Received: 8 September 2021 | Revised: 27 February 2023 | Accepted: 16 March 2023

DOI: 10.1112/plms.12520

RESEARCH ARTICLE

Proceedings of the London Mathematical Society

The elliptic sieve and Brauer groups

Subham Bhakta[1] | **Daniel Loughran**[2] | **Simon L. Rydin Myerson**[3] | **Masahiro Nakahara**[4]

[1]Mathematisches Institut, Georg-August-Universität Göttingen, Göttingen, Germany

[2]Department of Mathematical Sciences, University of Bath, Claverton Down, Bath, UK

[3]Mathematics Institute, Zeeman Building, University of Warwick, Coventry, UK

[4]Department of Mathematics, University of Washington, Seattle, Washington, USA

Correspondence
Daniel Loughran, Department of Mathematical Sciences, University of Bath, Claverton Down, Bath BA2 7AY, UK.
Email: dtl32@bath.ac.uk

Funding information
EPSRC, Grant/Award Number: EP/R021422/2; European Research Council, Grant/Award Number: 648329; DFG, Grant/Award Number: 255083470

Abstract

A theorem of Serre states that almost all plane conics over $\mathbb{Q}$ have no rational point. We prove an analogue of this for families of conics parametrised by elliptic curves using elliptic divisibility sequences and a version of the Selberg sieve for elliptic curves. We also give more general results for specialisations of Brauer groups, which yields applications to norm form equations.

MSC 2020
14G05 (primary), 11N36, 14F22, 11G05 (secondary).

Contents

1 | INTRODUCTION

1.1 | Sums of two squares

A famous theorem of Landau and Ramanujan states that almost all integers are not sums of two squares, when ordered by absolute value. In this paper we prove a version of this result for elliptic curves.

Theorem 1.1. *Let E be an elliptic curve over $\mathbb{Q}$ given by an integral Weierstrass equation. Let $P \in E(\mathbb{Q})$ have infinite order with $P \in E(\mathbb{R})^0$. Then there exists $\omega = \omega(E,P) > 0$ such that*

$$\#\{n \in \mathbb{Z} : |n| \leqslant B, y(nP) \text{ is a sum of two squares}\} \ll_{E,P} B/(\log B)^{\omega}. \tag{1.1}$$

Here $E(\mathbb{R})^0$ denotes the connected component of the identity of $E(\mathbb{R})$, and $y(nP)$ denotes the y-coordinate of the point nP; this is a rational number and we are asking that this is the sum of two rational squares. The result shows that for almost all multiples of P, the y-coordinate is not a sum of two (rational) squares. (See Section 1.4 for a discussion on sharpness of this result.)

The reader may wonder: Why consider the y-coordinate and not the x-coordinate? Well, the corresponding result is *false* otherwise: Consider the elliptic curve

$$y^2 = x^3 - k^2. \tag{1.2}$$

Evidently $x = (y^2 + k^2)/x^2$ is always a sum of two squares. Our methods are able to handle the x-coordinate problem, but only with additional assumptions on E (see Theorem 5.3).

The assumption that $P \in E(\mathbb{R})^0$ is slightly deeper and is intimately connected with our method; however without it we can obtain counter-examples to similar statements (see Example 1.3).

1.2 | Conic bundles

To understand exactly what is happening, we put our results into the more geometric framework of *conic bundles*. In an influential paper [22], Serre proved that almost all plane conics over $\mathbb{Q}$ have no rational point, when ordered by the size of their coefficients. This was a special case of a more general result [22, Theorem 2] on conic bundles $\pi : X \to \mathbb{P}^n_{\mathbb{Q}}$, which says that providing π has no rational section we have

$$\#\{x \in \mathbb{P}^n(\mathbb{Q}) : H(x) \leqslant B, x \in \pi(X(\mathbb{Q}))\} \ll_{X,E,P} B^{n+1}/(\log B)^{\Delta(\pi)} \tag{1.3}$$

for some $\Delta(\pi) > 0$, where H denotes the usual naive height on projective space. Here by a conic bundle, we mean a surjective morphism of varieties all of whose fibres are isomorphic to plane conics. This result was generalised in [18, Theorem 1.2] to other families of varieties over $\mathbb{P}^n$.

One of the aims of the paper is to obtain a version of Serre's result for conic bundles over elliptic curves. Here the crucial concept is that of a *non-split fibre*: This is an irreducible fibre isomorphic to two lines over a quadratic extension (called the splitting field of the fibre). The relevant conic bundle for Theorem 1.1 is

$$x_1^2 + x_2^2 = y x_0^2, \tag{1.4}$$

where the equation is an affine patch of the surface in $\mathbb{P}^2 \times E$. Here a non-split fibre occurs over the point at infinity, but in the example (1.2) one can check that every fibre of the relevant conic bundle is split. So to get savings one requires at least a non-split fibre; this is essentially the content of our next theorem.

Theorem 1.2. *Let E be an elliptic curve over $\mathbb{Q}$ given by an integral Weierstrass equation and $\pi : X \to E$ a non-singular conic bundle. Let $P \in E(\mathbb{Q})$ have infinite order with $P \in E(\mathbb{R})^0$. Assume that $\pi^{-1}(mP)$ is non-split with imaginary quadratic splitting field, for some $m \in \mathbb{Z}$. Then there exists $\omega = \omega(X, E, P) > 0$ such that*

$$\#\{n \in \mathbb{Z} : |n| \leqslant B, nP \in \pi(X(\mathbb{Q}))\} \ll_{X,E,P} B/(\log B)^{\omega}.$$

The theorem says that under some technical assumptions, for almost all multiples of a given non-torsion rational point the associated conic has no rational point. The assumption $P \in E(\mathbb{R})^0$ may look artificial, however it is *necessary* for the conclusion.

Example 1.3. Consider the elliptic curve with the point P of infinite order

$$E : y^2 = x(x+2)(x-3), \quad P = (-1, 2)$$

and the conic bundle

$$t_0^2 + t_1^2 = (x - x_1)(x - x_3)t_2^2,$$

where x_i denotes the x-coordinate of iP. This has non-split fibres over $\pm P$ and $\pm 3P$. Here $P \notin E(\mathbb{R})^0$ so the assumptions of Theorem 1.2 do not hold.

We claim that the fibre over every *even* multiple of P contains a rational point, so the conclusion of Theorem 1.2 in fact does not hold either. This is a special case of a more general construction (Proposition 5.7), but we explain the key ideas here.

Firstly, one checks that the fibre over O has a rational point. So let $2nP$ be a non-trivial even multiple of P. It is clear there are always p-adic points for $p \equiv 1 \bmod 4$. We will show that for every prime $p \equiv 3 \bmod 4$, we have $v_p((x - x_1)(x - x_3)) = 0$, which implies that the fibre has a $\mathbb{Q}_p$-point. Moreover as every element of $2\mathbb{Z}P$ lies in the real component of the identity it satisfies $x \geqslant 3$. Hence $(x - x_1)(x - x_3) > 0$ so the conic has a real point. Hilbert's version of quadratic reciprocity now shows that every conic has a $\mathbb{Q}_2$-point, hence has a $\mathbb{Q}$-point by Hasse–Minkowski.

So assume for a contradiction that there is some even multiple $2nP$ and $p \equiv 3 \bmod 4$ such that $v_p((x - x_1)(x - x_3)) > 0$. (One can check that $v_p(x_3) \geqslant 0$ for all $p \equiv 3 \bmod 4$, so the valuation cannot be negative.) Suppose for example that $v_p(x - x_1) > 0$, so that $2nP \equiv \pm P \bmod p$. Then P is divisible by 2 modulo p. However, our example was chosen so that 2-division field of P is $\mathbb{Q}(i)$ (this can be shown using the criterion from [4, Section 2]), and since p is inert in $\mathbb{Q}(i)$ it follows that P is *not* 2-divisible modulo p; a contradiction. The case $2nP \equiv \pm 3P \bmod p$ is analogous.

1.3 | Proof ingredients

Our key tools are sieves and elliptic divisibility sequences (EDSs).

In the classical sieve setting one usually sieves with respect to the homomorphisms $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, for primes p, or more general prime powers. We originally tried to mimic this setting by sieving with respect to the homomorphisms $E(\mathbb{Q}) \to E(\mathbb{F}_p)$, inspired by Kowalski's elliptic sieve [14, Section 4.4] used to study prime divisors in EDSs. However our method quickly diverges from the classical setting and Kowalski's setting, as in our case information modulo p is insufficient. A significant technical step in our proof is trying to control the p-adic valuations of the rational points we are sieving, which we achieve by sieving modulo p^{n_p} for varying primes p and growing exponents n_p, so our sieve has no classical analogue. This difficulty is related to the fact that elliptic curves do not satisfy weak approximation, and does not arise in the classical sieve setting where p-adic valuations are easy to control. Our exact valuation theoretic problems are closely related to p being a 'non-Wieferich prime for base $P \in E$' in the sense of Voloch [33], and it is not even known whether there exists a single elliptic curve with infinitely many such primes [24]. These issues greatly complicate our sieve set up, and we have to work with the filtration structure on $E(\mathbb{Q}_p)$ to control valuations. (See Remark 3.20.)

To come up with a sieve criterion we use EDSs: these are defined via the denominators of the x-coordinates of the multiples of P, multiplied by a sign to obtain better recurrence properties. We recall the relevant definitions in Section 3. The key property for us is that EDSs are periodic modulo an arbitrary integer (Proposition 3.7). We achieve this using the work of Verzobio [32] and does not seem to have been proven in the literature before in this generality. In our proof we also have to be careful with signs, which requires us to use the work [27] as well as equidistibution results for multiples of irrational numbers modulo 1. Whilst these sign issues may seem a mere technical step, in fact they are crucial and related to our necessary assumptions on the real components of $E(\mathbb{R})$ (cf. Example 1.3).

Theorem 1.2 is a quantitative strengthening of a result of the fourth author and Berg [5], which proves under suitable assumptions that for certain conic bundles $\pi : X \to E$, the image $\pi(X(\mathbb{Q}))$ does not contain a translate of a subgroup of finite index. In [5] the authors only consider elliptic curves which are Galois general in a sense captured by conditions (1)–(4) in their Theorem 3.5, and their results only apply to special conic bundles given by pulling back Châtelet surfaces from $\mathbb{P}^1$ which also have a non-split fibre over a rational point. Our results apply to an overlapping collection of elliptic curves and conic bundles, but the key point is that our conclusion is stronger: a subset of $\mathbb{Z}$ which contains no arithmetic progression may still have positive density (for example the set of squarefree numbers in $\mathbb{Z}$).

1.4 | Lower bounds and counting by height

We believe that our paper demonstrates the usefulness of sieve techniques and EDSs to counting problems on elliptic curves. The proof of Theorem 1.2 gives an explicit value for ω, but we doubt that our upper bound is sharp. Proving any kind of lower bound seems very difficult in general; we are only able to do this in various trivial cases where $\omega = 0$, so that $\pi(X(\mathbb{Q}))$ has positive density in $E(\mathbb{Q})$ (see Section 5). The following question seems quite challenging.

Question 1.4. Does there exist an elliptic curve E over $\mathbb{Q}$ such that the set

$$\{(x, y) \in E(\mathbb{Q}) : \ y \text{ is a sum of two squares}\} \tag{1.5}$$

is infinite?

Standard conjectures in arithmetic geometry seem to have nothing to say about this question, as the associated conic bundle surface is neither rationally connected nor of general type (over $\mathbb{Q}(i)$ it is birational to $\mathbb{P}^1 \times E$).

However, the following heuristic suggests (1.5) should be quite sparse. Let $E(\mathbb{Q})$ have rank r. Fix a norm $\|\cdot\|$ on $\mathbb{R}^r$. The numerator and denominator of $y(n_1P_1 + \cdots + n_rP_r)$ are both integers of size $\exp(O_{E,P}(\|\vec{n}\|^2))$, with the denominator being a perfect cube. A proportion $1/\|\vec{n}\|^2$ of such rational numbers are sums of two squares. One might therefore speculate that the set (1.5) has size $\ll \sum_{\vec{n}\in\mathbb{N}^r} 1/\|\vec{n}\|^2$, so can be infinite only when $r > 1$.

Versions of this problem were raised by Poonen [19, Questions 23, 33] and Browning [8, Problem 10, pp. 3181–3182]. Browning in particular asked about the number of points for which the denominator of y is a sum of two squares. A similar heuristic suggests the number of points $\{nP : n \leqslant B\}$ with this property might be around $\sum_{n\leqslant B} 1/n \sim \log B$. Our methods give upper bounds for problem without alteration.

One can rephrase our results in terms of the *canonical height* $\widehat{h}$ on E, as nP has height roughly n^2. In this language the heuristic just discussed suggests the following.

$$\#\{Q \in E(\mathbb{Q}) : \widehat{h}(Q) \leqslant H, y(Q) \text{ is a sum of two squares}\}$$
$$\asymp \begin{cases} 1, & \text{if } \operatorname{rank} E(\mathbb{Q}) \leqslant 1, \\ \log H, & \text{if } \operatorname{rank} E(\mathbb{Q}) = 2, \\ H^{(r-2)/2}, & \text{if } \operatorname{rank} E(\mathbb{Q}) > 2; \end{cases}$$

$$\#\{Q \in E(\mathbb{Q}) : \widehat{h}(Q) \leqslant H, \text{the denominator of } y(Q) \text{ is a sum of two squares}\}$$
$$\asymp \begin{cases} \log H, & \text{if } \operatorname{rank} E(\mathbb{Q}) = 1, \\ H^{(r-1)/2}, & \text{if } \operatorname{rank} E(\mathbb{Q}) \geqslant 2. \end{cases}$$

Our present method cannot handle the case of rank greater than 1; the key stumbling block is that we have no control over the prime p constructed in Proposition 3.19, which would be necessary to combine p-adic information at sums of points. We are however able to prove non-trivial upper bounds provided the curve has rank 1. Rather than stating the most general result in terms of conic bundles, we content ourselves with the following variant of Theorem 1.1.

Theorem 1.5. *Let E be an elliptic curve over $\mathbb{Q}$ given by an integral Weierstrass equation. Assume that E has rank 1. Let*

$$\eta = \begin{cases} 1 & \text{if } \#E(\mathbb{Q})^{\mathrm{tors}} \text{ has two distinct prime divisors,} \\ -1 & \text{otherwise.} \end{cases}$$

Then

$$\#\left\{ Q \in E(\mathbb{Q}) \cap E(\mathbb{R})^0 : \begin{array}{l} \widehat{h}(Q) \leqslant H, y(Q) \text{ is a} \\ \text{sum of two squares} \end{array} \right\} \ll_E \frac{H^{1/2}(\log\log\log H)^{\eta/2}}{(\log\log H)^{1/2}}.$$

The total number of rational points in $E(\mathbb{R})^0$ of height at most H is $\gg H^{1/2}$, since $2E(\mathbb{Q}) \subset E(\mathbb{R})^0$, so the theorem indeed shows that 0% of these have y-coordinate which is a sum of two squares. Note that if $E(\mathbb{R})$ is connected, then the upper bounds applies to all rational points on E.

1.5 | Generalisation to Brauer groups

We now state our most general result, of which Theorem 1.2 is a special case. Firstly, we are able to prove results for conic bundles whose non-split fibres have real quadratic splitting field. Secondly, we make explicit the dependence of ω and the leading constant on P. Thirdly, our methods are sufficiently robust that they allow applications to specialisations of Brauer group elements on elliptic curves. This is also the viewpoint taken by Serre in his paper [22], as well in the more recent papers [16, 18]. Brauer groups are formally easier to work with than conic bundles, since one does not require explicit equations and one can make use of Grothendieck's residue map. Here we take a Brauer group element which is ramified at a rational point. The ramification gives rise to a cyclic extension of $\mathbb{Q}$ to which we associate a Dirichlet character using Kronecker–Weber (see Section 4 for details and relevant background on Brauer groups). Our result here is as follows.

Theorem 1.6. *Let E be an elliptic curve over $\mathbb{Q}$ given by an integral Weierstrass equation. Let $P \in E(\mathbb{Q})$ have infinite order. Assume there is $m \in \mathbb{Z}$ such that $b \in \operatorname{Br}\mathbb{Q}(E)$ is ramified at mP and let the associated Dirichlet character χ have modulus $q(\chi)$. Let β_n be the EDS associated to P and let π be the period of the sequence $\beta_n \bmod q(\chi)$.*

Assume that there is some index $\alpha \in \mathbb{N}$ with $\gcd(\alpha, \pi) = 1$ which satisfies either

(1) $\chi(|\beta_\alpha|) \neq 0, 1$; *or*
(2) $\chi(-|\beta_\alpha|) \neq 0, 1$ *and* $P \in E(\mathbb{R})^0$; *or*
(3) $\chi(-|\beta_\alpha|) \neq 0, 1$ *and* $4 \nmid \pi$.

Then we have $\pi \ll_{E,\chi} 1$ and

$$\#\{|n| \leqslant B : b(nP) = 0 \in \operatorname{Br}\mathbb{Q}\} \leqslant C_{E,P,b} \frac{B \log\log B}{(\log B)^{1/2\varphi(\pi)}},$$

where φ denotes Euler's totient function and $C_{E,P,b}$ is a positive constant depending on E, P and b only and given by (4.4).

In the statement $b(Q) \in \operatorname{Br}\mathbb{Q}$ denotes the evaluation of the Brauer element b at Q. We abuse notation slightly and implicitly ignore the finitely many points where b is not defined.

The Brauer group framework essentially allows us to replace quadratic extensions by arbitrary cyclic extensions and conic bundles by higher dimensional Brauer–Severi varieties. Moreover, we can even handle some non-abelian extensions. As an example application in the style of Theorem 1.1, we have the following.

Theorem 1.7. *Let $K/\mathbb{Q}$ be a number field which contains a cyclic subfield which is not totally real. Let E be an elliptic curve over $\mathbb{Q}$ given by an integral Weierstrass equation and let $P \in E(\mathbb{Q})$ be a point of infinite order with $P \in E(\mathbb{R})^0$. Then there exists $\omega = \omega(E, K) > 0$ such that*

$$\#\{|n| \leqslant B : y(nP) \text{ is a norm from } K\} \ll_{E,P,K} B/(\log B)^{\omega},$$

where the implicit constant is $\exp(O_{E,K}(\widehat{h}(P)/\log \widehat{h}(P)))$.

The fields $K = \mathbb{Q}(\sqrt[n]{a}, \mu_n)$ satisfy these hypotheses, for $a \in \mathbb{Q}^\times$ and $n \geqslant 3$. The explicit dependence on the point P is included as it is needed to prove Theorem 1.5. (A version of Theorem 1.5

replaced with the condition that $y(Q)$ is a norm from K, where K is of the type in Theorem 1.7, would follow by the same proof.)

Let us consider the technical assumptions on EDSs in Theorem 1.6. We suspect that Condition (1) holds for all but finitely many χ of given order; but it seems incredibly difficult to prove this, and even the analogous statement for the much simpler cases of Fibonacci or Mersenne numbers seems to be an open problem [15, 30]. However if $|\beta_\alpha|$ is a non-square (say), which indeed holds for all but finitely many α [11, Theorem 1.1], then $\chi(|\beta_\alpha|) \neq 0, 1$ for a positive proportion of quadratic Dirichlet characters; the challenge is it show that these characters cover all but finitely many as α varies. We are able to show the modest result that Condition (1) holds 100% of the time under suitable assumptions; see Section 6 for details.

As for our applications, if χ is an odd Dirichlet character then we simply use that $\beta_1 = 1$ and $\chi(-1) = -1 \neq 0, 1$ to see that Condition (2) or (3) is satisfied. This is what makes stating Theorem 1.2 so simple, as for an imaginary quadratic extension $\mathbb{Q}(\sqrt{D})$ with D a fundamental discriminant, the associated Dirichlet character is simply the Kronecker symbol $(\frac{D}{\cdot})$, which takes the value -1 at -1 as D is negative.

We finish by returning to Example 1.3.

Example 1.8. Consider the elliptic curve from Example 1.3

$$E : y^2 = x(x+2)(x-3)$$

with $P = (-1, 2)$. As we have seen, this pair does not satisfy the conclusion of Theorem 1.2 with respect to $\mathbb{Q}(i)$. Let us verify that the hypotheses of Theorem 1.6 do not hold in this case. Firstly, $P \notin E(\mathbb{R})^0$ so Condition (2) does not hold. Here P has everywhere good reduction and the EDS β_n is

$$0, 1, 4, -65, -504, 242\,369, -58\,888\,180, -66\,048\,490\,369, 60\,955\,459\,632\,144, \ldots$$

The relevant Dirichlet character is the unique non-principal character χ modulo 4. The sequence $\beta_n \bmod 4$ is just

$$0, 1, 0, 3, 0, 1, 0, 3, 0, 1, 0, 3, 0, 1, 0, 3, 0, 1, 0, 3, 0, \ldots$$

which has period 4. Thus Condition (3) from Theorem 1.6 does not hold. Finally, the sequence $|\beta_n| \bmod 4$ is

$$0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, \ldots$$

so (1) does not hold either. In particular, this demonstrates that all hypotheses in Theorem 1.6 are necessary in general for the conclusion to hold.

Outline of the paper

In Section 2 we recall various facts about elliptic curves over $\mathbb{Q}_p$. The following Section 3 contains a detailed study of elliptic divisibility sequences. Here we prove periodicity modulo an arbitrary

integer, and show our main technical result (Proposition 3.19) on such sequences. In Section 4 we prove the theorems from the introduction. We give various examples illustrating our results in Section 5, as well as further examples which demonstrate that the conclusion of Theorem 1.2 does not hold for arbitrary conic bundles over elliptic curves. We finish in Section 6 by showing that the technical assumption in Theorem 1.6 holds for 100% of suitable Dirichlet characters of prime moduli.

1.6 | Notation and conventions

We choose an embedding $\mathbb{Q}/\mathbb{Z} \subset \mathbb{C}^\times$. This corresponds to a choice of a compatible system of nth roots of unity for all n. We denote by $O = (0 : 1 : 0) \in \mathbb{P}^2$. By a Weierstrass equation with coefficients a_i we mean

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1.6}$$

We denote by $\widehat{h}$ the canonical height on $E(\mathbb{Q})$ [26, Chapter VIII.9]. This extends to a positive definitive quadratic form on $E(\mathbb{Q}) \otimes \mathbb{R}$ [26, Proposition VIII.9.6]. By $O_{a,\dots,z}(A)$ we mean a quantity with absolute value at most CA for some positive constant C depending on $a, \dots, z$ only; if the subscripts are omitted the implied constant is absolute. We write $A \ll_{a,\dots,z} B$ for $A = O_{a,\dots,z}(B)$ and $A = o(B)$ for $A/B \to 0$.

2 | ELLIPTIC CURVES OVER $\mathbb{Q}_p$

In this section let E be an elliptic curve over $\mathbb{Q}_p$ given by a (not necessarily minimal) Weierstrass equation with coefficients in $\mathbb{Z}_p$. Denote by $E_0(\mathbb{Q}_p)$ the set of points of $E(\mathbb{Q}_p)$ with non-singular reduction modulo p. We say that $P \in E(\mathbb{Q}_p)$ has *bad reduction* if $P \notin E_0(\mathbb{Q}_p)$. There is a subgroup filtration

$$\cdots \subset E_2(\mathbb{Q}_p) \subset E_1(\mathbb{Q}_p) \subset E_0(\mathbb{Q}_p), \quad E_i(\mathbb{Q}_p) = \{P \in E_0(\mathbb{Q}_p) : P \equiv O \bmod p^i\},\ i \geqslant 1.$$

Definition 2.1. If $P \in E(\mathbb{Q}_p) \setminus E_1(\mathbb{Q}_p)$ we set $v_p(P) = 0$. If $P \in E_1(\mathbb{Q}_p)$ we define

$$v_p(P) = \sup\{i : P \in E_i(\mathbb{Q}_p)\}.$$

Definition 2.2. For $P \in E_0(\mathbb{Q}_p)$ and $k \in \mathbb{N}$ we denote by $P \bmod p^k$ the image of P in $E_0(\mathbb{Q}_p)/E_k(\mathbb{Q}_p)$. We denote by $\mathrm{ord}(P \bmod p^k)$ its order.

Lemma 2.3. *Let $P = (x, y) \in E(\mathbb{Q}_p)$. Then $v_p(P) = \max\{0, -v_p(x)/2\}$.*

Proof. If $v_p(x) \geqslant 0$ then $v_p(P) = 0$ so the result holds. So assume $v_p(x) < 0$. As the rational function x/y is a uniformising parameter at O, we find that $v_p(P) = v_p(x/y)$. However, using $v_p(x) < 0$ and the Weierstrass equation, one finds that $2v_p(y) = 3v_p(x)$, and the claim easily follows. □

Lemma 2.3 gives a more explicit definition of the filtration which is often used in texts (for example [26, Example VII.7.4]). We have the following inequality for the valuation of a multiple of a point.

Lemma 2.4. *Let $P \in E_1(\mathbb{Q}_p)$. Then $v_p(nP) \geqslant v_p(P) + v_p(n)$, with equality if $p \nmid n$.*

Proof. Hensel's lemma [7, Lemma 2.1] shows that $|E_i(\mathbb{Q}_p)/E_{i+1}(\mathbb{Q}_p)| = p$ for all $i \geqslant 1$, thus this quotient is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. The result now easily follows. □

Remark 2.5. Using the formal group law on E [26, Theorem IV.6.4(b), Proposition VII.2.2], one can show that equality in fact holds except possibly if $p = 2, v_p(P) = 1$ and $p \mid n$. (See also [29, Theorem 3] for a version over number fields.) The hypothesis is required for $p = 2$. Take

$$E : y^2 + xy = x^3 + 4x + 1, \quad P = (15/4, -83/8).$$

Then $v_2(P) = 1$, but one calculates that $v_2(2P) = 4$. (The issue here is that $E_1(\mathbb{Q}_2)$ has non-trivial 2-torsion, so is not isomorphic to $2\mathbb{Z}_2$.)

3 | ELLIPTIC DIVISIBILITY SEQUENCES

3.1 | Basic properties

Now let $E/\mathbb{Q}$ be an elliptic curve given by a Weierstrass equation (1.6) with coefficients $a_i \in \mathbb{Z}$. Let $P \in E(\mathbb{Q})$ be a non-torsion point. Throughout this section we consider E and P as being fixed.

For any integer $n \geqslant 0$, define the nth division polynomial $\psi_n \in \mathbb{Z}[x, y]$ as follows:

$$\begin{aligned}
&\psi_0 = 0, \quad \psi_1 = 1, \quad \psi_2 = 2y + a_1x + a_3,\\
&\psi_3 = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8,\\
&\psi_4 = \psi_2(2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + b_4b_8 - b_2^6),
\end{aligned}$$

where the b_i are defined in [26, Chapter III], with subsequent polynomials given by

$$\begin{aligned}
\psi_{2n+1} &= \psi_{n+2}\psi_n^3 - \psi_{n+1}^3\psi_{n-1}, \quad n \geqslant 2,\\
\psi_{2n}\psi_2 &= \psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2), \quad n \geqslant 3,
\end{aligned} \tag{3.1}$$

and extend this to negative n by setting $\psi_n = -\psi_{-n}$. These formulas are equivalent to the recurrence relation

$$\psi_{m+n}\psi_{m-n}\psi_r^2 = \psi_{m+r}\psi_{m-r}\psi_n^2 - \psi_{n+r}\psi_{n-r}\psi_m^2 \tag{3.2}$$

for any integers m, n, r. The sequence ψ_n forms a divisibility sequence in $\mathbb{Z}[x, y]$, that is, $\psi_n \mid \psi_m$ for $n \mid m$. One notion of an *EDS* in a commutative ring would be a divisibility sequence satisfying (3.2). The study of EDS in $\mathbb{Z}$, in this sense, was begun by Ward [34], and a modern exposition can be

found in [12, Chapter 10]. We will use a slightly different kind of EDS considered by Verzobio [32], which is better suited to our purpose.

We can interpret x, y and each ψ_n as rational functions on $E(\mathbb{Q})$. By [26, Example III.3.7], multiplication by n is given as a rational map by

$$[n](P) = \left(\frac{x(P)\psi_n^2 - \psi_{n-1}\psi_{n+1}}{\psi_n^2}, \frac{\psi_{n-1}^2\psi_{n+2} - \psi_{n-2}\psi_{n+1}^2}{4y(P)\psi_n^3} \right).$$

In particular ψ_n is the square root of the denominator of the x-coordinate; the problem for us is that in general there may be some common factors between the numerator and denominator, so it will not be in lowest terms. We want to work with the genuine denominator as it has better p-adic properties (cf. Lemma 2.3).

Definition 3.1. Define the sequence e_n by $nP = (a_n/e_n^2, b_n/e_n^3)$ with $\gcd(a_n b_n, e_n) = 1$ and $e_n > 0$. Writing $\operatorname{sign}(t) = t/|t|$ for any $t \neq 0$, set

$$\beta_0 = 0, \qquad \beta_n = \operatorname{sign}(\psi_n(P))\frac{e_n}{e_1}, \qquad (n \in \mathbb{Z} \setminus \{0\}).$$

The sequence β_n is *not* in general an EDS in the traditional sense, since it need not satisfy the recurrence relation (3.2); differences can occur if P admits primes of bad reduction. In [32] Verzobio calls such sequences EDSB, as opposed to sequences of the form $\psi_n(P)$ which he terms EDSA. He shows in [32, Theorem 1.9] that the following weakened version of (3.2) does hold for an EDSB.

Proposition 3.2 (Verzobio). *Set*

$$M = M(P) = \operatorname{lcm}\{\operatorname{ord}(P + E_0(\mathbb{Q}_p)) : p \text{ prime}\},$$

where $\operatorname{ord}(P + E_0(\mathbb{Q}_p))$ *denotes the order of the image of* P *in the finite group* $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$. *Let* $n, m, r \in \mathbb{Z}$ *of which two are multiples of* $M(P)$. *Then*

$$\beta_{n+m}\beta_{n-m}\beta_r^2 = \beta_{m+r}\beta_{m-r}\beta_n^2 - \beta_{n+r}\beta_{n-r}\beta_m^2. \tag{3.3}$$

Remark 3.3. Here M is the least positive integer such that MP has everywhere good reduction. It divides $\prod_p \#(E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p))$, which is the product of the Tamagawa numbers of E if the model is globally minimal.

Verzobio defines β_n for $n \geqslant 0$ and proves the theorem under the assumption $n \geqslant m \geqslant r > 0$; in our notation this can be removed by using $\beta_{-n} = -\beta_n$ and permuting the variables as appropriate.

To illustrate some of the nice p-adic properties of this sequence, we prove that it is a *strong divisibility sequence*. We first make explicit Lemma 2.3.

Lemma 3.4. *For all primes* p *we have* $v_p(\beta_n) = v_p(nP) - v_p(P)$.

Proof. Immediate from the definition and Lemma 2.3. □

Lemma 3.5. *For all $n, m \in \mathbb{Z}$ we have* $\gcd(\beta_m, \beta_n) = |\beta_{\gcd(m,n)}|$.

Proof. By Lemma 3.4, for any prime p and any $V \in \mathbb{N}$ we have

$$\{n \in \mathbb{Z} : v_p(\beta_n) \geqslant V\} = \{n \in \mathbb{Z} : nP \in E_{V+v_p(P)}(\mathbb{Q}_p)\} = q\mathbb{Z}$$

for some $q \in \mathbb{N}$. In particular $p^V \mid \beta_n$ if and only if $q \mid n$. Therefore

$$p^V \mid \gcd(\beta_m, \beta_n) \iff q \mid \gcd(m, n) \iff p^V \mid \beta_{\gcd(m,n)}. \qquad \square$$

We emphasise that an EDSA need not be a strong divisibility sequence if P admits primes of bad reduction. The elegance of Verzobio's EDSB is that it has both good p-adic properties and comes within a whisker of satisfying the recurrence relation.

3.2 | Symmetry law

A central part of Ward's work on EDSs is a *symmetry law* [34, Theorem 8.1] (see [1, Theorem 1.11] for a modern formulation). This says that an integral EDSA modulo a prime forms a periodic sequence of a certain form. We prove a version of this for EDSBs for general prime powers.

Proposition 3.6. *Let M be as in Proposition 3.2. Let $n, r \in \mathbb{Z}$ with $M \mid r$. Let p be a prime and let $k \in \mathbb{N}$. Suppose that p^k divides $\beta_r / \gcd(\beta_r, \beta_M)$. Then for all $\ell \in \mathbb{Z}$ we have*

$$\beta_{n+\ell r} \equiv \begin{cases} \left(\beta_{M+r}\beta_{M-r}\beta_M^{-2}\right)^{\frac{\ell(\ell-1)}{2}} (\beta_{n+r}\beta_n^{-1})^{\ell}\beta_n \bmod p^k, & \text{if } p^k \nmid \beta_n, \\ 0 \bmod p^k, & \text{if } p^k \mid \beta_n, \end{cases}$$

where in the first case the quotients $\beta_{M+r}\beta_{M-r}/\beta_M^2$ and β_{n+r}/β_n are p-adic units.

Proof. Lemma 3.5 gives us

$$|\beta_{\gcd(n,r)}| = \gcd(\beta_{n+\ell r}, \beta_r) = \gcd(\beta_n, \beta_r) \tag{3.4}$$

for every $\ell \in \mathbb{Z}$. This proves the proposition if $p^k \mid \beta_n$, so assume that $p^k \nmid \beta_n$.

Taking $m = M$ in Proposition 3.2, and replacing n by $n + \ell r$, we obtain

$$\beta_{M+r}\beta_{M-r}\beta_{n+\ell r}^2 \equiv \beta_{n+(\ell+1)r}\beta_{n+(\ell-1)r}\beta_M^2 \bmod \beta_r^2, \tag{3.5}$$

for any $\ell \in \mathbb{Z}$. We want to combine this with Lemma 3.5. Let

$$C = \frac{\beta_{M+r}\beta_{M-r}}{\beta_M^2}, \quad a_\ell = \frac{\beta_{n+\ell r}}{\gcd(\beta_n, \beta_r)}. \tag{3.6}$$

Since $M \mid r$, Lemma 3.5 shows that $C \in \mathbb{Z}$. Also (3.4) shows that a_ℓ is an integer coprime to $\beta_r / \gcd(\beta_n, \beta_r)$. Hence, dividing both sides of (3.5) by $\beta_{n+\ell r}^2 \beta_M^2$ gives

$$C \equiv \frac{a_{\ell+1} a_{\ell-1}}{a_\ell^2} \bmod \frac{\beta_r^2}{\gcd(\beta_n \beta_M, \beta_r)^2} \quad \text{for all } \ell \in \mathbb{Z}, \tag{3.7}$$

where every a_ℓ is coprime to the modulus. It follows by induction on ℓ from (3.7) that

$$a_\ell \equiv C^{\frac{\ell(\ell-1)}{2}} a_1^\ell a_0^{1-\ell} \bmod \frac{\beta_r^2}{\gcd(\beta_n \beta_M, \beta_r)^2}.$$

Multiplying by $\gcd(\beta_n, \beta_r)$ we obtain

$$a_\ell \gcd(\beta_n, \beta_r) \equiv C^{\frac{\ell(\ell-1)}{2}} (a_1 a_0^{-1})^\ell a_0 \gcd(\beta_n, \beta_r) \bmod \frac{\gcd(\beta_n, \beta_r) \beta_r^2}{\gcd(\beta_n \beta_M, \beta_r)^2}.$$

Here $\beta_r / \gcd(\beta_M, \beta_r)$ divides the modulus, and so the congruence holds modulo p^k. Inserting the definitions (3.6) proves the first case in the proposition.

Finally, since $p^k \mid \beta_r / \gcd(\beta_M, \beta_r)$ and $p^k \nmid \beta_n$, we see that p divides the modulus in (3.7). Since every a_ℓ is coprime to the modulus, we see that C and $\beta_{n+r} \beta_n^{-1} = a_1 a_0^{-1}$ are p-adic units, as claimed in the final part of the proposition. □

3.3 | Periodicity

We now use the symmetry law to prove that β_n is periodic modulo any prime power, and hence modulo any integer. Versions of this appear in the literature for differing definitions of EDS. Ward proved eventual periodicity modulo any prime in [34, Theorem 11.1]. Shipsey proved a version modulo p^2 for primes of good reduction [23, Theorem 3.5.4]. Ayad proved it modulo any integer, but assuming good reduction and avoiding $p = 2$ or 'rank of apparition 2' [3, Theorem D]. Silverman proved a version over finite fields [25, Theorem 1] as well as a version modulo prime powers whenever the curve has good ordinary reduction [25, Theorem 3]. Our version (Proposition 3.7) contains none of these technical assumptions and is a general version of periodicity, for Verzobio's arguably more elegant EDSB.

Our result is the following, which shows periodicity modulo an arbitrary prime power and gives an upper bound for the period. Note that the Chinese Remainder theorem then easily shows periodicity modulo an arbitrary integer.

Proposition 3.7. *Let M be as in Proposition 3.2, let $k \in \mathbb{N}$ and let p be a prime. Let*

$$r(p^k) = M \operatorname{ord}(MP \bmod p^{k+v_p(MP)}) \tag{3.8}$$

and

$$\pi(p^k) = \begin{cases} (p-1)p^{k-1} r(p^k), & \text{if } p \neq 2 \text{ and } \left(\frac{\beta_{M+r(p^k)} \beta_{M-r(p^k)}}{p} \right) = 1, \\ 2(p-1)p^{k-1} r(p^k), & \text{otherwise.} \end{cases} \tag{3.9}$$

Then for every $m \in \mathbb{Z}$ we have

$$m \equiv n \bmod \pi(p^k) \;\Rightarrow\; \beta_m \equiv \beta_n \bmod p^k.$$

In other words the sequence $\beta_m \bmod p^k$ is periodic with period dividing $\pi(p^k)$.

We could slightly simplify the proof by defining $\pi(p^k) = 2(p-1)p^{k-1}r(p^k)$ in all cases. However it is of some interest to find cases in which $4 \nmid \pi(p^k)$, because this allows us to remove the condition $P \in E(\mathbb{R})^0$ in some of our results (see Theorem 1.6). This is our reason to include the first case in (3.9).

Proof. For ease of notation we write $r = r(p^k)$ throughout the proof.

We first observe that $rP \equiv O \bmod p^{k+v_p(MP)}$ by (3.8). That is we have $k + v_p(MP) \leqslant v_p(rP)$, and hence by Lemma 3.4 and (3.8) we have

$$p^k \text{ divides } \frac{\beta_r}{\gcd(\beta_M, \beta_r)} \quad \text{and} \quad M \mid r. \tag{3.10}$$

Let $n \in \mathbb{Z}$. By (3.10), the hypotheses of Proposition 3.6 are satisfied. If $p^k \mid \beta_n$ then the result follows immediately; suppose therefore that $p^k \nmid \beta_n$. Proposition 3.6 shows that

$$\beta_{n+\ell r} \equiv \left(\beta_{M+r}\beta_{M-r}\beta_M^{-2}\right)^{\frac{\ell(\ell-1)}{2}} (\beta_{n+r}\beta_n^{-1})^{\ell}\beta_n \mod p^k,$$

for every $\ell \in \mathbb{Z}$, where $\beta_{M+r}\beta_{M-r}\beta_M^{-2}, \beta_{n+r}\beta_n^{-1}$ are p-adic units. In particular $\gcd(\beta_n, p^k) = \gcd(\beta_{n+\ell r}, p^k) = \gcd(\beta_n, \beta_r, p^k)$.

Now $\#(\mathbb{Z}/p^k\mathbb{Z})^\times = (p-1)p^{k-1}$, and so if $u \in \mathbb{Z}_p^\times$ then

$$2(p-1)p^{k-1} \mid \ell \Rightarrow u^{\frac{\ell(\ell-1)}{2}} \equiv 1 \bmod p^k.$$

Moreover if $p \neq 2$ and $\left(\frac{u}{p}\right) = 1$ then $u = v^2$ for $v \in \mathbb{Z}_p^\times$. So

$$(p-1)p^{k-1} \mid \ell,\ p \neq 2,\ \left(\frac{u}{p}\right) = 1 \Rightarrow u^{\frac{\ell(\ell-1)}{2}} \equiv 1 \bmod p^k.$$

Thus by definition of $\pi(p^k)$, if $\pi(p^k) \mid \ell r$ then

$$\left(\beta_{M+r}\beta_{M-r}\beta_M^{-2}\right)^{\frac{\ell(\ell-1)}{2}} (\beta_{n+r}\beta_n^{-1})^{\ell} \equiv 1 \bmod p^k,$$

which implies

$$\beta_{n+\ell r} \equiv \beta_n \bmod p^k.$$

Writing $m = n + \ell r$ completes the proof. □

There is a simpler, but slightly weaker, bound for the period.

Lemma 3.8. *Let M be as in Proposition 3.2, let $k \in \mathbb{N}$, and let p be a prime. Then the period of $\beta_n \bmod p^k$ divides*

$$\begin{cases} 2M(p-1)p^{2(k-1)} \operatorname{ord}(MP \bmod p), & \text{if } v_p(MP) = 0, \\ 2M(p-1)p^{2k-1}, & \text{otherwise.} \end{cases}$$

Proof. Let $Q = MP$. By Proposition 3.7, it suffices to show that

$$\operatorname{ord}(Q \bmod p^{k+v_p(Q)}) \text{ divides } r_1(p^k) := \begin{cases} p^{k-1} \operatorname{ord}(Q \bmod p), & \text{if } v_p(Q) = 0, \\ p^k, & \text{otherwise.} \end{cases}$$

If $v_p(Q) = 0$ then Lemma 2.4 implies that $v_p(p^{k-1} \operatorname{ord}(Q \bmod p)Q) \geqslant k - 1 + v_p(\operatorname{ord}(Q \bmod p)Q) \geqslant k$. If $v_p(Q) > 0$ then Lemma 2.4 yields $v_p(p^k Q) \geqslant k + v_p(Q)$. In both cases $r_1(p^k)Q \equiv 0 \bmod p^{k+v_p(Q)}$, as required. □

Remark 3.9. By definition M divides $\prod_p |E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)|$, hence is bounded uniformly with respect to P. Moreover $\operatorname{ord}(MP \bmod p)$ divides $|E_0(\mathbb{Q}_p)/E_q(\mathbb{Q}_p)|$. Thus Lemma 3.8 shows that the period of $\beta_n \bmod N$ can be bounded independently of P for all $N \in \mathbb{N}$, with the bound only depending on E and N.

3.4 | Signs

Recall from Definition 3.1 that the sign of β_n is the sign of the sequence $\psi_n(P)$. The following is [27, Theorem 4] (see also [2] for a generalisation.)

Proposition 3.10 (Silverman–Stephens). *There is a sign $\sigma \in \{\pm 1\}$ and an irrational number β such that for all $n \in \mathbb{N}$ we have*

$$\sigma^{n-1} \operatorname{sign}(\beta_n) = \begin{cases} (-1)^{\lfloor n\beta \rfloor}, & \text{if } P \in E(\mathbb{R})^0, \\ (-1)^{\lfloor n\beta \rfloor + \frac{n}{2}}, & \text{if } P \notin E(\mathbb{R})^0 \text{ and } n \text{ is even,} \\ (-1)^{\frac{n-1}{2}}, & \text{if } P \notin E(\mathbb{R})^0 \text{ and } n \text{ is odd.} \end{cases}$$

If $P \in E(\mathbb{R})^0$ then β is defined as follows. We fix an $\mathbb{R}$-analytic group isomorphism $\psi : E(\mathbb{R})^0 \to \mathbb{R}^*_{>0}/e^{\mathbb{Z}}$. Then let $\beta = \log u$ where u is a representative of $\psi(P)$ in $\mathbb{R}^*_{>0}$ with $e^{-1} < u < 1$.

In Silverman and Stephens' original statement of the theorem there is an isomorphism $E(\mathbb{R}) \to \mathbb{R}^*/q^{\mathbb{Z}}$, which maps $E(\mathbb{R})^0$ to either $\mathbb{R}^*_{>0}/q^{\mathbb{Z}}$ if $q > 0$ or $\mathbb{R}^*_{>0}/q^{2\mathbb{Z}}$ otherwise. Without loss of generality we can assume that $E(\mathbb{R})^0$ is mapped to $\mathbb{R}^*_{>0}/e^{\mathbb{Z}}$, or else we can compose our isomorphism with $v \mapsto v^{-1/\log q}$ or $v^{-1/2\log q}$. When $P \in E(\mathbb{R})^0$ their choice of u then satisfies $e^{-1} < u < 1$ as above.

We want to say something about the Diophantine approximation properties of the irrational number β from the theorem. Let $\exp_E : \mathbb{C} \to E(\mathbb{C})$ be the usual parametrisation of E using the Weierstrass $\wp$-function, see for example [26, Corollary VI.5.1.1]. Bosser and Gaudron [6, Theorem 1.2] proved:

Proposition 3.11 (Bosser–Gaudron). *Let $z \in \mathbb{C}$ such that $\exp_E(z) \in E(\mathbb{Q}) \setminus \{O\}$. Then we have*

$$\log|z| \gg_E -1 - \widehat{h}(\exp_E z),$$

where $\widehat{h}$ is the canonical height, as in Section 1.6.

A remark about the definition of $\exp_E : \mathbb{C} \to E(\mathbb{C})$ may be helpful. The usual convention would be to normalise this map so that in a certain sense the derivative of $\exp_E$ at the origin is the identity. This is not necessary for our purposes, and the naive parametrisation familiar from a first course on elliptic curves suffices. We use only the fact that $\exp_E$ is a fixed $\mathbb{R}$-analytic surjective additive group homomorphism, and Proposition 3.11 which holds regardless of normalisation. We use these to prove

Lemma 3.12. *Suppose the point P from the start of this section satisfies $P \in E(\mathbb{R})^0$. Let β be as in Proposition 3.10, and let $N \in \mathbb{Z} \setminus \{0\}$. Then*

$$\min_{M\in\mathbb{Z}} \log|N\beta - M| \gg_E -1 - \widehat{h}(NP).$$

Proof. Let $w \in \mathbb{C}^*$ such that $\exp_E(w) = P$, so that $\exp_E(w\mathbb{R}) = E(\mathbb{R})^0$ and $\psi(\exp_E(tw)) = e^{t\beta+\mathbb{Z}}$ for any $t \in \mathbb{R}$. For any $M \in \mathbb{Z}$ we deduce that

$$\exp_E(N + \beta^{-1}M) = \phi^{-1}(e^{N\beta+M+\mathbb{Z}}).$$

By the definition of β we deduce $\exp_E(N + \beta^{-1}M) = \phi^{-1}(u^N e^{\mathbb{Z}})$ which is NP by definition of u. That is,

$$\exp_E^{-1}(NP) \supseteq \{(N + \beta^{-1}M)w : M \in \mathbb{Z}\}.$$

Now by Proposition 3.11, any t such that $tw \in \exp_E^{-1}(NP)$ has $\log|t| \gg_E -1 - \widehat{h}(NP)$, and so

$$\min_{M\in\mathbb{Z}} \log|N\beta - M| \gg_E -1 - \widehat{h}(NP).$$

□

3.5 | Main result

We now provide the main technical input required for the results stated in the introduction (Proposition 3.19). Under certain assumptions, it stipulates the existence of many prime-numbered elements of the sequence β_n which are divisible by primes to a certain valuation that are non-trivial with respect to a given Dirichlet character. We require an effective version of uniform distribution modulo 1 for primes in an arithmetic progression multiplied by an irrational. This is deduced from an exponential sum estimate. To begin, we quote two standard results on exponential sums in primes from Vaughan [31, Theorem 3.1, Lemma 3.1].

Lemma 3.13 (Vinogradov). *If $\alpha \in \mathbb{R}, a \in \mathbb{Z}, q \in \mathbb{N}$ with $\gcd(a,q) = 1, q \leqslant y$, and $|\alpha - a/q| \leqslant q^{-2}$ then*

$$\sum_{\substack{p\leqslant y\\ p \text{ prime}}} (\log p)e(\alpha p) \ll (\log y)^4(yq^{-1/2} + y^{4/5} + y^{1/2}q^{1/2}).$$

Lemma 3.14 (Siegel–Walfisz for linear exponential sums). *Let $B > 0$. If $\alpha \in \mathbb{R}, a \in \mathbb{Z}, q \in \mathbb{N}$ with $\gcd(a,q) = 1, q \leqslant (\log y)^B$ and $|\alpha - a/q| \leqslant (\log y)^B/y$ then there is $C_B > 0$ such that*

$$\sum_{\substack{p \leqslant y \\ p \text{ prime}}} e(\alpha p) = \frac{\mu(q)}{\varphi(q)} \sum_{m=1}^{y} e((\alpha - a/q)m) + O_B(y \exp(-C_B\sqrt{\log y})),$$

where μ is the Möbius function and φ is the Euler totient function.

We use these to estimate sums of the form $\sum_{\ell \leqslant y, \ell \text{ prime}} (\log \ell) e(\alpha \ell)$.

Lemma 3.15. *Suppose that we have $\alpha \in \mathbb{R}, a \in \mathbb{Z}, q \in \mathbb{N}, y \in \mathbb{R}$ such that*

$$\gcd(a,q) = 1, \quad q \leqslant y \quad |\alpha - a/q| \leqslant 1/qy. \tag{3.11}$$

Then

$$\sum_{\substack{\ell \leqslant y \\ \ell \text{ prime}}} (\log \ell) e(\alpha \ell) \ll y(\log y)^{-1} + \frac{y \log\log q}{q}. \tag{3.12}$$

Proof. If $q \leqslant (\log y)^5$ we apply Lemma 3.14; otherwise we apply Lemma 3.13. Recalling the standard bound $\varphi(q) \gg \frac{q}{\log\log q}$ gives the result. □

From this simple estimate we pass to a more difficult exponential sum.

Lemma 3.16. *Let $s, t \in \mathbb{N}$ with $\gcd(s,t) = 1$ and let β be as in Proposition 3.10. For all $y \geqslant e^{e^e}$, $j \in \mathbb{N}$ we have*

$$\sum_{\substack{\ell \leqslant y \\ \ell \equiv s \bmod t \\ \ell \text{ prime}}} (\log \ell) e(j\ell\beta/2) \ll_E ytj \sqrt{\frac{\widehat{h}(P)}{\log y}} \log\log\log y. \tag{3.13}$$

Proof. Fix $y \geqslant 1, j \in \mathbb{N}$. We use the formula

$$\frac{1}{t} \sum_{m \in \mathbb{Z}/t\mathbb{Z}} e(m(n-s)/t) = \begin{cases} 1, & n \equiv s \bmod t, \\ 0, & \text{otherwise}, \end{cases}$$

which is valid for all integers n. This gives

$$\sum_{\substack{\ell \leqslant y \\ \ell \equiv s \bmod t}} (\log \ell) e(j\ell\beta/2) = \frac{1}{t} \sum_{m \in \mathbb{Z}/t\mathbb{Z}} e(-ms/t) \sum_{\ell \leqslant y} (\log \ell) e((m/t + j\beta/2)\ell).$$

We apply Lemma 3.15 to estimate the final sum in (3.13). We set

$$\alpha = m/t + j\beta/2. \tag{3.14}$$

We fix $a \in \mathbb{Z}, q \in \mathbb{N}$ satisfying (3.11), noting that the existence of such (a, q) is guaranteed by Dirichlet's approximation theorem. Then (3.12) becomes

$$\sum_{\ell \leqslant y} (\log \ell) e((m/t + j\beta/2)\ell) \ll \frac{y}{\log y} + \frac{y \log\log q}{q}. \tag{3.15}$$

For this to be useful we need to deduce from (3.11) and (3.14) a lower bound on q. We are going to prove that

$$\text{either} \quad y \leqslant t^{3/2} \quad \text{or} \quad q \geqslant \frac{1}{tj} \sqrt{\frac{\log y}{\widehat{h}(P)}}. \tag{3.16}$$

We start with the final condition in (3.11), and multiply it by $2tq$ to get

$$\log(2t/y) \geqslant \min_{M \in \mathbb{Z}} \log |2tq\alpha - M|.$$

The definition (3.14) gives

$$\min_{M \in \mathbb{Z}} \log |2tq\alpha - M| = \min_{M \in \mathbb{Z}} \log |tjq\beta - M|,$$

and by Lemma 3.12 with $N = tjq$ we have

$$\min_{M \in \mathbb{Z}} \log |tjq\beta - M| \gg_E -1 - \widehat{h}(tjqP).$$

Putting the last three displays together gives us

$$\widehat{h}(tjqP) + 1 \gg_E \log(y/2t).$$

Recalling that $\widehat{h}$ is a quadratic form on $E(\mathbb{Q}) \otimes \mathbb{R}$, we have $\widehat{h}(tjqP) = (tjq)^2 \widehat{h}(P)$ and so

$$-1 + \log(y/t) \ll_E (tjq)^2 \widehat{h}(P).$$

Provided $y \geqslant t^{3/2}$, this implies that $\log y \ll_E (tjq)^2 \widehat{h}(P)$, which is (3.16).

We substitute (3.16) into (3.15) and recall that $\log\log\log y \geqslant 1$ by assumption, to show that either

$$\sum_{\ell \leqslant y} (\log \ell) e(\ell(m/t + j\beta/2)) \ll_E y(\log y)^{-1} + ytj \sqrt{\frac{\widehat{h}(P)}{\log y}} \log\log\log y \quad \text{or} \quad y \leqslant t^{3/2}.$$

In the latter case we have $\sum_{\ell \leqslant y} (\log \ell) e(\ell(m/t + j\beta/2)) \ll y \leqslant y^{1/3} t$ by the Prime Number theorem. So in either case

$$\sum_{\ell \leqslant y} (\log \ell) e(\ell(m/t + j\beta/2)) \ll_E y^{1/3} t + y(\log y)^{-1} + ytj \sqrt{\frac{\widehat{h}(P)}{\log y}} \log\log\log y.$$

Since $\widehat{h}(P) \gg_E 1$ this implies (3.13). □

To apply the previous lemma we turn to the Erdős–Turán inequality [10, Theorem III]:

Lemma 3.17 (Erdős–Turán). *For any $0 \leqslant a < b \leqslant 1$, any real sequence t_m, any $M \in \mathbb{N}$ and any $H > 0$ we have*

$$\left|(b-a)M - \sum_{m=1}^{M} \mathbf{1}_{\{t_m\}\in[a,b)}\right| \ll \frac{M}{H} + \sum_{1\leqslant j\leqslant H} \frac{1}{j}\left|\sum_{m=1}^{M} e(jt_m)\right|,$$

where we write $\{\cdot\}$ for the fractional part, and $\mathbf{1}_{\{t_m\}\in[a,b)} = 1$ if $\{t_m\} \in [a,b)$ and 0 otherwise.

We are now ready to prove our equidistribution result.

Proposition 3.18. *Suppose the point P from the start of this section satisfies $P \in E(\mathbb{R})^0$. Let $s, t \in \mathbb{N}$ with $\gcd(s,t) = 1$ and let β be as in Proposition 3.10. For any $0 \leqslant a < b \leqslant 1$ and any $\epsilon > 0$ we have*

$$\begin{aligned}&\#\{\text{primes } \ell \leqslant x : \ell \equiv s \bmod t, \{\ell\beta/2\} \in [a,b)\}\\ &= \left(\frac{b-a}{\varphi(t)} + O_{E,\epsilon}\left(\frac{t^{\epsilon}(\log\log\log x)^2\widehat{h}(P)}{\log x}\right)^{1/4}\right)\frac{x}{\log x},\end{aligned}$$

where we write $\{\cdot\}$ for the fractional part. In particular for any $\epsilon > 0$ and any $\sigma \in \{\pm 1\}$ we have

$$\begin{aligned}&\#\{\text{primes } \ell \leqslant x : \ell \equiv s \bmod t, (-1)^{\lfloor \ell\beta\rfloor} = \sigma\}\\ &= \left(\frac{1}{2\varphi(t)} + O_{E,\epsilon}\left(\frac{t^{\epsilon}(\log\log\log x)^2\widehat{h}(P)}{\log x}\right)^{1/4}\right)\frac{x}{\log x}.\end{aligned}$$

Proof. For the second part, we note that $(-1)^{\lfloor \ell\beta\rfloor} = 1$ if and only if $0 \leqslant \{\ell(\beta/2)\} < 1/2$. So it suffices to prove the first claim in the proposition.

During the proof we will repeatedly use the fact that $\widehat{h}(P) \gg_E 1$, which holds by for example [26, Theorem VIII.9.10(a)]. If $t > (\log x)^{1/\epsilon}$ then the bound follows at once from this last result and the Prime Number theorem. We will assume from now on that $t \leqslant (\log x)^{1/\epsilon}$.

Throughout the proof we write $e(y) = \exp(2\pi i y)$.

We first apply Lemma 3.17 with M, t_m as follows. Denote the primes $\ell \equiv s \bmod t, \ell \leqslant x$ by $\ell_1, \dots, \ell_M$ and let $t_m = \{\ell_m\beta/2\}$. There is $c > 0$ such that for each $B > 0$ with $t \leqslant (\log x)^B$, we have

$$M = \frac{x}{\varphi(t)\log x} + O\left(\frac{x}{\varphi(t)(\log x)^2}\right) + O_B(x\exp(-c\sqrt{\log x})),$$

by the Siegel–Walfisz theorem [20, Corollary 11.21, see also p. 5]. In particular, setting $B = 1/\epsilon$ and recalling that $t \leqslant (\log x)^{1/\epsilon}$ and thus $\exp(c\sqrt{\log x}) \gg_{\epsilon} t(\log x)^2$, it follows that

$$M = \frac{x}{\varphi(t)\log x} + O\left(\frac{x}{\varphi(t)(\log x)^2}\right),$$

We substitute this into Lemma 3.17 to obtain

$$\#\{m \leqslant M : \{\ell_m \beta/2\} \in [a,b)\} - \frac{(b-a)x}{\varphi(t)\log x} \tag{3.17}$$

$$\ll \frac{x}{H\varphi(t)\log x} + \frac{x}{\varphi(t)(\log x)^2} + \sum_{1\leqslant j\leqslant H} \frac{1}{j} \left| \sum_{\substack{\ell \leqslant x \\ \ell \equiv s \bmod t}} e(j\ell\beta/2) \right|. \tag{3.17}$$

Our goal is to estimate the last sum above. As often happens it is convenient to count primes weighted by the von Mangoldt function. By partial summation,

$$\sum_{\substack{\ell \leqslant x \\ \ell \equiv s \bmod t \\ \ell \text{ prime}}} e(j\ell\beta/2) = \frac{1}{\log x} \sum_{\substack{\ell \leqslant x \\ \ell \equiv s \bmod t \\ \ell \text{ prime}}} (\log \ell) e(j\ell\beta/2)$$

$$+ \int_1^x \frac{1}{y(\log y)^2} \sum_{\substack{\ell \leqslant y \\ \ell \equiv s \bmod t \\ \ell \text{ prime}}} (\log \ell) e(j\ell\beta/2)\, \mathrm{d}y. \tag{3.18}$$

It follows from Lemma 3.16 and (3.18) that for each non-zero integer j we have

$$\sum_{\substack{\ell \leqslant x \\ \ell \equiv s \bmod t \\ \ell \text{ prime}}} e(j\ell\beta/2) \ll_E \frac{x}{\log x} \cdot tj\sqrt{\frac{\widehat{h}(P)}{\log x}} \log\log\log x.$$

Together with (3.17) and the choice

$$H = \left(\frac{\log x}{\widehat{h}(P)}\right)^{1/4} (t\varphi(t)\log\log\log x)^{-1/2},$$

this implies that

$$\#\{m \leqslant M : \{\ell_m \beta/2\} \in [a,b)\} - \frac{(b-a)x}{\varphi(t)\log x}$$

$$\ll \frac{x}{\log x} \cdot \left(\frac{1}{\varphi(t)\log x} + \left(\frac{\widehat{h}(P)}{\log x}\right)^{1/4} \left(\frac{t\log\log\log x}{\varphi(t)}\right)^{1/2} \right).$$

The result follows since $\widehat{h}(P) \gg_E 1$ and $\varphi(t) \gg_\epsilon t^{1-\epsilon}$. □

Our main result is now as follows. In the statement $\mathrm{ord}(\chi(p))$ denotes the multiplicative order of the root of unity $\chi(p)$.

Proposition 3.19. *Let χ be a Dirichlet character with modulus $q(\chi)$. Let π be the period of β_n mod $q(\chi)$. Suppose that there exists $\alpha \in \mathbb{N}$ such that*

$$\gcd(\alpha, \pi) = 1 \tag{3.19}$$

and such that one of the following holds:

$$\begin{aligned} &\chi(|\beta_\alpha|) \neq 0, 1, \quad \textit{or} \\ &\chi(-|\beta_\alpha|) \neq 0, 1 \textit{ and } 4 \nmid \pi, \quad \textit{or} \\ &\chi(-|\beta_\alpha|) \neq 0, 1 \textit{ and } P \in E(\mathbb{R})^0. \end{aligned} \tag{3.20}$$

Then for any $\epsilon > 0$ and $x > \exp(\pi^2)$ we have

$$\#\{\textit{primes } \ell \leqslant x : \operatorname{ord}(\chi(p)) \nmid v_p(\beta_\ell) \textit{ for some prime } p \nmid q(\chi)\} \geqslant \left(\frac{1}{2\varphi(\pi)} + O_{E,\epsilon}\left(\frac{\pi^\epsilon (\log\log\log x)^2 \widehat{h}(P)}{\log x}\right)^{1/4}\right)\frac{x}{\log x}.$$

Proof. From (3.20), there is $\tau \in \{\pm 1\}$ such that $\chi(\tau|\beta_\alpha|) \neq 0, 1$. We separate into two cases depending on the real properties of P.

Case 1. $P \in E(\mathbb{R})^0$: From Proposition 3.10 we have $\operatorname{sign}(\beta_n) = \sigma^{n-1}(-1)^{\lfloor n\beta \rfloor}$ for some $\sigma \in \{\pm 1\}$ and some irrational number β. Now consider the set of primes

$$\Lambda = \{\ell \text{ prime} : \ell \equiv \alpha \bmod \pi, \operatorname{sign}(\beta_\ell) = \tau \operatorname{sign}(\beta_\alpha)\}.$$

Let $\ell \in \Lambda$. Then by periodicity we have $\beta_\ell \equiv \beta_\alpha \bmod q(\chi)$, so $\chi(\beta_\ell) = \chi(\beta_\alpha)$ as χ is periodic modulo $q(\chi)$. Moreover, we have arranged signs so that $\chi(|\beta_\ell|) = \chi(\tau|\beta_\alpha|) \neq 0, 1$. Hence as χ is multiplicative we deduce the existence of a prime factor p of $|\beta_\ell|$ with $p \nmid q(\chi)$ and $\operatorname{ord}(\chi(p)) \nmid v_p(\beta_\ell)$. It thus suffices to note that $\{\ell \in \Lambda : \ell \leqslant x\}$ satisfies the required lower bound by (3.19) and Proposition 3.18.

Case 2. $P \notin E(\mathbb{R})^0$: In order to handle a number of subcases simultaneously, we show that there is $\iota \in \{0, 1, 2, 3\}$ such that $\alpha + \iota\pi$ is odd and

$$(-1)^{(\alpha+\iota\pi-1)/2} = \begin{cases} \tau \operatorname{sign}(\beta_\alpha), & \text{if } \alpha \text{ is even}, \\ \tau(-1)^{(\alpha-1)/2}, & \text{if } \alpha \text{ is odd}. \end{cases} \tag{3.21}$$

Case 2.1. $2 \mid \alpha$. Here π is odd by (3.19). Choosing $\iota \in \{1, 3\}$ we can arrange for $\frac{\alpha+\iota\pi-1}{2}$ to be odd or even, and hence $(-1)^{(\alpha+\iota\pi-1)/2} = -1$ or 1 to satisfy (3.21).

Case 2.2. $2 \nmid \alpha$ and $4 \mid \pi$. Here we have $\tau = 1$ by (3.20). Let $\iota = 0$ and then $(-1)^{(\alpha-1)/2} = \tau(-1)^{(\alpha-1)/2}$ as required for (3.21).

Case 2.3. $2 \nmid \alpha$ and $4 \nmid \pi$. We can choose $\iota \in \{0, 2\}$ so that $\iota\pi/2$ is odd or even as needed. So we arrange $(-1)^{\iota\pi/2} = \tau$ which gives (3.21).

We now let $q = \operatorname{lcm}(4, \pi)$ and consider primes ℓ of the form $\ell \equiv \alpha + \iota\pi \bmod q$. By Proposition 3.10 and (3.21) we then have $\operatorname{sign}(\beta_\ell) = \tau \operatorname{sign}(\beta_\alpha)$. But $\beta_\ell \equiv \beta_\alpha \bmod q(\chi)$ by periodicity, so $\chi(|\beta_\ell|) = \chi(\tau|\beta_\alpha|) \neq 0, 1$ by (3.20) as χ is periodic modulo $q(\chi)$. We are now in a similar situation to Case 1. Here (3.19) and the fact that $\alpha + \iota\pi$ is odd implies that $\gcd(\alpha + \iota\pi, q) = 1$. Together with the assumption that $\pi < \sqrt{\log x}$ in the proposition, this allows us to apply the Siegel–Walfisz

theorem [20, Corollary 11.21] to show that the set under consideration has size

$$\frac{x}{\varphi(q)\log x}+O\left(\frac{qx}{(\log x)^2}\right)\geqslant\left(\frac{1}{2\varphi(\pi)}+O\left(\frac{\pi}{\log x}\right)\right)\frac{x}{\log x}.$$

Using again the fact that $\pi<\sqrt{\log x}$, the claim follows. □

Remark 3.20. Aside from finitely many exceptions, we expect that the primes p constructed in Proposition 3.19 satisfy the stronger condition $v_p(\beta_\ell)=1$. This is the condition referred to in Section 1.3 as being a 'non-Wieferich prime for base $P\in E$'.

4 | BRAUER GROUPS

The aim of this section is to prove Theorem 1.6. We begin with some preliminaries on Brauer groups.

4.1 | Recap of Brauer groups

For a scheme X we denote by $\operatorname{Br}X=\mathrm{H}^2(X,\mathbb{G}_{\mathrm{m}})$ its (cohomological) Brauer group. If X is regular and integral and $D\subset X$ is a regular integral divisor, then there is an associated residue map

$$\partial_D:\operatorname{Br}(X\setminus D)[\ell^\infty]\to\mathrm{H}^1(D,\mathbb{Q}/\mathbb{Z}),$$

where ℓ is any prime which is invertible on X. We say that $b\in\operatorname{Br}(X\setminus D)$ whose order is invertible on X is *unramified* at D if $\partial_D(b)=0$; in which case Grothendieck's purity theorem [9, Theorem 3.7.1] implies that $b\in\operatorname{Br}X$.

For any $b\in\operatorname{Br}X$ and any point $x\in X$, there is a well-defined specialisation $b(x)\in\operatorname{Br}\kappa(x)$. For a field k we denote by

$$X(k)_b=\{x\in X(k):\ b(x)=0\in\operatorname{Br}k\}\tag{4.1}$$

the zero locus of b on k-rational points. If only $b\in\operatorname{Br}\kappa(X)$, then we abuse notation and write

$$X(k)_b=\{x\in X(k)\ :\ b\text{ defined at }x,b(x)=0\in\operatorname{Br}k\}.$$

If $\dim X=1$, then this just means we implicitly remove the finitely many points where b is ramified. For a number field k, there is an exact sequence

$$0\to\operatorname{Br}k\to\bigoplus_v\operatorname{Br}k_v\to\mathbb{Q}/\mathbb{Z}\to0,\tag{4.2}$$

where the last map is the sum of all local invariants $\operatorname{inv}_v:\operatorname{Br}k_v\to\mathbb{Q}/\mathbb{Z}$ of k [9, Theorem 13.1.8]. The local invariant is defined in terms of residues, by applying the residue to $\operatorname{Br}\mathcal{O}_v$ then using $\mathrm{H}^1(\mathbb{F}_v,\mathbb{Q}/\mathbb{Z})=\operatorname{Hom}(\operatorname{Gal}(\bar{\mathbb{F}}_v/\mathbb{F}_v),\mathbb{Q}/\mathbb{Z})$ and evaluating the resulting homomorphism at the Frobenius element [9, Definition 13.1.7].

4.2 | Specialisation of Brauer groups on elliptic curves

We now prepare for the proof of Theorem 1.6. Let E be an elliptic curve over $\mathbb{Q}$ given by a Weierstrass equation with coefficients in $\mathbb{Z}$. Let $b \in \mathrm{Br}\,\mathbb{Q}(E)$ which we assume is ramified at some rational point P. The residue of b at P is an element of $\mathrm{H}^1(\mathbb{Q}, \mathbb{Q}/\mathbb{Z})$. We associate to this a Dirichlet character χ as follows.

4.2.1 | Associated Dirichlet character

Firstly the residue of b at P yields a group homomorphism via the identification $\mathrm{H}^1(\mathbb{Q}, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \mathbb{Q}/\mathbb{Z})$. Let $K/\mathbb{Q}$ be the cyclic extension determined by the kernel. By the Kronecker–Weber theorem, there is an embedding $K \subseteq \mathbb{Q}(\mu_q)$ where q is the conductor of K. As $\mathrm{Gal}(\mathbb{Q}(\mu_q)/\mathbb{Q}) \cong (\mathbb{Z}/q\mathbb{Z})^\times$ canonically, composing with $\mathrm{Gal}(\mathbb{Q}(\mu_q)/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q})$ yields a homomorphism $(\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{Q}/\mathbb{Z}$. Recalling that we chose an embedding $\mathbb{Q}/\mathbb{Z} \subset \mathbb{C}^\times$ in Section 1.6, we obtain a primitive Dirichlet character χ modulo q on extending to $\mathbb{Z}$. (In our work we will care only about the order of $\chi(p)$, which is independent of the choice of embedding $\mathbb{Q}/\mathbb{Z} \subset \mathbb{C}^\times$.) For a prime p, this satisfies

$$\chi(p) = 0 \iff p \mid q, \quad \chi(p) = 1 \iff p \text{ is completely split in } K.$$

For example, if $K = \mathbb{Q}(\sqrt{D})$ where D is a fundamental discriminant, then we obtain the quadratic character $m \mapsto (\frac{D}{m})$ given by the Kronecker symbol.

4.2.2 | Specialisation

Let $\mathcal{E}$ be the natural projective model for E over $\mathbb{Z}$ determined by the Weierestrass equation. There exists a non-empty regular open subscheme $\mathcal{E}^\circ \subseteq \mathcal{E}$ such that $b \in \mathrm{Br}\,\mathcal{E}^\circ$.

We choose a finite set of primes S of $\mathbb{Q}$ containing all primes dividing $\mathrm{ord}(\chi)q(\chi)$, where $q(\chi)$ is the conductor of χ. We then have the following criterion for triviality of the specialisation, which gives a direct way of evaluating Brauer group elements via Dirichlet characters.

Proposition 4.1. *Assume that b is ramified at O with associated Dirichlet character χ. Let $p \notin S$ and $Q \in \mathcal{E}^\circ(\mathbb{Q}_p)$ with $v_p(Q) \geqslant 1$. Then $b(Q) = 0 \in \mathrm{Br}\,\mathbb{Q}_p$ if and only if $\mathrm{ord}(\chi(p)) \mid v_p(Q)$.*

Proof. We let $\mathcal{O}$ and $\mathcal{Q}$ be the closure of O and Q in $\mathcal{E}_p := \mathcal{E} \otimes \mathbb{Z}_p$, respectively. Note that $\mathcal{O}$ is a smooth subscheme of $\mathcal{E}_p$, since the partial derivative with respect to z is non-zero at O modulo p. As $v_p(Q) \geqslant 1$, by definition $Q \in E_1(\mathbb{Q}_p)$, so $\mathcal{Q} \equiv \mathcal{O} \bmod p$. Thus $\mathcal{Q} \cap \mathcal{O} = v_p(Q)O_p$ as a divisor on $\mathcal{Q}$, where $O_p = (0 : 1 : 0) \bmod p$.

We now apply [9, Theorem 3.7.5] with $X = (\mathcal{E}^\circ \otimes \mathbb{Z}_p) \cup \mathcal{O}, Y = \mathcal{O}$ and $f : \mathcal{Q} \to X$ the natural inclusion. This gives that the residue $\partial_{O_p}(f^*b) \in \mathrm{H}^1(O_p, \mathbb{Q}/\mathbb{Z})$ is equal to the image of $v_p(Q) \cdot (\partial_{\mathcal{O}}\, b)$ under the map

$$\mathrm{H}^1(\mathcal{O}, \mathbb{Q}/\mathbb{Z}) \to \mathrm{H}^1(O_p, \mathbb{Q}/\mathbb{Z}).$$

Let $\psi \in \mathrm{Hom}(\pi_1(\mathrm{Spec}\,\mathbb{Z}_p), \mathbb{Q}/\mathbb{Z})$ be the homomorphism corresponding to $\partial_{\mathcal{O}} b$. The local invariant $\mathrm{inv}_p(f^*b)$ is the evaluation of $\partial_{O_p}(f^*b)$ at the Frobenius element. We thus obtain

$$\mathrm{inv}_p(f^*b) = v_p(Q)\psi(\mathrm{Frob}_p).$$

But the Dirichlet character χ is defined by $\chi(p) = \psi(\mathrm{Frob}_p)$ after using our choice of embedding $\mathbb{Q}/\mathbb{Z} \subset \mathbb{C}^\times$. This gives

$$\mathrm{inv}_p(f^*b) = 0 \quad \Longleftrightarrow \quad \chi(p)^{v_p(Q)} = 1. \qquad \square$$

4.3 | Proof of Theorem 1.6

We now prove our main result. We first note that by Remark 3.9, the period π is bounded in terms of E and $q(\chi)$ only. So we focus on the main bound in the theorem.

We claim that we may assume that b is actually ramified at O, rather than just some multiple mP of P. Indeed, let b be ramified at mP and consider $t^*_{-mP}b$ where t_{-mP} denotes translation by $-mP$. Then $t^*_{-mP}b$ is ramified at O. Assume that we have proved the theorem in this case. Then for $n \in \mathbb{Z}$ we have $t^*_{-mP}b(nP) = 0$ if and only if $b(nP + mP) = 0$, so the two sets being counted differ by translation by m. This changes the size of the set by at most m. In conclusion, we may assume that $m = 0$ and b is ramified at O. We will do so until the last step of the proof, when we will verify that an error term of size m can be absorbed into the constant $C_{E,P,b}$.

We now begin the proof in earnest. Choose a finite set of primes S which contains all primes dividing $\mathrm{ord}(\chi)q(\chi)$ and all primes p at which E has bad reduction. Let

$$\begin{aligned}
\mathcal{P} &= \{\text{primes } p \notin S : \mathrm{ord}(P \bmod p) \text{ is prime and } \mathrm{ord}(\chi(p)) \nmid v_p(\mathrm{ord}(P \bmod p)P)\},\\
\Lambda &= \{\mathrm{ord}(P \bmod p) : p \in \mathcal{P}\},\\
T &= \{p \text{ prime} : v_p(P) > 0\}.
\end{aligned} \tag{4.3}$$

For $p \in \mathcal{P}$, we denote by $\ell_p = \mathrm{ord}(P \bmod p)$. To prove the result, we require the following, which comes from our analysis of the EDS β_n associated to P. We let π denote the period of the sequence $\beta_n \bmod q(\chi)$.

Lemma 4.2. *For any $\epsilon > 0$ and $x \gg_{E,\chi} 1$ we have*

$$\#\{\ell \in \Lambda : \ell \leqslant x\} \geqslant \left(\frac{1}{2\varphi(\pi)} + O_{\epsilon,E}\left(\frac{\pi^\epsilon(\log\log\log x)^2\widehat{h}(P)}{\log x}\right)^{1/4}\right)\frac{x}{\log x} - \#T - \#S.$$

One might assume that the $O_E(\cdot)$ term is the largest error term here, but at the end of this section it will actually be $\#T$ which contributes the most to our final bound.

Proof. Consider the multiples ℓP where ℓ runs over all primes. Let p be such that $v_p(\ell P) > v_p(P)$. Then we claim that either $\ell \in T$, or $\ell = \mathrm{ord}(P \bmod p)$. Indeed, as $v_p(\ell P) > 0$ we have $\ell P \equiv O \bmod p$. As ℓ is prime, we see that either $\ell = \mathrm{ord}(P \bmod p)$ or $P \equiv O \bmod p$. In the

latter case we have $p \in T$. In that case we also have $P \in E_{v_p(P)}(\mathbb{Q}_p)$, $P \notin E_{v_p(P)+1}(\mathbb{Q}_p)$ and $\ell P \in E_{v_p(P)+1}(\mathbb{Q}_p)$, and hence $\ell = |E_{v_p(P)}(\mathbb{Q}_p)/E_{v_p(P)+1}(\mathbb{Q}_p)|$ which is then $= p$ by Lemma 2.4. Thus $\ell \in T$ as claimed.

Now Remark 3.9, Proposition 3.19 and our assumptions in Theorem 1.6 imply that there is a set of at least

$$\left(\frac{1}{2\varphi(\pi)} + O_{E,\epsilon}\left(\frac{\pi^{\epsilon}(\log\log\log x)^2\widehat{h}(P)}{\log x}\right)^{1/4}\right)\frac{x}{\log x}$$

primes $\ell \leqslant x$ such that there exists $p \nmid q(\chi)$ with $\operatorname{ord}(\chi(p)) \nmid v_p(\beta_\ell)$. For such primes we have $v_p(\beta_\ell) > 0$ and hence $v_p(\ell P) > v_p(P)$ by Lemma 3.4. Excluding the finitely many primes $\ell \in T$, we have $\ell = \operatorname{ord}(P \bmod p)$ by the previous paragraph. So by Lemma 3.4 again we have $v_p(\beta_\ell) = v_p(\ell P)$. Similarly, as $\ell = \operatorname{ord}(P \bmod p)$, we see that by excluding at most $\#S$ of the primes ℓ we may assume that $p \notin S$. Such primes now lie in Λ, hence give the result. □

We now sieve modulo such primes. Our approach is inspired by the version of the elliptic sieve given in [14, Section 4.4] via the large sieve. From a philosophical perspective, we sieve with respect to the maps

$$E(\mathbb{Q}) \to E(\mathbb{Z}/p^2\mathbb{Z}), \quad p \in \mathcal{P}.$$

This is literally true providing $v_p(\ell_p P) = 1$, but in general we have no control over the size of this valuation, only its value modulo $\operatorname{ord}\chi$ (cf. Remark 3.20). What we actually do is remove suitable multiples of P where we *can* control the valuation. This is a key difference with our approach and that taken in [14, Section 4.4], as Kowalski only needed to sieve modulo p. The precise result is as follows.

Lemma 4.3. *There exists a finite subset $\mathcal{N} \subset \mathbb{Z}$, depending only on E and b, as follows. Let $p \in \mathcal{P}$ and $n \in \mathbb{Z} \setminus \mathcal{N}$ with $n \equiv \ell_p, 2\ell_p, \dots, (p-1)\ell_p \bmod p\ell_p$. Then $b(nP) \neq 0 \in \operatorname{Br}\mathbb{Q}_p$.*

Proof. As $\gcd(p, n/\ell_p) = 1$, applying Lemma 2.4 to $\ell_p P \in E_1(\mathbb{Q}_p)$ gives

$$v_p(nP) = v_p(\ell_p P) + v_p((n/\ell_p)) = v_p(\ell_p P),$$

which is not divisible by $\operatorname{ord}(\chi(p))$ by the definition of $\mathcal{P}$. The result follows from Proposition 4.1 provided we exclude the finitely many points in $(\mathcal{E} \setminus \mathcal{E}^\circ)(\mathbb{Q})$. □

We now stipulate that the condition in Lemma 4.3 cannot hold at 'moderately sized' primes $\ell \in \Lambda$, to deduce that the quantity in Theorem 1.6 is at most

$$\#\mathcal{N} \cup \left\{|n| \leqslant B : (p \in \mathcal{P} \text{ and } \log B \leqslant \ell_p \leqslant B) \Rightarrow (n \not\equiv 0 \bmod \ell_p \text{ or } n \equiv 0 \bmod p\ell_p)\right\},$$

where B is a parameter, assumed to be sufficiently large in terms of E and χ. This is bounded above by $N_0(B) + N_1(B)$, where

$$N_0(B) = \#\{|n| \leqslant B : n \not\equiv 0 \bmod \ell \text{ for all } \ell \in \Lambda \text{ with } \log B \leqslant \ell \leqslant B\},$$

$$N_1(B) = \#\{|n| \leqslant B : n \equiv 0 \bmod p\ell_p, \text{ for some } p \in \mathcal{P} \text{ with } \log B \leqslant \ell_p \leqslant B\}.$$

Lemma 4.4. $N_1(B) \ll B/\log B$.

Proof. We have

$$N_1(B) \ll \sum_{\log B \leqslant \ell_p \leqslant B} \#\{|n| \ll B : p\ell_p \mid n\} \ll \sum_{\log B \leqslant \ell_p \leqslant B} \frac{B}{p\ell_p}.$$

However, as ℓ_p is the order of P modulo p, by the Hasse bounds we have

$$\ell_p \leqslant |E(\mathbb{F}_p)| \leqslant p + 1 + 2\sqrt{p},$$

in particular $1/p \ll 1/\ell_p$. Extending the sum over all integers n then gives

$$N_1(B) \ll B \sum_{\substack{\log B \leqslant \ell \leqslant B \\ \ell \in \Lambda}} \frac{1}{\ell^2} \ll B \sum_{n \geqslant \log B} \frac{1}{n^2} \ll B/\log B.$$

□

We thus turn our attention to $N_0(B)$, which we deal with using the Selberg sieve.

Lemma 4.5.

$$N_0(B) \leqslant \exp(\#S + \#T + O_{E,\epsilon}(\pi^{\epsilon}\widehat{h}(P)^{1/4}))\frac{B\log\log B}{(\log B)^{1/2\varphi(\pi)}}.$$

Proof. We use the version of the Selberg sieve stated in [20, Theorem 3.6]. This gives

$$N_0(B) \ll B \prod_{\substack{\log B \leqslant \ell \leqslant \sqrt{B} \\ \ell \in \Lambda}} \left(1 - \frac{1}{\ell}\right).$$

However, by Mertens' theorem we have

$$\prod_{\substack{\ell \leqslant \log B \\ \ell \in \Lambda}} \left(1 - \frac{1}{\ell}\right)^{-1} \ll \prod_{\ell \leqslant \log B} \left(1 - \frac{1}{\ell}\right)^{-1} \ll \log\log B.$$

Thus it suffices to show that

$$\prod_{\substack{\ell \leqslant \sqrt{B} \\ \ell \in \Lambda}} \left(1 - \frac{1}{\ell}\right) \leqslant \frac{\exp(\#S + \#T + O_{E,\epsilon}(\pi^{\epsilon}\widehat{h}(P)^{1/4}))}{(\log B)^{1/2\varphi(\pi)}}.$$

To do so, we note that

$$\log \prod_{\substack{\ell \leqslant \sqrt{B} \\ \ell \in \Lambda}} \left(1 - \frac{1}{\ell}\right)^{-1} = -\sum_{\substack{\ell \leqslant \sqrt{B} \\ \ell \in \Lambda}} \log\left(1 - \frac{1}{\ell}\right) \geqslant \sum_{\substack{\ell \leqslant \sqrt{B} \\ \ell \in \Lambda}} \frac{1}{\ell}.$$

By partial summation this is

$$\sum_{\substack{\ell \leqslant \sqrt{B} \\ \ell \in \Lambda}} \frac{1}{\sqrt{B}} + \int_1^{\sqrt{B}} \sum_{\substack{\ell \leqslant u \\ \ell \in \Lambda}} \frac{1}{u^2} \, \mathrm{d}u,$$

and Lemma 4.2 shows that this is

$$\geqslant (1/2\varphi(\pi)) \log\log B - \#S - \#T + O_{E,\epsilon}(\pi^{\epsilon} \widehat{h}(P)^{1/4}).$$

Exponentiating and taking reciprocals gives the claim, and hence the result. □

Combining these lemmas, and the fact that $\pi = O_{E,\chi}(1)$ as observed at the start of Section 4.3, completes the proof of the bound in Theorem 1.6 with

$$C_{E,P,b} = \exp(\#T + O_{E,b}(\widehat{h}(P)^{1/4})), \tag{4.4}$$

where T is as in (4.3). At the start of the proof we assumed that $m = 0$, at the cost of an additive factor of size at most $m = O_b(1)$. This can be absorbed into the implicit constant in (4.4), and completes the proof.

In order to get the last bound in Theorem 1.7, which depends explicitly on P, we require the following supplement to Theorem 1.6.

Lemma 4.6. *Under the assumptions of Theorem 1.6, the constant from (4.4) satisfies*

$$C_{E,P,b} = \exp\left(O_{E,b}\left(\frac{\widehat{h}(P)}{\log \widehat{h}(P)}\right)\right).$$

Proof. By (4.4) it suffices to show that

$$\#T \ll_E \frac{\widehat{h}(P)}{\log \widehat{h}(P)}.$$

We have $\#T = \omega(\prod_{v_p(P)>0} p) = \omega(e_1)$ where e_1 is as in Definition 3.1 and we write $\omega(k)$ for the number of distinct prime factors of k.

From Definition 3.1 we have $e_1 \leqslant \sqrt{H(x(P))}$ where H is the naive height on $\mathbb{P}^1$. Now $\widehat{h}(P) = O_E(1) + \frac{1}{2}\log H(x(P))$ by [26, Theorem VIII.9.3(e)]. So $\log e_1 \leqslant O_E(1) + \widehat{h}(P)$, and since $\#T = \omega(e_1) \ll \frac{\log e_1}{\log\log e_1}$ and $\widehat{h}(P) \gg_E 1$, by say [26, Theorem VIII.9.10(a)], this completes the proof. □

5 | EXAMPLES AND APPLICATIONS

In this section we give various examples and applications of Theorem 1.6, including the proofs of the results from the introduction and a generalisation of Example 1.3.

5.1 | A worked example

Let

$$E: \quad y^2 + y = x^3 - x. \tag{5.1}$$

This curve has conductor 37. Its Mordell–Weil group is $\mathbb{Z}$ with generator $P = (0, 0)$, which has everywhere good reduction. In particular $M = 1$, and Ward's definition (EDSA) agrees with Verzobio's definition (EDSB). The EDS associated to P starting at β_0 reads

$$0, 1, 1, -1, 1, 2, -1, -3, -5, 7, -4, -23, 29, 59, 129, -314, -65, 1529, -3689, \dots .$$

However $P \notin E(\mathbb{R})^0$ so Theorem 1.1 does not apply. Still, we are able to show using Theorem 1.6 that the conclusion of Theorem 1.1 holds.

We apply Theorem 1.6 to the quaternion algebra $(-1, y)$. The associated Dirichlet character is then just the non-principal Dirichlet character χ modulo 4. Modulo 4, the EDS starting at β_0 becomes

$$0, 1, 1, 3, 1, 2, 3, 1, 3, 3, 0, 1, 1, 3, 1, 2, 3, 1, 3, 3, 0, \dots$$

which is periodic with period $\pi = 10$. One now searches the sequence for terms β_α with $\gcd(\alpha, 10) = 1$ and $\chi(|\beta_\alpha|) = -1$; one finds that $\beta_7 = -3$ suffices. Thus Theorem 1.6 shows that

$$\#\{n \in \mathbb{Z} : |n| \leqslant B, y(nP) \text{ is a sum of two squares}\} \ll_\epsilon B/(\log B)^{1/10-\epsilon}$$

using $1/2\varphi(10) = 1/10$. Alternatively, since $4 \nmid \pi$, we also obtain the result using simply $\beta_1 = 1$ and the fact that $\chi(-|\beta_1|) = 1$.

Remark 5.1. The keen reader may notice that we did not fully justify our calculation that the period equals 10. Thankfully, this is not necessary. Namely, Lemma 3.8 shows that the period divides

$$2 \cdot (2 - 1) \cdot 2^2 \cdot \mathrm{ord}(P \bmod 2) = 2^3 \cdot 5,$$

whence $\gcd(\pi, 7) = 1$. (Note that our bound is correct up to powers of 2 here.)

We take an example concerning higher order Dirichlet characters. Consider again (5.1) and let χ be a Dirichlet character modulo 7 of order 3. One finds that $\chi(|\beta_5|) = \chi(2)$ is non-trivial and that $|E(\mathbb{F}_7)| = 9$. But $\gcd(5, 2 \cdot (7 - 1)|E(\mathbb{F}_7)|) = 1$. Thus by Lemma 3.8 we may apply Theorem 1.6, without even having to calculate the period directly (in fact one finds that the period is $54 = (7 - 1)|E(\mathbb{F}_7)|$, so our criterion is again best possible up to powers of 2). The corresponding cyclic extension $K/\mathbb{Q}$ has polynomial $x^3 - x^2 - 2x + 1$; note that this is totally real unlike the hypotheses in Theorem 1.2. We now apply Theorem 1.6 to the cyclic algebra $b = (\chi, x) \in \mathrm{Br}\,\mathbb{Q}(E)$, which is easily checked to ramify at O with Dirichlet character $\chi^{-2} = \chi$ (since $\mathrm{ord}_O(x) = -2$). We deduce that

$$\#\{n \in \mathbb{Z} : |n| \leqslant B, x(nP) \text{ is a norm from } K\} \ll B/(\log B)^\omega$$

for some $\omega > 0$.

As we have seen, this E does indeed satisfy the conclusion of Theorem 1.1. We have counter-examples to similar looking statements (Example 1.3), but it does not seem to be possible to bootstrap these to get counter-examples involving the y-coordinate. In particular, we do not know the answer to the following question without imposing additional assumptions on E or the associated EDSB.

Question 5.2. Let E be an elliptic curve over $\mathbb{Q}$ given by an integral Weierstrass equation. Let $P \in E(\mathbb{Q})$ have infinite order. Then is

$$\#\{n \in \mathbb{Z} : |n| \leqslant B, y(nP) \text{ is a sum of two squares}\} = o(B)?$$

5.2 | Proof of Theorem 1.2

We translate a statement about conic bundles into a statement about quaternion algebras. We work over the local ring R at $Q := mP$. Restricting the conic bundle to $\operatorname{Spec} R$ we obtain a conic over R. It is a classical fact that any conic over R can be diagonalised [13, Corollary I.3.4], so we may write the equation for our conic bundle near Q as

$$sx^2 + ty^2 = z^2, \quad \text{where } s, t \in R.$$

However, as we assumed that X is non-singular it is checked that the valuation of st is at most 1. Thus we may assume without loss of generality that t is a uniformiser in R and that s is a unit in R. Let D be the image of s in $R/(t) = \mathbb{Q}$. Since the fibre over Q was assumed to be non-split with imaginary quadratic splitting field, it follows that D is negative. Moreover, up to a suitable change of variables, we may assume that D is a fundamental discriminant.

We now consider the quaternion algebra $b = (s, t)$ over $\mathbb{Q}(E)$, which gives rise to a 2-torsion element of $\operatorname{Br}\mathbb{Q}(E)$. The residue of b at Q is $D \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, since t is a uniformiser at Q and s is a unit. It follows that the associated Dirichlet character is the Kronecker symbol $\chi_D(\cdot) = (\frac{D}{\cdot})$. As D is negative we have $\chi_D(-1) = -1$, in particular $\chi_D(-|\beta_1|) = -1$. As $P \in E(\mathbb{R})^0$, it now follows from Theorem 1.6 that

$$\#\{|n| \leqslant B : b(nP) = 0 \in \operatorname{Br}\mathbb{Q}\} \ll B/(\log B)^\omega$$

for some $\omega > 0$. However, it is clear by construction that for all but finitely many $R \in E(\mathbb{Q})$, we have $b(R) = 0 \in \operatorname{Br}\mathbb{Q}$ if and only if $\pi^{-1}(R)$ has a rational point, and the result follows.

5.3 | Proof of Theorem 1.7

Let $L \subset K$ be a cyclic non-totally real subfield. If y is a norm from K, then it is certainly a norm from L. Thus it suffices to prove the result when K itself is a cyclic non-totally real extension of $\mathbb{Q}$. Let χ be a Dirichlet character corresponding to K via the Kronecker–Weber theorem, and consider the cyclic algebra $b = (y, \chi)$. For $Q \in E(\mathbb{Q})$ with $y(Q) \neq 0$, we have $b(Q) = 0$ if and only if $y(Q)$ is a norm from K. The rational function y has a pole of order 3 at O, so it follows that the residue of b at O has Dirichlet character χ^{-3}. However χ is odd as K has a complex embedding, so χ^{-3}

is also odd. As $\chi(-|\beta_1|) = -1$ and $P \in E(\mathbb{R})^0$, the main bound in the result thus follows from Theorem 1.6 with $m = 0$. The final estimate for the implicit constant follows from Lemma 4.6.

5.4 | Proof of Theorem 1.1

Follows from Theorem 1.7 for $K = \mathbb{Q}(i)$.

5.5 | x-Coordinate as sum of two squares

As the example (1.2) shows, there are elliptic curves such that $x(Q)$ is a sum of two squares for every $Q \in E(\mathbb{Q})$. We are able to obtain upper bounds for this counting problem providing one imposes additional assumptions on E and P.

Theorem 5.3. *Let E be an elliptic curve over $\mathbb{Q}$ given by an integral Weierstrass equation. Let $P \in E(\mathbb{Q})$ have infinite order with $P \in E(\mathbb{R})^0$. Assume that $x(mP) = 0$ for some non-zero $m \in \mathbb{Z}$. Then there exists $\omega = \omega(E, P) > 0$ such that*

$$\#\{|n| \leqslant B : x(nP) \text{ is a sum of two squares}\} \ll B/(\log B)^{\omega}.$$

Proof. The relevant conic bundle is given by

$$x_1^2 + x_2^2 = x x_0^2 \quad \subset \mathbb{P}^2 \times E.$$

The fibre over mP is non-split since $x(mP) = 0$. Thus the result follows from Theorem 1.2. □

This result applies for example to elliptic curves of the form

$$y^2 = x^3 + ax^2 + bx + c$$

where c is a square and one takes $P = (0, \sqrt{c})$, providing P has infinite order and lies in $E(\mathbb{R})^0$.

5.6 | Proof of Theorem 1.5

Let $G = E(\mathbb{Q})^{\mathrm{tors}} \cap E(\mathbb{R})^0$. For the rest of this proof, let S be the set of primes dividing $\#G$. Choose $P_0 \in E(\mathbb{Q})$, depending only on E, such that $E(\mathbb{Q}) \cap E(\mathbb{R})^0 = \langle P_0 \rangle \oplus G$ where G is finite. Then

$$\{Q \in E(\mathbb{Q}) \cap E(\mathbb{R})^0 : \widehat{h}(Q) \leqslant H\} = \bigcup_{\substack{k \in \mathbb{N},\, k \ll H^{1/2} \\ p \mid k \Rightarrow p \in S}} \{Q \in \langle kP_0 + G \rangle : \widehat{h}(Q) \leqslant H\}. \tag{5.2}$$

Note that we can discard the case $\#G = 1$, since there the result follows from Theorem 1.1. Then by Mazur's theorem $\#S = 1$ or 2.

We now count points $Q \in E(\mathbb{Q}) \cap E(\mathbb{R})^0$ such that $y(Q)$ is a sum of two squares. To do this, we break the union in (5.2) up into two parts according to the size of k. Firstly, for small k we will apply Theorem 1.7, and then for large k we will use a trivial bound.

The case $K = \mathbb{Q}(i)$ of Theorem 1.7 implies that for each $P \in E(\mathbb{Q}) \cap E(\mathbb{R})^0$ of infinite order, we have

$$\#\left\{ Q \in \langle P \rangle : \begin{array}{l} \widehat{h}(Q) \leqslant H, y(Q) \text{ is a} \\ \text{sum of two squares} \end{array} \right\} \leqslant \exp\left(O_E\left(\frac{\widehat{h}(P)}{\log \widehat{h}(P)} \right) \right) \frac{H^{1/2}}{(\log H)^{\omega}},$$

for some $\omega > 0$ which depends only on E. Let κ be a positive integer to be chosen later. By [26, Proposition VIII.9.6] we have $\widehat{h}(kP_0 + R) = C_{E,P_0} k^2$ for all torsion points R and some constant C_{E,P_0} depending only on E and P_0. Since P_0 depends only on E, it follows from the last display that

$$\begin{aligned} \sum_{k \in \mathbb{N},\, k \leqslant \kappa} \#\left\{ Q \in \langle kP_0 + G \rangle : \begin{array}{l} \widehat{h}(Q) \leqslant H, y(Q) \text{ is a} \\ \text{sum of two squares} \end{array} \right\} \\ \leqslant \exp\left(O_E\left(\frac{\kappa^2}{\log \kappa} \right) \right) \frac{H^{1/2}}{(\log H)^{\omega}}. \end{aligned} \tag{5.3}$$

To handle large k we claim that

$$\sum_{\substack{k \in \mathbb{N} \\ \kappa < k \ll H^{1/2} \\ p|k \Rightarrow p \in S}} \#\{ Q \in \langle kP_0 + G \rangle : \widehat{h}(Q) \leqslant H \} \ll_E \frac{H^{1/2} (\log \kappa)^{\#S - 1}}{\kappa}. \tag{5.4}$$

We will prove this in the case $\#S = 2$, leaving the similar and slightly simpler case $\#S = 1$ to the reader. Recalling that $\widehat{h}(kP_0 + R) = C_{E,P_0} k^2$ for all $R \in G$, we have

$$\#\{ Q \in \langle kP_0 + G \rangle : \widehat{h}(Q) \leqslant H \} \ll_E H^{1/2} k^{-1}$$

and so

$$\begin{aligned} \sum_{\substack{k \in \mathbb{N} \\ \kappa < k \ll H^{1/2} \\ p|k \Rightarrow p \in S}} \#\{ Q \in \langle kP_0 + G \rangle : \widehat{h}(Q) \leqslant H \} &\ll_E \sum_{\substack{a,b \in \mathbb{N} \cup \{0\}, \\ \kappa < p_1^a p_2^b \ll H^{1/2}}} H^{1/2} p_1^{-a} p_2^{-b} \\ &\leqslant H^{1/2} \sum_{\substack{j \in \mathbb{N} \\ \kappa \leqslant 2^j \ll H^{1/2}}} \sum_{\substack{a,b \in \mathbb{N} \cup \{0\}, \\ 2^{j-1} < p_1^a p_2^b \leqslant 2^j}} \frac{1}{2^{j-1}}, \end{aligned}$$

and since there are at most j pairs (a, b) appearing in the final sum, this is at most $H^{1/2} \sum_{2^j \geqslant \kappa} j/2^{j-1}$, which is $O(H^{1/2} \log \kappa / \kappa)$ as required for (5.4).

Combining (5.4) with (5.2) and (5.3) gives

$$\begin{aligned} &\#\left\{ Q \in E(\mathbb{Q}) \cap E(\mathbb{R})^0 : \begin{array}{l} \widehat{h}(Q) \leqslant H, y(Q) \text{ is a} \\ \text{sum of two squares} \end{array} \right\} \\ &\ll_E \frac{H^{1/2} (\log \kappa)^{\#S - 1}}{\kappa} + \exp\left(O_E\left(\frac{\kappa^2}{\log \kappa} \right) \right) \frac{H^{1/2}}{(\log H)^{\omega}}. \end{aligned}$$

We choose $\kappa = (\epsilon_{E,K} \log\log H \log\log\log H)^{1/2}$ for some small $\epsilon_{E,K} > 0$, so that $\frac{\kappa^2}{\log \kappa} \ll \epsilon_{E,K} \log\log H$, and we then obtain the claimed result in the form

$$\#\left\{ Q \in E(\mathbb{Q}) \cap E(\mathbb{R})^0 : \begin{array}{l} \widehat{h}(Q) \leqslant H, y(Q) \text{ is a} \\ \text{sum of two squares} \end{array} \right\} \ll_E \frac{H^{1/2} (\log\log\log H)^{\#S-3/2}}{(\log\log H)^{1/2}}.$$

5.7 | Unramified elements

Our results contain various technical assumptions. In the next two sections we demonstrate that these are necessary in general. Firstly we show that for the conclusion of Theorem 1.6, we need to impose ramification on the Brauer group elements. (See (4.1) for the notation $E(k)_b$.)

Lemma 5.4. *Let E be an elliptic curve over a number field k. Let $b \in \operatorname{Br} E$ with $E(k)_b \neq \emptyset$. Then $E(k)_b$ contains a translate of a subgroup of finite index. In particular $E(k)_b$ has positive density in $E(k)$.*

Proof. By performing a translation, we may assume that $O \in E(k)_b$. As b is unramified, there exists a finite set of places S such that $E(k_v)_b = E(k_v)$ for every $v \notin S$ [9, Proposition 13.3.1(iii)]. Moreover, for any place v by [9, Proposition 13.3.1(iii)] the evaluation map

$$b : E(k_v) \to \operatorname{Br} k_v$$

is locally constant. In particular, there exists an open neighbourhood $O \in U_v$ such that $U_v \subset E(k_v)_b$. But $E(k_v)$ is profinite, so such an open neighbourhood may be refined to an open subgroup U_v of $E(k_v)$, which necessarily has finite index as $E(k_v)$ is compact. So set $A = E(k) \cap_{v \in S} U_v$. By construction, this is a subgroup of $E(k)$ of finite index. Moreover, for all $P \in A$ and all places v we have $b(P) = 0 \in \operatorname{Br} k_v$. It now follows from the Hasse principle for $\operatorname{Br} k$ (4.2) that $A \subset E(k)_b$, as required. □

Let

$$b \in Б(E) = \ker(\operatorname{Br} E \to \prod_v \operatorname{Br} E_{k_v}),$$

where the product is over all places v of k. It follows easily from (4.2) that $b(P) = 0 \in \operatorname{Br} k$ for all $P \in E(k)$, so here $E(k)_b = E(k)$ even if $b \neq 0$. Such elements exactly correspond to the elements of Ш(E), providing it is finite (see [28, Theorem 6.2.3]).

For completeness, we give such an explicit example in the form of a conic bundle. Our example is based on a variant of the well-known counter-example to the Hasse principle $2y^2 = x^4 - 17$ due to Reichardt and Lind.

Proposition 5.5. *Let N be only divisible by primes which are* $1 \bmod 8$ *and consider the elliptic curve*

$$E : \quad y^2 = x(x^2 + N).$$

Let X be a smooth proper model for the conic bundle over E given by

$$t_0^2 - 2t_1 = xt_2^2.$$

(1) *The map $X(\mathbb{Q}) \to E(\mathbb{Q})$ is surjective.*
(2) *For $N = 17 \times 593$, E has positive rank and the conic bundle morphism admits no section.*

Proof.

(1) We use the equation for the curve $y^2 = xz(x^2 + Nz^2)$ in weighted projective space. The conic bundle X then has the equations

$$t_0^2 - 2t_1^2 = xzt_2^2, \quad \text{if } xz \neq 0 \tag{5.5}$$

and

$$t_0^2 - 2t_1^2 = (x^2 + Nz^2)t_2^2, \quad \text{if } x^2 + Nz^2 \neq 0. \tag{5.6}$$

We now verify that $X(\mathbb{Q}_v) \to E(\mathbb{Q}_v)$ is surjective for all places v of $\mathbb{Q}$. Firstly note that $X(\mathbb{Q}_v) \to E(\mathbb{Q}_v)$ is closed with respect to the v-adic topology. So it just suffices to show that there is $\mathbb{Q}_v$-point over each fibre with $xz(x^2 + Nz^2) \neq 0$.

For $v = \infty$, there is clearly the real point $(\sqrt{2} : 1 : 0)$ in (5.5). This also gives a solution for any $p \equiv 1 \bmod 8$, in particular for all $p \mid N$. So let $p \nmid 2N$. Here we may choose a representative so that p does not simultaneously divide x and z. If $v_p(x^2 + Nz^2)$ is even, then from the equation of E we find that $v_p(xz)$ is even, whence (5.5) has a solution by a Hilbert symbol calculation. If $v_p(x^2 + Nz^2)$ is odd, our assumptions imply that $v_p(xz) = 0$ so again a Hilbert symbol calculation shows that (5.5) has a solution.

Finally, for $p = 2$, here $N \equiv 1 \bmod 8$ is a square in $\mathbb{Q}_2^\times$, so making a change of variables we may assume that $N = 1$. Again from the equation of the curve, we may assume that 2 doesn't simultaneously divide x and z. Firstly suppose that $2 \nmid xz$. Then from the equation $v_2(x^2 + z^2)$ is even, which is a contradiction as $x^2 + z^2 \equiv 2 \bmod 8$. So assume without loss of generality that $2 \mid x$. Then $z, x^2 + z^2$ are both odd, hence from the equation $v_2(x)$ is even. Then $x^2 + z^2 \equiv 1 \bmod 8$, in which case (5.6) has a solution in $\mathbb{Q}_2$. So every fibre is everywhere locally soluble, hence has a rational point. This proves (1).

(2) Here `Sage` verifies that E has torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z}$. But it has the point $(1088 : 36\,040 : 1)$, which must have infinite order (in fact `Sage` verifies by 2-descent that $\operatorname{rank} E(\mathbb{Q}) = 2$). The conic bundle corresponds which by (1) and (4.2) can only happen if b is trivial. But, by the general theory of 2-descent for elliptic curves, the element b corresponds to a 2-covering of E; this 2-covering has the equation

$$C_2 : 2w^2 = 2^2 - 4Nz^4$$

(cf. [26, Example X.4.8]), which after a change of variables gives $C_2 : 2w^2 = z^4 - N$. However this curve fails the Hasse principle; for $N = 17$ this is the well-known example of Reichardt and Lind, whereas in our case $N = 17 \times 593$ this follows from a similar argument to Case I

of the proof of [26, Proposition X.6.5]. (The key point is that 2 is not a quartic residue modulo 17, see [21, Section 1]). It thus follows that this 2-covering is non-trivial, so b is non-trivial, as required. □

5.8 | Ramified examples

Lemma 5.4 shows that to get any hope of obtaining a version of Theorem 1.6 there needs to be ramification. Still this assumption is not sufficient in general, as was first shown for conic bundles in [5, Section 3]. In this section, we build on this example and generalise the construction to higher order Brauer group elements. We work over a number field k.

Definition 5.6. Let $P \in E(k)$ and $n \in \mathbb{N}$. We denote by $E_P[n]$ the scheme of points $Q \in E$ with $nQ = P$. This is a $E[n] = E_O[n]$ torsor.

Proposition 5.7. *Let ℓ be a prime, E an elliptic curve over k, and $P \in E(k)$ a primitive point of infinite order. Let $b \in \mathrm{Br}\, k(E)$ be ramified with ramification locus in $\mathbb{Z}P \setminus \ell\mathbb{Z}P$, whose residues have the same cyclic extension K/k. Assume that K is a subfield of the field of fractions of every irreducible component of $E_P[\ell]$.*

If $O \in E(k)_b$ then $E(k)_b$ contains a subgroup of finite index. In particular $E(k)_b$ has positive density in $E(k)$.

Proof. Choose a finite set of places S containing the archimedean places, the places ramified in K, and the places where $E_P[\ell]$ is not finite étale.

If v is completely split in K, then $b \otimes k_v$ is unramified, hence $E(k_v)_b = E(k_v)$ providing S is sufficiently large [17, Proposition 7.1]. So assume that v is not completely split in K. We claim that

$$\ell E(k) \subset E(k_v)_b. \tag{5.7}$$

To see this, assume instead that $\ell R \notin E(k_v)_b$ for some $R \in E(k)$. Then providing S is sufficiently large, by [17, Proposition 7.1] we must have $\ell R \equiv Q \bmod v$ where $Q \in E(k)$ is a ramification point of b. Since $Q \in \mathbb{Z}P \setminus \ell\mathbb{Z}P$ by assumption, we deduce that $\ell R \equiv qP \bmod v$ for some $q \in \mathbb{Z}$ with $\ell \nmid q$. So $qP \bmod v$ is ℓ-divisible. But $\ell \nmid q$, hence $P \bmod v$ is also ℓ-divisible. But as $E_P[\ell]$ is finite étale over v, Hensel's lemma shows that $E_P[\ell](k_v) \neq \emptyset$. However now K is a subfield of the field of fractions of every irreducible component of $E_P[\ell]$, so we deduce that K admits a place of degree 1 over v. This contradicts that v is not completely split in K and shows (5.7).

We have shown that $\ell E(k) \subset E(k_v)_b$ for all $v \notin S$. For the places in S we proceed as in the proof of Lemma 5.4, using the fact that $O \in E(k)_b$ to deduce that $E(k_v)_b$ contains a subgroup of finite index for all v. The result then follows from the fact that the intersection of finitely many finite index subgroups has finite index. □

We now explain how to construct such explicit examples. Let ℓ be a prime and E/k an elliptic curve with primitive point P of infinite order. Consider the natural map $f : E \to \mathbb{P}^1$ given by projecting to the x-coordinate. Let K/k be a non-trivial cyclic extension. By the Faddeev exact sequence [9, Theorem 1.5.2], there exists $a \in \mathrm{Br}\, k(\mathbb{P}^1)$ whose ramification consists of any given collection of two distinct rational points and whose residue at these points is K/k.

We therefore choose distinct non-Weierstrass points $P_1, P_2 \in (\ell\mathbb{Z}+1)P$ and choose a ramified at $f(P_1), f(P_2)$. We then define $b' = f^*a$. This is ramified at the points $\pm P_i$ with residues in K/k. However we may have $E(k)_{b'} = \emptyset$. So we set $b = b' - b'(O)$, which now satisfies $O \in E(k)_b$.

It remains to arrange that K is a subfield of the field of fractions of every irreducible component of $E_P[\ell]$, for which we need to impose further conditions on E and K. We assume E has full ℓ-torsion, which implies that k contains all ℓth roots of unity. As $E_P[\ell]$ is an $E[\ell]$-torsor, we find that it corresponds to some element of

$$\mathrm{H}^1(k, E[\ell]) = \mathrm{H}^1(k, \mu_\ell^2) = k^\times/k^{\times\ell} \times k^\times/k^{\times\ell},$$

where the last isomorphism is by Kummer theory. A pair $(\alpha, \beta) \in k^\times/k^{\times\ell} \times k^\times/k^{\times\ell}$ corresponds to the μ_ℓ^2-torsor given by

$$x^\ell = \alpha, \quad y^\ell = \beta \qquad \subset \mathbb{A}^2_k. \tag{5.8}$$

Now, the torsor $E_P[\ell]$ is non-trivial as P is not ℓ-divisible, so without loss of generality α is not an ℓth power in the notation of (5.8). But then the function fields of the irreducible component of the scheme (5.8) are either $k(\sqrt[\ell]{\alpha})$ or $k(\sqrt[\ell]{\alpha}, \sqrt[\ell]{\beta})$. These contain the field $K = k(\sqrt[\ell]{\alpha})$ which is non-trivial and cyclic of degree ℓ.

Writing down explicit curves and Brauer group elements which satisfy Proposition 5.7 is now relatively easy using explicit ramified cyclic algebras on $\mathbb{P}^1$. This is how we found Example 1.3.

6 | APPLICABILITY

In this final section we verify that Condition (1) in Theorem 1.6 holds for almost all Dirichlet characters, under suitable assumptions. Before restating the condition, we recall our setup along with the notation: Fix an elliptic curve E over $\mathbb{Q}$ with $P \in E(\mathbb{Q})$ a point of infinite order with β_n the associated EDSB. Let χ be a Dirichlet character with modulus $q(\chi)$, and $\pi(\chi)$ be the period of the sequence $\beta_n \bmod q(\chi)$.

Let us recall the technical condition.

$$\text{There exists } \alpha \in \mathbb{Z} \text{ relatively prime to } \pi(\chi) \text{ such that } \chi(|\beta_\alpha|) \notin \{0, 1\}. \tag{6.1}$$

We expect this to hold for all but finitely many Dirichlet characters, but it seems completely out of reach to prove this at present. Since this section is purely illustrative, we make numerous assumptions to simplify the statements and the proof.

We assume E does not have complex multiplication and that $P = (x, y)$ has integer coordinates with everywhere good reduction. (This is satisfied by the pair (E, P) from Section 5.1, for example.) Under these assumptions, we have

$$\beta_n = \psi_n(P), \ |\beta_n| = |e_n|.$$

For odd Dirichlet characters some of our other conditions are more likely to apply, so for simplicity we consider only even Dirichlet characters, which we also assume to have prime modulus:

$$\Sigma(D) = \{\text{Dirichlet characters } \chi \,:\, \chi(-1) = 1, q(\chi) \text{ is prime}, q(\chi) \leqslant D\}.$$

Theorem 6.1.

$$\lim_{D\to\infty} \frac{\#\{\chi \in \Sigma(D) : \chi \text{ satisfies (6.1)}\}}{\#\Sigma(D)} = 1,$$

that is, 100% *of Dirichlet characters in* $\Sigma(D)$ *satisfy (6.1) as* D *tends to infinity.*

Proof. As we consider only even characters we have $\chi(|\beta_\alpha|) = \chi(\beta_\alpha)$. If an α satisfying (6.1) exists, then considering the arithmetic progression $\alpha \bmod \pi(\chi)$ shows that there exists such an α with α prime. So let Ω be the set of all primes $\ell > 3$ with $|\beta_\ell| \neq 1$ (there are easily seen to be only finitely many such primes by Seigel's theorem on integral points on elliptic curves). For any subset $R \subseteq \Omega$, define the sets

$$\Phi(D,R) := \left\{\chi \in \Sigma(D) : \forall \ell \in R \text{ either } \chi(\beta_\ell) \in \{0,1\} \text{ or } \ell \mid \pi(\chi)\right\},$$
$$\Phi'(D,R) := \left\{\chi \in \Sigma(D) : \forall \ell \in R \text{ either } \chi(\beta_\ell) \in \{0,\pm 1\} \text{ or } \ell \mid \mathrm{ord}(P \bmod q(\chi))\right\},$$
$$\Phi''(D,R) := \left\{\chi \in \Sigma(D) : \forall \ell \in R \text{ either } \chi(\beta_\ell) \in \{\pm 1\} \text{ or } \ell \mid \mathrm{ord}(P \bmod q(\chi))\right\}.$$

Note that $\Phi(D,\Omega)$ contains all characters in $\Sigma(D)$ that fail (6.1). It suffices to show

$$\lim_{D\to\infty} \frac{\#\Phi(D,\Omega)}{\#\Sigma(D)} = 0. \tag{6.2}$$

Lemma 6.2. $\Phi(D,\Omega) \subseteq \Phi'(D,\Omega) = \Phi''(D,\Omega)$.

Proof. We first prove $\Phi(D,\Omega) \subseteq \Phi'(D,\Omega)$. Suppose $\chi \in \Phi(D,\Omega)$ but $\chi \notin \Phi'(D,\Omega)$. Let $q = q(\chi)$ be the modulus of χ. Then there exists a prime ℓ such that $\chi(\beta_\ell) \neq 0, \pm 1$ and $\ell \nmid \mathrm{ord}(P \bmod q)$, but $\ell \mid \pi(\chi)$. Let $\rho = \pi(\chi)/\ell^{v_\ell(\pi(\chi))}$. Note that $\mathrm{ord}(P \bmod q) \mid \rho$ and so $q \mid \beta_\rho$. For any integer k, we have the following implications:

$$q \mid \beta_{\ell+k\rho} \Rightarrow \mathrm{ord}(P \bmod q) \mid \ell + k\rho \Rightarrow \mathrm{ord}(P \bmod q) \mid \ell \Rightarrow \mathrm{ord}(P \bmod q) = \ell.$$

However, since $\ell \nmid \mathrm{ord}(P \bmod q)$ it follows $\chi(\beta_{\ell+k\rho}) \neq 0$ for any $k \in \mathbb{Z}$. Note that $\gcd(\pi(\chi), \ell + \rho) = \gcd(\pi(\chi), \ell - \rho) = 1$ by construction of ρ. Hence, there exists $k_1, k_2 \in \mathbb{Z}$ such that

$$\ell_1 = \ell + \rho + k_1\pi(\chi), \quad \ell_2 = \ell - \rho + k_2\pi(\chi)$$

are both primes in Ω and $\ell_1, \ell_2 \nmid \pi(\chi)$. Then we must have $\chi(\beta_{\ell_1}), \chi(\beta_{\ell_2}) = 1$ since $\chi \in \Phi(D,\Omega)$. By periodicity, $\chi(\beta_{\ell\pm\rho}) = 1$ as well. Using Proposition 3.2 (noting that $M = 1$ in our case) with $n = \ell, m = \rho$ and $r = 1$, we have

$$\beta_{\ell+\rho}\beta_{\ell-\rho} \equiv \beta_{\rho+1}\beta_{\rho-1}\beta_\ell^2 \bmod q. \tag{6.3}$$

Since $\chi(\beta_{\ell+\rho}\beta_{\ell-\rho}) = 1$ and $\chi(\beta_\ell^2) \neq 0, 1$, it follows that $\chi(\beta_{\rho+1}\beta_{\rho-1}) \neq 0, 1$. Using Proposition 3.2 again with $n = \ell + 2\rho, m = \rho, r = 1$, we have

$$\beta_{\ell+3\rho}\beta_{\ell+\rho} \equiv \beta_{\rho+1}\beta_{\rho-1}\beta_{\ell+2\rho}^2 \bmod q.$$

Hence, either $\chi(\beta_{\ell+2\rho}) \neq 0, 1$ or $\chi(\beta_{\ell+3\rho}) \neq 0, 1$. In either case, after choosing $k_1, k_2 \in \mathbb{Z}$ such that

$$\ell + 2\rho + k_1\pi(\chi), \quad \ell + 3\rho + k_2\pi(\chi)$$

are both primes in Ω (we use the assumption $\ell > 3$ here), we obtain a prime $\ell_0 \in \Omega$ such that $\chi(\beta_{\ell_0}) \neq 0, 1$ and $\ell_0 \nmid \pi(\chi)$, which contradicts $\chi \in \Phi(D, \Omega)$. This finishes the proof that $\Phi(D, \Omega) \subseteq \Phi'(D, \Omega)$.

The containment $\Phi''(D, \Omega) \subseteq \Phi'(D, \Omega)$ is clear. To show $\Phi'(D, \Omega) \subseteq \Phi''(D, \Omega)$, it suffices to prove the following implication

$$\chi(\beta_\ell) = 0 \Rightarrow \ell \mid \mathrm{ord}(P \bmod q) \tag{6.4}$$

for all $\ell \in \Omega$. If $\chi(\beta_\ell) = 0$, then $\mathrm{ord}(P \bmod q) \mid \ell$. However, since $\mathrm{ord}(P \bmod q) \neq 1$, we must have $\mathrm{ord}(P \bmod q) = \ell$. This establishes (6.4), and hence $\Phi'(D, \Omega) = \Phi''(D, \Omega)$. □

Lemma 6.3. *Let ℓ be a prime such that the ℓ-adic Galois representation $\rho_\ell : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for E is surjective. Then*

$$\limsup_{D\to\infty} \frac{\#\{\chi \in \Sigma(D) : \ell \mid \mathrm{ord}(P \bmod q(\chi))\}}{\#\{\chi \in \Sigma(D)\}} \leqslant \frac{\ell}{\ell^2 - 1}.$$

Proof. To calculate the limsup, we can ignore finitely many characters. Hence, we will ignore characters whose modulus is ramified in the extension $\mathbb{Q}(E[\ell])$. Let q be a prime unramified in $\mathbb{Q}(E[\ell])$ such that $\ell \mid \mathrm{ord}(P \bmod q)$. This implies that $E(\mathbb{F}_q)[\ell] \neq 0$, which is equivalent to

$$\det(I_2 - \rho_\ell(\mathrm{Frob}_q)) = 0. \tag{6.5}$$

There are $\ell(\ell+1)(\ell-1)^2$ elements in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, and among them there are $\ell^3 - \ell^2$ many elements $x \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ that satisfy the equation $\det(I_2 - x) = 0$. Thus, by the Chebotarev density theorem the proportion of primes q that satisfy (6.5) is

$$\frac{\ell^3 - \ell^2}{\ell(\ell+1)(\ell-1)^2} = \frac{\ell}{\ell^2 - 1}.$$

Let Ω_ℓ denote the set of primes that satisfy (6.5). Recall that if $\ell \mid \mathrm{ord}(P \bmod q)$, then $q \in \Omega_\ell$. As there are $q - 1$ Dirichlet characters of modulus q, the limit in question is less than or equal to

$$\lim_{D\to\infty} \frac{\#\{\chi \in \Sigma(D) : q(\chi) \in \Omega_\ell\}}{\#\{\chi \in \Sigma(D)\}} = \lim_{D\to\infty} \frac{\displaystyle\sum_{q\in\Omega_\ell,\, q\leqslant D} q - 1}{\displaystyle\sum_{q\leqslant D} q - 1} = \frac{\ell}{\ell^2 - 1},$$

where the last equality follows from simple application of the Chebotarev density theorem and partial summation. □

We now show (6.2). To do so we consider a finite subset $R \subset \Omega$, then take the limit over all R. We divide the quantity of interest into two parts as

$$\frac{\#\Phi''(D,R)}{\#\Sigma(D)} \leqslant \frac{\#\{\chi \in \Sigma(D) : \chi(\beta_\ell) \in \{\pm 1\} \text{ for some } \ell \in R\}}{\#\Sigma(D)} + \frac{\#\{\chi \in \Sigma(D) : \ell \mid \operatorname{ord}(P \bmod q(\chi)) \, \forall \ell \in R\}}{\#\Sigma(D)}.$$

We start with the first part. Fix some $\ell \in R$ and let $q \leqslant D$ be any prime not dividing β_ℓ. Let N be the order of β_ℓ in $(\mathbb{Z}/q\mathbb{Z})^\times/\{\pm 1\}$. Then the map

$$\{\chi \text{ modulus } q : \chi(-1) = 1\} \to \mu_N, \quad \chi \mapsto \chi(\beta_\ell)$$

is surjective. Hence

$$\frac{\#\{\chi \text{ modulus } q : \chi(-1) = 1, \ \chi(\beta_\ell) \in \{\pm 1\}\}}{\#\{\chi \text{ modulus } q : \chi(-1) = 1\}} = \frac{2}{N}. \tag{6.6}$$

Recall that by the definition of Ω we have $|\beta_\ell| \neq 1$. It follows that if $q > |\beta_\ell|$, then $N \geqslant \log((q-1)/2)/\log|\beta_\ell|$. By taking q very large compared to ℓ and sorting characters by their modulus, as well as safely ignoring characters of small modulus, one finds that

$$\lim_{D\to\infty} \frac{\#\{\chi \in \Sigma(D) : \chi(\beta_\ell) \in \{\pm 1\} \text{ for some } \ell \in R\}}{\#\Sigma(D)} = 0.$$

So, we are left with only the second part. Since E does not have complex multiplication, the ℓ-adic Galois representation $\rho_\ell : \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is surjective outside a finite set of primes by Serre's open image theorem [26, Theorem III.7.9]. Hence, shrinking Ω by finitely many primes if necessary, we can assume that ρ_ℓ is surjective for all $\ell \in \Omega$. Thus Lemma 6.3 gives

$$\lim_{D\to\infty} \frac{\#\Phi''(D,R)}{\#\Sigma(D)} \leqslant \min\left(\frac{\ell}{\ell^2-1}\right)_{\ell\in R}.$$

Hence using Lemma 6.2 and letting $R \to \Omega$ gives

$$\lim_{D\to\infty} \frac{\#\Phi(D,\Omega)}{\#\Sigma(D)} \leqslant \lim_{D\to\infty} \frac{\#\Phi''(D,\Omega)}{\#\Sigma(D)} \leqslant \lim_{R\to\Omega} \lim_{D\to\infty} \frac{\#\Phi''(D,R)}{\#\Sigma(D)} = 0. \qquad \square$$

ACKNOWLEDGEMENTS

We thank Gergely Harcos and Efthymios Sofos for helpful comments and advice on some of the proofs. We also thank the anonymous referee for a careful reading of the paper which led to an improvement of Theorem 1.5. D. Loughran and M. Nakahara were sponsored by EPSRC grant EP/R021422/2. S. Bhakta and S. L. Rydin Myerson were supported by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation program (grant ID 648329). S. L. Rydin Myerson was supported by DFG project number 255083470, and by a Leverhulme Early Career Fellowship. We thank the ZORP online seminar and its organisers. Initially there were two separate teams working on this problem using similar methods. But dur-

ing a gathertown meeting on ZORP on 11 December 2020, we became aware of each other during discussions with Efthymios Sofos. Each team had a slightly different viewpoint and results, so we decided to combine to create, in our view, an ultimately superior paper.

JOURNAL INFORMATION

The *Proceedings of the London Mathematical Society* is wholly owned and managed by the London Mathematical Society, a not-for-profit Charity registered with the UK Charity Commission. All surplus income from its publishing programme is used to support mathematicians and mathematics research in the form of research grants, conference grants, prizes, initiatives for early career researchers and the promotion of mathematics.

REFERENCES

1. A. Akbary, J. Bleaney, and S. Yazdani, *On symmetries of elliptic nets and valuations of net polynomials*, J. Number Theory **158** (2016), 185–216.
2. A. Akbary, M. Kumar, and S. Yazdani, *The signs in elliptic nets*, New York J. Math. **23** (2017), 1237–1264.
3. M. Ayad, *Périodicité (mod q) des suites elliptiques et points S-entiers sur les courbes elliptiques*, Ann. Inst. Fourier **43** (1993), no. 3, 585–618.
4. B. M. Bekker and Y. G. Zarkhin, *Division by 2 of rational points on elliptic curves*, St. Petersburg Math. J. **29** (2018), no. 4, 683–713.
5. J. Berg and M. Nakahara, *Rational points on conic bundles over elliptic curves*, Math. Z. **300** (2022), no. 3, 2429–2449.
6. V. Bosser and É. Gaudron, *Logarithmes des points rationnels des variétés abéliennes*, Canad. J. Math. **71** (2019), no. 2, 247–298.
7. T. Browning and D. Loughran, *Sieving rational points on varieties*, Trans. Amer. Math. Soc. **371** (2019), no. 8, 5757–5785.
8. J. Brüdern, K. Matomäki, R. Vaughan, and T. Wooley, *Analytic number theory*, Oberwolfach Rep. **16** (2019), 3141–3205, https://doi.org/10.4171/OWR/2019/50.
9. J.-L. Colliot-Thélène and A. Skorobogatov, *The Brauer–Grothendieck group*, Ergebnisse Mathematik, vol. 3.F, Springer, Berlin, 2021.
10. P. Erdős and P. Turán., *On a problem in the theory of uniform distribution*, Indag. Math. **10** (1949), 38–41.
11. G. Everest and J. Reynolds, and S. Stevens., *On the denominators of rational points on elliptic curves*, Bull. Lond. Math. Soc. **39** (2007), no. 5, 762–770.
12. G. Everest, A. van der Poorten, I. Shparlinski, and T. Ward, *Recurrence sequences*, Mathematical Surveys and Monographs, vol. 104, American Mathematical Society, Providence, RI, 2003.
13. D. Husemoller and J. Milnor, *Symmetric bilinear forms*, Springer, New York, 1973.
14. E. Kowalski, *The large sieve and its applications*, Cambridge Tracts in Mathematics, vol. 175, Cambridge University Press, Cambridge, 2008.
15. D. Loughran, *Sum of Fibonacci sequence evaluated at a Dirichlet character*. https://mathoverflow.net/questions/374689/sum-of-fibonacci-sequence-evaluated-at-a-dirichlet-character.
16. D. Loughran, *The number of varieties in a family which contain a rational point*, J. Eur. Math. Soc. **20** (2018), no. 10, 2539–2588.
17. D. Loughran and L. Matthiesen, *Frobenian multiplicative functions and rational points in fibrations*, J. Eur. Math. Soc., arXiv:1904.12845. In press.
18. D. Loughran and A. Smeets, *Fibrations with few rational points*, Geom. Funct. Anal. **26** (2016), no. 5, 1449–1482.
19. W. McCallum, W. Stein, and J. Voight, *Rational and integral points on higher dimensional varieties*, Lecture notes for ARCC workshop held at AIM in Palo Alto, December 11–20, 2002. https://aimath.org/WWN/qptsurface2/.
20. H. L. Montgomery and R. C. Vaughan, *Multiplicative number theory. I. Classical theory*, Cambridge Studies in Advanced Mathematics, vol. 97, Cambridge University Press, Cambridge, 2007.
21. B. Poonen, *An explicit algebraic family of genus-one curves violating the Hasse principle*, J. Théor. Nombres Bordeaux **13** (2001), no. 1, 263–274.

22. J.-P. Serre, *Spécialisation des éléments de* $\mathrm{Br}_2(\mathbb{Q}(T_1, \dots, T_n))$, C. R. Acad. Sci. Paris Sér. I Math. **311** (1990), no. 7, 397–402.
23. R. Shipsey, *Elliptic divisibility sequences*, Ph.D. thesis, University of London, 2000.
24. J. H. Silverman, *Wieferich's criterion and the abc-conjecture*, J. Number Theory **30** (1988), no. 2, 226–237.
25. J. H. Silverman, *p-Adic properties of division polynomials and elliptic divisibility sequences*, Math. Ann. **332** (2005), no. 2, 443–471.
26. J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.
27. J. H. Silverman and N. Stephens, *The sign of an elliptic divisibility sequence*, J. Ramanujan Math. Soc. **21** (2006), no. 1, 1–17.
28. A. Skorobogatov, *Torsors and rational points*, Cambridge University Press, Cambridge, 2001.
29. K. E. Stange, *Integral points on elliptic curves and explicit valuations of division polynomials*, Canad. J. Math. **68** (2016), no. 5, 1120–1158.
30. Z.-W. Sun, *Does each prime $p > 3$ have a quadratic nonresidue which is a Mersenne number*? https://mathoverflow.net/questions/301624/does-each-prime-p3-have-a-quadratic-nonresidue-which-is-a-mersenne-number.
31. R. C. Vaughan, *The Hardy-Littlewood method*, Cambridge University Press, Cambridge, 1997.
32. M. Verzobio, *A recurrence relation for elliptic divisibility sequences*, Riv. Math. Univ. Parma **3** (2022), no. 1, 223–242.
33. J. F. Voloch, *Elliptic Wieferich primes*, J. Number Theory. **81** (2000), no. 2, 205–209.
34. M. Ward, *Memoir on elliptic divisibility sequences*, Amer. J. Math. **70** (1948), 31–74.