Check for updates

Received: 20 March 2024 | Revised: 9 June 2024 | Accepted: 13 June 2024

DOI: 10.1112/mtk.12269

RESEARCH ARTICLE

Mathematika

Strong divisibility sequences and sieve methods

Tim Browning | **Matteo Verzobio**

With an appendix by Sandro Bettin

IST Austria, Klosterneuburg, Austria

Correspondence
Tim Browning, IST Austria, Am Campus 1, 3400 Klosterneuburg, Austria.
Email: timdanielbrowning@gmail.com

Funding information
FWF, Grant/Award Number: P36278; Horizon 2020, Grant/Award Number: 101034413

Abstract

We investigate strong divisibility sequences and produce lower and upper bounds for the density of integers in the sequence that only have (somewhat) large prime factors. We focus on the special cases of Fibonacci numbers and elliptic divisibility sequences, discussing the limitations of our methods. At the end of the paper, there is an appendix by Sandro Bettin on divisor closed sets that we use to study the density of prime terms that appear in strong divisibility sequences.

MSC 2020
11N36 (primary), 11A41, 11A51, 11B39, 11B83, 11G05 (secondary)

Contents

© 2024 The Author(s). *Mathematika* is copyright © University College London and published by the London Mathematical Society on behalf of University College London. This is an open access article under the terms of the Creative Commons Attribution License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.

1 | INTRODUCTION

The arithmetic of sparse integer sequences continues to present a considerable challenge in analytic number theory. In this paper, we shall use elementary sieve theory to prove some crude arithmetical properties of sparse sequences that admit a suitable divisibility structure. We begin by discussing some well-known sparse sequences and related literature.

Shifted exponentials

Given $a > 1$ and non-zero $b \in \mathbb{Z}$, a notorious open problem is to determine whether the sequence $a^n - b$ takes infinitely many prime values as n runs over $\mathbb{N}$. These sequences are sparse, having only $O(\log N)$ elements in the interval $[1, N]$. Recent work of Grantham and Granville [7] speculates on this for the sequence $a \cdot 2^n - b$ when $\gcd(a, b) = 1$ and $a > 0$; they conjecture that either there are finitely many primes in the sequence, or else the number of primes in the interval $[1, N]$ grows like $c_{a,b} \log N$ for a suitable constant $c_{a,b} > 0$. (When $a = b = 1$, which is the case of Mersenne primes, their heuristic suggests the asymptotic formula should hold with $c_{1,1} = e^{\gamma}/\log 2$.) In the opposite direction, in his book on sieve methods [13], Hooley conjectured that almost all numbers in the sequence $2^n + 5$ are composite. Hooley's conjecture has now been resolved by Järviniemi and Teräväinen [14], subject to Generalised Riemann Hypothesis (GRH) and a form of the pair correlation conjecture.

Markoff numbers

The sequence of Markoff numbers is obtained by listing all coordinates that arise as positive integer solutions to the Diophantine equation $x_1^2 + x_2^2 + x_3^2 = 3x_1x_2x_3$. Thanks to work of Bourgain, Gamburd and Sarnak [2], we know that almost all Markoff numbers are composite. This is a sparse sequence, as the interval $[1, N]$ contains $O((\log N)^2)$ elements of the sequence, by work of Zagier [27].

Elliptic curves

Let E be an elliptic curve defined by a Weierstrass equation with integer coefficients and let $P \in E(\mathbb{Q})$ be a non-torsion point. For each $n \in \mathbb{N}$ we may define $nP = (x_n : y_n : z_n)$, for relatively coprime $x_n, y_n, z_n \in \mathbb{Z}$. As we shall see in Section 4, we must have $x_n = a_n b_n$ and $z_n = b_n^3$, for $a_n, b_n \in \mathbb{Z}$. The sequence $\{b_n\}_{n \in \mathbb{N}}$ is even sparser than the previous examples, containing only $O(\sqrt{\log N})$ integers from the interval $[1, N]$. Nonetheless, it is still possible to prove non-trivial results about their arithmetic. In [16, section 4.4], Kowalski uses the large sieve to show that elements of the sequence with few prime divisors have density 0. More recently, similar sequences have been studied by Bhakta, Loughran, Rydin Myerson and Nakahara [1] in the context of local solubility for families of conics parametrised by elliptic curves. In [1, Theorem 1.1], for example, they show that the set of $n \in \mathbb{N}$ for which y_n is a sum of two squares has density 0, if P belongs to the connected component of the identity of $E(\mathbb{R})$. Due to the fact that the sequence is so sparse, it has been conjectured by Einsiedler, Everest and Ward [5] that there are only finitely many prime numbers appearing in the sequence b_n.

20417942, 2024, 4, Downloaded from https://londmathsoc.onlinelibrary.wiley.com/doi/10.1112/mtk.12269 by CochraneAustria, Wiley Online Library on [13/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

20417942, 2024, 4, Downloaded from https://londmathsoc.onlinelibrary.wiley.com/doi/10.1112/mtk.12269 by CochraneAustria, Wiley Online Library on [13/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Our results in this paper pertain to any *strong divisibility sequence* (SDS), which is a sequence of positive integers $\{x_n\}_{n\in\mathbb{N}}$ such that

$$\gcd(x_n, x_m) = x_{\gcd(n,m)}.$$

for all $m, n \geqslant 1$. We may henceforth assume without loss of generality that $x_1 = 1$, on noting that the general case can be deduced from this case by applying the results to the sequence x_n/x_1. The most basic example of an SDS is the sequence $x_n = n$, for which our results are all well-known or trivial. Further examples are provided by *elliptic divisibility sequences* (EDSs), corresponding to the sequence $\{b_n\}_{n\in\mathbb{N}}$ discussed above, and *Lucas sequences of the first kind*. The latter include sequences of *Fibonacci numbers*

$$F_n = \frac{\phi^n - (-\phi)^{-n}}{\sqrt{5}},$$

where ϕ is the golden ratio, as well as *Mersenne numbers* $2^n - 1$.

There is a rich literature around the arithmetic of such numbers; for example, in 1965 Erdős [6] conjectured that $\frac{1}{n}P(2^n - 1) \to \infty$ as $n \to \infty$, where $P(2^n - 1)$ is the size of the largest prime factor of $2^n - 1$. Stewart [26] has verified this conjecture in the wider context of Lucas sequences, showing in particular that $P(2^n - 1) > n \exp(c \log n / \log\log n)$, for a suitable constant $c > 0$. In a different direction, Luca and Stănică [20] provide heuristics about the typical size of $\omega(x_n)$ for the Lucas sequences $x_n = (a^n - 1)/(a - 1)$, for integer $a > 1$, conjecturing that $\omega(x_n) \geqslant (1 + o(1)) \log n \log\log n$ for almost all n. Recent work of Kontorovich and Lagarias [15] posits a new *toral affine sieve conjecture*, under which it is possible to study the total number of prime divisors of products like $F_n F_{n+1}$. Thus, it follows from [15, Theorem 1.5] that

$$\Omega(F_n) + \Omega(F_{n+1}) \gg \log n$$

for all sufficiently large n, conditionally on their toral affine sieve conjecture. Finally, a classification of those SDS that are simultaneously a *linear recurrence sequence* has been completed recently by Granville [8].

Definition 1.1. Let $\{x_n\}_{n\in\mathbb{N}}$ be an SDS and let $d \in \mathbb{N}$. Define m_d to be the smallest positive integer such that $d \mid x_{m_d}$. If no such integer exists, we put $m_d = \infty$.

There are two major challenges inherent in trying to apply sieve theory to an SDS. We shall see in Remark 2.2 that

$$\#\{n \leqslant N : d \mid x_n\} = \frac{N}{m_d} + O(1), \tag{1.1}$$

so that we have an associated *density function* $g(d) = 1/m_d$. Unfortunately, in most cases of interest the function $g(d)$ is not multiplicative, whereas one of the basic sieve axioms is that $g(d)$ should be a non-negative multiplicative function, with $0 < g(p) \leqslant 1$ for any prime p. The second issue to contend with is the fact that an SDS can grow exponentially, as in the case of Lucas sequences, or even quadratic exponentially, as in the case of elliptic divisibility sequences. Most successful applications of sieve theory involve sequences with at most polynomial growth.

The following is one of our main results and is based on the most basic sieve of Eratosthenes–Legendre.

Theorem 1.2. *Let $\{x_n\}_{n\in\mathbb{N}}$ be an SDS with the property that there exists $\alpha > 0$ such that, for all but finitely many primes p, we have $m_p < p^\alpha$. Then*

$$\#\left\{n \leqslant N : p \mid x_n \Rightarrow p > \tfrac{1}{2}(\log N)(\log\log N)\right\} \gg \frac{N}{\log\log N}.$$

This result provides a lower bound for the number of z-rough numbers in an SDS $\{x_n\}_{n\in\mathbb{N}}$, with $n \leqslant N$ and $z = \frac{1}{2}(\log N)(\log\log N)$. We will see that the hypothesis of the theorem is satisfied by Lucas sequences of the first kind, and by EDSs. Moreover, note that if $\{x_n\}_{n\in\mathbb{N}}$ and $\{y_n\}_{n\in\mathbb{N}}$ are SDSs that satisfy the hypothesis of Theorem 1.2, then also the sequence $\{\gcd(x_n, y_n)\}_{n\in\mathbb{N}}$ satisfies the hypothesis.

We shall illustrate our most general results with the sequence $\{F_n\}_{n\in\mathbb{N}}$ of Fibonacci numbers. Note that $\Omega(F_n) = O(n)$, as $\Omega(m) = O(\log m)$ for any $m \in \mathbb{N}$. (In fact, the latter bound is optimal, as one sees by considering the case in which m is a prime power.) The following shows that we can often improve on this trivial bound for $\Omega(F_n)$.

Corollary 1.3. *We have*

$$\#\left\{n \leqslant N : \Omega(F_n) \leqslant \frac{n}{\log\log n}\right\} \gg \frac{N}{\log\log N}.$$

Proof. This follows from Theorem 1.2, on noting that $\Omega(F_n) \leqslant \frac{n}{\log\log n}$ if $p > C\log N$ for all $p \mid F_n$, for a suitable constant $C > 0$. □

Under additional hypotheses, we can also prove an upper bound for the kind of set considered in Theorem 1.2. We say that the term x_n has a *primitive prime divisor* if there exists a prime q such that $q \mid x_n$, but $q \nmid x_k$ for $k < n$.

Theorem 1.4. *Let $\{x_n\}_{n\in\mathbb{N}}$ be an SDS with the property that x_n has a primitive prime divisor for all but finitely many terms. Then, there exists a strictly increasing continuous function $f : \mathbb{R}_{\geqslant 1} \to \mathbb{R}$ such that $n \leqslant f(z)$ implies $x_n \leqslant z$, for all $z \geqslant 1$. Moreover, for any such function f, we have*

$$\#\{n \leqslant N : p \mid x_n \Rightarrow p > z\} \ll \frac{N}{\log f(z)} + f(z)^2,$$

for any z such that $f(z) > 1$.

According to [22, Theorem 1] and [25, Proposition 10], respectively, both Lucas sequences of the first kind (except for some trivial examples) and EDSs satisfy the hypothesis of Theorem 1.4.

Our next result is concerned with the density of prime terms that appear in an SDS $\{x_n\}_{n\in\mathbb{N}}$. It is well-known that a Mersenne number $2^n - 1$ is composite if n is composite, so that the set of Mersenne primes among the sequence $\{2^n - 1\}_{n\in\mathbb{N}}$ has density 0. We shall generalise this result to a more general SDS, as follows.

20417942, 2024, 4, Downloaded from https://londmathsoc.onlinelibrary.wiley.com/doi/10.1112/mtk.12269 by CochraneAustria, Wiley Online Library on [13/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Theorem 1.5. *Let $\{x_n\}_{n\in\mathbb{N}}$ be an SDS and let $\mathcal{A} = \{n \in \mathbb{N} : x_n = 1\}$. Assume that $\mathcal{A}$ has density 0. Then the set $\{n \in \mathbb{N} : x_n$ is prime$\}$ has density 0.*

Apart from some trivial examples, Lucas sequences of the first kind satisfy the hypothesis of the theorem, as do EDSs. Moreover, the assumption on the density of $\mathcal{A}$ cannot be removed, as we will show in Remark 3.6. The proof of Theorem 1.5 relies on an auxiliary fact that is provided for us by Sandro Bettin in the Appendix. This states that, given any divisor closed set of density 0, the product set formed with the set of primes continues to have density 0.

As an application of our main results, let us record upper and lower bounds for the cardinality of z-rough numbers in the Fibonacci sequence $\{F_n\}_{n\in\mathbb{N}}$, with $n \leqslant N$ and $z = \frac{1}{2}(\log N)(\log\log N)$. (In fact, the following result shows that the set of $n \leqslant N$ for which F_n is z-rough has density 0.)

Corollary 1.6. *Let $\{F_n\}_{n\in\mathbb{N}}$ be the sequence of Fibonacci numbers. Then*

$$\frac{N}{\log\log N} \ll \#\left\{ n \leqslant N : p \mid F_n \Rightarrow p > \tfrac{1}{2}(\log N)(\log\log N) \right\} \ll \frac{N}{\log\log\log N}.$$

Proof. Recall that the assumptions of Theorems 1.2 and 1.4 hold for the Fibonacci sequence. The lower bound therefore follows from Theorem 1.2. For the upper bound, we put $z = \frac{1}{2}(\log N)(\log\log N)$ and deduce from Theorem 1.4 that

$$\#\left\{ n \leqslant N : p \mid F_n \Rightarrow p > \tfrac{1}{2}(\log N)(\log\log N) \right\} \ll \frac{N}{\log f(z)} + f(z)^2.$$

If $f(z) = \log_\phi(\sqrt{5}z - 1)$, then it is clear that $F_n \leqslant z$ if $n \leqslant f(z)$. The desired upper bound is now obvious. □

Much of this paper is devoted to understanding the size of the expected main term in the application of sieve methods to an SDS, with the associated quantities m_d from Definition 1.1. In view of (1.1), an application of inclusion–exclusion confers a special significance to the sum

$$M(\Pi) = \sum_{d\mid\Pi} \frac{\mu(d)}{m_d}, \tag{1.2}$$

for given $\Pi \in \mathbb{N}$. (If $m_d = \infty$, then we count $\mu(d)/m_d$ as 0 in this sum.) We shall prove the following lower bound.

Theorem 1.7. *Let $\{x_n\}_{n\in\mathbb{N}}$ be an SDS with the property that there exists $\alpha > 0$ such that $m_p < p^\alpha$ for all but finitely many primes. Then*

$$M(\Pi_z) \gg \frac{1}{\log z},$$

where $\Pi_z = \prod_{p<z} p$.

Consider the SDS given by Mersenne numbers $x_n = 2^n - 1$. In this case computational evidence seems to suggest that

$$M(\Pi_z) \sim \frac{1}{\log z},$$

20417942, 2024, 4, Downloaded from https://londmathsoc.onlinelibrary.wiley.com/doi/10.1112/mtk.12269 by CochraneAustria, Wiley Online Library on [13/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

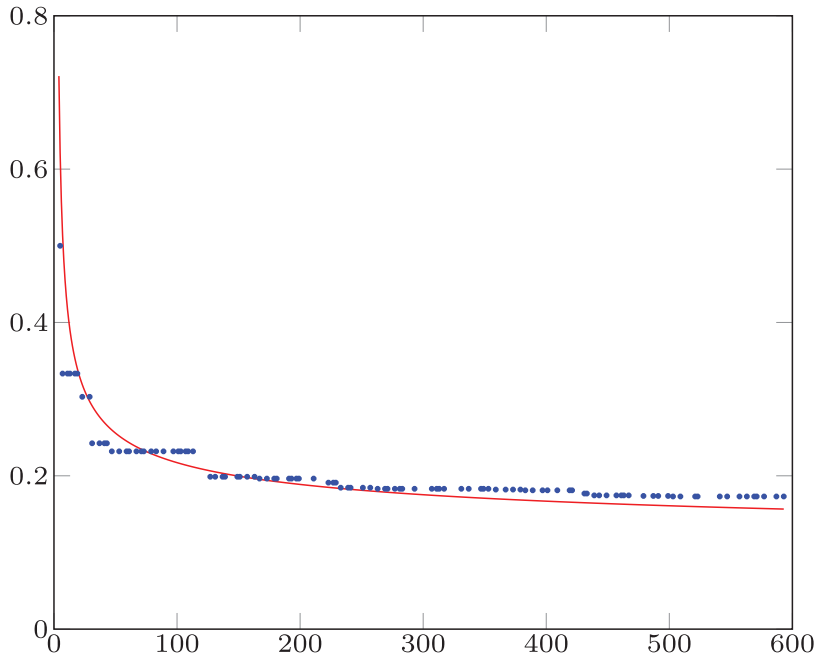

FIGURE 1 The blue graph is the graph of the function $M(\Pi_z)$ for Mersenne numbers, the red one is the graph of $\frac{1}{\log z}$.

as $z \to \infty$. We have illustrated this in Figure 1. (In Remark 3.5, we will see that $M(\Pi_z) \ll \frac{1}{\log\log z}$, for Mersenne numbers.)

In [7, section 7], Grantham and Granville briefly discuss the challenges around applying sieve methods to sequences of the form $2^n - b$. One of their suggested modifications involves changing the ordering in $M(\Pi_z)$, which is by the size of the prime divisors of d. In private communication with the authors, Granville has asked whether similar behaviour is expected for the sum

$$\sum_{\substack{d\in\mathbb{N}\\ m_d\leqslant z}} \frac{\mu(d)}{m_d},$$

as $z \to \infty$.

Let us close this introduction by outlining the contents of the paper. First, in Section 2 we shall study some properties of m_d and prove Theorem 1.7. With this to hand, the proof of Theorems 1.2, 1.4, and 1.5 will be carried out in Section 3, although the latter does not use any sieve theory. In Section 4, we shall specialise to EDSs, and investigate $M(\Pi)$ under additional hypotheses in Sections 5 and 6. In particular, in Theorem 6.3, we shall prove a refinement of Theorem 1.2 for non-CM (complex multiplication) elliptic curves, subject to some standard hypotheses. Finally, in the Appendix, Sandro Bettin has supplied a useful fact about the density of the product of the set of primes with a divisor closed set.

2 | PROPERTIES OF m_d

Let $\{x_n\}_{n\in\mathbb{N}}$ be an SDS, so that $\gcd(x_n, x_m) = x_{\gcd(n,m)}$ for all $m, n \in \mathbb{N}$. Clearly, this implies that $x_m \mid x_n$ if $m \mid n$, so that $\{x_n\}_{n\in\mathbb{N}}$ is a *divisibility sequence*. As we pointed out in the introduction,

20417942, 2024, 4, Downloaded from https://londmathsoc.onlinelibrary.wiley.com/doi/10.1112/mtk.12269 by CochraneAustria, Wiley Online Library on [13/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

we will work under the assumption $x_1 = 1$; the general case can be deduced from this case by applying the results to the sequence x_n/x_1. We begin by collecting together some basic properties of the function m_d from Definition 1.1.

Lemma 2.1. *We have $d \mid x_n$ if and only if $m_d \mid n$.*

Proof. If $m_d \mid n$, then $d \mid x_{m_d} \mid x_n$ because we are working with divisibility sequences. If $d \mid x_n$, then $d \mid \gcd(x_{m_d}, x_n) = x_{\gcd(n,m_d)}$. By definition, m_d is the smallest positive integer such that x_{m_d} is divisible by d, whence $\gcd(n, m_d) \geqslant m_d$. This happens only if $m_d \mid n$. □

Remark 2.2. Note that (1.1) is an immediate consequence of Lemma 2.1.

Lemma 2.3. *If $k \mid j$ then $m_k \mid m_j$.*

Proof. Let $k \mid j$. Then $k \mid j \mid x_{m_j}$, whence Lemma 2.1 implies that $m_k \mid m_j$. □

Lemma 2.4. *Let $d_1, d_2 \in \mathbb{N}$. Then*

$$m_{[d_1,d_2]} = [m_{d_1}, m_{d_2}],$$

where $[\cdot,\cdot]$ denotes the least common multiple.

Proof. As $d_1 \mid [d_1, d_2]$, we have $m_{d_1} \mid m_{[d_1,d_2]}$ by Lemma 2.3. In the same way, $m_{d_2} \mid m_{[d_1,d_2]}$ and so $[m_{d_1}, m_{d_2}] \mid m_{[d_1,d_2]}$.

The sequence $\{x_n\}_{n\in\mathbb{N}}$ is a divisibility sequence and so $x_{m_{d_1}} \mid x_{[m_{d_1},m_{d_2}]}$. Thus $d_1 \mid x_{m_{d_1}} \mid x_{[m_{d_1},m_{d_2}]}$ and, similarly, $d_2 \mid x_{[m_{d_1},m_{d_2}]}$. Thus, $[d_1, d_2] \mid x_{[m_{d_1},m_{d_2}]}$ and Lemma 2.1 yields $m_{[d_1,d_2]} \mid [m_{d_1}, m_{d_2}]$. □

We now turn to the estimation of the sum $M(\Pi)$ in (1.2), for suitable $\Pi \in \mathbb{N}$. Our first goal is to prove the lower bound in Theorem 1.7. For this, we shall apply a suitable result based on inclusion–exclusion.

Lemma 2.5. *Let $n \in \mathbb{N}$ and let $n_1, \dots, n_k$ be divisors of n. Then*

$$\sum_{\substack{d\mid n\\ d\nmid n_j,\forall j\leqslant k}} \mu(d) = \sum_{I\subseteq\{1,\dots k\}\cup\emptyset} (-1)^{\#I} \sum_{d\mid \gcd(n_i)_{i\in I}} \mu(d),$$

where we follow the convention that $\gcd(n_i)_{i\in I} = n$ when $I = \emptyset$.

Proof. We proceed by induction on k. Assume $k = 1$. Then

$$\sum_{\substack{d\mid n\\ d\nmid n_1}} \mu(d) = \sum_{d\mid n} \mu(d) - \sum_{d\mid n_1} \mu(d),$$

20417942, 2024, 4, Downloaded from https://londmathsoc.onlinelibrary.wiley.com/doi/10.1112/mtk.12269 by CochraneAustria, Wiley Online Library on [13/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

as required. We now prove the lemma for $k > 1$. Let $D = \{d \mid n : d \nmid n_j, \forall j \leqslant k-1\}$. Then we may write

$$\sum_{\substack{d \mid n \\ d \nmid n_j, \forall j \leqslant k}} \mu(d) = \sum_{\substack{d \in D \\ d \nmid n_k}} \mu(d) = \sum_{d \in D} \mu(d) - \sum_{\substack{d \in D \\ d \mid n_k}} \mu(d).$$

By induction,

$$\sum_{d \in D} \mu(d) = \sum_{I \subseteq \{1, \dots k-1\} \cup \emptyset} (-1)^{\#I} \sum_{d \mid \gcd(n_i)_{i \in I}} \mu(d).$$

Note that if $d \in D$ is such that $d \mid n_k$, then $d \mid n_k$ and $d \nmid \gcd(n_k, n_i)$ for each $1 \leqslant i \leqslant k-1$. Hence, by induction, we have

$$\sum_{\substack{d \in D \\ d \mid n_k}} \mu(d) = \sum_{\substack{d \mid n_k \\ d \nmid \gcd(n_j, n_k), \forall j \leqslant k-1}} \mu(d) = \sum_{I \subseteq \{1, \dots k-1\} \cup \emptyset} (-1)^{\#I} \sum_{d \mid \gcd(n_i, n_k)_{i \in I}} \mu(d).$$

The statement of the lemma follows. □

Next, the following key result allows us to express $M(\Pi)$ as a sum of non-negative terms.

Lemma 2.6. *Let $\Pi \in \mathbb{N}$ be square-free and such that $m_\Pi < \infty$. Then*

$$M(\Pi) = \sum_{\substack{j \mid m_\Pi \\ \gcd(x_j, \Pi) = 1}} \frac{\varphi(m_\Pi / j)}{m_\Pi},$$

where $\varphi(\cdot)$ is the Euler φ-function.

Proof. Recall from Lemma 2.3 that $m_d \mid m_\Pi$ if $d \mid \Pi$. Thus,

$$M(\Pi) = \sum_{d \mid \Pi} \frac{\mu(d)}{m_d} = \sum_{l \mid m_\Pi} \frac{1}{l} \sum_{\substack{m_d = l \\ d \mid \Pi}} \mu(d).$$

Now $m_d = l$ if and only if we have $d \mid x_l$, with $d \nmid x_{l'}$ for each proper divisor $l' \mid l$. Let $p_1, \dots, p_k$ be the distinct prime divisors of l. It follows that $m_d = l$ if and only if $d \mid x_l$ and $d \nmid x_{l/p_i}$, for each $1 \leqslant i \leqslant k$. Hence,

$$\sum_{\substack{m_d = l \\ d \mid \Pi}} \mu(d) = \sum_{\substack{d \mid \gcd(x_l, \Pi) \\ d \nmid \gcd(x_{l/p}, \Pi), \forall p \mid l}} \mu(d).$$

We now seek to apply Lemma 2.5, for which we note that

$$\gcd(x_{l/p_i})_{i \in I} = x_{\gcd(l/p_i)_{i \in I}} = x_{l / \prod_{i \in I} p_i},$$

20417942, 2024, 4, Downloaded from https://londmathsoc.onlinelibrary.wiley.com/doi/10.1112/mtk.12269 by CochraneAustria, Wiley Online Library on [13/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

as $\{x_n\}_{n\in\mathbb{N}}$ is an SDS. Hence,

$$\sum_{\substack{m_d=l\\ d\mid\Pi}}\mu(d)=\sum_{I\subseteq\{1,\dots k\}\cup\emptyset}(-1)^{\#I}\sum_{d\mid\gcd(x_{l/p_I},\Pi)}\mu(d),$$

where $p_1,\dots,p_k$ are the distinct prime divisors of l and $p_I=\prod_{i\in I}p_i$. The inner sum is 1 if $\gcd(x_{l/p_I},\Pi)=1$, and 0 otherwise. It therefore follows that

$$\sum_{\substack{m_d=l\\ d\mid\Pi}}\mu(d)=\sum_{\substack{k\mid l\\ \gcd(x_{l/k},\Pi)=1}}\mu(k).$$

Putting $l=jk$, we see that

$$M(\Pi)=\sum_{l\mid m_\Pi}\frac{1}{l}\sum_{\substack{l=jk\\ \gcd(x_j,\Pi)=1}}\mu(k)=\sum_{\substack{j\mid m_\Pi\\ \gcd(x_j,\Pi)=1}}\frac{1}{j}\sum_{k\mid m_\Pi/j}\frac{\mu(k)}{k}.$$

By the properties of the Euler-φ function, we have

$$M(\Pi)=\sum_{\substack{j\mid m_\Pi\\ \gcd(x_j,\Pi)=1}}\frac{1}{j}\frac{\varphi(m_\Pi/j)}{m_\Pi/j}=\sum_{\substack{j\mid m_\Pi\\ \gcd(x_j,\Pi)=1}}\frac{\varphi(m_\Pi/j)}{m_\Pi},$$

as desired. □

When $x_1=1$ the first term in this sum is $\varphi(m_\Pi)/m_\Pi$ and we get a lower bound for $M(\Pi)$ by focusing on this term and ignoring the terms associated to $j>1$. (Note that for the trivial sequence $x_n=n$ this is actually sharp, as then

$$M(\Pi)=\sum_{d\mid\Pi}\frac{\mu(d)}{d}=\frac{\varphi(\Pi)}{\Pi},$$

for any $\Pi\in\mathbb{N}$.) The following result is concerned with bounding from below $\varphi(m_\Pi)/m_\Pi$, under an additional assumption, for suitable $\Pi\in\mathbb{N}$.

Lemma 2.7. *Let $\{x_n\}_{n\in\mathbb{N}}$ be an SDS with the property that there exists $\alpha>0$ such that $m_p<p^\alpha$ for all but finitely many primes. Let S be the finite set of primes p such that $m_p=\infty$. Let $\Pi_{z,S}=\prod_{p<z,p\notin S}p$. Then*

$$\frac{\varphi(m_{\Pi_{z,S}})}{m_{\Pi_{z,S}}}\gg\frac{1}{\log z}.$$

Proof. On enlarging α, we can assume that $m_p<p^\alpha$ for all $p\notin S$. Let us write $\Pi=\Pi_{z,S}$ to ease notation, noticing that

$$\log(\Pi)=\sum_{p\leqslant z}\log p+O(1)=\theta(z)+O(1),$$

20417942, 2024, 4, Downloaded from https://londmathsoc.onlinelibrary.wiley.com/doi/10.1112/mtk.12269 by CochraneAustria, Wiley Online Library on [13/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

where $\theta(z)$ is the Chebyshev function. Thus, $\log(\Pi) \sim z$ as $z \to \infty$, by the prime number theorem. We have the familiar lower bound

$$\varphi(d) \gg \frac{d}{\log\log d}.$$

By Lemma 2.4 and the hypotheses of the lemma, it follows that

$$m_\Pi \leqslant \prod_{\substack{p \leqslant z \\ p \notin S}} m_p < \prod_{\substack{p \leqslant z \\ p \notin S}} p^\alpha = \Pi^\alpha.$$

But then

$$\log\log m_\Pi \leqslant \log\alpha + \log\log\Pi \leqslant \log z + O(1).$$

We have therefore proved that

$$\frac{\varphi(m_\Pi)}{m_\Pi} \gg \frac{1}{\log\log m_\Pi} \gg \frac{1}{\log z},$$

as required. □

It turns out that the lower bound in Lemma 2.7 is actually sharp under a further assumption on the SDS. This is the object of the following result.

Lemma 2.8. *Let $\{x_n\}_{n\in\mathbb{N}}$ be an SDS. Let S be the finite set of primes p such that $m_p = \infty$. Assume that there exists $\delta > 0$ such that, for all but finitely many primes q, there exists a prime $p < q^\delta$ such that $q \mid m_p$. Then*

$$\frac{\varphi(m_{\Pi_{z,S}})}{m_{\Pi_{z,S}}} \ll \frac{1}{\log z}.$$

Proof. Write $\Pi = \Pi_{z,S}$, as previously and note that

$$\frac{\varphi(m_\Pi)}{m_\Pi} = \prod_{q \mid m_\Pi} \left(1 - \frac{1}{q}\right).$$

The product will only get larger if we reduce the number of factors in the product. Now $q \mid m_\Pi$ if and only if there exists $p \mid \Pi$ such that $q \mid m_p$. By hypothesis, we have $q \mid m_p$ for at least one $p \mid \Pi$ for $q \ll z^{1/\delta}$, up to finitely many exceptions. Hence,

$$\frac{\varphi(m_\Pi)}{m_\Pi} = \prod_{q \mid m_\Pi} \left(1 - \frac{1}{q}\right) \ll \prod_{q \ll z^{1/\delta}} \left(1 - \frac{1}{q}\right) \ll \frac{1}{\log z},$$

by Mertens theorem. □

20417942, 2024, 4, Downloaded from https://londmathsoc.onlinelibrary.wiley.com/doi/10.1112/mtk.12269 by CochraneAustria, Wiley Online Library on [13/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Remark 2.9. Both Lucas sequences of the first kind and CM EDSs satisfy the assumption of Lemma 2.8, assuming GRH. For EDSs with CM, this will be proved in Proposition 5.4. For Lucas sequences, as explained by Lenstra [18, Lemma 2.5], we have $q \mid m_p$ if and only if the Frobenius of p belongs to certain conjugacy classes in a field depending only on q. But then one concludes using an effective form of the Chebotarev density theorem [17].

Proof of Theorem 1.7. Let S be the finite set of primes as in Lemma 2.7. If $d \mid \Pi_z$ and $d \nmid \Pi_{z,S}$, then there exists $p \in S$ such that $p \mid d$. So, $m_d = \infty$. Hence, on recalling the definition (1.2), we have $M(\Pi_z) = M(\Pi_{z,S})$. Lemma 2.6 implies that

$$M(\Pi_{z,S}) \geqslant \frac{\varphi(m_{\Pi_{z,S}})}{m_{\Pi_{z,S}}},$$

as $x_1 = 1$. But then Lemma 2.7 yields the desired lower bound. □

3 | ERATOSTHENES–LEGENDRE SIEVE AND PRIMES IN AN SDS

Let $\{x_n\}_{n\in\mathbb{N}}$ be an SDS satisfying the assumptions of Theorem 1.2. Let $\mathcal{P}$ be a set of rational primes, and let z and N be two positive parameters. We define

$$A(N,z) = \{n \leqslant N : \gcd(x_n, \Pi) = 1\},$$

where

$$\Pi = \Pi(z,\mathcal{P}) = \prod_{\substack{p\in\mathcal{P}\\ p\leqslant z}} p. \tag{3.1}$$

We can now prove the following result.

Lemma 3.1. *Let $M(\Pi)$ be given by (1.2). Then*

$$\#A(N,z) = NM(\Pi) + O\left(2^{\omega(\Pi)}\right).$$

Proof. It follows from inclusion–exclusion that

$$\#A(N,z) = \sum_{d\mid\Pi} \mu(d)\#A_d,$$

where $A_d = \{n \leqslant N : d \mid x_n\}$. On appealing to (1.1), we deduce that

$$\#A(N,z) = N\sum_{d\mid\Pi} \frac{\mu(d)}{m_d} + O\left(2^{\omega(\Pi)}\right),$$

as required. □

20417942, 2024, 4, Downloaded from https://londmathsoc.onlinelibrary.wiley.com/doi/10.1112/mtk.12269 by CochraneAustria, Wiley Online Library on [13/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Proof of Theorem 1.2. In this result, we take $\mathcal{P}$ to be the set of all rational primes. We have $\omega(\Pi) \leqslant z/\log z$ in Lemma 3.1, by the prime number theorem. Taking $z = \frac{1}{2}(\log N)(\log\log N)$, we note that $2^{z/\log z} \leqslant \sqrt{N}$ for sufficiently large values of N. Hence, it follows from Lemma 3.1 that

$$\#A(N,z) - NM(\Pi) \ll \sqrt{N}.$$

Theorem 1.7 now yields the statement of the theorem. □

We next proceed by searching for an upper bound for $\#A(N,z)$.

Definition 3.2. Let $\mathcal{F}$ be the family of strictly increasing continuous functions

$$f : \mathbb{R}_{\geqslant 1} \to \mathbb{R}$$

such that $\lim_{z\to\infty} f(z) = \infty$.

Bearing this definition in mind, we may establish the following result.

Lemma 3.3. *Let $\{x_n\}_{n\in\mathbb{N}}$ be an SDS such that, for all but finitely many $n \in \mathbb{N}$, x_n has a primitive prime divisor. Then there exists $f \in \mathcal{F}$ such that*

$$n \leqslant f(z) \Rightarrow x_n \leqslant z,$$

for all $z \geqslant 1$.

Proof. First, we notice that x_n cannot admit a constant subsequence, as there is a primitive prime divisor for all but finitely many terms. Hence, $\lim_{n\to\infty} x_n = \infty$ and we may form an unbounded increasing sequence $y_n = \max_{i\leqslant n}\{x_i\}$. Let $f_1 : \mathbb{R}_{\geqslant 1} \to \mathbb{R}_{\geqslant 1}$ be such that

$$f_1(z) = \max\{n \geqslant 1 : z \geqslant y_n\}.$$

Hence, f_1 is an increasing step-function that goes to infinity. Fix $z \geqslant 1$ and let $n \leqslant f_1(z) = m$. But then $y_m \leqslant z$ and $x_n \leqslant y_m \leqslant z$. Let f be a strictly increasing continuous function that goes to infinity such that $f(z) \leqslant f_1(z)$ for all $z \geqslant 1$. Then, if $n \leqslant f(z)$, we will have $n \leqslant f_1(z)$ and so $x_n \leqslant z$. □

Proof of Theorem 1.4. Let C be such that, for all $n > C$, x_n has a primitive prime divisor. Let $n \geqslant 1$ be divisible by a prime p with $C < p < f(z)$. Let q be a primitive prime divisor of x_p. Thus,

$$q \mid x_p \leqslant z,$$

as $p \leqslant f(z)$. Hence, $q \mid x_p \mid x_n$ and then $n \notin A(N,z)$. It therefore follows that

$$A(N,z) \subseteq \{n \leqslant N : p \mid n \Rightarrow p \leqslant C \text{ or } p \geqslant f(z)\}.$$

20417942, 2024, 4, Downloaded from https://londmathsoc.onlinelibrary.wiley.com/doi/10.1112/mtk.12269 by CochraneAustria, Wiley Online Library on [13/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

But then an application of the Selberg sieve [4, Theorem 7.1.1 and Corollary 7.1.2] yields

$$\#\{n \leqslant N : p \mid n \Rightarrow p \leqslant C \text{ or } p \geqslant f(z)\} \ll \frac{N}{\log f(z)} + f(z)^2,$$

which gives our desired upper bound for $\#A(N,z)$. □

Corollary 3.4. *Let $\{x_n\}_{n\geqslant 1}$ be an SDS such that, for all but finitely many terms, x_n has a primitive prime divisor and let f be as in Lemma 3.3. Let $g : \mathbb{R}_{\geqslant f(1)} \to \mathbb{R}$ be such that $f \circ g = \mathrm{Id}$ (which exists because f is continuous and strictly increasing). Then*

$$\#\left\{n \leqslant N : p \mid x_n \Rightarrow p > g\left(N^{1/3}\right)\right\} \ll \frac{N}{\log N}.$$

Proof. Fix N and let $z = g(N^{1/3})$. Then,

$$\log(f(z))f(z)^2 \leqslant f(z)^3 = f\left(g\left(N^{1/3}\right)\right)^3 = \left(N^{1/3}\right)^3 = N.$$

It follows that

$$f(z)^2 \leqslant \frac{N}{\log f(z)},$$

whence

$$\#\{n \leqslant N : p \mid x_n \Rightarrow p > z\} \ll \frac{N}{\log f(z)} + f(z)^2 \ll \frac{N}{\log f(z)} \ll \frac{N}{\log N},$$

by Theorem 1.4. □

In Corollary 1.6, we applied Theorem 1.4 to get an upper bound for $\#A(N,z)$ for the sequence $\{F_n\}_{n\in\mathbb{N}}$ of Fibonacci numbers, with $z = \frac{1}{2}(\log N)(\log\log N)$. In doing so we used the observation that $F_n \leqslant z$ if $n \leqslant f(z)$, with the choice $f(z) = \log_\phi(\sqrt{5}z - 1)$. Note that $f \circ g = \mathrm{Id}$, with $g(z) = \frac{1}{\sqrt{5}}(\phi^z + 1)$. But then Corollary 3.4 implies that

$$\#\left\{n \leqslant N : p \mid F_n \Rightarrow p > \tfrac{1}{\sqrt{5}}\phi^{N^{1/3}}\right\} \ll \frac{N}{\log N}.$$

It is interesting to compare this result with Lemma 3.1. For z of order $\phi^{N^{1/3}}$, the error term $O(2^{\omega(\Pi_z)})$ is much larger than N, rendering the estimate meaningless.

Remark 3.5. We can clearly prove an analogue of Corollary 1.6 for the sequence $x_n = 2^n - 1$ of Mersenne numbers, using instead the function $f(z) = \log_2(z+1)$. In fact, we claim that

$$M(\Pi_z) \ll \frac{1}{\log\log z},$$

20417942, 2024, 4, Downloaded from https://londmathsoc.onlinelibrary.wiley.com/doi/10.1112/mtk.12269 by CochraneAustria, Wiley Online Library on [13/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

for this sequence, where $\Pi_z = \prod_{p \leqslant z} p$. To see this we combine Lemma 3.1 with Theorem 1.4, in order to deduce that

$$\begin{aligned} NM(\Pi_z) &\ll \#A(N,z) + 2^{z/\log z} \\ &\ll \frac{N}{\log f(z)} + f(z)^2 + 2^{z/\log z} \\ &\ll \frac{N}{\log\log z} + \log^2 z + 2^{z/\log z}. \end{aligned}$$

The claim follows on dividing through by N and taking the limit as $N \to \infty$.

We conclude this section by proving Theorem 1.5, which gives a mild condition under which the set of primes in an SDS has density 0.

Proof of Theorem 1.5. Let $\{x_n\}_{n\in\mathbb{N}}$ be an SDS. Let $\mathcal{A}$ be the set of indices n such that $x_n = 1$ and assume that $\mathcal{A}$ has density 0. Assume that $x_n = q$ is a prime and write $n = \prod_{i\leqslant u} p_i^{a_i}$. For all $i \leqslant u$, let $n_i = n/p_i^{a_i}$ and notice that x_{n_i} is equal to 1 or q (as it must be a divisor of q). Moreover, $\gcd_{i\leqslant u}(n_i) = 1$. If, for all $i \leqslant u$ we have $x_{n_i} = q$, then

$$x_1 = x_{\gcd_{i\leqslant u}(n_i)} = \gcd_{i\leqslant u}(x_{n_i}) = q,$$

which is not true. Thus, there exists $i \leqslant u$ such that $x_{n_i} = 1$ and then $n_i \in \mathcal{A}$. Therefore, n can be written as the product of a prime power and an element in $\mathcal{A}$. Let $\mathcal{P}^\infty$ be the set of prime powers and $\mathcal{P}^\infty \cdot \mathcal{A} = \{n \in \mathbb{N} : n = rx,\ r \in \mathcal{P}^\infty,\ x \in \mathcal{A}\}$. In conclusion, we have shown that

$$\{n \in \mathbb{N} : x_n \text{ is prime }\} \subseteq \mathcal{P}^\infty \cdot \mathcal{A}.$$

Note that $\mathcal{A}$ is divisor closed, meaning that $d \in \mathcal{A}$ whenever $n \in \mathcal{A}$ and $d \mid n$. This follows, as $x_d \mid x_n = 1$. We conclude by applying Theorem A.1, which shows that if $\mathcal{A}$ has density 0 and is divisor closed, then $\mathcal{P}^\infty \cdot \mathcal{A}$ has density 0. □

Remark 3.6. Notice that the assumption that $\mathcal{A}$ has density 0 cannot be removed. Indeed, let $\{x_n\}_{n\in\mathbb{N}}$ be the sequence defined by

$$x_n = \begin{cases} 2 & \text{if } 2 \mid n, \\ 1 & \text{if } 2 \nmid n. \end{cases}$$

This is an SDS and we see that $\mathcal{A}$ has density $1/2$. Moreover, x_n is prime for a positive density set of indices.

4 | ELLIPTIC DIVISIBILITY SEQUENCES

The goal of this section is to prove some properties of EDSs, and in particular that they satisfy the hypotheses of Theorem 1.2. Let E be a rational elliptic curve defined by a Weierstrass equation with

20417942, 2024, 4, Downloaded from https://londmathsoc.onlinelibrary.wiley.com/doi/10.1112/mtk.12269 by CochraneAustria, Wiley Online Library on [13/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

integer coefficients. Let $P \in E(\mathbb{Q})$ be a non-torsion point. For each $n \in \mathbb{N}$, define

$$nP = (x_n : y_n : z_n) \in \mathbb{P}^2(\mathbb{Q})$$

with $x_n, y_n, z_n \in \mathbb{Z}$ such that $\gcd(x_n, y_n, z_n) = 1$. If we add the hypothesis $z_n > 0$, then the choice of $(x_n : y_n : z_n)$ is unique. As the Weierstrass equation defining the curve has integer coefficients, so it follows that $x_n = a_n b_n$ and $z_n = b_n^3$, for $a_n, b_n \in \mathbb{Z}$. Indeed, if $p^k \| z_n$ then $p^k \mid x_n^3$, by the equation defining the curve. But then $\gcd(p, y_n) = 1$ and $p^k \| x_n^3$. Hence, z_n is a cube and $p^j \| x_n$ if $p^{3j} \| z_n$ The sequence $\{b_n\}_{n\in\mathbb{N}}$ is an EDS. Moreover, possibly after a change of variables, we can henceforth assume that $b_1 = 1$. As explained by Silverman [25, section 2], it follows from properties of the formal group of an elliptic curve that the sequence $\{b_n\}_{n\in\mathbb{N}}$ is an SDS.

Let p be a prime. Note that m_p, as given by Definition 1.1, is the smallest positive integer such that $m_p P$ is the identity element $(0 : 1 : 0) \in E(\mathbb{F}_p)$ on reducing modulo p. Furthermore, we note that $p \mid b_n$ if and only if nP reduces to the identity modulo p. The next result shows that an EDS satisfies the hypothesis in Theorem 1.2.

Lemma 4.1. *If p is a prime of good reduction for E, then $m_p \mid \#E(\mathbb{F}_p)$. In particular, $m_p \leqslant p + 1 + 2\sqrt{p}$. If p is not a prime of good reduction for E, then there exists a constant C_E depending only on E such that $m_p \leqslant C_E p$.*

Proof. Assume that p is a prime of good reduction. Then the order of P in $E(\mathbb{F}_p)$ divides the cardinality of the group $E(\mathbb{F}_p)$. But, by definition, m_p is the order of P in $E(\mathbb{F}_p)$. Thus,

$$m_p \mid \#E(\mathbb{F}_p) \leqslant p + 2\sqrt{p} + 1,$$

by the Hasse bound.

Assume that p is not a prime of good reduction. Then it follows from [24, Corollary C.15.2.1] that there exists a constant C', depending only on E, such that mP is non-singular in $E(\mathbb{F}_p)$ for at least one $m < C'$. The group of non-singular points in $E(\mathbb{F}_p)$ has order at most $2p + 1$. We conclude as before. □

Building on this, we can prove general upper and lower bounds for m_d, for any $d \in \mathbb{N}$. While not directly used in our work, the following result shows that there is a wide gap between our lower and upper bounds for m_d.

Lemma 4.2. *There exists constants $C_1, C_2 > 0$, depending only on E and P, such that*

$$C_1 \sqrt{\log d} \leqslant m_d \leqslant C_2^{\omega(d)} d,$$

for any square-free $d \in \mathbb{N}$.

Proof. We begin by proving the lower bound. Let $\varepsilon > 0$. As explained by Silverman [25, Lemma 8], Siegel's theorem implies that

$$(1 - \varepsilon) n^2 \hat{h}(P) + O_{\varepsilon,E}(1) \leqslant \log b_n \leqslant (1 + \varepsilon) n^2 \hat{h}(P) + O_{\varepsilon,E}(1), \tag{4.1}$$

where $\hat{h}(P) > 0$ is the canonical height of the point P. We know $d \mid b_{m_d}$ and so it follows that $\log d \leqslant \log b_{m_d}$, whence $\log d \leqslant (1 + \varepsilon) m_d^2 \hat{h}(P) + O_{\varepsilon,E}(1)$. The lower bound easily follows.

20417942, 2024, 4, Downloaded from https://londmathsoc.onlinelibrary.wiley.com/doi/10.1112/mtk.12269 by CochraneAustria, Wiley Online Library on [13/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Turning to the upper bound, let $d = p_1 \dots p_r$ and let Δ_E denote the discriminant of E. It follows from Lemma 2.4 that $m_d \leqslant m_{p_1} \dots m_{p_r}$. Applying Lemma 4.1, we deduce that

$$m_p \leqslant \begin{cases} p(1 + 2p^{-1/2} + p^{-1}) & \text{if } p \nmid \Delta_E, \\ C_E p & \text{if } p \mid \Delta_E, \end{cases}$$

for any prime p. But then it follows that

$$m_d \leqslant d \prod_{\substack{p \mid d \\ p \nmid \Delta_E}} \left(1 + 2p^{-1/2} + p^{-1}\right) \prod_{\substack{p \mid d \\ p \mid \Delta_E}} C_E \leqslant C_2^{\omega(d)} d,$$

for a suitable constant $C_2 > 0$. □

Note that it follows from (4.1) that the EDS $\{b_n\}_{n \in \mathbb{N}}$ contains only $O(\sqrt{\log N})$ elements in the interval $[1, N]$.

5 | A CHEBOTAREV ARGUMENT FOR EDSs

In Lemma 2.7, we proved a lower bound for $\varphi(m_\Pi)/m_\Pi$ and in Lemma 2.8 we proved a matching upper bound, subject to some additional hypotheses on the SDS. The goal of this section is to check that the hypotheses hold for EDS, associated to a rational elliptic curve E and a non-torsion point $P \in E(\mathbb{Q})$. Throughout this section, we shall need to work under the assumption that GRH holds, and we shall assume that E has CM, with $\mathrm{End}(E) = \kappa$.

Given an ideal I in κ, let $\kappa_I = \kappa(E[I])$ and $L_I = \kappa_I(P/I)$. As E is defined over $\mathbb{Q}$, it follows that κ has class number one (as proved in [23, Theorem II.4.3]). By P/I we mean a point Q in $E(\overline{\mathbb{Q}})$ such that $\alpha Q = P$ if $I = (\alpha)$. Notice that the choice of Q is not unique but the field L_I does not depend on this choice. Building on work of Gupta and Murty [9, 10], we can establish the following result.

Lemma 5.1. *Let p a prime that splits in κ and let $q \nmid 6p$ be a prime. Let π_p be the Frobenius of p in κ. Then $q \mid m_p$ if and only if there is a prime $\mathfrak{q}_1$ over q and $k_1 \geqslant 1$ such that π_p splits completely in $\kappa_{\mathfrak{q}_1^{k_1}}$ and does not split completely in $\kappa_{\mathfrak{q}_1^{k_1+1}}$ and $L_{\mathfrak{q}_1^{k_1}}$.*

Proof. Let $\mathbb{F}_{\pi_p} = \mathcal{O}_\kappa / \pi_p \mathcal{O}_\kappa$ where $\mathcal{O}_\kappa$ is the ring of integers of κ and notice that $\mathbb{F}_{\pi_p} = \mathbb{F}_p$. Recall that the ring of integers of κ is a principal ideal domain, as E is a rational elliptic curve. We start by doing the case when q splits in κ, so that $q = \mathfrak{q}_1 \mathfrak{q}_2$ in κ. Recall from [10, Lemma 3] that $\#E(\mathbb{F}_p) = N(\pi_p - 1)$. Given $j \in \mathbb{N}$, we claim that $\mathfrak{q}_1^j$ divides $(\pi_p - 1)$ if and only if π_p splits completely in $\kappa_{\mathfrak{q}_1^j}$. If $\mathfrak{q}_1^j$ divides $(\pi_p - 1)$ then $\pi_p \equiv 1 \bmod \mathfrak{q}_1^j$, and it follows that π_p acts trivially on $E[\mathfrak{q}_1^j]$. Therefore, π_p splits completely in $\kappa_{\mathfrak{q}_1^j}$. Conversely, if $\mathfrak{q}_1^j$ does not divide $(\pi_p - 1)$, then π_p does not act trivially on $E[\mathfrak{q}_1^j]$ and π_p does not split completely in $\kappa_{\mathfrak{q}_1^j}$.

Let k_1 (respectively, k_2) be the largest integer such that $\pi_p \equiv 1 \bmod \mathfrak{q}_1^{k_1}$ (respectively, modulo $\mathfrak{q}_2^{k_2}$). Thus, π_p splits completely in $\kappa_{\mathfrak{q}_1^{k_1}}$ (respectively, $\kappa_{\mathfrak{q}_2^{k_2}}$) and does not split completely in $\kappa_{\mathfrak{q}_1^{k_1+1}}$ (respectively, $\kappa_{\mathfrak{q}_2^{k_2+1}}$). We have $\pi_p - 1 = \mathfrak{q}_1^{k_1} \mathfrak{q}_2^{k_2} I$ for I an ideal coprime with $\mathfrak{q}_1$ and $\mathfrak{q}_2$. Hence, $\#E(\mathbb{F}_p) = q^{k_1+k_2} N(I)$ and so the q-primary part of $E(\mathbb{F}_p)$ has order $q^{k_1+k_2}$. Moreover, the

20417942, 2024, 4, Downloaded from https://londmathsoc.onlinelibrary.wiley.com/doi/10.1112/mtk.12269 by CochraneAustria, Wiley Online Library on [13/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

q-primary part of $E(\mathbb{F}_p)$ is $E[\mathfrak{q}_1^{k_1}] \times E[\mathfrak{q}_2^{k_2}]$, as π_p acts trivially on $E[\mathfrak{q}_1^{k_1}]$ (respectively, $E[\mathfrak{q}_2^{k_2}]$) and does not act trivially on $E[\mathfrak{q}_1^{k_1+1}]$ (respectively, $E[\mathfrak{q}_2^{k_2+1}]$). Here, we are using that $E[\mathfrak{q}_1^{k_1}]$ and $E[\mathfrak{q}_2^{k_2}]$ have trivial intersection, as the two ideals are coprime.

Let $E(\mathbb{F}_{\pi_p}) = E[\mathfrak{q}_1^{k_1}] \times E[\mathfrak{q}_2^{k_2}] \times G$ with G a group of order coprime with q. Let $\overline{P}$ be the reduction modulo π_p of P and note that $q \mid m_p$ if and only if q divides the order of $\overline{P}$. Write $\overline{P} = P_1 + P_2 + P_3$ with $P_1 \in E[\mathfrak{q}_1^{k_1}]$, $P_2 \in E[\mathfrak{q}_2^{k_2}]$, and $P_3 \in G$. Note that multiplication by $\mathfrak{q}_1^{k_1}$ is an isomorphism on $E[\mathfrak{q}_2^{k_2}]$ and G. Hence, $\overline{P}$ is divisible by $\mathfrak{q}_1^{k_1}$ if and only if P_1 is divisible by $\mathfrak{q}_1^{k_1}$. This happens if and only if $P_1 = 0$. In the same way, $\overline{P}$ is divisible by $\mathfrak{q}_2^{k_2}$ if and only if $P_2 = 0$. Hence, q does not divide the order of $\overline{P}$ if and only if $P_1 = 0$ and $P_2 = 0$. It follows that $\overline{P}$ has order divisible by q if and only if $\overline{P}/\mathfrak{q}_1^{k_1}$ does not have a solution in $E(\mathbb{F}_{\pi_p})$ or $\overline{P}/\mathfrak{q}_2^{k_2}$ does not have a solution in $E(\mathbb{F}_{\pi_p})$. Hence, π_p does not have a first-degree prime factor in $L_{\mathfrak{q}_1^{k_1}}$ or in $L_{\mathfrak{q}_2^{k_2}}$. For more details, see the proof of [9, Lemma 2]. As $L_{\mathfrak{q}_1^{k_1}}/\kappa$ is Galois, this happens if and only if π_p does not split completely. In summary, q divides m_p if and only if there exists a prime $\mathfrak{q}_1$ over q and a strictly positive integer k_1 such that π_p splits completely in $\kappa_{\mathfrak{q}_1^{k_1}}$, does not split completely in $\kappa_{\mathfrak{q}_1^{k_1+1}}$, and does not split completely in $L_{\mathfrak{q}_1^{k_1}}$.

Assume now that q does not split. In this case there is only one prime $\mathfrak{q}_1$ in κ over q. Let k_1 be such that $(\pi_p - 1) = \mathfrak{q}_1^{k_1} I$, with I and $\mathfrak{q}_1$ coprime. Proceeding as above, $E(\mathbb{F}_{\pi_p}) = E[\mathfrak{q}_1^{k_1}] \times G$ with G of order coprime with q. We conclude as before. □

Armed with this result, we can now use the Chebotarev density theorem to assess the density of rational primes that split in the endomorphism ring of E and satisfy the property $q \mid m_p$, for a fixed prime q. The analogous result for the property $q \mid \#E(\mathbb{F}_p)$ has been proved by Cojocaru [3, section 2.2].

Lemma 5.2. *Assume that E has CM with $\mathrm{End}(E) = \kappa$, and assume GRH. Let $q > 3$ be a prime of good reduction. Then there exists $\delta_q \geqslant 0$ such that*

$$\#\{p \leqslant x : p \text{ splits in } \kappa, q \mid m_p\} = \delta_q \,\mathrm{li}(x) + O\Big(x^{1/2}\log^3 x\Big),$$

where the implied constant depends on E and P.

Proof. Let $\pi_q(x) = \#\{p \leqslant x : p \text{ splits in } \kappa, q \mid m_p\}$. Given a prime $\mathfrak{q}_1$ in κ, define

$$A_{\mathfrak{q}_1,k_1} = \left\{ p \leqslant x : \begin{array}{l} \pi_p \text{ splits completely in } \kappa_{\mathfrak{q}_1^{k_1}} \\ \pi_p \text{ does not split completely in } \kappa_{\mathfrak{q}_1^{k_1+1}} \text{ or } L_{\mathfrak{q}_1^{k_1}} \end{array} \right\}.$$

It follows from [17, Theorem 1.1] (see also [10, Lemma 7]) and an inclusion–exclusion argument, that

$$\begin{aligned} \#A_{\mathfrak{q}_1,k_1} = {} & \frac{\mathrm{li}(x)}{\left[\kappa_{\mathfrak{q}_1^{k_1}} : \kappa\right]} - \frac{\mathrm{li}(x)}{\left[\kappa_{\mathfrak{q}_1^{k_1+1}} : \kappa\right]} - \frac{\mathrm{li}(x)}{\left[L_{\mathfrak{q}_1^{k_1}} : \kappa\right]} + \frac{\mathrm{li}(x)}{\left[L_{\mathfrak{q}_1^{k_1}}\kappa_{\mathfrak{q}_1^{k_1}+1} : \kappa\right]} \\ & + O\Big(x^{1/2}(\log x + k_1 \log q)\Big). \end{aligned} \tag{5.1}$$

20417942, 2024, 4, Downloaded from https://londmathsoc.onlinelibrary.wiley.com/doi/10.1112/mtk.12269 by CochraneAustria, Wiley Online Library on [13/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Thus,

$$\#A_{\mathfrak{q}_1,k_1} = \delta_{\mathfrak{q}_1,k_1}\,\mathrm{li}(x) + O(x^{1/2}(\log x + k_1 \log q)),$$

with

$$\delta_{\mathfrak{q}_1,k_1} = \frac{1}{\left[\kappa_{\mathfrak{q}_1}^{k_1} : \kappa\right]} - \frac{1}{\left[\kappa_{\mathfrak{q}_1}^{k_1+1} : \kappa\right]} - \frac{1}{\left[L_{\mathfrak{q}_1}^{k_1} : \kappa\right]} + \frac{1}{\left[L_{\mathfrak{q}_1}^{k_1}\kappa_{\mathfrak{q}_1}^{k_1+1} : \kappa\right]}. \tag{5.2}$$

In a similar way, if $q = \mathfrak{q}_1\mathfrak{q}_2$, then

$$\#(A_{\mathfrak{q}_1,k_1} \cap A_{\mathfrak{q}_2,k_2}) = \delta_{\mathfrak{q}_1,k_1,\mathfrak{q}_2,k_2}\,\mathrm{li}(x) + O(x^{1/2}(\log x + \max\{k_1,k_2\}\log q)),$$

for a suitable constant $\delta_{\mathfrak{q}_1,k_1,\mathfrak{q}_2,k_2}$.

Assume that $(q) = \mathfrak{q}_1\mathfrak{q}_2$ splits in κ. By Lemma 5.1, we have

$$\{p \leqslant x : p \text{ splits in } \kappa, q \mid m_p\} = \left(\cup_{k_1\geqslant 1} A_{\mathfrak{q}_1,k_1}\right) \bigcup \left(\cup_{k_2\geqslant 1} A_{\mathfrak{q}_2,k_2}\right).$$

Note that, by definition, $A_{k_1,\mathfrak{q}_1} \cap A_{k_1',\mathfrak{q}_1} = \emptyset$ for $k_1 \neq k_1'$. Hence, it follows that

$$\pi_q(x) = \sum_{k_1\geqslant 1} \#A_{\mathfrak{q}_1,k_1} + \sum_{k_2\geqslant 1} \#A_{\mathfrak{q}_2,k_2} - \sum_{k_1,k_2\geqslant 1} \#(A_{\mathfrak{q}_1,k_1} \cap A_{\mathfrak{q}_2,k_2}).$$

If $k_1 > \frac{\log 2x}{\log q}$, then $q^{k_1} > 2x > \#E(\mathbb{F}_p)$. As we noted during the proof of Lemma 5.1, we have $q^{k_1} \mid \#E(\mathbb{F}_p)$ if $p \in A_{\mathfrak{q}_1,k_1}$. Thus, $A_{\mathfrak{q}_1,k_1}$ is empty if $k_1 > \frac{\log 2x}{\log q}$. Putting $K = \frac{\log 2x}{\log q}$, we deduce that

$$\pi_q(x) = \sum_{k_1\leqslant K} \mathrm{li}(x)\delta_{\mathfrak{q}_1,k_1} + \sum_{k_2\leqslant K} \mathrm{li}(x)\delta_{\mathfrak{q}_2,k_2} - \sum_{\substack{k_1\leqslant K\\ k_2\leqslant K}} \mathrm{li}(x)\delta_{\mathfrak{q}_1,k_1,\mathfrak{q}_2,k_2}$$
$$+ O\Big(K^2 x^{1/2}(\log x + K\log q)\Big).$$

Putting

$$\delta_q = \sum_{1\leqslant k_1} \delta_{\mathfrak{q}_1,k_1} + \sum_{1\leqslant k_2} \delta_{\mathfrak{q}_2,k_2} - \sum_{1\leqslant k_1,k_2} \delta_{\mathfrak{q}_1,k_1,\mathfrak{q}_2,k_2},$$

we obtain

$$\left|\pi_q(x) - \delta_q\,\mathrm{li}(x)\right| \ll x^{1/2}\log^3 x$$
$$+ \mathrm{li}(x)\left(\left|\sum_{k_1>K} \delta_{\mathfrak{q}_1,k_1} + \sum_{k_2>K} \delta_{\mathfrak{q}_2,k_2} - \sum_{\max\{k_1,k_2\}>K} \delta_{\mathfrak{q}_1,k_1,\mathfrak{q}_2,k_2}\right|\right).$$

20417942, 2024, 4, Downloaded from https://londmathsoc.onlinelibrary.wiley.com/doi/10.1112/mtk.12269 by CochraneAustria, Wiley Online Library on [13/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Notice that

$$\sum_{k_1>K} \delta_{\mathfrak{q}_1,k_1} + \sum_{k_2>K} \delta_{\mathfrak{q}_2,k_2} - \sum_{\max\{k_1,k_2\}>K} \delta_{\mathfrak{q}_1,k_1,\mathfrak{q}_2,k_2} \geqslant 0$$

and so

$$\left(\left|\sum_{k_1>K} \delta_{\mathfrak{q}_1,k_1} + \sum_{k_2>K} \delta_{\mathfrak{q}_2,k_2} - \sum_{\max\{k_1,k_2\}>K} \delta_{\mathfrak{q}_1,k_1,\mathfrak{q}_2,k_2}\right|\right) \leqslant \sum_{k_1>K} \delta_{\mathfrak{q}_1,k_1} + \sum_{k_2>K} \delta_{\mathfrak{q}_2,k_2}.$$

We have $[\kappa_{\mathfrak{q}_i^{k_i}} : \kappa] = q^{k_i-1}(q-1)$, for $i = 1, 2$, as q is a prime of good reduction and coprime to 6. By (5.2),

$$\delta_{\mathfrak{q}_i,k_i} \leqslant \frac{4}{[\kappa_{\mathfrak{q}_i^{k_i}} : \kappa]} = \frac{4}{q^{k_i-1}(q-1)}.$$

By this inequality, one can easily show that δ_q is well-defined. Moreover,

$$\operatorname{li}(x) \sum_{k_1>K} \delta_{\mathfrak{q}_1,k_1} + \operatorname{li}(x) \sum_{k_2>K} \delta_{\mathfrak{q}_2,k_2} \leqslant \frac{8\operatorname{li}(x)}{q-1} \sum_{k>\log 2x/\log q} \frac{1}{q^{k-1}} \leqslant 1$$

and then

$$\left|\pi_q(x) - \delta_q \operatorname{li}(x)\right| \ll x^{1/2} \log^3 x.$$

Finally, $\delta_q \geqslant 0$ because

$$\delta_q = \lim_{x\to\infty} \frac{\pi_q(x)}{\operatorname{li}(x)} \geqslant 0.$$

This completes the proof of the lemma when q splits in κ; the case in which q does not split is similar. □

We will need some control over the dependence of the leading constant δ_q on q, which we achieve in the following result.

Lemma 5.3. *There exists $\lambda > 0$, depending only on E and P, such that $\delta_q > q^{-\lambda}$ for all primes $q > 3$ of good reduction.*

Proof. We do the case q split, the other case being similar. Notice that

$$A_{\mathfrak{q}_1,k_1} \subseteq \{p \leqslant x : p \text{ splits in } \kappa, q \mid m_p\},$$

20417942, 2024, 4, Downloaded from https://londmathsoc.onlinelibrary.wiley.com/doi/10.1112/mtk.12269 by CochraneAustria, Wiley Online Library on [13/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

and so $\delta_q \geqslant \delta_{\mathfrak{q}_1,k_1}$. Thus, we just need to prove that $\delta_{\mathfrak{q}_1,k_1} \geqslant q^{-\lambda}$ for some $\mathfrak{q}_1 \mid q$ and $k_1 \geqslant 1$. By (5.2), we have

$$\begin{aligned}\delta_{\mathfrak{q}_1,k_1} &\geqslant \frac{1}{\left[\kappa_{\mathfrak{q}_1^{k_1}} : \kappa\right]} - \frac{1}{\left[L_{\mathfrak{q}_1^{k_1}} : \kappa\right]} - \frac{1}{\left[\kappa_{\mathfrak{q}_1^{k_1+1}} : \kappa\right]} \\ &= \frac{1}{(q-1)q^{k_1-1}} - \frac{1}{\left[L_{\mathfrak{q}_1^{k_1}} : \kappa_{\mathfrak{q}_1^{k_1}}\right]\left[\kappa_{\mathfrak{q}_1^{k_1}} : \kappa\right]} - \frac{1}{(q-1)q^{k_1}}.\end{aligned}$$

If $L_{\mathfrak{q}_1^{k_1}} \neq \kappa_{\mathfrak{q}_1^{k_1}}$, then $[L_{\mathfrak{q}_1^{k_1}} : \kappa_{\mathfrak{q}_1^{k_1}}] \geqslant 2$ and so

$$\delta_{\mathfrak{q}_1,k_1} \geqslant \frac{1}{(q-1)q^{k_1-1}}\left(1 - \frac{1}{2} - \frac{1}{q}\right) \geqslant \frac{1}{q^{k_1+1}}.$$

It is known that there exists a constant M (that depends only on E and P) such that for all prime q and $k \geqslant M$, we have $L_{q^k} \neq \kappa_{q^k}$ (see [12, Lemma 14]. For a reference on this problem, see [19, section 6]). Let $k \geqslant M$ and assume that $L_{\mathfrak{q}_i^k} = \kappa_{\mathfrak{q}_i^k}$ for $i = 1, 2$ and $\mathfrak{q}_1\mathfrak{q}_2 = q$. Then,

$$\kappa_{\mathfrak{q}^k} = \kappa_{\mathfrak{q}_1^k}\kappa_{\mathfrak{q}_2^k} = L_{\mathfrak{q}_1^k}L_{\mathfrak{q}_2^k} = L_{q^k},$$

contradiction. Hence, $L_{\mathfrak{q}_i^k} \neq \kappa_{\mathfrak{q}_i^k}$ for i equal 1 or 2. Therefore, for all $k \geqslant M$,

$$\delta_{\mathfrak{q}_i,k} \geqslant \frac{1}{q^{k+1}}$$

and the lemma easily follows. □

We are finally ready to prove that the hypotheses in Lemma 2.8 are valid for an EDS, under suitable assumptions. Let $\lambda > 0$ be the constant appearing in the previous result.

Proposition 5.4. *Assume that E has CM and assume GRH. Let $q > 3$ be a prime of good reduction. If q is large enough, then there exists $p \leqslant q^{3\lambda}$ such that $q \mid m_p$.*

Proof. Let $x = q^{3\lambda}$. Lemma 5.3 implies that

$$\delta_q \operatorname{li}(x) > \frac{\operatorname{li}(x)}{q^\lambda} = \operatorname{li}(x)x^{-\frac{1}{3}} \gg \frac{x^{\frac{2}{3}}}{\log x}.$$

Hence, Lemma 5.2 yields

$$\#\{p \leqslant x : p \text{ splits in } \kappa, q \mid m_p\} \gg \frac{x^{\frac{2}{3}}}{\log x}.$$

Therefore, if q is large enough, then $\#\{p \leqslant x : p \text{ splits in } \kappa, q \mid m_p\} > 0$. □

20417942, 2024, 4, Downloaded from https://londmathsoc.onlinelibrary.wiley.com/doi/10.1112/mtk.12269 by CochraneAustria, Wiley Online Library on [13/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

With this result we have finally achieved the goal of this section, that was to show, under suitable assumptions, that EDSs satisfy the hypothesis of Lemma 2.8.

Proposition 5.5. *Let E be a rational elliptic curve defined by a Weierstrass equation with integer coefficients. Let $P \in E(\mathbb{Q})$ be a non-torsion point and let $\{b_n\}_{n\in\mathbb{N}}$ be the associated EDS. Assume that E has CM and that GRH holds. Let $\Pi_z = \prod_{p<z} p$. Then,*

$$\frac{1}{\log z} \ll \frac{\varphi(m_{\Pi_z})}{m_{\Pi_z}} \ll \frac{1}{\log z}.$$

Proof. Follows from Lemma 2.7, Lemma 2.8, and Proposition 5.4. □

6 | SIEVING ON KOBLITZ PRIMES

In this section, we keep the focus on EDS and return to our argument in Section 3, involving the Eratosthenes–Legendre sieve. However, rather than working with the set of all primes, we consider the effect of taking $\mathcal{P}$ to be the set of primes p for which $E(\mathbb{F}_p)$ has prime order. The infinitude of this set is an open question.

Conjecture 6.1 (Koblitz conjecture). *Let E be a non-CM elliptic curve defined over $\mathbb{Q}$, with conductor N_E, which is not $\mathbb{Q}$-isogenous to a curve with non-trivial $\mathbb{Q}$-torsion. Then there exists a positive constant C_E, depending on E, such that*

$$\#\{p \leqslant x : p \nmid N_E \text{ and } \#E(\mathbb{F}_p) \text{ is prime}\} \sim C_E \frac{x}{\log^2 x},$$

as $x \to \infty$

It follows from this conjecture that

$$\sum_{\substack{p\nmid N_E \\ \#E(\mathbb{F}_p) \text{ is prime}}} \frac{1}{p} < \infty. \tag{6.1}$$

The convergence of this sum has been established by Cojocaru [3, Corollary 8] for non-CM elliptic curves E over $\mathbb{Q}$, under the assumption that GRH holds.

Let $\{b_n\}_{n\in\mathbb{N}}$ be an EDS associated to a non-CM elliptic curve E and a point $P \in E(\mathbb{Q})$ of infinite order. Let

$$A(N, z) = \{n \leqslant N : \gcd(b_n, \Pi) = 1\},$$

where $\Pi = \Pi(z, \mathcal{P})$ is given by (3.1) and

$$\mathcal{P} = \{p : \#E(\mathbb{F}_p) \text{ is prime}\}.$$

20417942, 2024, 4, Downloaded from https://londmathsoc.onlinelibrary.wiley.com/doi/10.1112/mtk.12269 by CochraneAustria, Wiley Online Library on [13/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

If $\mathcal{P}$ is empty, then trivially $\#A(N,z) = N$. As the goal of this section is to estimate $\#A(N,z)$, we shall assume that $\mathcal{P}$ is not empty (which follows if we assume the Koblitz conjecture). We begin by establishing the following result.

Lemma 6.2. *Assume that Conjecture 6.1 or GRH holds. Then there exists a decreasing function* $h(z) : \mathbb{R}_{\geqslant 2} \to (0,1]$ *with* $\lim_{z\to\infty} h(z) = \delta \in (0,1)$*, such that*

$$\#A(N,z) = Nh(z) + O\Big(2^{\omega(\Pi)}\Big).$$

Proof. In view of Lemma 3.1, it suffices to study $M(\Pi)$. Lemma 2.6 yields

$$M(\Pi) = \sum_{\substack{j \mid m_\Pi \\ \gcd(b_j,\Pi)=1}} \frac{\varphi(m_\Pi/j)}{m_\Pi}.$$

Let $j \mid m_\Pi$. If $j \neq 1$, then $m_p \mid j$ for at least one $p \mid \Pi$, as m_p is prime for each $p \in \mathcal{P}$. Thus, $p \mid b_j$ and then $\gcd(b_j,\Pi) \neq 1$. Let $\mathcal{P}' \subseteq \mathcal{P}$ be a subset of primes such that for each $m \in \{m_p : p \in \mathcal{P}\}$ there exists a unique $p' \in \mathcal{P}'$ for which $m_{p'} = m$. Then

$$M(\Pi) = \frac{\varphi(m_\Pi)}{m_\Pi} = \prod_{\substack{p\leqslant z \\ p\in\mathcal{P}'}} \left(1 - \frac{1}{m_p}\right).$$

Let

$$h(z) = \prod_{\substack{p\leqslant z \\ p\in\mathcal{P}'}} \left(1 - \frac{1}{m_p}\right).$$

If the set $\{p \leqslant z : p \in \mathcal{P}'\}$ is empty, we put $h(z) = 1$. Notice that, for z large enough, the set is not empty and then $h(z) < 1$. The function h is clearly decreasing, positive, and satisfies $h(z) \leqslant 1$ for all z. We may write

$$h(z) = \exp\left(\log\left(\prod_{\substack{p\leqslant z \\ p\in\mathcal{P}'}} \left(1 - \frac{1}{m_p}\right)\right)\right) = \exp\left(-\sum_{\substack{p\leqslant z \\ p\in\mathcal{P}'}} \sum_{n\geqslant 1} \frac{1}{nm_p^n}\right).$$

It follows from the Hasse bound that $m_p \geqslant p/2$, whence

$$\sum_{\substack{p\leqslant z \\ p\in\mathcal{P}'}} \sum_{n\geqslant 2} \frac{1}{nm_p^n} = O(1).$$

Furthermore, it follows from (6.1) that the sum

$$\sum_{\substack{p\leqslant z \\ p\in\mathcal{P}'}} \frac{1}{m_p}$$

20417942, 2024, 4, Downloaded from https://londmathsoc.onlinelibrary.wiley.com/doi/10.1112/mtk.12269 by CochraneAustria, Wiley Online Library on [13/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

has a limit as $z \to \infty$. So,

$$\sum_{\substack{p \leqslant z \\ p \in \mathcal{P}'}} \sum_{n \geqslant 1} \frac{1}{n m_p^n} = O(1).$$

The statement of the lemma follows. □

Conditionally under Conjecture 6.1 or GRH, we are now ready to prove that a positive proportion of elements of the sequence $\{b_n\}_{n \in \mathbb{N}}$ are devoid of primes small prime factors p for which $\#E(\mathbb{F}_p)$ is prime.

Theorem 6.3. *Assume that E is a non-CM elliptic curve. Assume that Conjecture 6.1 or GRH holds, and let $\mathcal{P} = \{p : \#E(\mathbb{F}_p)$ is prime$\}$. Then there exists $\delta \in (0,1)$ such that*

$$\#\{n \leqslant N : (p \mid b_n \text{ and } p \in \mathcal{P}) \Rightarrow p > \log N\} \sim \delta N,$$

as $N \to \infty$.

Proof. We take $z = \log N$, noting that

$$\#\{p \in \mathcal{P} : p \leqslant z\} \ll \frac{\log N}{\log \log N},$$

whence $2^{\omega(\Pi_z)} \ll N^{1/\log \log N}$. Given $\varepsilon > 0$, it follows from Lemma 6.2 that

$$N(\delta - \varepsilon) - 2^{\omega(\Pi_z)} < \#A(N,z) < N(\delta + \varepsilon) + 2^{\omega(\Pi_z)},$$

if z is sufficiently large in terms of ε. The statement of the theorem follows. □

APPENDIX: ON THE NATURAL DENSITY OF THE PRODUCT OF A DIVISOR CLOSED SET AND THE SET OF PRIMES BY Sandro Bettin

Given $\mathcal{A}, \mathcal{B} \subseteq \mathbb{N}$, let $\mathcal{A} \cdot \mathcal{B} := \{ab \mid a \in \mathcal{A}, b \in \mathcal{B}\}$. Also, for any $m \in \mathbb{Z}_{\geqslant 0}$, let

$$\mathbb{P}_m := \{n \in \mathbb{N} \mid \omega(n) \leqslant m\},$$

where $\omega(n) = \sum_{p \mid n} 1$. Finally, we say that $\mathcal{A} \subseteq \mathbb{N}$ is divisor closed if whenever $n \in \mathcal{A}$ and $d \mid n$ one has $d \in \mathcal{A}$. Notice that if $\mathcal{A}$ is divisor closed then so is $\mathcal{A} \cdot \mathbb{P}_m$ for all m.

The goal of this appendix is to prove the following result.

Theorem A.1. *Let $m \geqslant 0$. If $\mathcal{B}$ is a divisor closed set of density 0, then also $\mathcal{B} \cdot \mathbb{P}_m$ has density 0.*

Remark A.2. The theorem does not hold without the assumption that $\mathcal{B}$ is divisor closed. Indeed, if q_N is a sequence of primes going sufficiently slowly to infinity with N, then

$$\mathcal{B} = \cup_N \{n \in (e^{(N-1)^2}, e^{N^2}] \mid n \equiv 1 \pmod{q_N}\}$$

20417942, 2024, 4, Downloaded from https://londmathsoc.onlinelibrary.wiley.com/doi/10.1112/mtk.12269 by CochraneAustria, Wiley Online Library on [13/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

has density 0, but $\mathscr{B} \cdot \mathbb{P}_1$ has density 1. This can be proved easily using the fundamental lemma of sieve theory. We leave the details to the interested reader.

A set $\mathscr{B}$ is divisor closed if and only if its complement $\mathbb{N} \setminus \mathscr{B}$ is a set of multiples, where we remind that, given a (finite or infinite) sequence $\mathscr{A} \subseteq \mathbb{N}$, the set of multiples of $\mathscr{A}$ is

$$\mathcal{M}(\mathscr{A}) := \{da \mid d \in \mathbb{N}, a \in \mathscr{A}\}.$$

We say that a sequence $\mathscr{A} \subseteq \mathbb{N}$ is a Behrend sequence if $\mathcal{M}(\mathscr{A})$ has density 1. We also let $\mathbf{t}(\mathcal{A}) = 1 - \delta(\mathcal{M}(\mathcal{A}))$, with δ denoting the logarithmic density. We state two well-known results on Behrend sequences (see [11, (0.68) and Corollary 0.14]).

Lemma A.3. *We have that $\mathscr{A} = \{a_1, a_2, \dots\} \subseteq \mathbb{N}$ is a Behrend sequence if and only if $\mathbf{t}(\{a_1, \dots, a_n\}) \to 0$ as $n \to \infty$.*

Lemma A.4. *Let $\mathscr{A}, \mathscr{B} \subseteq \mathbb{N}$. If $\mathscr{A} \cup \mathscr{B}$ is a Behrend sequence, then so is at least one of $\mathscr{A}$ and $\mathscr{B}$.*

Ruzsa and Tenenbaum [21, Theorem 2] showed that any Behrend sequence can be split into an infinite disjoint union of Behrend sequences. A modification of their proof gives the following result (see also [11, Corollary 0.15]).

Proposition A.5. *Let $\mathscr{A}$ be a Behrend sequence. Then $\mathscr{A}$ contains infinitely many disjoint Behrend sequences $\mathscr{A}_1, \mathscr{A}_2, \dots$ such that $(a, b) = 1$ for all $a \in \mathscr{A}_i$, $b \in \mathscr{A}_j$ with $i \neq j$.*

Proof. We start with the observation that if $\mathscr{B}$ is a Behrend sequence and $S \subseteq \mathbb{N}$ is a finite set then $\mathscr{B}[S] := \{b \in \mathcal{B} \mid (b, s) = 1 \ \forall s \in S\}$ is a Behrend sequence. This follows immediately from Lemma A.4 because $\mathcal{M}(S)$ has density smaller than 1.

Let $\mathscr{A} = \{a_1, a_2, \dots\}$ and let $\mathscr{B}_1 := \{a_1, \dots, a_{n_1}\}$ with n_1 such that $\mathbf{t}(\mathscr{B}_1) < 1/2$, as possible by Lemma A.3. Also, let $\mathscr{A}^{(1)} := \mathscr{A}[\mathscr{B}_1] = \{a'_1, a'_2, \dots\}$, which is a Behrend set by the above observation. Next, we let $\mathscr{B}_2 := \{a'_1, \dots, a'_{n_2}\}$, with n_2 such that $\mathbf{t}(\mathscr{B}_2) < 1/3$, and $\mathscr{A}^{(2)} := \mathscr{A}^{(1)}[\mathscr{B}_2]$. Repeating this process, we define sequences $\mathscr{B}_1, \mathscr{B}_2, \dots$ such that $\mathbf{t}(\mathscr{B}_j) < 1/(j+1)$ for all $j \geqslant 1$. By construction $(b_i, b_j) = 1$ if $b_i \in \mathscr{B}_i, b_j \in \mathscr{B}_j$ with $i \neq j$. To conclude it suffices to let $\mathscr{A}_i = \bigcup_{n \in \mathcal{N}_i} \mathscr{B}_n$, where $\mathcal{N}_1, \mathcal{N}_2, \dots$ is any sequence of disjoint infinite subsets of $\mathbb{N}$. Indeed, $\mathbf{t}(\mathscr{A}_i) \leqslant \inf_{n \in \mathcal{N}_i}(1/(1+n)) = 0$ and thus $\mathscr{A}_i$ is a Behrend sequence by Lemma A.3. □

Remark A.6. In general, it is not possible to choose the sequences $\mathscr{A}_i$ so that $\bigcup_i \mathscr{A}_i = \mathscr{A}$. For example, this is clearly not possible in the case

$$\mathscr{A} = \{p_1 p_2 \mid p_1, p_2 \text{ distinct primes}\}.$$

Given a sequence $\mathscr{A} \subseteq \mathbb{N}$, we let

$$\mathscr{A}^* := \{[a_1, \dots, a_m] \mid m \geqslant 2,\ a_i \in \mathscr{A},\ (a_1, \dots, a_m) = 1\}.$$

From Proposition A.5, one immediately obtains the following corollary, which would hold also if we fix m to be any integer greater than or equal to 2.

20417942, 2024, 4, Downloaded from https://londmathsoc.onlinelibrary.wiley.com/doi/10.1112/mtk.12269 by CochraneAustria, Wiley Online Library on [13/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Corollary A.7. *If $\mathscr{A} \subseteq \mathbb{N}$ is a Behrend sequence, then so is $\mathscr{A}^*$.*

Lemma A.8. *We have that $\mathcal{M}(\mathscr{A}^*) = (\mathcal{M}(\mathscr{A}))^*$. In particular, if $\mathscr{A}$ is the set of multiples of some set, then so is $\mathscr{A}^*$.*

Proof. Let $n \in \mathcal{M}(\mathscr{A}^*)$. Thus, $n = \ell \cdot [a_1, \dots, a_m]$ with $\ell \in \mathbb{N}$, $m \geqslant 2$, $a_i \in \mathscr{A}$ and $(a_1, \dots, a_m) = 1$. For any prime p, let $j_p \in \{1, \dots, m\}$ be such that $v_p(a_{j_p}) = v_p([a_1, \dots, a_m])$, with v_p denoting the p-adic valuation, and let $a_j' := a_j \prod_{p \mid \ell, j_p = j} p^{v_p(\ell)} \in \mathcal{M}(\mathscr{A})$ for $j = 1, \dots, m$. Then, $n = [a_1', \dots, a_m']$ and $(a_1', \dots, a_m') = 1$ and so $n \in (\mathcal{M}(\mathscr{A}))^*$.

Vice versa, let $n \in (\mathcal{M}(\mathscr{A}))^*$. Then $n = [\ell_1 a_1, \dots, \ell_m a_m]$ with $\ell \in \mathbb{N}$, $m \geqslant 2$, $a_i \in \mathcal{A}$ and $(\ell_1 a_1, \dots, \ell_m a_m) = 1$. Thus, $(a_1, \dots, a_m) = 1$ and $[a_1, \dots, a_m]$ divides n and so $n \in \mathcal{M}(\mathscr{A}^*)$. □

Proposition A.9. *Let $\mathscr{A} \subseteq \mathbb{N}$. Then*

$$\mathbb{N} \setminus \mathcal{M}(\mathscr{A}^*) = (\mathbb{N} \setminus \mathcal{M}(\mathscr{A})) \cdot \mathbb{P}_1.$$

Proof. We can assume $1 \notin \mathscr{A}$ because otherwise $\mathcal{M}(\mathscr{A}) = \mathbb{N}$ and the claim is trivial.

Let $n \in (\mathbb{N} \setminus \mathcal{M}(\mathscr{A})) \cdot \mathbb{P}_1$ so that there exists a prime p and $r \geqslant 0$ such that $p^r \mid n$ and $n/p^r \notin \mathcal{M}(\mathscr{A})$. If we had $n \in \mathcal{M}(\mathscr{A}^*)$, then by Lemma A.8 we would have $n = [a_1, \dots, a_m]$ for some $m \geqslant 2$ and $a_i \in \mathcal{M}(\mathscr{A})$ with $(a_1, \dots, a_m) = 1$. As $(a_1, \dots, a_m) = 1$, then there exists $j \in \{1, \dots, m\}$ such that $p \nmid a_j$. In particular, a_j divides n/p^r and so $n/p^r \in \mathcal{M}(\mathscr{A})$, which is a contradiction. Thus, $n \in \mathbb{N} \setminus \mathcal{M}(\mathscr{A}^*)$.

Now, let $n \notin (\mathbb{N} \setminus \mathcal{M}(\mathscr{A})) \cdot \mathbb{P}_1$. As $1 \notin \mathscr{A}$ then $(\mathbb{N} \setminus \mathcal{M}(\mathscr{A})) \cdot \mathbb{P}_1$ contains the prime powers. In particular, the prime factor decomposition of n, $n = p_1^{r_1} \cdots p_m^{r_m}$, has $m \geqslant 2$. By hypothesis for all $j = 1, \dots, m$ we have $n/p_j^{r_j} \in \mathcal{M}(\mathscr{A})$. Also, clearly $n = [n/p_1^{r_1}, \dots, n/p_m^{r_m}]$ with $(n/p_1^{r_1}, \dots, n/p_m^{r_m}) = 1$ and thus $n \in (\mathcal{M}(\mathscr{A}))^* = \mathcal{M}(\mathscr{A}^*)$. □

Proof of Theorem A.1. We have $\mathbb{P}_m = \mathbb{P}_1 \cdot \mathbb{P}_{m-1}$ for $m \geqslant 1$ and thus, as $\mathscr{B} \cdot \mathbb{P}_1$ is also divisor closed if $\mathscr{B}$ is, then by induction we can assume $m = 1$.

Let $\mathscr{A} := \mathbb{N} \setminus \mathscr{B}$. In particular, $\mathscr{A}$ is a set of multiples of density 1 and in fact $\mathcal{M}(\mathscr{A}) = \mathscr{A}$, so that $\mathscr{A}$ is a Behrend sequence. The theorem then follows by Corollary A.7 and Proposition A.9. □

ACKNOWLEDGEMENTS

The authors are very grateful to Andrew Granville, Dimitris Koukoulopoulos, Davide Lombardo, Florian Luca, Igor Shparlinski and Joni Teräväinen for useful comments. While working on this paper, the first author was supported by a FWF Grant (DOI 10.55776/P36278) and the second author was supported by the European Union's Horizon 2020 research and innovation program under the Marie Skłodowska-Curie Grant Agreement Number 101034413.

JOURNAL INFORMATION

Mathematika is owned by University College London and published by the London Mathematical Society. All surplus income from the publication of *Mathematika* is returned to mathematicians and mathematics research via the Society's research grants, conference grants, prizes, initiatives for early career researchers and the promotion of mathematics.

20417942, 2024, 4, Downloaded from https://londmathsoc.onlinelibrary.wiley.com/doi/10.1112/mtk.12269 by CochraneAustria, Wiley Online Library on [13/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

REFERENCES

1. S. Bhakta, D. Loughran, S. L. Rydin Myerson, and M. Nakahara, *The elliptic sieve and Brauer groups*, Proc. Lond. Math. Soc. **126** (2023), 1884–1922.
2. J. Bourgain, A. Gamburd, and P. Sarnak, *Markoff triples and strong approximation*, C. R. Math. Acad. Sci. Paris **354** (2016), 131–135.
3. A. C. Cojocaru, *Reductions of an elliptic curve with almost prime orders*, Acta Arith. **119** (2005), 265–289.
4. A. C. Cojocaru and M. R. Murty, *An introduction to sieve methods and their applications*, Cambridge University Press, Cambridge, 2005.
5. M. Einsiedler, G. Everest, and T. Ward, *Primes in elliptic divisibility sequences*, LMS J. Comput. Math. **4** (2001), 1–13.
6. P. Erdős, *Some recent advances and current problems in number theory*, Lectures on modern mathematics, vol. III, T. L. Saaty (ed.), Wiley, New York, 1965, pp. 196–244.
7. J. Grantham and A. Granville, *Fibonacci primes, primes of the form* $2^n - k$ *and beyond*, J. Number Theory **261** (2024), 190–219.
8. A. Granville, *Classifying linear division sequences*, arXiv:2206.11823, 2022.
9. R. Gupta and M. R. Murty, *Cyclicity and generation of points mod p on elliptic curves*, Invent. Math. **101** (1990), 225–235.
10. R. Gupta and M. R. Murty, *Primitive points on elliptic curves*, Compos. Math. **58** (1986), 13–44.
11. R. R. Hall, *Sets of multiples*, Cambridge Tracts in Mathematics, vol. 118, Cambridge University Press, Cambridge, 1996.
12. M. Hindry, *Autour d'une conjecture de Serge Lang*, Invent. Math. **94** (1988), no. 3, 575–603.
13. C. Hooley, *Applications of sieve methods to the theory of numbers*, Cambridge Tracts in Mathematics, vol. 70, Cambridge University Press, Cambridge, 1976.
14. O. Järviniemi and J. Teräväinen, *Composite values of shifted exponentials*, Adv. Math. **429** (2023), Paper No. 109187.
15. A. Kontorovich and J. Lagarias, *On toric orbits in the affine sieve*, Exp. Math. **30** (2021), 575–587.
16. E. Kowalski, *The large sieve and its applications: arithmetic geometry, random walks and discrete groups*, Cambridge University Press, Cambridge, 2008.
17. J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem*, Algebraic number fields: *L*-functions and Galois properties (Proc. Sympos. Univ. Durham, Durham, 1975), Academic Press, London, 1977, pp. 409–464.
18. H. W. Lenstra, *On Artin's conjecture and Euclid's algorithm in global fields*, Invent. Math. **42** (1977), 201–224.
19. D. Lombardo and S. Tronto, *Some uniform bounds for elliptic curves over* $\mathbb{Q}$, Pacific J. Math. **320** (2022), 133–175.
20. F. Luca and P. Stănică, *Prime divisors of Lucas sequences and a conjecture of Skałba*, Int. J. Number Theory **1** (2005), 583–591.
21. I. Z. Ruzsa and G. Tenenbaum, *A note on Behrend sequences*, Acta Math. Hung. **72** (1996), 327–337.
22. A. Schinzel, *Primitive divisors of the expression* $A^n - B^n$ *in algebraic number fields*, J. Reine Angew. Math. **268/269** (1974), 27–33.
23. J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer Science & Business Media, Berlin, 1994.
24. J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.
25. J. H. Silverman, *Wieferich's criterion and the abc-conjecture*, J. Number Theory **30** (1988), 226–237.
26. C. L. Stewart, *On divisors of Lucas and Lehmer numbers*, Acta Math. **211** (2013), 291–314.
27. D. Zagier, *On the number of Markoff numbers below a given bound*, Math. Comp. **39** (1982), 709–723.

20417942, 2024, 4, Downloaded from https://londmathsoc.onlinelibrary.wiley.com/doi/10.1112/mtk.12269 by CochraneAustria, Wiley Online Library on [13/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License