_2$$

for all $P \in E(K)$. See, for example, [18] for some explicit constants when $K = \mathbb{Q}$. Note that, by the conditions above, $\hat{h}$ is a quadratic form on $E(K)$. Thus if $P_1, \ldots, P_k$ are a set of generators for $E(K)$, then there is a matrix $R$, the regulator matrix of $E$, such that

$$\hat{h}(n_1 P_1 + \cdots n_k P_k) = \begin{bmatrix} n_1 & \cdots & n_k \end{bmatrix} R \begin{bmatrix} n_1 \\ \vdots \\ n_k \end{bmatrix}.$$

This matrix depends, naturally, on the generators chosen, but only up to similarity. There seems to be a great deal of disagreement as to whether or not this height ought to be scaled by a factor of $\frac{1}{2}$, but this is, of course, of little import as long as consistency is maintained.

## 1.3 Diophantine analysis

Every undergraduate mathematics student learns, in some initial course in analysis, that the set of rational numbers is dense in the set of real numbers (and most, sometime later, come to think of this as a definition of $\mathbb{R}$ rather than a theorem). But one might still ask how efficiently a given real number may be approximated by rationals. That is, how does the error in a given approximation compare to the 'complexity' of the rational number doing the approximating? One may, in fact, approximate some real numbers quite successfully, but algebraic numbers are, in some sense, too close to the rationals to be approximated particularly well (and rational numbers are downright lousy approximations to each other, except in the trivial case). The first theorem in this direction is that of Liouville, that for an algebraic number $\alpha$ of degree $d$ over $\mathbb{Q}$, there is a constant $c(\alpha)$ such that

$$\left|\alpha - \frac{p}{q}\right| > c(\alpha) H\left(\frac{p}{q}\right)^{-d}.$$

This result follows immediately from the mean value theorem once one notes that, if $f(x) \in \mathbb{Z}[x]$ is the minimal polynomial of $\alpha/\mathbb{Q}$, $|f(p/q)| \geqslant |q|^{-d}$. The

history of improvements on this result is an interesting one, but we shall skip ahead to the strongest possible result.

**Theorem 1.3 (Roth [14]).** *Let $\varepsilon > 0$ and let $\alpha$ be an algebraic number. Then there is a constant $c(\alpha, \varepsilon)$ such that for all rationals $p/q \in \mathbb{Q}$,*

$$\left|\alpha - \frac{p}{q}\right| > c(\alpha, \varepsilon) H\left(\frac{p}{q}\right)^{-2-\varepsilon}.$$

This result, relying on the pigeonhole principle, is entirely ineffective. There is no known method for constructing such a $c(\alpha, \varepsilon)$ in general. Indeed, the proof assumes the existence of arbitrarily many *very* good approximations to $\alpha$, which is a rare occurrence to say the least (but, of course, if that supposition fails, the theorem follows).

There are various effective results in this direction (see, for example, [7]), but none even remotely near the strength of Theorem 1.3. The exponents, in most cases, are very slightly smaller than that in Liouville's result (although, this is enough to ensure, for example, the effective solution of Thue equations). For some particular algebraic numbers, reasonably good results are known ([6] and Chapter 3), but the general state of the art for effective irrationality measures lags far behind Roth's Theorem. Note, also, that the theory of continued fractions allows one to construct, for a given *irrational* $\alpha$ and sufficiently small $c(\alpha) > 0$, infinitely many rationals $p/q$ satisfying

$$\left|\alpha - \frac{p}{q}\right| \leqslant c(\alpha) H\left(\frac{p}{q}\right)^{-2},$$

demonstrating the strength of Theorem 1.3. To see this, fix $\alpha_0 = \alpha$ and define a sequence of integers $a_i$ by

$$a_i = \lfloor \alpha_i \rfloor, \quad \alpha_{i+1} = \frac{1}{\alpha_i - a_i}.$$

If we write

$$\frac{p_k}{q_k} = [a_0, \ldots, a_k] = a_o + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \frac{1}{a_k}}}$$

then it is rather elementary (see [11] or [13]) to show that

$$\left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{q_k^2}.$$

These tools are the main means by which we derive the results in Chapters 2 and 3, and, through the effective solution of Thue equations, those in Chapter 4. Compare Theorem 1.3, also, with the discussion in Chapter 6 on the approximation of rational numbers by $j$-invariants of elliptic curves.

## 1.4 Integral Points on elliptic curves

Consider the Diophantine problem of finding all integral solutions to a given polynomial equation

$$F(X,Y) = 0.$$

If the curve defined by this condition is of genus one (and has a rational point), then there are several ways in which we can bring our knowledge of elliptic curves to bear on the problem. It is a well-known result of Siegel (see [17]) that such an equation admits only finitely many integral solutions, but this result is ineffective; it provides no computable bound on the sizes of the solutions. There is an algorithm for solving an equation of the above form which relies on lower bound on linear forms in logarithms, but in Chapter 5 we eschew this method in favour of a method based on lower bounds on linear forms in elliptic logarithms. This latter process, while not algorithmic in general (as it depends on finding a complete set of generators for the Mordell-Weil group of the curve), seems more natural from the viewpoint of the arithmetic of elliptic curves.

Suppose the equation above defines an elliptic curve $E/\mathbb{Q}$ (note that to talk coherently about integral points, we must be considering a particular *model* of an elliptic curve), and suppose that $Q \in E(\mathbb{Q})$ is an integral point on $E$. For simplicity of exposition we will assume that $E$ is presented in short Weierstrass form, although we see in Chapter 5 how this is done more generally. Then we know that $h(Q) = \log|x(Q)|$. Write $Q = n_1P_1 + \cdots + n_rP_r + T$, where $P_1, \ldots, P_r$ are generators for the free part of $E(\mathbb{Q})$ and $T$ is some arbitrary element of $E(\mathbb{Q})_{\text{Tors}}$. Then, if $\mathbf{n} = \langle n_1, \ldots, n_r \rangle$ and $R$ is the regulator matrix defined in Section 2, one obtains

$$\hat{h}(P) \geqslant \mathbf{n}^T R \mathbf{n} \geqslant c \max\{n_i^2\},$$

where $c$ is the smallest eigenvalue of $R$. Combining these two facts with the bounds on the difference $\hat{h}(Q) - h(Q)$ mentioned in Section 1, one obtains

$$\frac{1}{|x(Q)|} \leqslant c_1 e^{-c_2 N^2}, \tag{1.1}$$

for some constants $c_1$ and $c_2$ and for $N = \max|n_i|$. This may, in turn, be used to bound the 'elliptic logarithm' of the point $Q$. If $E$ is isomorphic to the curve

$$y^2 = f(x) = 4x^3 - g_2x - g_3$$

and one defines

$$\psi(P) = \int_{\infty}^{x(P)} \frac{dt}{\sqrt{f(t)}}$$

one obtains a mapping $\psi : E(\mathbb{C}) \to \mathbb{C}/\Lambda$ for the lattice $\Lambda$ generated by

$$\omega_1 = 2\int_{\gamma_1}^{\gamma_2} \frac{dt}{\sqrt{f(t)}}$$
$$\omega_2 = 2\int_{\gamma_3}^{\gamma_2} \frac{dt}{\sqrt{f(t)}},$$

where the $\gamma_i$ are the roots of $f(x)$ chosen in such a way as to ensure $\omega_1 \in \mathbb{R}$. In particular, one obtains, for $|x(Q)| > 2\max|\gamma_i|$,

$$|\psi(Q)|^2 \leqslant \frac{8}{|x(Q)|}.$$

This bound is elementary, and does not depend on $Q$ being integral, but when combined with (1.1) yields a bound of the form

$$|\psi(Q)| \leqslant c_3 e^{-c_4 N^2}. \tag{1.2}$$

On the other hand, $\psi$ turns out to be a homomorphism satisfying

$$\psi(Q_1 + Q_2) = \psi(Q_1) + \psi(Q_2) \pmod{\Lambda}.$$

Thus $\psi(Q)$ may be written as

$$n_1\psi(P_1) + \cdots n_r\psi(P_r) + \psi(T) + m\omega_1,$$

where $|m| \leqslant rN + 2$. It is a result of Hirata-Kohno [9], made explicit by David [8], that such a linear form in elliptic logarithms has an absolute lower bound of the form

$$\exp\left(-c_5(\log N + c_6)(\log\log N + c_7)^{r+2}\right),$$

where $c_5$, $c_6$, and $c_7$ are effectively computable constants. Comparing this with (1.2) yields an upper bound on $N$. In practice this upper bound is rather ungainly, and must be lowered through an application of the LLL algorithm (see, for example, [19]).

# Bibliography

[6] M. A. Bennett. Effective measures of irrationality for certain algebraic numbers. *J. Austral. Math. Soc. Ser. A*, 62(3):329–344, 1997.

[7] Y. Bugeaud and K. Győry. Bounds for the solutions of Thue-Mahler equations and norm form equations. *Acta Arith.*, 74(3):273–292, 1996.

[8] S. David. Minorations de formes linéaires de logarithmes elliptiques. *Mém. Soc. Math. France (N.S.)*, (62), 1995.

[9] N. Hirata-Kohno. Formes linéaires d'intégrales elliptiques. In *Séminaire de Théorie des Nombres, Paris 1988–1989*, volume 91 of *Progr. Math.*, pages 117–140. Birkhäuser Boston, Boston, MA, 1990.

[10] S. Kamienny. Torsion points on elliptic curves. *Bull. Amer. Math. Soc. (N.S.)*, 23(2):371–373, 1990.

[11] A. Y. Khinchin. *Continued Fractions.* Dover Publications, New York, 1964.

[12] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.

[13] I. Niven, H. S. Zuckerman, and H. L. Montgomery. *An introduction to the theory of numbers.* John Wiley and Sons, Toronto, 1991.

[14] K. F. Roth. Rational approximations to algebraic numbers. *Mathematika*, 2:1–20; corrigendum, 168, 1955.

[15] W. M. Schmidt. *Diophantine approximation*, volume 785 of *Lecture Notes in Mathematics.* Springer, Berlin, 1980.

[16] W. M. Schmidt. *Diophantine approximations and Diophantine equations*, volume 1467 of *Lecture Notes in Mathematics.* Springer-Verlag, Berlin, 1991.

[17] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[18] J. H. Silverman. The difference between the Weil height and the canonical height on elliptic curves. *Math. Comp.*, 55, 1990.

[19] N. P. Smart. *The algorithmic resolution of Diophantine equations*, volume 41 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1998.

# Chapter 2

# Torsion subgroups of elliptic curves in short Weierstrass form

## 2.1 Introduction

In a recent paper of Wieczorek [28], 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

$$A \geqslant |B| > 0, \tag{2.1}$$

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

$$y^2 = x^3 + 121361253948260608 5x - 844976094618678570 \tag{2.2}$$

is an elliptic curve satisfying inequality (2.1) 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 (2.2) provides the "smallest". The main difficulty is that the results of [28] rely heavily upon those of [21] (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 [28] which turn out to be true. Our first result is

[1] A version of this chapter has been published. Bennett, M. A. and Ingram, P. (2005) *Torsion subgroups of elliptic curves in short Weierstrass form.* Transactions of the American Mathematical Society 357:3325–3337

**Theorem 2.1.** *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 2.2.** *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*

$$|A| > |B|^{2+\varepsilon} > 0 \tag{2.3}$$

*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 $\delta$.

The outline of this paper is as follows. In Section 2.2, we describe the basic structure of our argument and prove a more precise version of Theorem 2.1. In Section 2.3, we produce families of examples to demonstrate that our results are sharp and subsequently indicate a number of counterexamples to the claims of [28]. Section 2.4 is devoted to the proof of Theorem 2.2 and a corresponding result (Proposition 2.8) which guarantees that this theorem is essentially best possible. Finally, in Section 2.5, we address the problem of finding effective and unconditional versions of Theorems 2.1 and 2.2.

## 2.2 Proof of Theorem 2.1

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

**Lemma 2.3.** *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. □

From this and work of Mazur [24], classifying possible rational torsion subgroups, it follows, if $E_{A,B}(\mathbb{Q})_{\text{Tors}}$ is nontrivial, that

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

Theorem 2.1 is thus an immediate consequence of the following

**Proposition 2.4.** *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 [23]). 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 [25], there can be only finitely many such $p/q$.

It is known (see e.g. [23]) that any elliptic curve over $\mathbb{Q}$ with ($\mathbb{Q}$-rational) torsion group isomorphic to $\mathbb{Z}/N\mathbb{Z}$ 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 [26]) 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 2.4 for minimal pairs $(A, B)$.

### 2.2.1 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

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

and

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

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 (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 2.5.** *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 $p \equiv -q \pmod 3$.*

*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

$$\gcd\left(q^{2N-6}A_N(p/q), q^{3N-9}B_N(p/q)\right) \tag{2.4}$$

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,

$$q^6 B_5^*(p/q) \equiv (p^2+q^2)((p^2-pq-q^2)^2+3p^2q^2) \equiv 8 \pmod{16},$$
$$q^8 A_7^*(p/q) \equiv (p^4+p^2q^2+q^4)^2 \equiv 1 \pmod 2$$

and

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

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 (2.4). In case $N = 5$, we have

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

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

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

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

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

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 $p \equiv -q \pmod 3$, however, implies the congruences

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

and

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

Since $p$ and $q$ are coprime and $p \equiv -q \pmod 3$ (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. □

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 2.5 ensures that $B$ is necessarily even. In particular, this precludes the possibility that $B = \pm 1$. It follows that Theorem 2.1 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 2.5.

### 2.2.2 Connections to Diophantine approximation

Given Lemma 2.5, 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 2.6.** *Let $\varepsilon$ 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 $p \equiv -q \pmod 3$, 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,*

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

*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

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

implies the inequality

$$|B_5(p/q)| < |A_5(p/q)|^{\frac{1}{1+\varepsilon}} \cdot q^{-2-\varepsilon_5}. \tag{2.5}$$

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

$$|B_5(p/q)| < \max\{1, |A_5(p/q)|\} \cdot q^{-2}. \tag{2.6}$$

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 (2.6). 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 (2.6),

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

This inequality implies, after a short calculation, that

$$\left|\theta_{5,i} - \frac{p}{q}\right| < 5 \times 10^{-8} \tag{2.7}$$

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 $\zeta$ between $\theta_{5,i}$ and $p/q$. From (2.5) and the fact that $|A_5(p/q)| > 1$ on the intervals defined by (2.7), we thus have

$$\left|\theta_{5,i} - \frac{p}{q}\right| < |A_5(p/q)| \cdot |B_5'(\zeta)|^{-1} \cdot q^{-2-\varepsilon_5}. \tag{2.8}$$

From (2.7), it is an exercise in calculus to verify that, for $\zeta$ 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 (2.8), then, it follows that

$$\left|\theta_{5,i} - \frac{p}{q}\right| < \frac{1}{C_{5,i}\, q^{2+\varepsilon_5}}, \tag{2.9}$$

as claimed.

If $N \in \{7, 9\}$, we argue similarly, with a few minor complications. Here the analogues of inequality (2.5) 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 $p \equiv -q \pmod 3$ 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. □

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.

## 2.3 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 2.6 :

**Proposition 2.7.** *Let $N \in \{5,7,9\}$. If $A$ and $B$ are integers such that $E_{A,B}$ has rational $N$-torsion and*

$$|A| > |B|^{\frac{2N-6}{3N-11}}, \tag{2.10}$$

*then, in the sense of Proposition 2.6, the pair $(A,B)$ corresponds to a rational number $p/q$ such that $p/q = p_j/q_j$ is the $j$th 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 $\theta$ 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* $p_j \equiv -q_j \pmod 3$, *and* $\delta = 0$, *otherwise. Then we have both (2.10) and*

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

*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 (2.10), then applying Proposition 2.6 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 $j$th convergent in the simple continued fraction expansion to $\theta_{N,i}$, for some $j$. From the well-known inequalities

$$\frac{1}{(a_{j+1}+2)q_j^2} < \left|\theta_{N,i} - \frac{p_j}{q_j}\right| < \frac{1}{a_{j+1}q_j^2} \tag{2.11}$$

(see e.g. Khinchin [22]; 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 (2.11),

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

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 $E_{A,B}(\mathbb{Q})_{\text{Tors}} \cong \mathbb{Z}/7\mathbb{Z}$). 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 2.6, 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

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

where

$$\alpha_5 = [1, 9, 1, 19, 12, 32, 1, 5, 1090, 10, \ldots]$$

and

$$\beta_5 = [3, 12, 14, 1, 8, 1, 8, 4, 4, 1, 6, \ldots].$$

Note that

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

From Proposition 2.7, it follows that counterexamples to the main theorem of [28], 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 $\alpha_5$ with $a_i = 21$ or $22$ (possibly) or $a_i \geq 23$ (definitely). The first two such counterexamples are the curve (2.2) and that given by

$$y^2 = x^3 + 184641841486018241292297885 3\, x + 3881292199322894617937650 2.$$

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 $\beta_5$ 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

$$\alpha_7 = [1, 1, 2, 8, 1, 2, 1, 2, 1, 1, 1, 27, \ldots]$$

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

$$\alpha_9 = [2, 10, 1, 2, 7, 5, 1, 1, 6, 2, 56, \ldots]$$

and

$$\beta_9 = [2, 5, 2, 14, 1, 4, 1, 1, 1, 2, 1, 6, \ldots].$$

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 $\alpha_7$, $\beta_7$, $\alpha_9$ and $\beta_9$ for "large" partial quotients. The curve of lowest height satisfying either of these inequalities is one we encountered during the proof of Proposition 2.6, namely

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

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

## 2.4 Proof of Theorem 2.2

We will now proceed with the proof of Theorem 2.2. From Proposition 2.4, it suffices to consider curves with a rational 2-torsion or 3-torsion point, for which the pair $(A, B)$ satisfies (2.3) 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 $\alpha$ and $\beta$ 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 $\alpha$ 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 (2.3).

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. [26]), $x$ and $y$ are integers). Using the duplication formula for points on $E_{A,B}$, we see that both

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

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 $x^3 + 6A_0x + 4B = t^2$, 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 $\varepsilon$. 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 (2.3), completing the proof of Theorem 2.2.

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

**Proposition 2.8.** *There exist infinitely many pairs of integers $(A, B)$ for which both*

$$A > B^2 > 0$$

*and*

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

*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,

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

□

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

## 2.5 Effective, unconditional results

In this section, we will concentrate on effective results along the lines of Theorem 2.1 (i.e. ones which do not rely upon Roth's theorem) and on an unconditional version of Theorem 2.2. 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 2.9.** *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 2.6 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

$$\left|\theta_{5,i} - \frac{p}{q}\right| < \frac{1}{C_{5,i}\, q^4} \tag{2.12}$$

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

$$\left|\theta_{5,i} - \frac{p}{q}\right| = \left|\frac{f\,(p/q)}{f'(\xi)}\right| \tag{2.13}$$

for some $\xi$ between $\theta_{5,i}$ and $p/q$. Consideration of the continued fraction expansions of the $\theta_{5,i}$ shows that inequality (2.12) 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, (2.12) and (2.13), it follows that

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

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. □

For $N \in \{7,9\}$, the polynomial $B_N^*(t)$ is irreducible. As a result, we cannot obtain an analogous result to Proposition 2.9 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 [20], 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 [28], 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 [28] 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 2.2, we desire an unconditional criterion to guarantee trivial rational torsion, we may derive the following :

**Proposition 2.10.** *Let $\varepsilon > 0$ be given. Then there exists an effectively computable constant $c_\varepsilon$ 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 [27], we have

$$\log \max(|M|, s^2) \ll |B|^{1+\varepsilon}, \tag{2.14}$$

where the implied constant depends only on $\varepsilon$. 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 $\kappa$ such that

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

whence the desired inequality obtains from (2.14). □

## 2.6 Concluding remarks

Theorem 2.2 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" $B$.

# Bibliography

[20] Y. Bugeaud and K. Győry. Bounds for the solutions of Thue-Mahler equations and norm form equations. *Acta Arith.*, 74(3):273–292, 1996.

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

[22] A. Y. Khinchin. *Continued Fractions.* Dover Publications, New York, 1964.

[23] D. S. Kubert. Universal bounds on the torsion of elliptic curves. *Proc. London Math. Soc. (3)*, 33(2):193–237, 1976.

[24] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.

[25] K. F. Roth. Rational approximations to algebraic numbers. *Mathematika*, 2:1–20; corrigendum, 168, 1955.

[26] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1986.

[27] H. Stark. Effective estimates of solutions of some Diophantine equations. *Acta Arith.*, 24, 1973.

[28] M. Wieczorek. Torsion points on certain families of elliptic curves. *Canad. Math. Bull.*, 46(1):157–160, 2003.

# Chapter 3

# Diophantine analysis and torsion on elliptic curves

## Introduction

The claim was made in a paper of Wieczorek, [38], that for any elliptic curve

$$E = E(A, B) : y^2 = x^3 + Ax + B,$$

where $A$ and $B$ are integers satisfying $A > |B| > 0$, the torsion subgroup of $E(\mathbb{Q})$ must be isomorphic to the trivial group, $\mathbb{Z}/3\mathbb{Z}$, or $\mathbb{Z}/9\mathbb{Z}$. This claim, as it turns out, is false, and in [30] Bennett and the author constructed potentially infinitely many counterexamples. However, a result similar in flavour was derived from Roth's Theorem on diophantine approximation, namely that for any $\varepsilon > 0$ and for all but finitely many integers $A, B$ satisfying

$$|A| > |B|^{2+\varepsilon} > 0,$$

the torsion subgroup of $E(\mathbb{Q})$ is trivial or isomorphic to $\mathbb{Z}/3\mathbb{Z}$. Moreover, assuming the *abc* Conjecture of Masser and Oesterlé, we can eliminate the possibility of points of order three. The proof centres on showing how the above inequality obstructs the existence of points of order 2, 5, 7, or 9 which, by Mazur's theorem on the possible torsion subgroups of elliptic curves over the rationals, produces the desired result. As it turns out, similar inequalities in the other direction also inhibit torsion. Examining the methods of [30] more closely, we demonstrate the following.

**Proposition 3.1.** *For each $\varepsilon > 0$ there are at most finitely many $A, B \in \mathbb{Z}$ such that $|B| > |A|^{6+\varepsilon}$ and $E(A, B)(\mathbb{Q})$ contains a point of order not dividing 4.*

[2] A version of this chapter has been accepted for publication. Ingram, P. *Diophantine analysis and torsion on elliptic curves.* Proceedings of the London Mathematical Society.

This result is, as stated, sharp, as we can see by considering the family of elliptic curves

$$y^2 = x^2 + 3sx - \frac{1}{4}(27s^6 + 18s^3 - 1)$$

as $s$ varies over the odd integers, each of which carries a rational 3-torsion point

$$P = \left(3s^2, \frac{9s^3 + 1}{2}\right).$$

We note also that each curve

$$y^2 = x^3 + x - n(n^2 + 1)$$

contains the rational 2-torsion point $P = (n, 0)$, and so we cannot produce any result similar to Proposition 3.1, but ruling out all points of finite order. It is likely, however, that condition $|B| > |A|^{6+\varepsilon}$ prevents $E(A, B)$ from having a rational point of order 4, as we shall see below in an argument relying on the *abc* Conjecture.

If $E/\mathbb{Q}$ is an elliptic curve with a $\mathbb{Q}$-rational point of order $N$, then one may construct a $\mathbb{Q}$-rational isogeny of degree $N$ on $E$ (i.e., a $\mathbb{Q}$-rational morphism whose kernel is generated by said point of order $N$). It is therefore reasonable to ask if the results in [30] are special cases of a more general result on isogenies between elliptic curves. This is answered affirmatively by the following proposition, although the specific results we obtain regarding torsion are slightly stronger than those regarding isogenies (as one might expect).

**Proposition 3.2.** *Let $\varepsilon > 0$. There are at most finitely many $A, B \in \mathbb{Z}$ such that $|A| > |B|^{2+\varepsilon}$ and $E(A, B)$ admits a non-trivial $\mathbb{Q}$-rational isogeny of degree other than 3. There are at most finitely many $A, B \in \mathbb{Z}$ with $|B| > |A|^{6+\varepsilon}$ such that $E(A, B)$ admits a non-trivial $\mathbb{Q}$-rational isogeny of odd degree other than 5.*

These results, like those in the previous paper, rely on Roth's Theorem on diophantine approximation, and as such are ineffective. In Section 3, we derive effective analogues of some of our results, some derived by elementary means and some relying on effective irrationality measures. In Section 4, we extend these results, in a limited fashion, to elliptic curves over certain number fields, and in the final section we consider similar results for elliptic curves in another common form. In particular, we prove

**Proposition 3.3.** *Let $K$ be an imaginary quadratic extension of $\mathbb{Q}$ and let $\varepsilon > 0$. Then for all but finitely many algebraic integers $A, B \in K$ satisfying $|A| > |B|^{2+\varepsilon}$, $E(A,B)(K)$ contains no points of finite order other than those of order 3 or 11.*

If we consider curves of the form

$$E_{a,b} : y^2 = x(x^2 + ax + b),$$

we may show

**Proposition 3.4.** *For each $\varepsilon > 0$ there are at most finitely many $a, b \in \mathbb{Z}$ such that $b > |a|^{4+\varepsilon}$ and*

$$E_{a,b}(\mathbb{Q})_{\text{Tors}} \notin \{\mathbb{Z}/2n\mathbb{Z} : n = 1, 2, 3\}.$$

**Remark.** Note that, throughout, when considering elliptic curves $E(A,B)$, we shall always assume that $AB \neq 0$ and that $B \neq \pm 1$ in order to avoid certain trivialities. The torsion subgroups of elliptic curves with $AB = 0$ are very well understood (see, for example, [36]). It is similarly straightforward to characterize the torsion on elliptic curves with $B = \pm 1$. In particular, one sees in [30] that if $E(A,B)(\mathbb{Q})$ contains a point of order 5, 7, or 9, then $B$ is even. Considering the factorization of $x^3 + Ax \pm 1$ over $\mathbb{Z}$ one can see readily that $E(A, \pm 1)$ cannot admit full 2-torsion over $\mathbb{Q}$, and hence any torsion on said curve must be cyclic of order $2^\alpha 3^\beta$ for $\alpha \leqslant 3$ and $\beta \leqslant 1$. Considering the relevant parametrizations from [30] or the appendix one sees that if $\varepsilon \in \{1, -1\}$,

$$E(A,\varepsilon)(\mathbb{Q})_{\text{Tors}} \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & (A,\varepsilon) \in \{(-2,-1),(0,-1)\} \\ \mathbb{Z}/4\mathbb{Z} & (A,\varepsilon) = (-2,1) \\ \mathbb{Z}/6\mathbb{Z} & (A,\varepsilon) = (0,1) \\ \{0\} & \text{otherwise.} \end{cases}$$

In particular, if $E(A, \pm 1)(\mathbb{Q})$ contains a point of order three then $A = 27s^4 + 6st$ where $\pm 1 = t^2 - 27s^6$, the latter equations being easily solved as the elliptic curves $Y^2 = X^3 \pm 1$ are both of rank 0. Examining again the factorization of $x^3 + Ax \pm 1$ gives one all curves over $\mathbb{Q}$ with 2-torsion, and an elementary argument shows that the only curve $E(A, \pm 1)$ with a point of order 4 is that above (it is, in fact, simpler to consider the parametrization of curves with isogenies of degree 4).

## 3.1 Results for all possible torsion groups

Although the previous work constructed only upper bounds on $\log|A|/\log|B|$ for elliptic curves $y^2 = x^3 + Ax + B$ with certain torsion subgroups, it is possible to arrive at lower bounds using similar techniques. It is also possible to construct bounds, usually sharp, for all possible torsion groups, rather than simply relying on the bounds imposed by the prime divisors of the order of the group. The proofs are similar to those of previous results, relying on techniques of diophantine analysis.

We summarize our main results on rational torsion below. For finite groups $G$ we define

$$P^-(G) = \liminf_{a_0,b_0\to\infty} \left\{ \frac{\log|a|}{\log|b|} : G \hookrightarrow E(a,b)(\mathbb{Q}),\ a,b\in\mathbb{Z}, |a|>a_0, |b|>b_0 \right\}$$

$$P^+(G) = \limsup_{a_0,b_0\to\infty} \left\{ \frac{\log|a|}{\log|b|} : G \hookrightarrow E(a,b)(\mathbb{Q}),\ a,b\in\mathbb{Z}, |a|>a_0, |b|>b_0 \right\}.$$

More specifically than Proposition 3.1, we prove that $P^{\pm}$ takes the following values:

| $G$ | $P^-(G)$ | $P^+(G)$ |
|---|---|---|
| $\mathbb{Z}/2\mathbb{Z}$ | 0 | 2 |
| $\mathbb{Z}/3\mathbb{Z}$ | 1/6 | 2 † |
| $\mathbb{Z}/4\mathbb{Z}$ | 1/6 † | 1 † |
| $\mathbb{Z}/5\mathbb{Z}$ | 1/3 | 1 |
| $\mathbb{Z}/6\mathbb{Z}$ | 1/3 | 1 |
| $\mathbb{Z}/7\mathbb{Z}$ | 1/2 | 4/5 |
| $\mathbb{Z}/8\mathbb{Z}$ | 1/2 | 4/5 |
| $\mathbb{Z}/9\mathbb{Z}$ | 5/9 | 3/4 |
| $\mathbb{Z}/10\mathbb{Z}$ | 5/9 | 3/4 |
| $\mathbb{Z}/12\mathbb{Z}$ | 7/12 | 8/11 |
| $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ | 2/3 | 1 |
| $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ | 2/3 | 1 |
| $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ | 2/3 | 4/5 |
| $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$ | 2/3 | 8/11 |

**Remark.** Entries marked with † are obtained only under the additional assumption of the *abc* Conjecture of Masser and Oesterlé. Recall that this

conjecture states that for any $\varepsilon > 0$ and integers $a + b = c$ we have

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

where the above product is taken over primes and the implied constant depends only on $\varepsilon$. For elliptic curves with cyclic torsion of order 4 we are unable to improve on the bounds that follow simply from the existence of a point of order 2 unless we assume this conjecture. See Lemma 3.8 for this case, and [30] for $P^+(\mathbb{Z}/3\mathbb{Z})$.

Proposition 3.1 is a corollary to the above table, which is in turn a consequence of the following result once one examines the parametrizations of the given torsion structures (see the appendix). Special care is needed for curves with rational points of order 3 or full 2-torsion.

**Lemma 3.5.** *Fix $\varepsilon > 0$. Let $A(X)$ and $B(X) \in \mathbb{Z}[X]$ be square-free polynomials of degree $2d$ and $3d$ respectively, with nonzero resultant. Then for all but finitely many nonzero integers $a$ and $b$ with $b \neq \pm 1$ and $E(a,b) \cong_{\mathbb{C}} E(A(t), B(t))$ for some $t \in \mathbb{Q}$, we have*

$$\frac{2}{3}\left(1 - \frac{1}{d}\right) - \varepsilon < \frac{\log|a|}{\log|b|} < \frac{2}{3 - 2/d} + \varepsilon.$$

In fact, we will see in the proof below that these bounds are sharp, i.e., that one can construct infinite families of such curves $E(a,b)$ with $\log|a|/\log|b|$ tending towards $\frac{2}{3-2/d}$ or $\frac{2}{3}(1 - 1/d)$. Furthermore, if the partial quotients of the roots of $A(X)$ and $B(X)$ are sufficiently large infinitely often, these families can be made such that $\log|a|/\log|b|$ approaches $\frac{2}{3-2/d}$ from above or $\frac{2}{3}(1 - 1/d)$ from below (so that the $\varepsilon$ in the Lemma must truly be positive). If $d$ is even then these bounds are sharp even within the subfamily parametrized by $A(X)$ and $B(X)$ up to $\mathbb{Q}$-isomorphism.

*Proof.* For relatively prime $p, q \in \mathbb{Z}$, set

$$\overline{A}(p,q) = q^{2d}A(p/q),$$
$$\overline{B}(p,q) = q^{3d}B(p/q).$$

Additionally, let $\tilde{A}(t)$ and $\tilde{B}(t)$ be the least integers in absolute value (taking, without loss of generality, $|\tilde{B}|$ minimal and $\tilde{B} \geqslant 0$) such that

$$E(\tilde{A}(t), \tilde{B}(t)) \cong_{\mathbb{C}} E(A(t), B(t)).$$

Note that, if we avoid $ab = 0$, the $\mathbb{C}$-isomorphic images of $E(a, b)$ are precisely $E(s^2a, s^3b)$ for non-zero $s \in \mathbb{Q}$. Thus, as $\overline{A}(p, q), \overline{B}(p, q)$ are integers, we have immediately that

$$|\tilde{A}(p/q)| \leqslant |\overline{A}(p, q)|$$
$$|\tilde{B}(p/q)| \leqslant |\overline{B}(p, q)|.$$

But we must have, for some integer $m$, $\overline{A}(p, q) = m^2\tilde{A}(p/q)$ and $\overline{B}(p, q) = m^3\tilde{B}(p/q)$. Let $R \in \mathbb{Z}$ be the resultant of $A(X)$ and $B(X)$, supposed above to be non-zero. Then, for $(p, q) = 1$, if $m^2 \mid \overline{A}(p, q)$ and $m^3 \mid \overline{B}(p, q)$, we have $m^2 \mid R$. In particular,

$$|\overline{A}(p, q)| \leqslant R|\tilde{A}(p/q)|$$
$$|\overline{B}(p, q)| \leqslant R^{\frac{3}{2}}|\tilde{B}(p/q)|.$$

Now, applying Roth's Theorem to $\overline{B}(p, q)$, we obtain, for $\delta > 0$ and some constant $c_\delta$,

$$|\tilde{B}(p/q)| > c_\delta \max\{|p|, |q|\}^{3d-2-\delta}$$

while clearly, if $c_A$ is the sum of the moduli of the coefficients of $A(X)$,

$$|\tilde{A}(p/q)| \leqslant |\overline{A}(p, q)| \leqslant c_A \max\{|p|, |q|\}^{2d},$$

We thus obtain

$$\frac{\log|\tilde{A}(p/q)|}{\log|\tilde{B}(p/q)|} < \frac{2dh(p/q) + \log c_A}{(3d - 2 - \delta)h(p/q) + \log c_\delta},$$

where $h$ is the usual (logarithmic) height

$$h\left(\frac{p}{q}\right) = \log \max\{|p|, |q|\}.$$

This is clearly implies

$$\frac{\log|\tilde{A}(p/q)|}{\log|\tilde{B}(p/q)|} < \frac{2}{3 - 2/d} + \varepsilon$$

by selecting $\delta = \delta(\varepsilon)$ appropriately, with at most finitely many exceptions.

Now suppose that $a$ and $b$ are nonzero integers, $b \neq \pm 1$, such that $E(a,b) \cong_{\mathbb{C}} E(\tilde{A}(p/q), \tilde{B}(p/q))$, which is to say, such that $a = t^2\tilde{A}(p/q)$ and $b = t^3\tilde{B}(p/q)$, for some nonzero $t \in \mathbb{Z}$. Then we have

$$\frac{\log|a|}{\log|b|} = \frac{2\log|t| + \log|\tilde{A}(p/q)|}{3\log|t| + \log|\tilde{B}(p/q)|} \leqslant \frac{\log|\tilde{A}(p/q)|}{\log|\tilde{B}(p/q)|}$$

Thus if $a$ and $b$ violate the above upper bound, so do $\tilde{A}(p/q), \tilde{B}(p/q)$, and $E(a,b)$ is $\mathbb{C}$-isomorphic to one of our finitely many exceptional curves above. Furthermore, as the middle term above converges to $\frac{2}{3}$ as $|t| \to \infty$, we see that

$$\frac{\log|a|}{\log|b|} > \frac{2}{3} + \varepsilon'$$

induces an upper bound on $|t|$, and so at most finitely many isomorphic copies of each of the finitely many exceptional curves may violate our upper bound. Reproducing the analogous argument with Roth's Theorem applied to $A(X)$ we produce the lower bound above.

To demonstrate the sharpness of these bounds, we may simply note that, applying the theory of continued fractions (see, for example, [33]), we may construct sequences $p_k/q_k, s_k/t_k$ such that for appropriate constants $c_1$ and $c_2$,

$$|\overline{A}(p_k,q_k)| \leqslant c_1 \max\{|p_k|,|q_k|\}^{2d-2}$$
$$\text{and } |\overline{B}(s_k,t_k)| \leqslant c_2 \max\{|s_k|,|t_k|\}^{3d-2}.$$

Also note that $d$ being even ensures that $E(\overline{A}(p,q), \overline{B}(p,q))$ is always $\mathbb{Q}$-isomorphic to $E(A(p/q), B(p/q))$. □

**Remark.** It is worth noting briefly that elliptic curves which approach the above bounds, i.e., for which $A$ is sufficiently larger than $B$ or vice versa, will have $j$-invariant rather close to either 0 or 1728. Indeed, if one fixes $\varepsilon > 0$ and bounds $j(E(A,B))$ away from these two values, then

$$\left|\frac{\log|A|}{\log|B|} - \frac{2}{3}\right| < \varepsilon$$

with finitely many exceptions (independent of any structure on $E$). One might, however, inquire as to how well the $j$-invariants of elliptic curves in

short Weierstrass form with integral coefficients approximate various other rational values, subject to the level structure on those curves.

Note also, in a similar vein, that if $A(X)$ or $B(X)$ has no real roots then we see immediately that $\log|a|/\log|b|$ is bounded below by $\frac{2}{3}-\varepsilon$ or above by $\frac{2}{3}+\varepsilon$ respectively. Furthermore, effective results may be stated. In particular, the existence of non-negative minima of $|A_{\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}}(X)|$, $|A_{\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}}(X)|$, and $|A_{\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}}(X)|$ lead us to effective statements on curves with these torsion structures over $\mathbb{Q}$.

We shall proceed now to prove the bounds in the cases requiring more attention.

**Lemma 3.6.** $P^-(\mathbb{Z}/3\mathbb{Z}) = 1/6$.

*Proof.* As in [30], note that the curves $E(A,B)$ with points of order 3 are parametrized by

$$A = 27s^4 + 6sM$$
$$B = M^2 - 27s^6,$$

where $s, M \in \mathbb{Z}$. For convenience we write $t = 9s^3 + 2M$ so that

$$A = 3st$$
$$B = \frac{-1}{4}\left(27s^6 + 18s^3t - t^2\right).$$

We now note readily that for $s$ and $t$ nonzero, $A \geqslant \max\{|s|,|t|\}$, while $B \leqslant \frac{27}{4}\max\{|s|^6,|t|^2\}$. From this we see that $P^-(\mathbb{Z}/3\mathbb{Z}) \geqslant 1/6$. On the other hand, by choosing $s$ odd above we may set $t = 1$ (i.e., $M = \frac{1}{2}(1-9s^3)$); from this family we see that $P^-(\mathbb{Z}/3\mathbb{Z}) \leqslant 1/6$. □

The case of curves with full 2-torsion is similar to the other cases, but not exactly the same as the parametrization takes a slightly different form.

**Lemma 3.7.** $P^-((\mathbb{Z}/2\mathbb{Z})^2) = \frac{2}{3}$, $P^+((\mathbb{Z}/2\mathbb{Z})^2) = 1$.

*Proof.* Suppose that $E(A,B)(\mathbb{Q})$ exhibits full 2-torsion. By examining the factorization

$$x^3 + Ax + B = (x-e_1)(x-e_2)(x-e_3)$$

we see that

$$A = -(e_1^2 + e_1e_2 + e_2^2)$$
$$B = e_1e_2(e_1 + e_2)$$

for some integers $e_1, e_2$. Assuming $AB \neq 0$, we have $|A| \geqslant \frac{3}{4}\max\{|e_1|, |e_2|\}^2$. On the other hand $|B| \leqslant 2\max\{|e_1|, |e_2|\}^3$, whence

$$\frac{\log|A|}{\log|B|} \geqslant \frac{2h(e_1/e_2) + \log(\frac{3}{4})}{3h(e_1/e_2) + \log(2)},$$

proving that $P^-((\mathbb{Z}/2\mathbb{Z})^2) \geqslant \frac{2}{3}$. To prove the bound in the other direction, simply consider the (isomorphic) curves of the form $E(-7t^4, 6t^6)$ for $t \in \mathbb{Z}$, all of which have full two torsion. Clearly, as $t \to \infty$, this family demonstrates that $P^-((\mathbb{Z}/2\mathbb{Z})^2) \geqslant \frac{2}{3}$.

For the other equality note that if we take, without loss of generality, $|e_1| > |e_2|$, then $|A| \leqslant 3|e_1|^2$. On the other hand, either $|e_1| \leqslant 2|e_2|$, in which case

$$|B| \geqslant |e_1||e_2| \geqslant \frac{1}{2}|e_1|^2,$$

or $|e_1| > 2|e_2|$, from which we have $|e_1 + e_2| \geqslant \frac{1}{2}|e_1|$ and the same lower bound on $|B|$. To prove sharpness of the bound on $P^+((\mathbb{Z}/2\mathbb{Z})^2)$ simply consider the family defined by $e_2 = e_1 - 1$. □

**Lemma 3.8.** *$P^-(\mathbb{Z}/4\mathbb{Z}) \leqslant 1/6$ and $P^+(\mathbb{Z}/4\mathbb{Z}) \geqslant 1$. If the abc Conjecture holds then these inequalities are strict.*

*Proof.* We prove the second equality and leave the first to the reader. We rewrite the parametrizations in the appendix as

$$A_{\mathbb{Z}/4\mathbb{Z}}(X) = -27(4X^2 + 24X + 33)$$
$$B_{\mathbb{Z}/4\mathbb{Z}}(X) = 54(4X + 9)(9 - 2X^2).$$

Let $X = p/q$ where $(p, q) = 1$. As in the previous cases, the result is trivial unless $3q = \pm[p\sqrt{2}]$, where $[\cdot]$ denotes the nearest integer function, so suppose that one of these equalities holds. If we set $q = lN^2$, with $l$ square-free, then the minimal coefficients in any isomorphism class are given by

$$A = -27l^2(4p^2 + 24plN^2 + 33l^2N^4)$$
$$B = 54l^3(4p + 9lN^2)(9l^2N^4 - 2p^2).$$

By the *abc* Conjecture, if

$$F = 9l^2N^4 - 2p^2$$

then

$$l^2N^4 \ll |FplN|^{1+\varepsilon}.$$

Noting that $|p| \leqslant \frac{3}{\sqrt{2}}q + \frac{1}{\sqrt{2}}$ we have, then,

$$|F| \gg l^{-\varepsilon}N^{1-\varepsilon}$$

and hence

$$|B| \gg l^{4-\varepsilon}N^{3-\varepsilon}.$$

As $|A| \ll l^4N^3$ we have $P^+(\mathbb{Z}/4\mathbb{Z}) \leqslant 1$. To show that $P^+(\mathbb{Z}/4\mathbb{Z}) \geqslant 1$, simply let $p, q$ satisfy $9q^2 - 2p^2 = 1$, that is, let

$$(q\sqrt{3} + p2\sqrt{2}) = (\sqrt{3} + 2\sqrt{2})^k$$

for large, odd $k$. □

## 3.2 Curves admitting $\mathbb{Q}$-rational isogenies

It is natural to ask if the results in Section 1 can be extended to the more general case of curves admitting nontrivial $\mathbb{Q}$-rational isogenies. A $\mathbb{Q}$-rational isogeny of degree $N$ on $E$ is a $\mathbb{Q}$-rational morphism (necessarily a group homomorphism) $\varphi : E \to E'$ with a kernel, in $E(\overline{\mathbb{Q}})$, of order $N$. If $E(\mathbb{Q})$ contains a point of order $N$ then we may readily construct such a map (see [37]). For the sake of simplicity we restrict our attention to isogenies with cyclic kernel.

**Proposition 3.2.** *Let $\varepsilon > 0$. Then there are only finitely many $A, B \in \mathbb{Z}$ such that $|A| > |B|^{2+\varepsilon}$ and $E(A, B)$ admits a $\mathbb{Q}$-rational isogeny of degree other than 3.*

As before, our results are somewhat better when considering only isogenies of particular degrees. By results of Mazur [35], for

$$N \notin \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25\}$$

there are at most finitely many elliptic curves over $\mathbb{Q}$, up to twisting, admitting isogenies of degree $N$, and so if $E(A, B)$ admits a $\mathbb{Q}$-rational isogeny of

degree $N$ then $A = d^2A_0$ and $B = d^3B_0$ for some $d \in \mathbb{Z}$ and some $A_0$ and $B_0$ members of a finite set depending on $N$. It follows immediately that, if $\varepsilon > 0$,

$$\frac{2}{3} - \varepsilon < \frac{\log|A|}{\log|B|} < \frac{2}{3} + \varepsilon$$

for all but finitely many such $A$ and $B$. We will, then, consider only $N$ in this set. Note that if $E$ admits a $\mathbb{Q}$-rational isogeny of degree $N$ and $M \mid N$, then $E$ admits a $\mathbb{Q}$-rational isogeny of degree $M$. If we define $\mathcal{E}(a_0, b_0)$ to be the set of all pairs of integers $(a, b)$ such that $|a| > a_0, |b| > b_0$ and $E(a, b)$ admits a $\mathbb{Q}$-rational isogeny of degree $N$ and

$$I^-(N) = \liminf_{a_0,b_0\to\infty} \left\{ \frac{\log|a|}{\log|b|} : (a,b) \in \mathcal{E}(a_0,b_0) \right\}$$
$$I^+(N) = \limsup_{a_0,b_0\to\infty} \left\{ \frac{\log|a|}{\log|b|} : (a,b) \in \mathcal{E}(a_0,b_0) \right\}$$

then it will suffice to prove that the following bounds apply:

| $N$ | $\leqslant I^-(N)$ | $I^-(N) \leqslant$ | $\leqslant I^+(N)$ | $I^+(N) \leqslant$ |
|---|---|---|---|---|
| 2 | 0 | 0 | 2 | 2 |
| 3 | 1/6 | 1/6 | 2 | |
| 4 | 0 | 0 | 2 | 2 |
| 5 | 0 | 1/3 | 1 | 2 |
| 6 | 1/3 | 1/3 | 1 | 1 |
| 7 | 1/6 | 1/3 | 1 | 4/3 |
| 9 | 1/3 | 1/3 | 1 | 1 |
| 13 | 8/21 | 1/2 | 4/5 | 14/15 |
| 25 | 8/15 | 5/9 | 3/4 | 10/13 |

Note that as every point of order $N$ induces a rational isogeny of degree $N$ we have

$$I^-(N) \leqslant P^-(\mathbb{Z}/N\mathbb{Z}) \leqslant \frac{2}{3} \leqslant P^+(\mathbb{Z}/N\mathbb{N}) \leqslant I^+(N).$$

Some of the results above, then, are trivial results of the analogous results in Section 1.

The arguments in this section are similar in character to the arguments in Section 1, but here the parametrizing polynomials often share common factors. As a result, Lemma 3.5 does not apply, and each case must be considered separately. The exception to this is the case of curves admitting

isogenies of degree 9, which succumb to the simpler methods applied above. We proceed with the case of curves admitting rational isogenies of degree 5. The other cases are variations of the argument.

**Lemma 3.9.** *There is a constant $c$ such that if $A$ and $B$ integers such that $E(A, B)$ admits a rational isogeny of degree 5, then $|A| < c|B|^2$.*

*Proof.* Let

$$A_5^*(X) = -3(X^2 + 12X + 16)(X^2 + 4)$$
$$B_5^*(X) = 2(X^2 + 18X + 76)(X^2 + 4)^2$$

as in the appendix, so that $E(A, B)$ admits a $\mathbb{Q}$-rational isogeny of degree five if and only if it is isomorphic to $E(A_5^*(t), B_5^*(t))$ for some $t \in \mathbb{Q}$. For any relatively prime integers $p$ and $q$, let $N = N(p, q)$ be the greatest integer whose square divides $p^2 + 4q^2$. In particular, $N^{-2}q^4A_5^*(p/q)$ and $N^{-3}q^6B_5^*(p/q)$ are integers. Let $\tilde{A}(p, q)$ and $\tilde{B}(p, q)$ (taking, arbitrarily, $\tilde{B}(p, q) > 0$) be the least integers (taking, arbitrarily, $\tilde{B}(p, q) > 0$) such that $E(\tilde{A}(p, q), \tilde{B}(p, q))$ is isomorphic to $E(A_5^*(p/q), B_5^*(p/q))$. Thus $|N^{-2}q^4A_5^*(p/q)|$ and $|N^{-3}q^6B_5^*(p/q)|$ are bounded below by $|\tilde{A}(p, q)|$ and $|\tilde{B}(p, q)|$ respectively. We wish to show that, up to a constant, the inequality may be reversed.

For brevity, set

$$f = p^2 + 12pq + 16q^2$$
$$g = p^2 + 18pq + 76q^2$$
$$h = p^2 + 4q^2.$$

so that

$$N^{-2}q^4A_5^*(p/q) = N^{-2}fh$$
$$N^{-3}q^6B_5^*(p/q) = N^{-3}gh^2.$$

Computing resultants

$$\mathrm{res}(f, h) = 2^4 3^2 5q^4$$
$$\mathrm{res}(g, h) = 2^4 3^4 5q^4$$
$$\mathrm{res}(f, g) = -2^4 3^2 q^4$$

and noting that $(p,q)=1$, we can see that if $l$ is a prime with

$$l^2 \mid N^{-2}q^4A_5^*(p/q) \text{ and } l^3 \mid N^{-3}q^6B_5^*(p/q),$$

then $l \in \{2,3,5\}$. This follows as, if the assumption holds, either $l \mid f$ and $l \mid gh$, in which case $l \mid 30q$, or $l^2 \mid N^{-2}h$. The case $l \mid q$ and $l \mid fgh$ leads to $l \mid (p,q)=1$, a contradiction, while the second case defies the definition of $N$. We now consider $l \in \{2,3,5\}$. Note that we cannot have $3 \mid fh$, as

$$f \equiv h \equiv p^2+q^2 \ (\pmod 3),$$

whence $3 \mid fh$ if and only if $3 \mid (p,q)=1$.

Let $2 \mid fh$. Then clearly $2 \mid p$, so let $p=2^\alpha p_2$, with $p_2$ odd. Then $h=2^2(2^{2\alpha-2}p_2^2+q^2)$, and so $2^2 \| h$ as long as $\alpha \geqslant 2$. Similarly, if $\alpha \geqslant 3$,

$$2^4 \| f = 2^4\left(2^{2\alpha-4}p_2^2+2^{\alpha-2}3p_2q+q^2\right).$$

Thus if $2^\beta \mid q^4A_5^*(p/q)$ and $2^\alpha \mid p$ then $\alpha \geqslant 3$ ensures $\beta \leqslant 6$. Now, if $\alpha=1$, we have $h=2^2(p_2^2+q^2)$ and $p_2^2+q^2 \equiv 2 \ (\pmod 4)$, and so $2^4 \nmid h$. Similarly, $2^{-2}f \equiv 1 \ (\pmod 2)$, and so $\beta \leqslant 5$. Finally, if $\alpha=2$, $2^2 \| h$ as above and $2^{-4}f \equiv 1 \ (\pmod 2)$, whence $\beta \leqslant 6$. In summary, if $2^{2a} \mid N^{-2}q^4A_5^*(p/q)$ and $2^{3a} \mid N^{-3}q^6B_5^*(p/q)$ then certainly $a \leqslant 3$.

Finally we will deal with $l=5$. We observe that if $5 \mid f \equiv (p+q)^2 \ (\pmod 5)$ then for some $r \in \mathbb{Z}$ we have $p=5r-q$, and so $f=5(5r^2+10qr+q^2)$. In particular, $5^2 \nmid f$. The definition of $N$ prevents $5^2 \mid N^{-2}h$, and so we have $5^{2a} \mid N^{-2}q^4A_5^*(p/q)$, $5^{3a} \mid N^{-3}q^6B_5^*(p/q)$ for at worst $a \leqslant 1$. Combined with the above we get

$$N^{-2}q^4A_5^*(p/q) \leqslant 2^6 5^2 A(p,q)$$
$$N^{-3}q^6B_5^*(p/q) \leqslant 2^9 5^3 B(p,q).$$

Using the fact that $N \leqslant \sqrt{p^2+4q^2}$ and some calculus we can see that for $p/q \notin [-12,-4]$, $|N^{-3}B_5^*(p/q)| > 2|N^{-2}A_5^*(p/q)|$ which in turn yields $|B| > 2^{-8}5^{-3}|A|$. So now assume that $p/q \in [-12,-4]$, and consequently $|f| \leqslant 20q^2$

Write, for a particular $(p,q)$, $\lambda = \lambda(p,q) = \log(N)/\log(h)$. For $p/q \in [-12,-4]$ we have $|g| \geqslant 1$. This then gives

$$|B(p,q)| \geqslant 2^{-9}5^{-3}|N|^{-3}|2gh^2| = 2^{-8}5^{-3}|h^{2-3\lambda}|$$

while

$$|A(p,q)| \leqslant 3N^{-2}|fh| \leqslant 60|q^2h^{1-2\lambda}|.$$

We then have

$$\left|\frac{B^2}{A}\right| \geqslant \frac{1}{2^{18}\cdot 3\cdot 5^7}q^{-2}|h|^{3-4\lambda} \geqslant \frac{1}{2^{16}\cdot 3\cdot 5^7}$$

as $0 \leqslant \lambda \leqslant 1/2$ and $h \geqslant 4q^2$.

This proves the result with $c = 2^{16}\cdot 3\cdot 5^7$. □

The other cases are treated similarly, and the details of these proofs are left to the reader. The exception to this is the question of the values of $\log|A|/\log|B|$ when $E(A,B)$ admits a rational 3-isogeny. One notes, in this case, that we may write

$$D^2A = 27s^4 + 6st$$
$$D^3B = t^2 - 27s^6,$$

for some integers $D$, $s$, and $t$, and we may assume, without loss of generality, that there is no prime $l$ with both $l^2 \mid A$ and $l^3 \mid B$. An elementary argument shows that $s \mid A$, and so $I^-(3) \geqslant \frac{1}{6}$. This is the best possible result, of course, as $I^-(3) \leqslant P^-(\mathbb{Z}/3\mathbb{Z}) = \frac{1}{6}$. It seems, however, rather difficult to bound $I^+(3)$, even under the *abc* Conjecture. A naïve computation leads one to believe that $I^+(3) = 2$.

**Remark.** It is perhaps interesting to note that, by the above, one might construct a family of elliptic curves $E(A_k, B_k)$ each admitting a rational isogeny of degree 9 such that

$$\frac{\log|A_k|}{\log|B_k|} > \frac{9}{10},$$

say. By the results in [30], at most finitely many of these may contain a rational point of order 9.

## 3.3 Elliptic curves over quadratic extensions

For what follows let $D \in \mathbb{Z}^+$, and let $K = \mathbb{Q}(\sqrt{-D})$. The main aim is to prove:

**Proposition 3.3.** *Let $K$ be an imaginary quadratic extension of $\mathbb{Q}$ and let $\varepsilon > 0$. Then for all but finitely many algebraic integers $A, B \in K$ satisfying $|A| > |B|^{2+\varepsilon}$, $E(A,B)(K)$ contains no points of finite order other than those of order 3 or 11.*

Work by Kamienny [32] shows that for any elliptic curve $E$ over $K$,

$$E(K)_{\text{Tors}} \cong \begin{cases} \mathbb{Z}/m\mathbb{Z} & m \leqslant 16, m = 18 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z} & m \leqslant 6 \\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3m\mathbb{Z} & m \leqslant 2 \\ (\mathbb{Z}/4\mathbb{Z})^2. \end{cases}$$

Note, then, that the above claim implies that $E(A,B)(K)_{\text{Tors}} \cong \{0\}, \mathbb{Z}/3\mathbb{Z}$, $(\mathbb{Z}/3\mathbb{Z})^2$, or $\mathbb{Z}/11\mathbb{Z}$ for all but finitely many $K$-integers $A, B$ satisfying $|A| > |B|^{2+\varepsilon} > 0$.

*Proof.* We treat the case that $E(K)$ contains a point of order $n$, for $n \in \{2,5,7,9\}$.

Case $n = 2$: If $E(A,B)(K)$ has a point of order 2 over $K$ then we have, for some $\alpha$ and $\beta \in \mathcal{O}_K$,

$$x^3 - Ax + B = (x - \alpha)(x^2 + \alpha x + \beta).$$

Now we have $A = \beta - \alpha^2$, $B = -\alpha\beta$, and so under the hypothesis $|A| > |B|^{2+\varepsilon} > 0$ we have

$$1 < \frac{|A|}{|B|^{2+\varepsilon}} = \frac{|\beta - \alpha^2|}{|\alpha|^{2+\varepsilon}|\beta|^{2+\varepsilon}} \leqslant 2\frac{\max\{|\alpha|^2, |\beta|\}}{|\alpha|^{2+\varepsilon}|\beta|^{2+\varepsilon}}.$$

If $|\alpha|^2 \geqslant |\beta|$ then the above becomes

$$1 < 2\frac{|\alpha|^2}{|\alpha|^{2+\varepsilon}|\beta|^{2+\varepsilon}} = 2|\alpha|^{-\varepsilon}|\beta|^{-2}.$$

Thus $|\alpha| \leqslant 2^{\frac{1}{\varepsilon}}$ and $|\beta| \leqslant \sqrt{2}$ as $|\gamma| \geqslant 1$ for all $\gamma \in \mathcal{O}_K$. As the integers in $K$ are discrete, this gives us only finitely many possible pairs $\alpha, \beta$. We may proceed similarly in the case $|\alpha|^2 < |\beta|$.

Case $n = 5$:

**Lemma 3.10.** *For a fixed $K$ and $\varepsilon$, there are only finitely many integers $A, B \in \mathcal{O}_K$ such that $E(A,B)(K)$ contains a point of order 5 and $|A| > |B|^{2+\varepsilon} > 0$.*

*Proof.* Let $A_5$ and $B_5$ be the polynomials in [30] parametrizing elliptic curves with points of order five. By the standard argument from resultants, it suffices to prove the result for elliptic curves of the form $E(A, B)$, where

$$A = \beta^4 A_5(\alpha/\beta)$$
$$B = \beta^6 B_5(\alpha/\beta)$$

and where $\alpha$ and $\beta$ are algebraic integers in $K$. As $B_5$ is of higher degree than $A_5$, we find that $|B| > |A|$ for $|\alpha/\beta|$ sufficiently large, and thus will assume that $|\alpha/\beta| < N$ for some $N$. Furthermore, we will suppose that in this domain, $|A_5(\alpha/\beta)| < M$ for some fixed $M$. Now, suppose that $|B|^{2+\varepsilon} < |A|$. Then

$$|B_5(\alpha/\beta)| < M_2|\beta|^{-4-\varepsilon'}$$

for $\varepsilon' = 2\varepsilon/(2+\varepsilon)$ and $M_2^{2+\varepsilon} = M$. As in [30], this bounds $|\beta|$ unless $\alpha/\beta$ is particularly close to a root of $B_5$. If $|\beta|$ is bounded then so too is $|\alpha|$ and, as $K$-integers are discrete, there are only finitely many $\alpha/\beta$ to consider. Thus we assume that

$$\left|\frac{\alpha}{\beta} - \theta\right| < \gamma$$

for some $\theta \in \mathbb{C}$ with $B_5(\theta) = 0$ and some fixed $\gamma$ of our choosing. We will choose $\gamma$ sufficiently small that we may apply the mean value theorem to bound

$$\left|\frac{\alpha}{\beta} - \theta\right| < M_3 B_5(\alpha/\beta)$$

for some constant $M_3$. By inspection, the roots of $B_5$ are $\pm i$ and four real roots.

First consider the case of $\theta$ real. Note that if $\alpha/\beta \in \mathbb{R}$ then $\alpha/\beta \in \mathbb{Q}$ and so we may simply apply Roth's Theorem, as in [30], to show that

$$|\beta|^{-2-\delta} \ll \left|\frac{\alpha}{\beta} - \theta\right| \ll |\beta|^{-4-\varepsilon'},$$

thereby bounding $|\beta|$. So we assume $\mathrm{Im}(\alpha/\beta) \neq 0$. From this,

$$\left|\frac{\alpha}{\beta} - \theta\right| \geqslant \mathrm{Im}\left(\frac{\alpha}{\beta}\right) \geqslant |2\beta|^{-2}\sqrt{D}$$

by considering $\alpha\overline{\beta}/|\beta|^2$ and noting that $2\alpha\overline{\beta} \in \mathbb{Z}[\sqrt{-D}]$. This again restricts $|\beta|$.

Now suppose that $\theta = \pm i$. As above, if $\mathrm{Re}(\alpha/\beta) \neq 0$ then one obtains rather easily a bound on $\beta$, so suppose that $\mathrm{Re}(\alpha/\beta) = 0$. Then, if $\alpha/\beta = \pm p\sqrt{-D}/q$, with $p, q \in \mathbb{Z}$, we have

$$\left|\frac{\alpha}{\beta} - \theta\right| = \left|\frac{p\sqrt{D}}{q} - 1\right| \geqslant \frac{1}{2+\delta}\,|\beta|^{-2}.$$

This again restricts us to only finitely many options for $\alpha/\beta$. □

**Remark.** Note that the above proof actually establishes the result for all $K$ simultaneously. The obstruction to stating the result for all $K$ simultaneously lies only in the case of points of order 13.

CASE $n = 7, 9$: These are similar to the last case and are left to the reader.

CASE $n = 13$: Here it suffices to observe that as $X_1(13)$ has genus two, Faltings' Theorem (see [31]) ensures that $X_1(13)(K)$ is finite, and so there are only finitely many isomorphism classes of curves over $K$ with a point of order 13.

□

In general, the results above do not extend readily even to real quadratic fields. We do have, however, the following special case.

**Proposition 3.11.** *For any real Galois extension $K/\mathbb{Q}$ there is a constant $c$ such that for all $A, B \in \mathcal{O}_K$ such that $E(A,B)(K)$ contains a point of order 5,*

$$|N_{K/\mathbb{Q}}(A)| < cN_{K/\mathbb{Q}}(B)^2.$$

*Proof.* If $E(A,B)$ contains a point of order five over $K$, then $E(A,B)$ is isomorphic to $E(A_5, B_5)$, where

$$A_5 = -27\left(\alpha^4 - 12\alpha^3\beta + 14\alpha^2\beta^2 + 12\alpha\beta^3 + \beta^4\right),$$
$$B_5 = 54\left(\alpha^2 + \beta^2\right)\left(\alpha^4 + 18\alpha^3\beta + 74\alpha^2\beta^2 + 18\alpha\beta^3 + \beta^4\right),$$

for some $\alpha, \beta \in \mathcal{O}_K$. Applying the same argument about resultants as in the rational case, we may find a constant $C \in \mathcal{O}_K$ depending only on $K$ such that

$$A_5 | C^4 A, B_5 | C^6 B.$$

In particular, it suffices to prove the result for $A_5, B_5$. Note that $|N_{K/\mathbb{Q}}(\xi)| \geqslant 1$ for all $\xi \in \mathcal{O}_K$ and so, if we define

$$m(\alpha, \beta) = \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \max\{|\alpha^\sigma|, |\beta^\sigma|\},$$

we have

$$|N_{K/\mathbb{Q}}(B_5)| \geqslant 54^d |N_{K/\mathbb{Q}}(\alpha^2 + \beta^2)| \geqslant 108^d m(\alpha, \beta)^2,$$

where $d = [K : \mathbb{Q}]$. On the other hand, calculus shows that

$$|N_{K/\mathbb{Q}}(A_5)| = 27^d |N_{K/\mathbb{Q}}(\alpha^4 - \cdots + \beta^4)| \leqslant 1080^d m(\alpha, \beta)^4.$$

We thus obtain

$$|N_{K/\mathbb{Q}}(A_5)| < \left(\frac{5}{54}\right)^d N_{K/\mathbb{Q}}(B_5)^2,$$

from which the result is immediate, with

$$c = \left(\frac{5C^8}{54}\right)^d.$$

As $C^4 | \mathrm{Res}(A_5, B_5)$ we see that $c$ can me made to depend only on $d = [K : \mathbb{Q}]$. □

**Corollary 3.12.** *Let $K$ be a real Galois extension of $\mathbb{Q}$. For any $\varepsilon > 0$ there are, up to multiplication by units, at most finitely many $A, B \in \mathcal{O}_K$ such that $E(A, B)(K)$ contains a point of order 5, and*

$$|N_{K/\mathbb{Q}}(A)| > |N_{K/\mathbb{Q}}(B)|^{2+\varepsilon}.$$

## 3.4 Effective results

We return our attention to elliptic curves defined over $\mathbb{Q}$. The results of Sections 1 and 2, most of which depend heavily on Roth's Theorem, are of course computationally ineffective. Effective results may be obtained in any case where one may explicitly improve upon the "naïve" Liouville theorem, that if $f(\theta) = 0$ for some (possibly reducible) $f(X) \in \mathbb{Q}[X]$ of degree $d$, then

$$\left|\theta - \frac{p}{q}\right| > \frac{1}{c_\theta q^d}.$$

The most glaring improvement occurs when $f$ factors over $\mathbb{Q}$, in which case we may apply Lemma 3.13. By the results on lower bounds on linear forms in logarithms we may, of course, always improve upon the above, but these small improvements do not yield interesting explicit results about elliptic curves. In the case of isogenies of degree nine, we apply an effective irrationality measure for $\sqrt[3]{2}$ due to Bennett to obtain an effective statement.

We will make use of the following analogue to Lemma 3.5:

**Lemma 3.13.** *Let $A(X)$ and $B(X)$ be square-free polynomials of degree $2d$ and $3d$ respectively, and suppose that $B(X) = \prod f_i(X)$ over $\mathbb{Z}$, $d_1 = \max\{\deg(f_i)\}$. Then for all integers $a$ and $b$ with $E(a,b) \cong E(A(t), B(t))$, we have*

$$|a| < c_1 |b|^{\frac{2}{3-d_1/d}}$$

*for some effectively computable $c_1$. Similarly, if $A(X) = \prod g_i$, and if we set $d_2 = \max\{\deg(g_i)\}$, then we have*

$$|b| < c_2 |a|^{\frac{3}{2-d_2/d}}.$$

*Proof.* The proof is similar in spirit to that of Lemma 3.5, but rather than rely on Roth's Theorem we simply note that if $B(X)$ factors as above, then

$$|B(p/q)| > c \max\{|p|, |q|\}^{-d_1}$$

for a readily computable constant $c$. The first inequality then follows from the same argument as in Lemma 3.5. The result in the case that $A(X)$ factors is similar. □

**Proposition 3.14.** *There exist effectively computable constants $c_1, ..., c_{22}$*

*such that for all* $A, B \in \mathbb{Z}$,

$$\begin{aligned}
\mathbb{Z}/4\mathbb{Z} \hookrightarrow E(A,B)(\mathbb{Q})_{\text{Tors}} &\implies |A| \leqslant c_1|B|^2 \\
\mathbb{Z}/5\mathbb{Z} \hookrightarrow E(A,B)(\mathbb{Q})_{\text{Tors}} &\implies |A| \leqslant c_2|B|^2 && (3.1)\\
\mathbb{Z}/6\mathbb{Z} \hookrightarrow E(A,B)(\mathbb{Q})_{\text{Tors}} &\implies |A| \leqslant c_3|B|^2, |B| \leqslant c_4|A|^6 && (3.2)\\
\mathbb{Z}/7\mathbb{Z} \hookrightarrow E(A,B)(\mathbb{Q})_{\text{Tors}} &\implies |B| \leqslant c_5|A|^6 && (3.3)\\
\mathbb{Z}/8\mathbb{Z} \hookrightarrow E(A,B)(\mathbb{Q})_{\text{Tors}} &\implies |A| \leqslant c_6|B|^2 \\
\mathbb{Z}/9\mathbb{Z} \hookrightarrow E(A,B)(\mathbb{Q})_{\text{Tors}} &\implies |B| \leqslant c_7|A|^{\frac{150}{31}} && (3.4)\\
\mathbb{Z}/10\mathbb{Z} \hookrightarrow E(A,B)(\mathbb{Q})_{\text{Tors}} &\implies |A| \leqslant c_8|B|^{\frac{6}{5}} \\
\mathbb{Z}/12\mathbb{Z} \hookrightarrow E(A,B)(\mathbb{Q})_{\text{Tors}} &\implies |A| \leqslant c_9|B|^2, |B| \leqslant c_{10}|A|^6 \\
\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \hookrightarrow E(A,B)(\mathbb{Q})_{\text{Tors}} &\implies |A| \leqslant c_{11}|B|, |B| \leqslant c_{12}|A|^{\frac{3}{2}} \\
\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \hookrightarrow E(A,B)(\mathbb{Q})_{\text{Tors}} &\implies |A| \leqslant c_{13}|B|, |B| \leqslant c_{14}|A|^{\frac{3}{2}} \\
\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \hookrightarrow E(A,B)(\mathbb{Q})_{\text{Tors}} &\implies |A| \leqslant c_{15}|B|, |B| \leqslant c_{16}|A|^{\frac{3}{2}} \\
E(A,B) \in X_0(5) &\implies |A| \leqslant c_{17}|B|^2 && (3.5)\\
E(A,B) \in X_0(7) &\implies |B| \leqslant c_{18}|A|^6 && (3.6)\\
E(A,B) \in X_0(9) &\implies |B| \leqslant c_{19}|A|^{\frac{150}{31}} && (3.7)\\
E(A,B) \in X_0(13) &\implies |A| \leqslant c_{20}|B|^{\frac{14}{3}}, |B| \leqslant c_{21}|A|^{\frac{21}{2}} \\
E(A,B) \in X_0(25) &\implies |A| \leqslant c_{22}|B|^2. && (3.8)
\end{aligned}$$

Note that some of these results may be redundant. For example, (3.5) clearly implies both (3.1) and (3.8), although the constants in the later cases may be different.

**Remark.** It is also worth noting that (3.3), which follows directly from (3.6), provides an explicit irrationality measure

$$\left|\theta - \frac{p}{q}\right| \geqslant Cq^{-10.666\ldots}$$

for the roots of the polynomial $B_7$ (as found in [30]), an irreducible polynomial of degree 12. This may be shown simply by considering the converse of the proof in [30]. Similarly, (3.4), which follows directly from (3.7), provides an irrationality measure

$$\left|\theta - \frac{p}{q}\right| > Cq^{-8.28}$$

for the various roots of $B_9$, some of which are algebraic numbers of degree 9.

*Proof.* We apply the factorizations of these polynomials to acquire most of the effective results, but (12) is obtained from the following inequality of Bennett (see [29]):

$$\left|\frac{p}{q} - \sqrt[3]{3}\right| > \frac{2}{5}q^{-2.76}$$

for all rationals $p/q$. Note that the exponent in the second inequality in (3.2) may be effectively improved using similar techniques.

We will, for purpose of example, prove the first claim in (3.2) with $c_3 = \frac{15}{484}$. This is sharp as $y^2 = x^3 - 15x + 22$ contains a rational point of order six. For another example, $c_2 = 59/6750000$, with sharpness demonstrated by

$$y^2 = x^3 + 25488x - 54000.$$

We will write $A = A_{\mathbb{Z}/6\mathbb{Z}}$, $B = B_{\mathbb{Z}/6\mathbb{Z}}$. In the notation of Section 1, it is easy to show that

$$\tilde{A}(p/q) = N^{-4}q^4A(p/q)$$
$$\tilde{B}(p/q) = N^{-6}q^6B(p/q),$$

for some divisor $N$ of 6. Note that for $t \notin [-4, 3]$ we have $c_3|6^{-6}B(t)|^2 > |6^{-4}A(t)|$, and so in particular, $|\tilde{A}(t)| < c_3\tilde{B}^2(t)$. On the other hand, if $\theta_1 < \ldots < \theta_4$ are the real roots of $B$, we have, for $t \in X = [-4, 3] \setminus \bigcup_{i=1}^{4}(\theta_i - \varepsilon, \theta_i + \varepsilon)$,

$$|B(t)| \geqslant 0.79$$
$$|A(t)| \leqslant 53163,$$

where $\varepsilon = 0.01$. This yields

$$|\tilde{A}(t)| \geqslant c_3\tilde{B}^2(t)$$

only if, for $t = p/q$,

$$6^{-4}q^4|A(p/q)| \geqslant c_3 6^{-12}q^{12}B^2(p/q),$$

which in turn implies $q \leqslant 25$. We can enumerate all such $p/q$ easily, and we see that $|\tilde{A}(p/q)|/\tilde{B}^2(p/q)$ is maximized with $p = -15, q = 22$ (note: it is in fact maximized by $p = -1, q = 9$, but this yields a singular curve).

For $t = p/q \in (\theta_1 - \varepsilon, \theta_1 + \varepsilon)$ we can see that $|B(X)/(X - \theta_1)|$ is bounded below by 445000 while $|A(X)|$ is bounded above by 18600. Thus if we have

$$6^{-4}q^4|A(p/q)| \geqslant c_3 6^{-12}q^{12}B^2(p/q),$$

then we obtain

$$\left|\theta_1 - \frac{p}{q}\right| < 2.26q^{-4}.$$

Let $F(X, Y)$ be the binary form associated with the minimal polynomial of $\theta_1$. Then on the interval in question,

$$|F(p, q)| \leqslant 190q^4 \left|\theta_1 - \frac{p}{q}\right|$$

which, when combined with the above inequality, tells us that any counterexample to our claim occurs with $|F(p, q)| < 430$. There are only two non-trivial solutions to this inequality ($p/q = 1$ and $p/q = 1/2$), neither of which offers a counterexample to our claim.

We perform the same computation in $(\theta_3 - \varepsilon, \theta_3 + \varepsilon)$ to see that a counterexample here implies that

$$\left|\theta_3 - \frac{p}{q}\right| < 146q^{-4}.$$

This in turn implies $|F(p, q)| \leqslant 1022$. The one solution to $F = 792$ is our optimal value of $A/B^2$.

The roots $\theta_2$ and $\theta_4$ are roots of the quadratic factor of $B$. On the first of these intervals we have, for counterexamples $p/q$,

$$6^{-4}q^4|A(p/q)| \geqslant c_3|6^{-6}q^6B(p/q)|^2 \geqslant 2^{-10}3^{-8}c_3|F(p/q, 1)|^2q^8,$$

which in turn yields $q \leqslant 41$. Checking these values we find no counterexamples. On the final interval, a counterexample would have $q \leqslant 5$, which again produces no counterexamples to our claim. □

## 3.5 Curves in another common form

It is natural to ask to what extent the results above are artifacts of the chosen form of the elliptic curve and to what extent the results are more general. To this end we prove similar results for curves of the form:

$$E_{a,b} : y^2 = x(x^2 + ax + b).$$

Note that such curves always contain the point $(0,0)$ of order two.

In particular, we obtain

**Proposition 3.4.** *For all $\varepsilon > 0$ there are at most finitely many $a, b \in \mathbb{Z}$ such that $b > |a|^{4+\varepsilon}$ and*

$$E_{a,b}(\mathbb{Q})_{\text{Tors}} \notin \{\mathbb{Z}/2n\mathbb{Z} : n = 1, 2, 3\}.$$

Note that results of Mazur (see, for example, [36]) tell us that in general

$$E_{a,b}(\mathbb{Q})_{\text{Tors}} \in \{\mathbb{Z}/2n\mathbb{Z} : n = 1, 2, 3, 4, 5, 6\} \cup \{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} : n = 1, 2, 3, 4\}.$$

The primary tool here is the obvious analogue to Lemma 3.5. We present the particular results below, where $P_2^{\pm}$ are defined as $P^{\pm}$ but in terms of $\log|a|/\log|b|$ in the notation above.

| $G$ | $P_2^-(G)$ | $P_2^+(G)$ |
|---|---|---|
| $\mathbb{Z}/2\mathbb{Z}$ | 0 | $\infty$ |
| $\mathbb{Z}/4\mathbb{Z}$ | 0 | $\infty$ |
| $\mathbb{Z}/6\mathbb{Z}$ | 0 | $\infty$ |
| $\mathbb{Z}/8\mathbb{Z}$ | 1/4 | 1 |
| $\mathbb{Z}/10\mathbb{Z}$ | 1/3 | 3/5 |
| $\mathbb{Z}/12\mathbb{Z}$ | 3/8 | 4/7 |
| $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ | 1/2 | $\infty$ |
| $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ | 1/2 | 1 |
| $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ | 1/2 | 4/5 |
| $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ | 1/2 | 2/3 |

**Lemma 3.15.** *Fix $\varepsilon > 0$ and $d > 2$, and let $A(X)$ and $B(X) \in \mathbb{Z}[X]$ be square-free polynomials of degree $d$ and $2d$ respectively, with nonzero resultant. Then for all but finitely many nonzero $a, b \in \mathbb{Z}$ with $E_{a,b} \cong_{\mathbb{C}} E_{A(t),B(t)}$ for some $t \in \mathbb{Q}$, we have*

$$\frac{1 - 2/d}{2} - \varepsilon < \frac{\log|a|}{\log|b|} < \frac{1}{2 - 2/d} + \varepsilon.$$

As in Section 1, these bounds are sharp, and if $d$ is even are sharp within the subfamily parametrized by $A, B$ up to $\mathbb{Q}$-isomorphism.

The proposition is then proven by referring to the parametrizations in the appendix, first noting that if $E$ exhibits full 2-torsion over $\mathbb{Q}$ then $4b < a^2$, as $x^2 + ax + b = 0$ must have rational solutions, and so $a^2 < 4b$ implies

$$E_{a,b}(\mathbb{Q})_{\text{Tors}} = \mathbb{Z}/2n\mathbb{Z}, n \in \{1, 2, 3, 4, 5, 6\}.$$

The details of the above table are left to the reader and are essentially the same as those in Section 1.

## 3.6 The parametrizations

Though the parametrizations for curves with given torsion subgroups used above are obtained easily from those in [34] by computing the standard invariants $c_4$ and $c_6$ of the given families presented in Tate normal form, we provide the reader with a few examples here. For any elliptic curve $E$ containing $G$ as a subgroup, $E$ is isomorphic (over the field in question) to $E(A_G(t), B_G(t))$ for some parameter $t$.

$$\begin{aligned}
A_{\mathbb{Z}/4\mathbb{Z}}(X) &= -27(16X^2+16X+1)\\
B_{\mathbb{Z}/4\mathbb{Z}}(X) &= -54(8X+1)(8X^2-16X-1)\\
A_{\mathbb{Z}/5\mathbb{Z}}(X) &= -27(X^4-12X^3+14X^2+12X+1)\\
B_{\mathbb{Z}/5\mathbb{Z}}(X) &= 54(X^2+1)(X^4-18X^3+74X^2+18X+1)\\
A_{\mathbb{Z}/6\mathbb{Z}}(X) &= -27(3X+1)(3X^3+3X^2+9X+1)\\
B_{\mathbb{Z}/6\mathbb{Z}}(X) &= -54(3X^2-6X-1)(9X^4+36X^3+30X^2+12X+1)\\
A_{\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}}(X) &= -27(X^4+14X^2+1)\\
B_{\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}}(X) &= -54(X^2+1)(X^2-6X+1)(X^2+6X+1)
\end{aligned}$$

Similarly, let $E$ be an elliptic curve defined over $\mathbb{Q}$ admitting a $\mathbb{Q}$-rational isogeny of degree $N$ with $j(E) \notin \{0, 1728\}$. Then $E$ is a twist of the curve $E(A_N^*(s), B_N^*(s))$ for some $s \in \mathbb{Q}$ where

$$\begin{aligned}
A_3^*(X) &= -3(X+1)(X+9)\\
B_3^*(X) &= 2(X+1)(X^2-18X-27)\\
A_5^*(X) &= -3(X^2+12X+16)(X^2+4)\\
B_5^*(X) &= 2(X^2+18X+76)(X^2+4)^2\\
A_7^*(X) &= -3(X^2-11X+25)(X^2-3X+9)\\
B_7^*(X) &= 2(X^4-18X^3+111X^2-298X+393)(X^2-3X+9)\\
A_9^*(X) &= -3X(X^3-24)\\
B_9^*(X) &= 2(X^6-36X^3+216).
\end{aligned}$$

Here we simply apply the standard, well-known $j$-parametrization, noting that, if we let

$$E = E\left(\frac{-3J}{(J-1728)}, \frac{-2J}{(J-1728)}\right)$$

(where this is defined and non-singular) then $j(E) = J$.

# Bibliography

[29] M. A. Bennett. Effective measures of irrationality for certain algebraic numbers. *J. Austral. Math. Soc. Ser. A*, 62(3):329–344, 1997.

[30] M. A. Bennett and P. Ingram. Torsion subgroups of elliptic curves in short Weierstrass form. *Trans. Amer. Math. Soc.*, 357(8):3325–3337 (electronic), 2005.

[31] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[32] S. Kamienny. Torsion points on elliptic curves. *Bull. Amer. Math. Soc. (N.S.)*, 23(2):371–373, 1990.

[33] A. Y. Khinchin. *Continued Fractions*. Dover Publications, New York, 1964.

[34] D. S. Kubert. Universal bounds on the torsion of elliptic curves. *Proc. London Math. Soc. (3)*, 33(2):193–237, 1976.

[35] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.

[36] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[37] J. Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. A-B*, 273:A238–A241, 1971.

[38] M. Wieczorek. Torsion points on certain families of elliptic curves. *Canad. Math. Bull.*, 46(1):157–160, 2003.

# Chapter 4

# Elliptic divisibility sequences over certain curves

## 4.1 Introduction

In a recent work, Everest, Mclaren, and Ward [41] consider the following problem, suggested by Silverman [44] : let $E/\mathbb{Q}$ be an elliptic curve, $P \in E(\mathbb{Q})$ be a point of infinite order, and define a sequence of integers $\{B_n\}_{n\geqslant 1}$ by

$$nP = \left(\frac{A_n}{B_n}, \cdot\right),$$

in lowest terms (taking, without loss of generality, $B_n > 0$). The sequence, denoted $B(E,P)$, satisfies the condition that $n \mid m$ implies $B_n \mid B_m$, that is, it is a divisibility sequence. Can one derive results analogous to those that Zsigmondy [45] and Bilu-Hanrot-Voutier [39] prove for other classes of divisibility sequences? That is, if we define the Zsigmondy bound of an arbitrary divisibility sequence $\{A_n\}_{n\geqslant 1}$ to be

$$Z(\{A_n\}) = \sup\{m : A_m \text{ has no primitive divisor}\},$$

where a primitive divisor of $A_m$ is a prime divisor that doesn't divide $A_n$ for any $n < m$, can we bound $Z(B(E,P))$?

It is a result of Silverman, [44], that $Z(B(E,P))$ is always finite, but the proof relies on Siegel's Theorem and is, as such, ineffective. Indeed, if one allows non-minimal models of elliptic curves, $Z(B(E,P))$ can be made arbitrarily large in the same way that one constructs elliptic curves with arbitrarily many integer points. There are, however, some results along these lines due to Everest, Mclaren, and Ward [41]. In particular, for divisibility

[3] A version of this chapter has been submitted for publication. Ingram, P. *Elliptic divisibility sequences over certain curves.*

sequences associated with the congruent number curves

$$E_N : y^2 = x^3 - N^2 x,$$

it is shown (Theorem 2.2 of [41]) that if $B_n$ has no primitive divisor and $n$ is even, then $n \leqslant 18$ (note the lack of dependence on $N$), while under certain additional restrictions on $P$, $n \leqslant 21$ independent of parity. By considering certain Thue equations arising from the division polynomials of the elliptic curves in question, we improve their result to the following :

**Theorem 4.1.** *Let $N$ be square free, and $P$ a point of infinite order on the congruent number curve $y^2 = x^3 - N^2 x$, and suppose that $B_n(E, P)$ has no primitive divisor. Then $2 \nmid n$ unless $n = 2$, and $5 \nmid n$. Furthermore, if one of the following conditions holds, $n \leqslant 2$ or[1] $n = 11$ :*

1. *$P = 2Q$ for some $Q \in E(\mathbb{Q})$,*
2. *$x(P) < 0$, or*
3. *$x(P)$ is a rational square.*

To see the deficit in this result, one need look no further than the point $(12, 36)$ on the curve $y^2 = x^3 - 36x$, which fails to meet any of the three conditions in the theorem.

Note that Theorem 2.2 of [41] shows that if $2 \mid n$, then $n \leqslant 18$, while conditions (2) and (3) respectively ensure that $n \leqslant 5$ and $n \leqslant 21$ respectively for $n$ odd (and, of course, condition (1) implies that $n \leqslant 9$ immediately, by applying Theorem 2.2 to $B(E, Q)$). It is interesting to note that, while the authors of [41] treat case (3) directly, the hypothesis that one of $\{x(P), x(P) + N, x(P) - N\}$ is a square ensures that $P = 2Q$ for $Q$ a point on $E$ over some quadratic field. In this case, Everest, Mclaren, and Ward's proof may be extended to said quadratic field to give a slightly sharper bound, but there seems, in light of Theorem 4.1, little reason to present that proof. It also seems unlikely that this technique can be extended to quartic fields, which would produce the chief desideratum : a uniform bound on $Z(B(E_N, P))$. Many terms in [41] are estimated quite generously, and it is useful to note that a more careful analysis of this work does show that in this last case, $n \leqslant 15$.

Theorem 4.1 follows from a more general result by carrying out some reasonably straightforward, but nonetheless nontrivial computations.

[1]For an improved result, see Chapter 6.

**Theorem 4.2.** *Let $S$ be a finite set of primes. Then the set of pairs $(E, P)$ where*

- *$E/\mathbb{Q}$ is a minimal model of an elliptic curve with $j(E) \in \{0, 1728\}$;*
- *$P \in E(\mathbb{Q})$ is a point of infinite order; and*
- *$B_n = B_n(E, P)$ fails to have a primitive divisor, where $n \geqslant 5$ is a product of primes in $S$*

*is finite and effectively computable.*

The additional claim in Theorem 4.1, that $B_{5m}$ has a primitive divisor for all $m$, is proved using techniques similar to those in [41], but exploiting the 5-isogeny on curves with $j = 1728$. In any case where such an isogeny exists, similar results may be derived.

One finds, in the literature, a startling dearth of examples of sequences in which terms beyond the first fail to have primitive divisors. To provide the reader with some reason to believe that these exist, we display two families of examples. First, apropos of Theorem 4.1, note the points

$$P = \left(\frac{T(T^3 - 16T)}{4}, \frac{(T^3 - 16T)^2}{8}\right)$$
$$2P = \left(\frac{(T^2 + 16)^2}{16}, \frac{(T^2 + 16)(T^2 + 8T - 16)(T^2 - 8T - 16)}{64}\right)$$

on the curve $y^2 = x^3 - (T^3 - 16T)^2 x$. As $(T^3 - 16T)$ is square free infinitely often (see Mirsky [42]), this provides infinitely many examples witnessing the sharpness of Theorem 4.1.

In general, we may show that there exist infinitely many (non-trivial) elliptic divisibility sequences with $Z(B(E, P)) \geqslant 3$ by considering the equation

$$3(0, T) = \left(8T^2(8T^4 + 1), T(512T^8 + 96T^4 + 3)\right)$$

on the curve $y^2 = x^3 + x + T^2$. Notice, though, that none of these curves have $j$-invariant 0 or 1728 (for $T > 0$).

## 4.2 Curves of the form $y^2 = x^3 + B$

The proof of Theorem 4.2 is broken down into the two obvious cases. Although the general technique is the same for all curves under consideration, the details differ slightly.

We will compute, for fixed square free $n \geqslant 5$, all (sixth-power free) $B$ and rational points of infinite order $P$ on $E : y^2 = x^3 + B$ such that $B_n(E, P)$ has no primitive divisor. Note that, for arbitrary $n$, if $B_n(E_N, P)$ has no primitive divisor, then neither does $B_r(E_N, \frac{n}{r}P)$, where $r = \mathrm{rad}(n)$. In each example below there turn out to be no such examples, and so it suffices to show this for $n$ square free (except in the cases where $\mathrm{rad}(n) \leqslant 4$, which we discuss below). In general, for fixed $N$ and $n$, [41] bounds $\hat{h}(P)$ such that $B_n(E_N, P)$ has no primitive divisor. Thus, once we have found all cases wherein $B_{\mathrm{rad}(n)}(E_N, P)$ has no primitive divisor, it is a simple search to find any points of which a given $P$ is a multiple (this requires a lower bound on the canonical heights of rational points on a given curve, which is known for curves of these forms).

We must also consider the case where $n$ is a power of two or three. By the same argument as above, it suffices to show that $B_9$ is divisible by some prime not dividing $B_3$ and that $B_8$ is divisible by some prime not dividing $B_4$. these proofs follow the exact same schema as those below. Indeed, when $j(E) = 1728$ we may show that $B_4$ always has a primitive divisor, and when $E$ is a congruent number curve, that $B_3$ does as well.

For arbitrary $n$, we define the polynomials $\psi_m$, $\varphi_m$, and $\omega_m \in \mathbb{Z}[x, y, B]$ as in [43] by

$$\begin{gathered}
\psi_1 = 1, \qquad \psi_2 = 2y \\
\psi_3 = 3x^4 + 12Bx \\
\psi_4 = 4y(x^6 + 20Bx^3 - 8B^2) \\
\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \\
2y\psi_{2m} = \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \\
\varphi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1} \\
4y\omega_m = \psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2,
\end{gathered}$$

so that

$$[m]\,(x, y) = \left(\frac{\varphi_m}{\psi_m^2}, \frac{\omega_m}{\psi_m^3}\right).$$

Note, in fact, that under the relation $y^2 = x^3 + B$, $\psi_m \in \mathbb{Z}[x, B]$ for $m$ odd and $\psi_m \in y\mathbb{Z}[x, B]$ for $m$ even. Note also, either by induction or the relation

$$\psi_m^2 = m^2 \prod_{P \in E[m]} (x - x(P))$$

that for $m$ odd (respectively, even), $\psi_m$ (respectively, $\psi_m/y$) is a binary form in $x^3$ and $B$ of degree $\frac{1}{6}(m^2 - 1)$ (respectively $\frac{1}{6}(m^2 - 4)$), and we will refer to them as such. Indeed, $\psi_m^2$ can always be written as a binary form in $x^3$ and $B$ (of degree $\frac{1}{6}(m^2 - 1)$, and we will abuse notation by denoting this $\psi_m^2(x^3, B)$. Finally, note that, again by the above relation,

$$\mathrm{lcm}_{l|m} \psi_{m/l} \mid \psi_m,$$

where the product is taken over primes. In light of this, we will define

$$\Psi_m(x^3, B) = \psi_m \left(\mathrm{lcm}_{l|m,\ l \neq m} \psi_{m/l}\right)^{-1},$$

making $\Psi_m$ a binary form in $x^3$ and $B$ with integer coefficients (independent of $B$).

**Lemma 4.3.** *Let $n \geqslant 5$ be square free, and suppose that $B_n(E, P)$ has no primitive divisor. Then if $x(P) = a/b^2$, and $X = a^3/(a^3, B)$, $Y = Bb^6/(a^3, B)$, we have*

$$\Psi_n(X, Y) = \pm 2^\alpha 3^\beta \prod_{l|n} l^{\varepsilon(l)},$$

*where $\alpha \leqslant 8d$, $\beta \leqslant 15d/2$, and $\varepsilon(l) \leqslant 6d + 1$, $d = \frac{1}{6}n^2(n^2 - 1)$.*

Note that, under the conditions that $B$ be sixth-power free, $(a, b) = 1$, and $a^3 + Bb^6 = c^2$ for some $c \in \mathbb{Z}$, we may recover a unique pair $a/b^2$, $B$ from each solution $X, Y$ to the above. Thus the above lemma injects the examples of sequences in which the $n$th term fails to have a primitive divisor into the set of solutions to a family of Thue equations, finite as $\deg(\Psi_n) \geqslant 3$ for $n \geqslant 5$.

Note also that solutions wherein $XY = 0$ may be ignored. Clearly, $B = 0$ yields a singular curve, while $X = 0$ gives rise to $P$ a point of order three on $y^2 = x^3 + B$.

*Proof.* We will make use of the following observations:

**Claim 4.4.** *(For $n \geqslant 5$ square free)*

1. *The resultant of $\varphi_n$ and $\psi_n^2$ in $\mathbb{Z}[B]$ is $(432B^2)^d$, where $d = \frac{1}{6}n^2(n^2-1)$.*
2. *$\Psi_n(1,-1) = \pm 3^{(n^2-1)/4}$ for $n$ odd, $\pm 3^{(n^2-4)/4}n$ for $n$ even.*
3. *If $n$ is prime then $\Psi_n(1,0) = n$. Otherwise, $\Psi_n(1,0) = 1$.*

*Proof.* By induction on $n$ (in general, the assumption that $n$ is square free is superfluous). □

Now, suppose that $P$ and $B$ are as in the statement of the lemma, with $x(P) = a/b^2$. We have

$$x(nP) = \frac{\varphi_n}{\psi_n^2} = \frac{b^{2n^2}\varphi_n}{b^{2n^2}\psi_n^2}.$$

Note that the numerator and denominator of the last term are both integers, and so $B_n g^2 = b^2\psi_n^2(a^3, Bb^6)$, where $g^2$ is the greatest common divisor of the aforementioned numerator and denominator (necessarily a square). Note that, by the claim, $g$ divides $(432B^2)^{d/2}$. Thus, primes dividing $\Psi_n(a^3, Bb^6)$ must also divide $6Bb$. Our aim is to show that, in fact, the only primes dividing $\Psi_n(a^3, Bb^6)$ are 2, 3, and the divisors of $n$, and that each may occur only to certain powers.

Let $l \nmid 6n$ be a prime. Note that, if $l \mid b$, then $l \nmid a$, and so

$$l \nmid \Psi_n(a^3, Bb^6) \equiv n^* a^{3\deg(\Psi_n)} \pmod{l},$$

where

$$n^* = \begin{cases} n & \text{if } n \text{ is prime} \\ 1 & \text{otherwise.} \end{cases}$$

Thus, if $l \mid \Psi_n(a^3, Bb^6)$, we have $l \mid B$ and $l \nmid b$. If $\mathrm{ord}_l(a^3) \neq \mathrm{ord}_l(B)$, then $l \nmid \Psi_n(X, Y)$, where $X = a^3/(a^3, B)$, $Y = Bb^6/(a^3, B)$ as above (because precisely one of $X$ and $Y$ is divisible by $l$). But suppose that $\mathrm{ord}_l(a^3) = \mathrm{ord}_l(B)$. As $B$ is sixth-power free (and, by hypothesis, $\mathrm{ord}_l(B) > 0$), this means that $\mathrm{ord}_l(a^3) = \mathrm{ord}_l(B) = 3$. But $\mathrm{ord}_l(a^3 + Bb^6)$ is even, and so $X \equiv -Y \not\equiv 0 \pmod{l}$. It follows that

$$\Psi_n(X, Y) \equiv X^{\deg(\Psi_n)}\Psi_n(1,-1) \pmod{l}.$$

By the claim, the right-hand side of the above is not divisible by $l$. We have, now, that the only primes possibly dividing $\Psi_p(X,Y)$ are 2, 3, and those dividing $n$. It remains to consider the power to which they might occur.

Since $\mathrm{ord}_l(B_n) = \mathrm{ord}_l(B_1) + 2\mathrm{ord}_l(n)$ for all $l \mid B_1$ (see, e.g., [41] or [43]), we have that

$$\Psi_n(a^6, Bb^6) \mid (432B^2)^{d/2} n, \tag{4.1}$$

where $d = \frac{1}{6}n^2(n^2-1)$ as above. If $l \mid B$ is a prime (at least five) not dividing $n$, the argument above shows that $l \not| \Psi_n(X,Y)$. As $B$ is sixth-power free, then, its contribution in (4.1) divides $(6n)^6$, yielding

$$\Psi_n(X,Y) \mid 2^{8d} 3^{15d/2} n^{6d+1},$$

which was what was wanted. □

In fact, we may do much better than the above rough estimate in special cases. Note that the above argument, in the case where $n$ is odd and hence $\Psi_n(1,-1)$ is a power of three, in fact shows that primes $l > 5$ may divide $\Psi_n(X,Y)$ to at most the first power. A more careful analysis also shows exactly which powers of 2 and 3 may occur in values of $\Psi_n(X,Y)$, which we see below simplifies the computations in some cases.

**Example.** There are no sequences arising from curves with $j = 0$ wherein the $5^\alpha$th or $7^\alpha$th term has no primitive divisor, $\alpha > 0$.

*Proof.* One notes that, for $n = 5^\alpha$, such an example must come from a solution to

$$\Psi_5(X,Y) = 5X^4 + 326X^3Y - 708X^2Y^2 - 2616XY^3 - 256Y^4 = \pm 2^\alpha 3^\beta 5^\varepsilon,$$

with $\alpha$, $\beta$, and $\varepsilon$ bounded. Indeed, a careful examination of this form shows that $\alpha \in \{0, 6, 8\}$ while a comparison of $\psi_5$ and $\varphi_5$ show that not both may be divisible by 3 (and so $\beta = 0$). By the remarks above, $\varepsilon \in \{0, 1\}$. At this point we may take the remaining equations to PARI and see that none admits (nontrivial) solution.

For $n = 7^\alpha$, such a sequence must come from a solution to $\Psi_7(X,Y) = \pm 2^\alpha 3^\beta 7^\varepsilon$. This, factoring $\Psi_7$, yields a simultaneous solution to

$$X^6 + 564X^5Y - 5808X^4Y^2 - 123136X^3Y^3 - 189696X^2Y^4 \\ - 49152XY^5 + 4096Y^6 = \pm 2^{\alpha_1} 3^{\beta_1} 7^{\varepsilon_1}$$

and

$$7X^2 - 4XY + 16Y^2 = \pm 2^{\alpha_2} 3^{\beta_2} 7^{\varepsilon_2}$$

where, after some consideration of these forms modulo 2 and 3, we must have $\alpha_1 \in \{0, 6, 12\}$, $\beta_1 \in \{0, 6\}$, $\alpha_2 \in \{0, 2, 4\}$, $\beta_2 \in \{0, 2, 3\}$, and $\varepsilon_1 + \varepsilon_2 \leqslant 1$. Solving these systems of equations is a straightforward, if somewhat tedious, exercise, yielding only the trivial solutions. □

## 4.3 Curves of the form $y^2 = x^3 + Ax$

The proofs here are very similar. The division polynomials, defined by the same recursion as above with

$$\psi_3 = 3x^4 + 6Ax^2 - A^2$$
$$\psi_4 = 4y(x^6 + 5Ax^4 - 5A^2x^2 - A^3),$$

are now, after squaring, forms in $x^2$ and $A$. Note, also, that in this case $\Psi_4(X, Y)$ has degree 3, and so we may reduce the hypothesis of the Theorem to $n \geqslant 4$ (if we restrict ourselves to curves with $j \neq 1728$).

**Claim 4.5.** *(For $n$ square free)*

1. *For all $m$, the resultant of $\varphi_m$ and $\psi_m^2$ in $\mathbb{Z}[A]$ is $(4A)^{d(n)}$, where $d = \frac{1}{2}n^2(n^2 - 1)$.*
2. *$\Psi_n(1, -1) = \pm 2^{\deg(\Psi_n)}$ for $n$ odd and $\pm 2^{\deg(\Psi_n)-1} n$ for $n$ even.*
3. *If $n$ is prime then $\Psi_n(1, 0) = n$. Otherwise, $\Psi_n(1, 0) = 1$.*

**Lemma 4.6.** *Let $n \geqslant 5$ be square free, and suppose that $B_n(E, P)$ has no primitive divisor. Then if $x(P) = a/b^2$, and $X = a^2/(a^2, A)$, $Y = Ab^4/(a^2, A)$, we have*

$$\Psi_n(X, Y) = \pm 2^{\alpha} \prod_{l|n} l^{\varepsilon(l)},$$

*where $\alpha \leqslant 3d$ and $\varepsilon(l) \leqslant 2d + 1$, $d = \frac{1}{4}n^2(n^2 - 1)$.*

*Proof.* Follows from the claim above in an identical manner. □

**Example.** There are no sequences $B(E, P)$, $j(E) = 1728$, in which the $p^k$th term has no primitive divisor, where $k \geqslant 1$ and $p \in \{5, 7, 13, 17\}$.

Note that solutions $(X, Y)$ to the Thue equations for which $XY = 0$ or $X = -Y$ correspond to torsion points or singular curves, and so may be disregarded. Also note that, as above, it suffices to consider the cases wherein $k = 1$.

For $p = 5$, we see that such a sequence would correspond to a solution to

$$\Psi_5(X,Y) = (Y^2+2YX+5X^2)(Y^4-52Y^3X-26X^2Y^2+12X^3Y+X^4) = \pm 2^\alpha 5^\varepsilon$$

for $\varepsilon \in \{0,1\}$ and $\alpha \in \{0,6,9\}$. Noting that

$$Y^2 + 2YX + 5X^2 = (Y+X)^2 + (2X)^2 \geqslant \min\{(Y+X)^2, (2X)^2\},$$

one might conduct a simple search for nontrivial solutions. There are none.

In the case $p = 7$, a careful analysis shows that we are in fact solving

$$\Psi_7(X,Y) = \pm 2^\alpha 7^\varepsilon,$$

where $\varepsilon \in \{0,1\}$ and $\alpha \in \{0,12,18\}$. Solving this in PARI yields no non-trivial solutions.

For $n = 13$, we see that

$$\Psi_{13}(X,Y) = \pm 2^\alpha 13^\varepsilon$$

for $\alpha \in \{0,42,63\}$ and $\varepsilon \in \{0,1\}$, which in turn yields (by factoring $\Psi_{13}$) a simultaneous solution to

$$-26X^5Y+39Y^2X^4+228X^3Y^3+235Y^4X^2+22Y^5X+13X^6+Y^6 = \pm 2^{\alpha_1} 13^{\varepsilon_1}$$

and

$$F(X,Y) = \pm 2^{\alpha_2} 13^{\varepsilon_2}$$

for a form $F$ of degree 36, where $\alpha_1 \in \{0,6,9\}$, $\alpha_2 \in \{0,36,54\}$, and $\varepsilon_1+\varepsilon_2 \leqslant 1$. Solving the various systems of equations requires only basic algebra and yields no non-trivial solutions.

$\Psi_{17}(X,Y)$ factors as well and, again, we see that there are no solutions (beyond the trivial ones).

## 4.4 Congruent number curves

We return to the special case of curves of the form

$$E_n : y^2 = x^3 - N^2 x,$$

with $N$ square free, the congruent number curves. This is, of course, a special case of the material presented in Section 4.3. Lemma 4.8 and the following computation, based on Lemma 4.6, complete the proof of Theorem 4.1.

**Lemma 4.7.** *Let $N$ be square free, $P \in E_N(\mathbb{Q})$ be a point of infinite order, and*

$$n \in \{2^\alpha, 2^\beta 3^\gamma, 2^\beta 5^\gamma, 2^\beta 7^\gamma, 3^\beta 5^\gamma, 13^\gamma : \alpha \geqslant 2, \beta \geqslant 0, \gamma \geqslant 1\}.$$

*Then $B_n$ has a primitive divisor. Assuming GRH, if $n = 11^\alpha$, $\alpha \geqslant 1$, then $B_n$ has a primitive divisor.*

*Proof.* We proceed case by case. Note that it suffices to consider $n$ square free (except to treat powers of two, where we must consider $n = 4$). In light of the computations in the previous section, it suffices to consider

$$n \in \{3, 4, 6, 10, 11, 14, 15\}.$$

Let $n = 4$. In this case $B_4 \mid 4B_2$. If $x(P) = a/b^2$, we have, by computing the relevant division polynomials, that

$$\frac{\psi_4}{\psi_2} = 2\left(a^2 + N^2b^4\right)\left(a^2 + 2aNb^2 - N^2b^4\right)\left(a^2 - 2aNb^2 - N^2b^4\right) \mid 2^\alpha N^\beta$$

for some $\alpha, \beta$. Setting $X = a/(a, N)$ and $Y = Nb^2/(a, N)$ we have, as above,

$$\left(X^2 + Y^2\right)\left(X^2 + 2XY - Y^2\right)\left(X^2 - 2XY - Y^2\right) = \pm 2^\beta$$

for $\beta \in \{0, 3\}$. It is simple enough to enumerate the solutions to $X^2 + Y^2 \leqslant 8$, and we see that there are no non-trivial ones (note that trivial solutions here are ones with $XY = 0$ or $X = \pm Y$. These correspond to torsion points). Alternately, we might note that the second two terms must be equal, whence $4XY = 0$.

Let $n = 3$. Let $x(P) = a/b^2 = a/B_1$ with $(a, b) = 1$, so that

$$B_3 = B_1(3a^4 - 6a^2N^2b^4 - b^8)^2/g$$

with $g \mid 2^i N^j$. As we have seen above, this implies

$$3X^4 - 6X^2Y^2 - Y^4 = \pm 2^\alpha 3^\varepsilon$$

where $\varepsilon \in \{0, 1\}$, $\alpha \in \{0, 2\}$, $X = a/k$, and $Y = Nb^2/k$, $k$ as above. Using PARI, we see that the only solutions to the above have $XY = 0$, or $X = \pm Y$.

Suppose $n = 6$ and that $B_n$ has no primitive divisors. Then, by the above,

$$\Psi_6(X,Y) = \frac{\psi_6}{\psi_2\psi_3} = (-3Y^4 + 6Y^2X^2 + X^4)F_6(X,Y)F_6(-X,Y) = \pm 2^\alpha 3^\varepsilon.$$

where

$$F_6(X,Y) = Y^4 - 4Y^3X - 6Y^2X^2 - 4YX^3 + X^4$$

with $\alpha \in \{0,6\}$ and $\varepsilon \in \{0,1\}$. Note that for 3 to divide $\Psi_6(X,Y)$, we must have $3 \mid X$, and that the value of the form is even if and only if $X \equiv Y \equiv 1 \pmod 2$. The various cases all result in $F_6(X,Y) = F_6(-X,Y)$, and so

$$8XY(X^2 + Y^2) = 0.$$

There are only the trivial solutions.

Now let $n = 10$. Just as above,

$$\Psi_{10}(X,Y) = \frac{\psi_{10}}{\psi_2\psi_5} = \pm 2^\alpha 5^\varepsilon$$

where $\varepsilon \in \{0,1\}$, $\alpha \in \{0,18\}$, and

$$\frac{\psi_{10}}{\psi_2\psi_5} = (5Y^4 - 2Y^2X^2 + X^4)(Y^8 - 12Y^6X^2 - 26Y^4X^4 + 52X^6Y^2 + X^8)$$
$$F_{10,1}(X,Y)F_{10,1}(-X,Y)F_{10,2}(X,Y)F_{10,2}(-X,Y).$$

where

$$F_{10,1}(X,Y) = Y^4 + 4Y^3X + 10Y^2X^2 + 4YX^3 + X^4$$

and

$$F_{10,2}(X,Y) = Y^8 + 16Y^7X + 20Y^6X^2 - 16Y^5X^3 - 26Y^4X^4 - 16Y^3X^5 + 20X^6Y^2 + 16YX^7 + X^8.$$

Note that the various cases always result in $F_{10,1}(X,Y) = F_{10,1}(-X,Y)$, whereupon

$$8XY(X^2 + Y^2) = 0.$$

This has, of course, only the trivial solutions.

Consider $n = 14$. This yields the Thue equation

$$\Psi_{14}(X,Y) = \frac{\psi_{14}}{\psi_2\psi_7} = \pm 2^\alpha 7^\varepsilon$$

for $\varepsilon \in \{0,1\}$ and $\alpha \in \{0,36\}$, with

$$\frac{\psi_{14}}{\psi_2\psi_7} = (-7Y^{24} + 308Y^{22}X^2 + 2954X^4Y^{20} - 19852X^6Y^{18} + 35231X^8Y^{16} - 82264X^{10}Y^{14} + 111916X^{12}Y^{12} - 42168X^{14}Y^{10} - 15673X^{16}Y^8 + 14756X^{18}Y^6 - 1302X^{20}Y^4 + 196X^{22}Y^2 + X^{24})F_{14}(X,Y)F_{14}(-X,Y)$$

Where

$$F_{14}(X,Y) = X^{24} + Y^{24} - 116Y^{22}X^2 + 2562X^4Y^{20} - 4004X^6Y^{18} + 29423X^8Y^{16} - 64488X^{10}Y^{14} + 60956X^{12}Y^{12} - 64488X^{14}Y^{10} + 29423X^{16}Y^8 - 4004X^{18}Y^6 + 2562X^{20}Y^4 - 116X^{22}Y^2 + 16776Y^7X^{17} + 2072X^{19}Y^5 - 456X^{21}Y^3 - 24Y^{23}X - 24X^{23}Y - 55792Y^{15}X^9 + 29232Y^{13}X^{11} + 29232Y^{11}X^{13} - 55792Y^9X^{15} + 16776Y^{17}X^7 + 2072Y^{19}X^5 - 456Y^{21}X^3.$$

In all cases we have $F_{14}(X,Y) = F_{14}(-X,Y)$, and thus

$$F_{14}(X,Y) - F_{14}(-X,Y) = 16YX(Y^2+X^2)(-3Y^4+6Y^2X^2+X^4)(-Y^2+2YX+X^2)(-Y^2-2YX+X^2)(3X^4-6Y^2X^2-Y^4)(Y^8+20Y^6X^2-26Y^4X^4+20X^6Y^2+X^8) = 0$$

As the factors above are all irreducible, we see that there are only the trivial solutions.

Finally, $n = 15$. In this case, one agains sees that the division polynomials factors, and comparing the two factors shows that there are no non-trivial solutions. □

**Remark.** The form $\Psi_{11}(X,Y)$ is of degree 30, and so finding all ways of representing a small integer by this form involves a nontrivial amount of computation. Considering $\Psi_{11}$ modulo several small primes shows that any sequence wherein the 11th term fails to have a primitive divisor corresponds to a solution to

$$\Psi_{11}(X,Y) = (-1)^{\alpha+1}2^{\alpha}$$

where $\alpha \in \{0,30,45\}$. Although the computation of all solutions to this is incomplete at this time, an initial computation assuming the Generalized Riemann Hypothesis shows that none exist.

**Lemma 4.8.** *Let $N$ be square free, $P \in E_N(\mathbb{Q})$ be a point of infinite order, and $B = B(E_N, P)$. Then for all $m$, $B_{5m}$ has a primitive divisor.*

*Proof.* Factoring $\psi_5$, one sees through elementary calculus that

$$\log|B_{5m}| = \log|b^{50}\psi_5(a/b^2)^2/g| \geqslant 9h(a/b^2) - 9\log N - 2\log 5 - \log g$$

where

$$g = \gcd(b^{50}\varphi_5(a/b^2), b^{50}\psi_5(a/b^2)^2)$$

and $x(mP) = a/b^2$. Comparing powers of various primes in the above (and considering resultants) shows that $g \mid 2^{12}N^{25}$, whence

$$\log|B_{5m}| \geqslant 9\hat{h}(mP) - 43\log N - 14.6597$$

using the bounds on the difference between naïve and canonical height given in [40]. Under the assumption that $B_{5m}$ has no primitive divisor, the above and (9) of [41] combine to yield $n = 5m \leqslant 33$. All such $n$ are considered in Lemma 4.7 except for $n = 30$ which is dealt with by Theorem 2.2 of [41]. □

## 4.5 Some special cases

Although there are examples of elliptic divisibility sequences over congruent number curves in which the second term has no primitive divisor, we may, in certain cases, restrict $Z(B(E,P))$ further. Combining the lemma below with Theorem 4.1 yields the best possible Zsigmondy bound for the appropriate family of elliptic divisibility sequence (in light of the fact that infinitely many of these sequences start at a integral point).

**Lemma 4.9.** *Suppose $p > 5$ is prime, $P \in E_p(\mathbb{Q})$,*

$$E_p : y^2 = x^3 - p^2x,$$

*and $B = B(E_p, P)$. Then for all $n$, $B_{2n}$ has a prime divisor which doesn't divide $B_n$.*

*Proof.* Suppose not, and let $x(nP) = a/b^2$ (so that $B_n = b^2$). If $B_{2n}$ is divisible only by primes which divide $b$, we have from the above that $4ab^2(a^2 - p^2b^4) \mid 2^3p^4s$, where $s$ is a product of (powers of) primes dividing $b$. Thus $a(a^2 - p^2b^4) \mid 2p^4s_2$, for $s_2$ also a product of primes dividing $b$. Note that

if $l \mid b$ is a prime, $l$ cannot divide $a(a^2 - p^2b^4)$ as $(a, b) = 1$, so we have $a(a^2 - p^2b^4) \mid 2p^4$ (with the left-hand side even only if $b$ isn't). Now, if $p$ is a divisor of $a$, then

$$\left(\frac{a}{p}\right)\left(\left(\frac{a}{p}\right)^2 - b^4\right) \Bigg| 2p,$$

while otherwise

$$a\left(a^2 - p^2b^4\right) \mid 2.$$

The second case yields three possibilities:

$$\begin{aligned} 1 - p^2b^2 &= \pm 1 \\ 1 - p^2b^4 &= \pm 2 \\ 4 - p^2b^4 &= \pm 1, \end{aligned}$$

which one can check admit no solution. Considering the first case similarly, one sees that this condition ensures that $p = 3, 5$. □

**Remark.** Similar results can be shown for curves of the form $y^2 = x^3 \pm p^\alpha$ and $y^2 = x^3 \pm p^\beta x$, where $\alpha \leqslant 6$ and $\beta \leqslant 4$.

# Bibliography

[39] Yu. Bilu, G. Hanrot, and P. M. Voutier. Existence of primitive divisors of Lucas and Lehmer numbers. *J. Reine Angew. Math.*, 539, 2001. With an appendix by M. Mignotte.

[40] A. Bremner, J. H. Silverman, and N. Tzanakis. Integral points in arithmetic progression on $y^2 = x(x^2 - n^2)$. *J. Number Theory*, 80, 2000.

[41] G. Everest, G. Mclaren, and T. Ward. Primitive divisors of elliptic divisibility sequences. preprint, 2005.

[42] L. Mirsky. Note on an asymptotic formula connected with $r$-free integers. *Quart. J. Math., Oxford Ser.*, 18.

[43] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[44] J. H. Silverman. Wieferich's criterion and the *abc*-conjecture. *J. Number Theory*, 30, 1988.

[45] K. Zsigmondy. Zur theorie der potenzreste. *Monatshefte für Mathematik*, 3, 1892.

# Chapter 5

# On $k$th-power Numerical Centres

## 5.1 Two results

We will call an integer $N$ a $k$th power numerical centre for $n$ if

$$1^k + 2^k + \cdots + N^k = N^k + (N+1)^k + \cdots + n^k. \tag{5.1}$$

This equation is trivial in the case $k = 0$, while the solutions to the problem in the case $k = 1$ correspond to the solutions of the Pell equation $X^2 - 2Y^2 = 1$, with $X = 2n + 1$, $Y = 2N$. In [49] and [53] the cases with $k = 2, 3$ were treated, and it was shown that the only solutions to (5.1) were the trivial ones, i.e., those with $(N, n) \in \{(0, 0), (1, 1)\}$. We will prove the following:

**Proposition 5.1.** *For fixed $k > 1$, equation (5.1) has only finitely many solutions. In particular, for $k = 5$ there are only the trivial solutions.*

Equation (5.1) is, of course, equivalent to

$$S_k(N) + S_k(N-1) = S_k(n), \tag{5.2}$$

where

$$S_k(x) = 1^k + 2^k + \cdots + x^k,$$

which may be written in a closed form. For $k$ even the curves defined by (5.2) are smooth and so have genus $\frac{1}{2}k(k-1)$ by a straightforward application of a theorem of Hurwitz (see [51], p. 41). When $k$ is odd, the above admits the change of variables $x = (2n+1)^2, y = (2N)^2$ and the resulting curves are smooth in $x$ and $y$ of degree $\frac{k+1}{2}$, and so have genus $\frac{1}{8}(k-1)(k-3)$. The general claim, then, follows from the celebrated result of Faltings [48]. For

[4] A version of this paper has been accepted for publication. Ingram, P. *On k-th power numerical centres.* Comptes rendus mathématiques de l'Académie des sciences 27:105-110

a more direct proof we apply results of Bilu and Tichy [46] on the number of solutions to the Diophantine equation $f(x) = g(y)$. More specifically, we apply a refinement of this by Rakaczki [50] which applies just in case $f(x) = S_k(x)$.

For the result in the case $k = 5$, we apply the results of David [47], as presented in [55] (see also [54] and [56]). The problem of finding all integral points on the curve (5.1) in the case $k = 5$ reduces to that of locating all integral points on a certain non-Weierstrass model of an elliptic curve. As it turns out, integer points with sufficiently large naïve height on this model correspond to rational points on a Weierstrass model abnormally close to a particular $K$-rational point, for some cubic extension $K/\mathbb{Q}$. Using David's explicit lower bounds on linear forms in elliptic logarithms one may thence obtain a bound on the heights of these points.

We also note how one might go about finding all solutions to (5.1) in the case $k = 4$, although the required computations are daunting.

*Proof of the general claim.* If $g_k(x) := S_k(x) + S_k(x-1) = S_k(y)$ has infinitely many solutions then $g_k$ takes one of the forms presented in [50], and we will preserve the case numbering found in that paper. We note that cases VI and VII in this list require $k = 3$, which is a case dealt with by [53]. We note also that Case V is a special case of Case II. As noted in [50], if $k$ is odd then $S_k(x) = \psi_k((x+1/2)^2)$, for some polynomial $\psi_k$, clearly of degree $\frac{k+1}{2}$.
Case I : $g_k(x) = S_k(q(x))$, where $q(x) \in \mathbb{Q}[x]$ is non-constant. Clearly in this case $\deg(q) = 1$, and so $q(x) = \mu x + \lambda$, $\mu, \lambda \in \mathbb{Q}$. As the leading coefficient of $S_k(x)$ is $\frac{1}{k+1}$, we have

$$S_k(q(x)) = \frac{\mu^{k+1}}{k+1}x^{k+1} + \cdots .$$

On the other hand, the leading coefficient of $g_k(x)$ is $\frac{2}{k+1}$, and so $\mu^{k+1} = 2$, implying $k = 0$.
Case II : $k$ is odd and $g_k(x) = \psi_k(\delta(x)q(x)^2)$, with $\delta(x), q(x) \in \mathbb{Q}[x]$, $\delta$ linear. Here we see, by comparing degrees, that $\delta$ is constant and $q$ linear. Again, the leading coefficient of $\psi_k$ is $\frac{1}{k+1}$, and so the leading coefficient of $\psi(\delta q(x)^2)$ is $\frac{(\delta\mu^2)^{\frac{k+1}{2}}}{k+1}$, where $q(x) = \mu x + \lambda$, $\delta(x) = \delta$. We have then $(\delta\mu^2)^{\frac{k+1}{2}} = 2$, implying $k \leqslant 1$.
Case III : $k$ is odd and $g_k(x) = \psi_k(c\delta(x)^t)$, where $\delta$ is linear, $c \in \mathbb{Q} \setminus \{0\}$, and $t \geqslant 3$ is an odd integer. This is impossible as then $\deg(g_k) = t\left(\frac{k+1}{2}\right) > k+1$.

Case VI : $k$ is odd and $g_k(x) = \psi_k((a\delta(x)^2 + b)q(x)^2)$ where $a, b \in \mathbb{Q} \setminus \{0\}$ and $\delta, q$ are as above. This case, once degrees are compared, reduces to our analysis of Case II. □

*Proof of the specific claim.* It now remains to deal with the case where $k = 5$. This will be resolved using lower bounds on linear forms in elliptic logarithms, as per [47] and [55]. For the solution of the general cubic elliptic diophantine equation see also [54].

In the case $k = 5$, the change of variables $x = (2n+1)^2$, $y = (2N)^2$ yields the elliptic curve

$$x^3 - 5x^2 + 7x - 3 = 2y^3 + 20y^2 - 16y.$$

Note that we are passing from a curve with only finitely many rational points to one with (it turns out) infinitely many. This is, in fact, an improvement of the situation as there are much better tools for finding integer points on a curve like this than for finding the rational points on a genus eight curve. We will, however, find it more convenient to deal with the following model, obtained by a shift of one in the $x$-coordinate, which clearly preserves integrality of points:

$$f(t, v) = t^3 - 2t^2 - 2v^3 - 20v^2 + 16v = 0. \tag{5.3}$$

The transformation

$$X = \frac{-4t - 3v + 8}{v}$$
$$Y = -2\left(\frac{4t^2 - 4t + 10v^2 - t^3 + 2v^3}{v^2}\right)$$

yields a minimal Weierstrass model for (5.3), specifically

$$E : Y^2 = X^3 - X^2 - 41X + 441. \tag{5.4}$$

Our method of proof, following [55], will be to bound some linear form in elliptic logarithms from above, and then from below using the explicit bounds of [47]. We will identify points on the various models of the elliptic curve.

**Claim 5.2.** *On the curve in (5.4),*

$$-8.025 \leqslant \hat{h}(P) - h(P) \leqslant 7.072$$

*Proof.* These are the height bounds presented in [52], although it is worth noting that we are using the definition of height found in [51], which differs from that found in [52] by a factor of two. □

**Claim 5.3.** *The Mordell-Weil group of $E/\mathbb{Q}$ is generated by the points $T = (-9, 0)$ and $P_0 = (1, 20)$, the former having order two, and the latter having infinite order.*

*Proof.* Noting that 7 and 37 are primes of good reduction for $E$, and that $\#E(\mathbb{F}_7) = 8$ and $\#E(\mathbb{F}_{37}) = 46$, we see instantly that the order of torsion for $E/\mathbb{Q}$ divides two. A descent (using MAGMA) shows that the curve has rank at most one. The two points above demonstrate the sharpness of this, and all that remains is to establish that $(1, 20)$ is indivisible. Suppose that $(1, 20) = nR$ or $nR + T$ for some $R \in E(\mathbb{Q})$ and $n \geqslant 2$. Then one sees, through basic computation and height bounds, that $h(R) \leqslant 17.26$, and of course $R$ must be an integer point. Thus $X(R)$ is an integer of modulus at most $3.13 \times 10^7$, and a search of all such points confirms our claim. □

The following claim is a simple computation, performed in Pari/GP.

**Claim 5.4.** *The only solutions to (5.3) with $|t|, |v| \leqslant 10^4$ are*

$$(t, v) \in \{(0, 0), (2, 0), (8, -8), (8, -6), (8, 4)\}.$$

**Claim 5.5.** *Let $P = (t, v) = mP_0 + jT$ be an integer point on (5.3) with $|t|, |v| \geqslant 10^4$. Then*

$$\frac{1}{|v|} \leqslant \exp(9.157 - 0.31m^2).$$

*Proof.* Our first order of business is to bound $h(X(P))$ in terms of $|v|$. By examining (5.3) we see that the condition that $|t|, |v|$ are large implies that $P$ lies quite close to the asymptote $T = \alpha V + \beta$, where $\alpha$ is the real cube root of 2, and $\beta = \frac{10\alpha+2}{3}$. In particular, for $|v| \geqslant 10^4$, $|t - (\alpha v + \beta)| < 0.002$. As $t$ and $v$ are integers, we have

$$\begin{aligned} \hat{h}(P) - 7.072 \leqslant h(X(P)) &\leqslant \log \max\{|8 - 4t - 3v|, |v|\} \\ &\leqslant \log \max\{8 + (4\alpha + 3)v + 4\beta + 0.008, |v|\} \\ &\leqslant \log |(4\alpha + 3.003)v| \leqslant \log |v| + 2.085. \end{aligned}$$

From this we conclude that

$$-\log |v| \leqslant 9.157 - \hat{h}(P) \leqslant 9.157 - 0.31m^2.$$

□

Let $Q_0$ be the limit point of points on (5.4) arising from the asymptote of (5.3), i.e., $X(Q_0) = -4\alpha - 3$. We wish to translate the above into an upper bound on the difference between the elliptic logarithms of $Q_0$ and $P$. Note that as $Q_0$ is defined only over $K = \mathbb{Q}(\alpha)$, we must consider elliptic logs over a number field. First note that

$$\hat{h}(Q_0) \leqslant 10$$

and

$$|u(Q_0)| = 1.52086...,$$
$$|u(P_0)| = 1.11199...,$$

where, as Section 4 of [55], $u$ denotes the elliptic logarithm. We set

$$\mathcal{L} = u(P) - u(Q_0).$$

**Claim 5.6.**

$$|\mathcal{L}| \leqslant \frac{1}{4|v|}.$$

*Proof.* As in [55], we note that

$$|\mathcal{L}| = \left| \int_{v(P)}^{\infty} \frac{dv}{\partial f/\partial t} \right|.$$

One may verify that $|\partial f/\partial t| \geqslant 4v^2$ for $|v| \geqslant 10^4$, from which the above bound follows. □

Now we have

$$u(P) = mu(P_0) + ju(T) + m_0\omega,$$

where $m_0$ is chosen to specify the branch of the log and where $j \in \{0, 1\}$, so

$$|\mathcal{L}| = \left| mu(P) - u(Q_0) + (2m_0 + j)\frac{\omega}{2} \right| \leqslant \exp(7.771 - 0.31m^2).$$

Note that (see [55]) $m_0 \leqslant 2m + 1$, and so if $M$ is the largest coefficient in the linear form, $M \leqslant 4m + 3$.

It remains to determine a lower bound on $|\mathcal{L}|$. In the notation of [47] we have $D = 3$, $\beta_0 = 0, \beta_1 = m, \beta_2 = -1, \beta_3 = 2m_0 + j$. We will be considering

$u_1 = u(P_0), u_2 = u(Q_0), u_3 = u(T)$. So $\gamma_1 = P_0, \gamma_2 = Q_0, \gamma_3 = T$. The conditions on $B, \hat{E}, V_1, ..., V_3$ become (note, our $\hat{E}$ is David's $E$)

$$\begin{gathered} 3\log(B) \geqslant \log(V_1) \geqslant \log(V_2) \geqslant \log(V_3) \\ \log(B) \geqslant \max\{37.425, 4m+3\} \\ \log(V_1) \geqslant \max\{13.76769, 5.7114\} \\ \log(V_2) \geqslant \max\{13.76769, 10.6837\} \\ \log(V_3) \geqslant 13.76769 \\ e \leqslant \hat{E} \leqslant 5.344 \end{gathered}$$

which is obtained by making sharp the inequalities for the $V_i$, $\hat{E} = 5.344$, $B = 4m + 3$ (at least for $m \geqslant 9$). This yields

$$\log|\mathcal{L}| \geqslant 2.891 \times 10^{75}(\log(B) + 2.7747)(\log\log(B) + 16.5424)^4.$$

Combining we obtain the absolute bound

$$|m| \leqslant 10^{42}.$$

Applying the LLL algorithm in a fashion similar to that in Section 5 of [55] we may reduce this bound to 27 at which point the result is easily verified using PARI. One notes that the only integer points on the original curve corresponding to points $nP + jT$ with $|n| \leqslant 27$ are the points $\mathcal{O}, T, P + T, 2P, -P$, corresponding to the points in Claim 3. The only integer points on the original curve arising from these are $(0, 0)$ and $(1, 1)$. □

**Remark.** In the case $k = 4$, one may, by performing the change of variables

$$\begin{gathered} x = \frac{2n+1}{N} \\ y = \frac{48n^5 + 120n^4 + 100n^3 + 30n^2 - 1 - 96N^5 - 80N^3}{N^3}, \end{gathered}$$

reduce the problem of finding rational points on the (in this case genus six) curve defined by (5.1) to that of finding rational points on the hyperelliptic curve

$$y^2 = x^6 - 24x^5 + 400x^3 + 336x + 7936.$$

Unfortunately, this curve isn't easily treated with the methods of Chabauty; the sextic above has Galois group $S_6$, and the method consequently requires computing the Mordell-Weil groups of elliptic curves over number fields of degree 45.

# Bibliography

[46] Yu. F. Bilu and R. F. Tichy. The Diophantine equation $f(x) = g(y)$. *Acta Arith.*, 95, 2000.

[47] S. David. Minorations de formes linéaires de logarithmes elliptiques. *Mém. Soc. Math. France (N.S.)*, (62), 1995.

[48] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[49] R. Finkelstein. The house problem. *Amer. Math. Monthly*, 72, 1965.

[50] Cs. Rakaczki. On the diophantine equation $S_m(x) = g(y)$. *Publ. Math. Debrecen*, 65, 2004.

[51] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[52] J. H. Silverman. The difference between the Weil height and the canonical height on elliptic curves. *Math. Comp.*, 55, 1990.

[53] R. Steiner. On $k$th-power numerical centers. *Fibonacci Quart.*, 16, 1978.

[54] R. J. Stroeker and B. M. M. de Weger. Solving elliptic Diophantine equations: the general cubic case. *Acta Arith.*, 87, 1999.

[55] R. J. Stroeker and N. Tzanakis. Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms. *Acta Arith.*, 67, 1994.

[56] R. J. Stroeker and N. Tzanakis. Computing all integer solutions of a genus 1 equation. *Math. Comp.*, 72, 2003.

# Chapter 6

# Concluding remarks and future directions

In this final installment we explore some further avenues of research.

## 6.1 Approximating rationals by $j(E)$

As noted in the preface and in Chapter 3, the results of Chapter 2 may be viewed as an answer to the question of how closely one might approximate 0 with the $j$-invariant of an elliptic curve with a rational point of a certain order. Similarly, the results of Chapter 3 may be seen as results on how closely one might approximate 1728 with the $j$-invariants of various types of elliptic curves. One might ask about approximating other rational values by $j$-invariants of certain classes of elliptic curves over $\mathbb{Q}$. This problem, as it betides, bears remarkable resemblance to that of approximating algebraic numbers by rationals (although this is perhaps due more the the provenance of our results than any deep correspondence). For the remainder of this thesis, the term 'elliptic curve' is an abreviation for 'elliptic curve in short Weierstrass form with integral coefficients' unless otherwise noted. First, a remark.

**Remark.** Fix an integer $N \geqslant 2$. Then the set

$$\{j(E) : E(\mathbb{Q})_{\text{Tors}} \supseteq \mathbb{Z}/N\mathbb{Z}\}$$

is either empty or dense in $\mathbb{Q}$.

*Proof.* Note, as in the appendix, that there is a rational function $j_N \in \mathbb{Q}(t)$ such that for any field $K$, an elliptic curve $E/K$ is $K$-isomorphic to an elliptic curve with a $K$-rational point of order $N$ if and only if $j(E) = j_N(t)$ for some $t \in K$. As $j_N$ is continuous for each $N$, it suffices to check that the image of $\mathbb{R}$ by $j_N$ is dense in $\mathbb{R}$. But $j_N$ maps $\mathbb{R}$ onto $\mathbb{R}$, as every elliptic curve $E/\mathbb{R}$ contains an $\mathbb{R}$-rational point of order $N$. □

The following result may be extended to cover all possible torsion/isogeny structures over $\mathbb{Q}$ as in Chapter 3. A weakened version is stated here for simplicity of statement and proof.

**Theorem 6.1.** *Let $N \in \{5, 7, 9\}$, and let $r \in \mathbb{Q}$. Then for any $\varepsilon > 0$, there exists a constant $C = C(N, r, \varepsilon)$ such that for all elliptic curves $E/\mathbb{Q}$ with a rational point of order $N$ and $j(E) \neq r$,*

$$|j(E) - r| > C|\Delta(E)|^{-\mu(N,r)-\varepsilon},$$

*where*

$$1/\mu(N, r) = \begin{cases} N - 3 & r = 0 \\ \frac{3}{2}(N-3) & r = 1728 \\ 3(N-3) & \text{otherwise.} \end{cases}$$

*Suppose, further, that $r$ is not the $j$-invariant of an elliptic curve $E/\mathbb{Q}$ with a point of order $N$. Then there are infinitely many elliptic curves $E/\mathbb{Q}$ containing a rational point of order $N$ such that*

$$|j(E) - r| < C'|\Delta(E)|^{-\mu(N,r)},$$

*where $C' = C'(N, r)$ is some explicit constant.*

Compare this with the discussion of Roth's Theorem in Section 1.3. Note that the level structure is completely critical to the result. In general, one might observe that if $r \in \mathbb{Q}$ and $r \neq j(E)$, then

$$|j(E) - r| > |C\Delta(E)|^{-1}, \tag{6.1}$$

where $C$ is the least positive integer with $Cr \in \mathbb{Z}$ (the denominator of $r$). As every rational number is the $j$-invariant of some elliptic curve over $\mathbb{Q}$, this is the best one can do in full generality.

*Sketch of the proof of Theorem 6.1 for $N = 5$.* Let $E_t$ and $j(t)$ be as in the proof above, and write $j(t) = f(t)/g(t)$. We will take $t = p/q$ throughout, $(p, q) = 1$. Note that the discriminant of $f(t) - rg(t)$ in $\mathbb{Z}[r]$ is $5^{13}r^8(r-1728)^6$, and so for $r \neq 0, 1728$, the polynomial $f(t) - rg(t)$ is squarefree. We restrict our attention to this case, as the other two cases are essentially treated in Chapters 2 and 3. Note that $\Delta(E_t) = 6^{12}g(t)$, which has no roots in common with $f(t) - rg(t)$ unless $r = 0$ (a case we're ignoring for now). Note, also, as

in Chapter 2, that if $E$ is an elliptic curve isomorphic over $\mathbb{Q}$ to $E_t$ and with integral coefficients, $|\Delta(E)| \geqslant c_1 q^{12} g(p/q)$ for some constant $c_1$.

There are two cases : If $|\theta - t| > \delta$ for all roots $\theta$ of $f(t) - rg(t)$ and some fixed $\delta > 0$, then $|j(t) - r|$ is bounded below by a constant. By Roth's Theorem there is, for any given $\varepsilon_0$, a constant $c_2 = c_2(\varepsilon_0)$ such that $|\Delta(E)| > c_2 q^{10-\varepsilon_0}$, and we are done.

So suppose $t$ is sufficiently close to some root $\theta$. Again by Roth's Theorem we have

$$|j(t) - r| = \left| \frac{f(t) - rg(t)}{g(t)} \right| > c_2(\varepsilon_0) q^{-2-\varepsilon_0},$$

for some $\varepsilon_0$ to be chosen later. As noted, we may choose

$$\delta = \frac{1}{2} \min\{|\theta - \xi| : g(\xi) = 0 \text{ and } f(\theta) - rg(\theta) = 0\} > 0.$$

Let

$$c_3 = \inf\{|g(t)| : |t - \theta| < \delta \text{ whenever } f(\theta) - rg(\theta) = 0\},$$

so that for all $E$ as in the statement, $|\Delta(E)| \geqslant c_1 c_3 q^{12}$. Then we see that, choosing $\varepsilon_0$ sufficiently small and $c_4$ sufficiently large, we have

$$|j(E) - r| > c_4 |\Delta(E)|^{-\frac{1}{6}-\varepsilon}.$$

□

This result is a more specific, unconditional form of a result of Silverman to appear in [61]. Using effective methods, as in [58], we may always provide effective results in this direction, but the improvements in the exponent in (6.1) will be very small. Notice, though, that (as in Section 3.4), substantial effective improvements on (6.1) are available when $f(t) - rg(t)$, in the notation of the proof, factors. This occurs precisely when there is some elliptic curve $E/K$ with $j(E) = r$ such that $E(K)$ contains a point of order $N$ for some extension $K/\mathbb{Q}$ with Galois group a *proper* subgroup of $(\mathbb{Z}/(N-1)\mathbb{Z})^2$.

## 6.2 More on elliptic divisibility sequences

In Chapter 4 we mentioned a generalisation of Everest, Mclaren, and Ward's [59] methods which apply over quadratic fields. When Chapter 3 was written, this generalisation seemed largely superfluous, but the claims in [59] have

subsequently been relaxed (Chapter 3 has been modified to account for this). In this section we establish a bound for $Z(E_N, P)$ where

$$E_N : y^2 = x^3 - N^2 x,$$

$N$ square free as usual, and $P \in E(\mathbb{Q})$ a point of infinite order with the property that

$$\text{for some } Q \in E(\overline{K}),\ 2Q = P \text{ and } [\mathbb{Q}(x(Q)) : \mathbb{Q}] \leqslant 2. \tag{6.2}$$

Note that in general, every point in $E(\mathbb{Q})$ be may written as twice a point in some extension of $\mathbb{Q}$ with Galois group a subgroup of $(\mathbb{Z}/2\mathbb{Z})^2$ (see, for example, [62]). We note also that a careful examination of doubling points on $E_N$ shows that $P$ has the above property if the set $\{x(P), x(P)-N, x(P)+N\}$ contains a rational square.

The bound on even $n$ such that $B_n$ has no primitive divisor in [59] is obtained by contructing upper and lower bounds on $B_n$ which conflict for sufficiently large $n$. The upper bound, which applies for any $n$ such that $B_n$ has no primitive divisor, is as follows:

**Lemma 6.2.** *If $B_n$ has no primitive divisor, then*

$$\log B_n \leqslant \eta(n) + \rho(n) n^2 \hat{h}(P) + \omega(n)(\log N + 0.347),$$

*where*

$$\eta(n) = \sum_{p|n} 2\log p, \qquad \rho(n) = \sum_{p|n} p^{-2}, \qquad \omega(n) = \sum_{p|n} 1,$$

*all sums taken over primes.*

Note that $\rho(n) < 0.453$, while $\eta(n), \omega(n)$ are of order at most $\log(n)$.

By contrast Everest, Mclaren, and Ward [59] obtain, for $n$ even, the following:

$$\log B_n \geqslant \frac{n^2}{2}\hat{h}(P) - 7\log N - \log(N^2+1) - 1.774.$$

One may derive similar results for $n$ divisible by $p$, where $E$ admits an isogeny of degree $p$, but these are in general much weaker bounds than obtained by an isogeny of degree two (see, for example, the case $p = 5$ in Chapter 4).

We shall prove, using some straightforward analysis of doubling point on $E_N$, that the following holds :

**Lemma 6.3.** *For any $n$, if $P \in E_N(\mathbb{Q})$ satisfies property 6.2, then*

$$\log B_n \geqslant \frac{n^2}{2}\hat{h}(P) - \frac{11}{2}\log N - \frac{1}{4}\log(N^2+1) - 7.7142.$$

Combining Lemma 6.2 with Lemma 6.3 we obtain a bound on $n$ for $N$ fixed. To make this bound uniform we use an explicit statement of Lang's Conjecture for congruent number curves, found in [57]

**Lemma 6.4 (Bremner, Silverman, Tzanakis).** *For all $P \in E_N(\mathbb{Q})$,*

$$\hat{h}(P) \geqslant \frac{1}{8}\log 2N^2.$$

Note that as $E_N(\mathbb{Q})$ is finite for $N \leqslant 5$, we are free to assume $N \geqslant 5$. Combining Lemmas 6.2, 6.3, and 6.4 we obtain

$$n^2 \leqslant \frac{16\left(\eta(n) + \omega(n)(\log N + 0.347) + \frac{11}{2}\log N + \frac{1}{4}\log(N^2+1) + 7.7142\right)}{(1-2\rho(n))\log(2N^2)}.$$

Applying the bounds

$$\eta(n) \leqslant 2\log n, \qquad \omega(n) \leqslant \log n/\log 3, \qquad \rho(n) < 0.203,$$

one see immediately that $n \leqslant 13$, while a more careful case-by-case analysis (with the exact values of $\eta(n)$, $\omega(n)$, and $\rho(n)$) show in fact that the above condition implies $n \leqslant 9$. Thus we obtain the following result, which, in addition to being stronger than Theorem 4.1, does not depend on the Generalised Riemann Hypothesis :

**Theorem 6.5.** *Let $N$ be square free, and $P$ a point of infinite order on the congruent number curve $y^2 = x^3 - N^2x$, and suppose that $B_n(E,P)$ has no primitive divisor. Then $2 \nmid n$ unless $n = 2$, and $5 \nmid n$. Furthermore, if one of the following conditions holds, $n \leqslant 2$ :*

1. *$P = 2Q$ for some $Q \in E(\mathbb{Q})$,*
2. *$x(P) < 0$, or*
3. *$\{x(P), x(P)-N, x(P)+N\}$ contains a rational square.*

The remainder of the section is devoted to the proof of this.

*Proof of Lemma 6.2.* We reproduce the proof in [59] for completeness.

The following claim, from [62], also follows from the discussion of multiplication by $n$ in Chapter 4.

**Claim 6.6.** *For $p$ prime, $p \mid B_n$,*

$$\mathrm{ord}_p(B_{kn}) = \mathrm{ord}_p(B_n) + 2\mathrm{ord}_p(k).$$

From this we may derive that

$$\gcd(B_n, B_m) = B_{\gcd n,m}.$$

Note, then, that if $B_n$ has no primitive divisor, then every prime $l \mid B_n$ must divide $B_{n/p}$ for some prime $p$, and that the order to which $l$ divides $B_n$ is at most $\mathrm{ord}_l(B_{n/l}) + 2$. It follows that $B_n$ divides

$$\prod_{p|n} p^2 B_{n/p},$$

from which Lemma 6.2 follows by taking logs. □

*Proof of Lemma 6.3.* The proof of 6.3 uses techniques similar to those applied in [59] to bound $m$ for which $B_{2m}$ has no primitive divisor. The gain is obtained in part by extending the argument to quadratic fields, and in part by being somewhat more careful with various estimates.

If $P$ has property 6.2, we must first consider which fields $K$ may occur. We will assume that property 6.2 holds non-trivially, that is, that $P$ is not of the form $2R$ for any point $R \in E(\mathbb{Q})$ (the trivial case is treated in Chapter 4). Then by a standard argument using the Kummer pairing (again see [62]), one sees that $K$ is unramified outside the set of primes containing 2 and the prime divisors of $\Delta(E_N)$ (the primes of bad reduction for $E_N$). In particular, if $K = \mathbb{Q}(\sqrt{D})$ where $D \in \mathbb{Z}$ is chosen to be square free, then $D \mid 2N$. Although a minor observation, this restriction on the discriminant of $K/\mathbb{Q}$ allows a bound which is uniform. We should mention that while the explicit decimal values below have been rounded in the direction which favours the given inequality, the actual computations were carried out to a higher precision to avoid compound generosity in the estimates.

**Claim 6.7.** *Let $K = \mathbb{Q}(\sqrt{D})$, where $D \mid 2N$. Then for any $\xi \in K$, we may find $\alpha, \beta \in \mathcal{O}_K$ (with $\beta \neq 0$) such that $\beta\xi = \alpha$ and*

$$\log|\mathcal{N}(\gcd(\alpha, \beta))| \leqslant \frac{1}{2}\log N + \frac{5}{2}\log 2 - \log \pi.$$

*Proof.* We may write $\xi = A/B$ for relatively prime integral ideals $A$ and $B$. These are clearly in the same ideal class, so let $(\alpha) = AI$, $(\beta) = BI$, where $I$ is a representative of the inverse of this ideal class. Then, up to multiplication by units (which doesn't change norms), $\xi = \alpha/\beta$, while $(\alpha, \beta) = I$. By a theorem of Minkowski (see [60]), we may choose representatives of the various ideal classes with norm each less than $\frac{4}{\pi}\sqrt{D}$. □

The following bound on the difference between the naïve and canonical heights over $\mathbb{Q}$ will be used to estimate the difference in the heights over $K$.

**Claim 6.8 (Bremner, Silverman, Tzanakis [57]).** *For all $P \in E_N(\mathbb{Q})$,*

$$-c_1(N) \leqslant h(P) - \hat{h}(P) \leqslant c_2(N),$$

*where $c_1 = \frac{1}{2}\log(N^2+1) + 0.116$ and $c_2 = \log N + 0.347$.*

Now, we write the doubling map on $E_N$ as

$$2\left(\frac{a}{b}, \cdot\right) = \frac{(a^2 + b^2N^2)^2}{4ab(a^2 - b^2N)} = \frac{F(a,b)}{G(a,b)},$$

and use this to construct an explicit lower bound on $\log B_n$. If $nP = Q$, for $Q \in E_N(K)$, write $x(Q) = \alpha/\beta$, with $\alpha$ and $\beta$ algebraic integers in $K$ chosen as in Lemma 6.7. We introduce a third height on $K$. Throughout we will let $\theta = \gcd(\alpha, \beta)$.

**Claim 6.9.** *Let $h^*(\alpha, \beta) = \frac{1}{2}\log\max\{|\mathcal{N}(\alpha)|, |\mathcal{N}(\beta)|, |\mathrm{Tr}(\alpha\overline{\beta})|\}$. Then*

$$-c_5(N, D) \leqslant h^*(\alpha, \beta) - h(\alpha/\beta) \leqslant c_6(N, D),$$

*where $c_5 = 2\log 2$, $c_6 = \log 2 + \log|\mathcal{N}(\theta)|$.*

Here $\mathcal{N}$ and Tr are the standard norm and trace functions

$$\mathcal{N}(x) = \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} x^\sigma$$

$$\mathrm{Tr}(x) = \sum_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} x^\sigma.$$

Note that if we write

$$\Gamma = \left|\mathcal{N}\Big(\gcd\big(F(\alpha,\beta), G(\alpha,\beta)\big)\Big)\right|,$$

then $\log B_n = \frac{1}{2}\log|\mathcal{N}(G)| - \frac{1}{2}\log\Gamma$. Our lower bound is now the result of some elementary calculus.

**Claim 6.10.** *We write $F = F(\alpha, \beta)$ and $G = G(\alpha, \beta)$ for brevity.*

$$\frac{1}{2}\log\max\{|\mathcal{N}(F)|, |\mathcal{N}(G)|\} \leqslant 4h(\alpha/\beta) + 2\log(N) + 7\log 2 + 2\log|\mathcal{N}(\theta)|$$
$$\frac{1}{2}\log\max\{|\mathcal{N}(F)|, |\mathcal{N}(G)|\} \geqslant 4h(\alpha/\beta) - \log N + 0.9163$$

*Proof of the claim.* Expanding the expressions for $\log|\mathcal{N}(F)|$ and $\log|\mathcal{N}(G)|$ yields

$$\log|\mathcal{N}(F)| = 2\log\left|(\mathcal{N}(\alpha) - N^2\mathcal{N}(\beta))^2 + N^2\mathrm{Tr}(\alpha\overline{\beta})^2\right|$$
$$\log|\mathcal{N}(G)| = \log|\mathcal{N}(4\alpha\beta)| + \log\left|(\mathcal{N}(\alpha) + N^2\mathcal{N}(\beta))^2 - N^2\mathrm{Tr}(\alpha\overline{\beta})^2\right|.$$

We will make use of the observation that for any $X$ and $Y$, either

$$\frac{1}{2} < \frac{Y}{X} < 2 \tag{6.3}$$

or $\log|X - Y| \geqslant \log\max\{|X|, |Y|\} - \log 2$.

Now, notice that

$$\begin{aligned}\log|\mathcal{N}(F)| &\geqslant 2\log\max\{|\mathcal{N}(\alpha) - N^2\mathcal{N}(\beta)|^2, N^2\mathrm{Tr}(\alpha\overline{\beta})^2\}\\ &\geqslant 4\log\max\{|\mathcal{N}(\alpha)|, |\mathcal{N}(\beta)|, |\mathrm{Tr}(\alpha\overline{\beta})|\} - 2\log A\\ &\geqslant 8h^*(\alpha,\beta) - 2\log 2.\end{aligned}$$

unless the inequalities (6.3) hold with $X = \mathcal{N}(\alpha)$ and $Y = N^2\mathcal{N}(\beta)$. So suppose they do, and suppose further that $N^2 \geqslant 2$ (which is a modest assumption). This implies $|\mathcal{N}(\beta)| < |\mathcal{N}(\alpha)|$, whence

$$h^*(\alpha,\beta) = \frac{1}{2}\log\max\{|\mathcal{N}(\alpha)|, |\mathrm{Tr}(\alpha\overline{\beta})|\}.$$

For $\alpha, \beta$ with $|N\mathrm{Tr}(\alpha\overline{\beta})| > |\mathcal{N}(\alpha)|$ we have, from the above,

$$\log|\mathcal{N}(F)| \geqslant 4\log|N\mathrm{Tr}(\alpha\overline{\beta})| > 4\log|\mathcal{N}(\alpha)|,$$

and so

$$\log|\mathcal{N}(F)| \geqslant 8h^*(\alpha,\beta).$$

Finally, suppose that $|N\mathrm{Tr}(\alpha\overline{\beta})| \leqslant |\mathcal{N}(\alpha)|$, and furthermore that $N > 1$, so that

$$h^*(\alpha,\beta) = \frac{1}{2}\log|\mathcal{N}(\alpha)|.$$

We have also that $N^2|\mathcal{N}(\beta)| > \frac{1}{2}|\mathcal{N}(\alpha)|$, and so

$$\log|\mathcal{N}(G)| \geqslant 4\log|\mathcal{N}(\alpha)| + \log 2 + \log 5 - 2\log N.$$

Combining this with Claim 6.9, we obtain one of the bounds. The other bound is similar. □

Note that as $2Q \in E_N(\mathbb{Q})$, we may combine this with Claim 6.8 to obtain bounds on the difference between the cannonical and naïve heights over $K$. We produce only the bound of interest to us. Note that while one may obtain a cleaner looking result by replacing $\theta$ and $\Gamma$ with worst-case estimates, keeping track of these terms pays off in a better bound on $n$.

**Claim 6.11.** *Let $Q$ be as above. Then*

$$h(Q) - \hat{h}(Q) \geqslant -\log N - \frac{1}{8}\log|N^2+1| - \log|\mathcal{N}(\theta)| + \frac{1}{8}\log\Gamma - 1.2421.$$

*Proof.* Write

$$h(Q) - \hat{h}(Q) = \frac{1}{4}\Big(4h(Q) - h(2Q)\Big) + \frac{1}{4}\Big(h(2Q) - \hat{h}(2Q)\Big).$$

The result now follows from 6.8 and 6.10. □

**Claim 6.12.** $\log\Gamma \leqslant \log|\mathcal{N}(2^3N^4\theta^4)|$.

*Proof.* We will in fact prove a stronger divisibility result, that $\Gamma \mid \mathcal{N}(2^3N^4\theta^4)$. Using resultants, if $g = \gcd(F(\alpha,\beta), G(\alpha,\beta))$, then $g \mid 2^{12}N^{12}\beta^{16}$. Let $l$ be a prime (in $K$). Note that

$$\begin{aligned}\mathrm{ord}_l(F(\alpha,\beta)) &= 2\mathrm{ord}_l(\alpha^2 + N^2\beta^2)\\ \mathrm{ord}_l(G(\alpha,\beta)) &= 2\mathrm{ord}_l(2) + \mathrm{ord}_l(\alpha) + \mathrm{ord}_l(\beta) + \mathrm{ord}_l(\alpha^2 - N^2\beta^2)\end{aligned}$$

while

$$\mathrm{ord}_l\{\alpha^2 \pm N^2\beta^2\} = 2\min\mathrm{ord}_l\{\alpha, N\beta\}$$

unless these orders are equal, in which case

$$\begin{aligned}\min\mathrm{ord}_l\{\alpha^2 \pm N^2\beta^2\} &\leqslant 2\mathrm{ord}_l(N) + 2\mathrm{ord}_l(\beta) + \mathrm{ord}_l(2)\\ \min\mathrm{ord}_l\{\alpha^2 \pm N^2\beta^2\} &\leqslant 2\mathrm{ord}_l(\alpha) + \mathrm{ord}_l(2).\end{aligned}$$

We wish to show that for each prime $l$ of $K$,

$$\mathrm{ord}_l(g) \leqslant 3\mathrm{ord}_l(2) + 4\mathrm{ord}_l(\theta) + 4\mathrm{ord}_l(N).$$

Suppose that $\mathrm{ord}_l(\alpha) > \mathrm{ord}_l(N\beta)$. Then $\mathrm{ord}_l(\theta) = \mathrm{ord}_l(\beta)$, and

$$\mathrm{ord}_l(g) \leqslant \mathrm{ord}_l(F) = 4\mathrm{ord}_l(N\beta) = 4\mathrm{ord}_l(N) + 4\mathrm{ord}_l(\theta).$$

So we will assume that $\mathrm{ord}_l(\alpha) \leqslant \mathrm{ord}_l(N) + \mathrm{ord}_l(\beta)$.

If $\mathrm{ord}_l(\alpha) < \mathrm{ord}_l(N\beta)$ then $\mathrm{ord}_l(F) = 4\mathrm{ord}_l(\alpha) \leqslant 4\mathrm{ord}_l(N) + 4\mathrm{ord}_l(\theta)$ as either $\mathrm{ord}_l(\theta) = \mathrm{ord}_l(\alpha)$ or $\mathrm{ord}_l(\theta) = \mathrm{ord}_l(\beta)$ and $\mathrm{ord}_l(N) \geqslant 0$.

Finally suppose that $\mathrm{ord}_l(\alpha) = \mathrm{ord}_l(N\beta)$, and hence $\mathrm{ord}_l(\theta) = \mathrm{ord}_l(\beta)$. Then the above indicates that either

$$\mathrm{ord}_l(\alpha^2 + N^2\beta^2) \leqslant 2\mathrm{ord}_l(N) + 2\mathrm{ord}_l(\beta) + \mathrm{ord}_l(2),$$

in which case we have

$$\mathrm{ord}_l(F) \leqslant 4\mathrm{ord}_l(N) + 4\mathrm{ord}_l(\theta) + 2\mathrm{ord}_l(2),$$

or $\mathrm{ord}_l(\alpha^2 - N^2\beta^2) \leqslant 2\mathrm{ord}_l(N) + 2\mathrm{ord}_l(\beta) + \mathrm{ord}_l(2)$, in which case

$$\begin{aligned} \mathrm{ord}_l(G) &\leqslant 3\mathrm{ord}_l(2) + \mathrm{ord}_l(\alpha) + 3\mathrm{ord}_l(\beta) + 2\mathrm{ord}_l(N) \\ &= 3\mathrm{ord}_l(2) + 3\mathrm{ord}_l(N) + 4\mathrm{ord}_l(\theta). \end{aligned}$$

In either case we are done. □

The following result, proved in a similar fashion to Claim 6.10, completes the basis of our proof.

**Claim 6.13.**

$$\log|\mathcal{N}(G)| \geqslant 4h^*(\alpha,\beta) + \log 2 - 2\log N.$$

The proof is now, essentially, complete. As

$$B_n^2 = \mathcal{N}(B_n) = \frac{|\mathcal{N}(G(\alpha,\beta))|}{\Gamma},$$

we have by 6.13 that

$$\log|B_n| \geqslant 2h^*(\alpha,\beta) + \frac{1}{2}\log 2 - \log N - \frac{1}{2}\log\Gamma.$$

Applying Claims 6.9 and 6.11 we then obtain

$$\log|B_n| \geqslant 2\hat{h}(Q) - 3\log N - \frac{1}{4}\log(N^2+1) - 2\log|\mathcal{N}(\theta)| - \frac{1}{4}\log\Gamma - 4.9101,$$

while using Claims 6.7 and 6.12 (recall that $2Q = nP$), this begets

$$\log|B_n| \geqslant \frac{n^2}{2}\hat{h}(P) - \frac{11}{2}\log N - \frac{1}{4}\log(N^2+1) - 7.7142.$$

□

Unfortunately, as mentioned in Chapter 4, it seems rather impossible to extend this result to the case where $P = 2Q$ for some $Q \in E(K)$, where $[K:\mathbb{Q}] = 4$ (a condition satisfied by every rational point $P$). An absolute, uniform bound on $Z(E_N, P)$, then, is still out of reach.

# Bibliography

[57] A. Bremner, J. H. Silverman, and N. Tzanakis. Integral points in arithmetic progression on $y^2 = x(x^2 - n^2)$. *J. Number Theory*, 80, 2000.

[58] Y. Bugeaud and K. Győry. Bounds for the solutions of Thue-Mahler equations and norm form equations. *Acta Arith.*, 74(3):273–292, 1996.

[59] G. Everest, G. Mclaren, and T. Ward. Primitive divisors of elliptic divisibility sequences. preprint, 2005.

[60] Pierre Samuel. *Algebraic theory of numbers*. Translated from the French by Allan J. Silberger. Houghton Mifflin Co., Boston, Mass., 1970.

[61] J. H. Silverman. unpublished work.

[62] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

# Appendix A

# Parametrizing polynomials

## A.1 By coefficients

The following polynomials parametrize elliptic curves over $\mathbb{Q}$ with a given torsion group. For each admissable group $G$, $E/\mathbb{Q}$ contains a subgroup isomorphic to $G$ if and only if $E$ is $\mathbb{Q}$-isomorphic to a curve of the form $E(A_G(t), B_G(t))$ for some $t \in \mathbb{Q}$. The parametrizations for curves with torsion subgroups isomorphic to $\mathbb{Z}/2\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^2$, or $\mathbb{Z}/3\mathbb{Z}$ are of a slightly different form, and readers are directed to the presentations in Chapter 3. The following parametrizations are obtained simply by re-writing those found in [64].

$$
\begin{aligned}
A_{\mathbb{Z}/4\mathbb{Z}}(X) &= -27(16X^2 + 16X + 1) \\
B_{\mathbb{Z}/4\mathbb{Z}}(X) &= -54(8X + 1)(8X^2 - 16X - 1) \\
A_{\mathbb{Z}/5\mathbb{Z}}(X) &= -27(X^4 - 12X^3 + 14X^2 + 12X + 1) \\
B_{\mathbb{Z}/5\mathbb{Z}}(X) &= 54(X^2 + 1)(X^4 - 18X^3 + 74X^2 + 18X + 1) \\
A_{\mathbb{Z}/6\mathbb{Z}}(X) &= -27(3X + 1)(3X^3 + 3X^2 + 9X + 1) \\
B_{\mathbb{Z}/6\mathbb{Z}}(X) &= -54(3X^2 - 6X - 1)(9X^4 + 36X^3 + 30X^2 + 12X + 1) \\
A_{\mathbb{Z}/7\mathbb{Z}}(X) &= -27(X^8 - 12X^7 + 42X^6 - 56X^5 + 35X^4 - 14X^2 \\
&\quad +4X + 1) \\
B_{\mathbb{Z}/7\mathbb{Z}}(X) &= 54(X^{12} - 18X^{11} + 117X^{10} - 354X^9 + 570X^8 - 486X^7 \\
&\quad +273X^6 - 222X^5 + 174X^4 - 46X^3 - 15X^2 + 6X + 1) \\
A_{\mathbb{Z}/8\mathbb{Z}}(X) &= -27(16X^8 - 64X^7 + 224X^6 - 448X^5 + 480X^4 - 288X^3 \\
&\quad +96X^2 - 16X + 1) \\
B_{\mathbb{Z}/8\mathbb{Z}}(X) &= -54(8X^4 - 16X^3 + 16X^2 - 8X + 1)(8X^8 - 32X^7 \\
&\quad -80X^6 + 352X^5 - 456X^4 + 288X^3 - 96X^2 + 16X - 1)
\end{aligned}
$$

$$
\begin{aligned}
A_{\mathbb{Z}/9\mathbb{Z}}(X) &= -27(X^3-3X^2+1)(X^9-9X^8+27X^7-48X^6+54X^5\\
&\quad -45X^4+27X^3-9X^2+1)\\
B_{\mathbb{Z}/9\mathbb{Z}}(X) &= 54(X^{18}-18X^{17}+135X^{16}-570X^{15}+1557X^{14}\\
&\quad -2970X^{13}+4128X^{12}-4230X^{11}+3240X^{10}\\
&\quad -2032X^9+1359X^8-1080X^7+735X^6-306X^5\\
&\quad +27X^4+42X^3-18X^2+1)\\
A_{\mathbb{Z}/10\mathbb{Z}}(X) &= -27(16X^{12}-128X^{11}+416X^{10}-720X^9+720X^8\\
&\quad -288X^7-256X^6+432X^5-240X^4+40X^3+16X^2\\
&\quad -8X+1)\\
B_{\mathbb{Z}/10\mathbb{Z}}(X) &= 54(2X^2-2X+1)(2X^4-2X+1)(4X^4-12X^3+6X^2\\
&\quad +2X-1)(4X^8-32X^7+104X^6-176X^5+146X^4\\
&\quad -48X^3-4X^2+6X-1)\\
A_{\mathbb{Z}/12\mathbb{Z}}(X) &= -27(6X^4-12X^3+12X^2-6X+1)(24X^{12}-144X^{11}\\
&\quad +864X^{10}-3000X^9+6132X^8-8112X^7+7368X^6\\
&\quad -4728X^5+2154X^4-684X^3+144X^2-18X+1)\\
B_{\mathbb{Z}/12\mathbb{Z}}(X) &= -54(24X^8-96X^7+216X^6-312X^5+288X^4-168X^3\\
&\quad +60X^2-12X+1)(72X^{16}-576X^{15}-1008X^{14}\\
&\quad +17136X^{13}-65880X^{12}+146304X^{11}-222552X^{10}\\
&\quad +248688X^9-211296X^8+138720X^7-70632X^6\\
&\quad +27696X^5-8208X^4+1776X^3-264X^2+24X-1)\\
A_{\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}}(X) &= -27(X^4+14X^2+1)\\
B_{\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}}(X) &= -54(X^2+1)(X^2-6X+1)(X^2+6X+1)\\
A_{\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}}(X) &= -27(X^2-6X+21)(X^6-18X^5+75X^4+180X^3\\
&\quad -825X^2-2178X+6861)\\
B_{\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}}(X) &= 54(X^4-12X^3+30X^2+228X-759)(X^4-12X^3\\
&\quad +30X^2-156X+393)(X^4-12X^3+30X^2\\
&\quad +36X-183)\\
A_{\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}}(X) &= -27(256X^{16}+2048X^{15}+7168X^{14}\\
&\quad +14336X^{13}+17664X^{12}+12800X^{11}+3200X^{10}\\
&\quad -3712X^9-4624X^8-1856X^7+800X^6+1600X^5\\
&\quad +1104X^4+448X^3+112X^2+16X+1)\\
B_{\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}}(X) &= 54(16X^8+64X^7+96X^6+64X^5+32X^4+32X^3\\
&\quad +24X^2+8X+1)(32X^8+128X^7+192X^6+128X^5\\
&\quad +16X^4-32X^3-24X^2-8X-1)(8X^8+32X^7\\
&\quad +48X^6+32X^5-8X^4-32X^3-24X^2-8X-1)
\end{aligned}
$$

## A.2 By $j$-invariants

An elliptic curve $E/\mathbb{Q}$ admits an isogeny of order $N$ if $j(E) = j_N(t)$ for some $t \in \mathbb{Q}$. These parametrizations have been known for some time, but seem to appear explicitly only in [63].

$$
\begin{aligned}
j_2(t) &= \frac{(t+256)^3}{t^2} \\
j_3(t) &= \frac{(t+27)(t+243)^3}{t^3} \\
j_4(t) &= \frac{(t^2+256t+4096)^3}{t^4(t+16)} \\
j_5(t) &= \frac{(t^2+250t+3125)^3}{t^5} \\
j_7(t) &= \frac{(t^2+13t+49)(t^2+245t+2401)^3}{t^7} \\
j_9(t) &= \frac{(t+9)^3(t^3+243t^2+2187t+6561)^3}{t^9(t^2+9t+27)} \\
j_{13}(t) &= \frac{(t^2+5t+13)(t^4+247t^3+3380t^2+15379t+28561)^3}{t^{13}}.
\end{aligned}
$$

# Bibliography

[63] Imin Chen and Noriko Yui. Singular values of Thompson series. In *Groups, difference sets, and the Monster (Columbus, OH, 1993)*, volume 4 of *Ohio State Univ. Math. Res. Inst. Publ.*, pages 255–326. de Gruyter, Berlin, 1996.

[64] D. S. Kubert. Universal bounds on the torsion of elliptic curves. *Proc. London Math. Soc. (3)*, 33(2):193–237, 1976.