ON THE REFINED KOBLITZ CONJECTURE

SAMPA DEY, ARNAB SAHA, JYOTHSNAA SIVARAMAN, AND AKSHAA VATWANI

ABSTRACT. Given a non-CM elliptic curve E over $\mathbb{Q}$, let N_p be the number of points on $E \pmod p$. Given $t \in \mathbb{N}$, we are concerned with the density of primes for which N_p/t is a prime. The constant appearing in this density was first postulated by Koblitz for $t = 1$ and the conjecture was later refined by Zywina. Assuming certain conjectures, this paper gives the first explicit computation of this constant in the literature, and confirms existing heuristic predictions for the same.

More precisely, we postulate sufficient cancellation in the sum of the Möbius function running over the sequence N_p/t, and show that this is equivalent to the refined Koblitz conjecture, under the assumption of suitable elliptic analogues of the classical Elliott-Halberstam conjecture.

1. NOTATION

Throughout this article, p will be used to denote a rational prime. We will use the standard notation for the logarithmic integral

$$\mathrm{Li}(x) := \int_2^x \frac{dt}{\log t}.$$

The von Mangoldt function $\Lambda(n)$, is defined by

$$\Lambda(n) = \begin{cases} \log p, \text{ if } n = p^r, \ r \geq 0 \\ 0, \text{ otherwise.} \end{cases}$$

We let $\mathrm{rad}(n)$ denote the product of distinct prime factors of n. For a non-negative function $g(x)$, the notation $f(x) = O(g(x))$, or equivalently, $f(x) \ll g(x)$ means that there is a constant C such that $|f(x)| \leq Cg(x)$ as $x \to \infty$. The notation $f(x) = o(g(x))$ is used to denote that $\frac{f(x)}{g(x)} \to 0$ as $x \to \infty$. The notation $f(x) \sim g(x)$ means that $\frac{f(x)}{g(x)} \to 1$ as $x \to \infty$. We will use $\tau_k(n)$ to denote the number of ways of writing n as a product of k positive integers. The number of divisors of n will be denoted by $\tau(n)$.

2. INTRODUCTION

Let E be an elliptic curve without complex multiplication, defined over $\mathbb{Q}$ with conductor N_E. Let $\mathbb{F}_p$ be the finite field of order p. Suppose E has good reduction at p, that is $p \nmid N_E$. Let E_p be the elliptic curve E reduced modulo p and $E_p(\mathbb{F}_p)$ be the set of $\mathbb{F}_p$-rational points on the curve E_p defined over $\mathbb{F}_p$. This is a finite group of cardinality

$$\#E_p(\mathbb{F}_p) = p + 1 - a_p,$$

where a_p is an integer satisfying the Hasse bound

$$|a_p| \leq 2\sqrt{p}.$$

Henceforth, we denote the cardinality $\#E_p(\mathbb{F}_p)$ by N_p.

2010 *Mathematics Subject Classification.* Primary 11N05; Secondary 11R45, 11G05.

Keywords and phrases. Elliptic curves modulo p, Koblitz conjecture, Elliott-Halberstam conjecture.

In 1988, motivated by applications in cryptography, Koblitz [12] studied the distribution of N_p for certain elliptic curves over the rationals. By drawing analogies with the celebrated twin-prime conjecture in classical number theory, he proposed the following conjecture for non-CM elliptic curves.

Conjecture 1. [Koblitz [12] 1988] *Let $E/\mathbb{Q}$ be a non-CM elliptic curve with conductor N_E. Assume that E is not $\mathbb{Q}$-isogenous to a curve with non-trivial $\mathbb{Q}$ torsion. Then there exists a positive constant $C(E)$ such that*

$$\#\{p \le x : \ p \nmid N_E, N_p \text{ is prime}\} \sim C(E)\frac{x}{(\log x)^2},$$

as $x \to \infty$.

Moreover, Koblitz conjectured a value for the constant $C(E)$. The constant he suggested is given by

$$C(E) = \prod_{\ell} a(\ell),$$

where the product runs over primes ℓ,

$$a_\ell = \frac{1 - \dfrac{\#\{g \in G_\ell : g \text{ has eigenvalue } 1\ \}}{|G_\ell|}}{1 - \dfrac{1}{\ell}}, \tag{2.1}$$

and G_ℓ denotes the Galois group of the ℓ-division points of E over $\mathbb{Q}$, identified upto isomorphism with a subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. It is instructive to interpret the numerator of (2.1) as the probability that N_p is *not* divisible by the given prime ℓ, and the denominator as the probability of a random integer not being divisible by ℓ. Let us also remark that for a Serre curve, where G_ℓ is always isomorphic to $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, the above constant can be written explicitly as

$$C(E) = \prod_{\ell \text{ prime}} \left(1 - \frac{\ell^2 - 2}{(\ell^2-1)(\ell-1)}\right)\left(1 - \frac{1}{\ell}\right)^{-1}.$$

One of the first results in the direction of Koblitz's conjecture was by Miri and Murty [15]. Assuming the Generalised Riemann hypothesis, they showed that the number of primes $p \le x$ such that N_p is a product of at most 16 prime factors (counting multiplicity) is $\gg x/(\log x)^2$, as $x \to \infty$. This was followed by work of Steuding and Weng [28, 27], who obtained such results under GRH with N_p being a product of atmost 6 distinct prime factors. David and Wu [8] were able to show this with N_p being a product of atmost 8 prime factors, under the weaker assumption of a suitable zero-free region instead of GRH. For CM curves, Cojocaru [5] showed *unconditionally* that the number of primes $p \le x$ such that N_p has at most 5 prime factors is $\ge C(E)x/(\log x)^2$, for some positive constant $C(E)$.

The Koblitz conjecture is known to hold on average over certain families of elliptic curves due to the work of Balog, Cojocaru and David [2] and subsequent results of Giberson [9] in the number field setting. Related questions about the size and arithmetic behaviour of N_p as p varies over primes of good reduction have been investigated by Iwaniec and Jiménez Urroz [11], and Akbary, Ghioca and Murty [1]. We refer the interested reader to the excellent articles [4] and [6] by Cojocaru for an introduction to related problems on elliptic curves.

Based on some known examples with respect to the Lang-Trotter conjecture, it is known that there are curves for which $C(E) = 0$. This occurs because the probabilities of the events $\ell \nmid N_p$ may not be multiplicative, since the events may not be independent. This crucial observation was first made by Jones [3] and Zywina [30]. In particular, Zywina points out that in some cases, there may be an obstruction to the primality of N_p in the form of an integer $t_E > 1$ which divides almost all of the values of N_p. In order to take this into account and still continue to count prime values of

N_p up to such obstructions, Zywina formulated a refined version of the Koblitz conjecture. While Zywina's conjecture is more general and applies to an elliptic curve over a number field K, we state the same below in the case $K = \mathbb{Q}$.

Conjecture 2 (Zywina [30], 2009)**.** *Let $E/\mathbb{Q}$ be an elliptic curve with conductor N_E. Let t be a positive integer. Then there exists an explicit constant $C_{E,t} \geq 0$ such that*

$$\#\left\{p \leq x :\ p \nmid N_E,\ \frac{N_p}{t} \text{ is prime}\right\} \sim C_{E,t} \frac{x}{(\log x)^2},$$

as $x \to \infty$.

We may express the above asymptotic as

$$\sum_{\substack{p \leq x, p \nmid N_E \\ N_p \equiv 0 \ (\mathrm{mod}\ t)}} \Lambda\left(\frac{N_p}{t}\right) \sim C_{E,t} \operatorname{Li}(x). \tag{2.2}$$

In this paper, we are motivated by Koblitz's initial analogy of his conjecture with the twin prime problem. The twin prime conjecture is intimately connected to a phenomenon known as the parity problem. This principle was heuristically formulated by Selberg [22] to capture the inability of sieve methods to detect prime numbers. In recent work, Murty and Vatwani [19] reformulated the parity problem in terms of cancellations in certain summatory functions involving the Möbius function. More precisely, they formulated an analogue of the Chowla conjecture asserting equidistribution of the Möbius function over shifted primes, and established a concrete link between this and the twin prime conjecture (cf. Theorem 1.1, [19]).

In the context of Koblitz's conjecture, it is natural to examine a variant of the Chowla conjecture which would capture equidistribution of the Möbius function over values of N_p as p runs over the primes. More precisely, we conjecture that

$$\sum_{p \leq x,\, p \nmid N_E} \mu(N_p) = o(\operatorname{Li}(x))$$

as $x \to \infty$. In line with the refined Koblitz conjecture formulated by Zywina, one would be led to expect the following.

Conjecture 3. *We have, as $x \to \infty$,*

$$\sum_{\substack{p \leq x,\, p \nmid N_E \\ N_p \equiv 0 \ (\mathrm{mod}\ t)}} \mu\left(\frac{N_p}{t}\right) = o(\operatorname{Li}(x)). \tag{2.3}$$

In what follows, we will establish that Conjecture 3 is indeed closely connected to the Koblitz conjecture, in fact is equivalent to it under some assumptions. Before stating our main theorem, we proceed to introduce some conjectures which will arise naturally while trying to estimate the density of primes p for which N_p/t is prime.

A fundamental ingredient involved in the study of the twin prime problem is the distribution of primes in arithmetic progressions. More generally, one may formulate an equidistribution result for primes in arithmetic progressions, with "level of distribution" $0 < \theta < 1$ as follows.

Elliott-Halberstam Conjecture EH(x^θ). *Let $\pi(x, q, a) = \#\{p \leq x : p \equiv a \ (\mathrm{mod}\ q)\}$. For any $A > 0$, we have*

$$\sum_{q \leq x^\theta} \max_{y \leq x} \max_{(a,q)=1} \left|\pi(y, q, a) - \frac{\operatorname{Li} y}{\phi(q)}\right| \ll_A \frac{x}{(\log x)^A}. \tag{2.4}$$

For $\theta < 1/2$, this conjecture is true and is called the Bombieri-Vinogradov theorem. As we will see, in the context of Koblitz's conjecture, the arithmetic progression $p \equiv a \pmod q$ is replaced by $N_p \equiv 0 \pmod q$, calling for equidistribution of primes lying in certain Chebotarev sets instead of arithmetic progressions. It is thus expected that what will come into play is an "average" result related to the Chebotarev density theorem. We will precisely formulate such an elliptic analogue of the Elliott-Halberstam Conjecture, referred to as $\mathbf{EH}_{E,t}(x^\theta)$, in Section 6.

Conjecture $\mathbf{EH}_{E,t}(x^\theta)$ does not suffice to break the parity barrier, as in the classical twin-prime case. We also require equidistribution of the Möbius function on the values of N_p, in arithmetic progressions. We thus postulate the following conjecture which can be thought of as an elliptic analogue of the Elliott-Halberstam conjecture with a Möbius shift.

Conjecture $\mathbf{EH}_{E,t,\mu}(x^\theta)$. (Elliptic analogue of the Elliott-Halberstam Conjecture with a Mobius shift) *Let t be a fixed positive integer and $L = L(E)$ be the integer appearing in Theorem 3.3. Then for any $A > 0$, we have*

$$\sum_{d \le x^\theta} \max_{y \le x} \left|\Delta_{E,\mu}(y,d,t)\right| \ll_A \frac{x}{(\log x)^A} \tag{2.5}$$

where,

$$\Delta_{E,\mu}(y,d,t) := \sum_{\substack{p \le y \\ N_p \equiv 0 \ (\mathrm{mod}\ dt) \\ p \nmid dtN_E}} \mu\left(\frac{N_p}{t}\right) - \frac{1}{\omega(td_1)\delta(d_2)} \sum_{\substack{p \le y \\ p \nmid N_E}} \mu\left(\frac{N_p}{t}\right), \tag{2.6}$$

and $d = d_1 d_2$ is the unique factorization of d such that rad$(d_1) | tL$, and $(d_2, tL) = 1$. The functions ω and δ will be precisely defined in Section 3 (see (3.4)).

In our approach, a significant distinction between the Koblitz conjecture and the twin prime conjecture arises from the fact that the former necessitates bounding the number of primes p such that $N_p = p + 1 - a_p$ takes a given value n. In the twin prime case, as one is dealing with a *fixed* shift $p + 2$, this aspect does not arise. Accordingly, letting n be a fixed positive integer, consider the arithmetic function

$$M_E(n) := \#\{p : N_p = n\}.$$

By the Hasse bound, a trivial bound for $M_E(n)$ is

$$M_E(n) \ll \frac{\sqrt{n}}{\log(n+1)}.$$

In [13], Kowalski posed a question about the asymptotic growth of $M_E(n)$ as $n \to \infty$. He conjectured the bound

$$M_E(n) \ll_{E,\epsilon} n^\epsilon,$$

for any $\epsilon > 0$, and was able to show this when E has complex multiplication. More precisely, he showed the following when E has CM by an order $\mathcal{O}$ in the ring of integers $\mathcal{O}_K$ of an imaginary quadratic field K.

Proposition 2.1. [13, Proposition 5.3] *Let $r_K(n) = \#\{\mathfrak{a} \subset \mathcal{O}_K : N(\mathfrak{a}) = n\}$, where $N(\mathfrak{a}) := |\mathcal{O}_K/\mathfrak{a}|$ denotes the norm of a nonzero ideal $\mathfrak{a}$ of $\mathcal{O}_K$. We have*

$$M_E(n) \ll_E r_K(n).$$

While it is expected based on heuristic evidence that $M_E(n)$ should be even smaller, no result better than the trivial bound is known for non-CM curves. In [7], David and Smith predicted via a probabilistic model that the order of magnitude of $M_E(n)$ is likely to be close to $\frac{1}{\log n}$ and were able to show this on average over a family of elliptic curves. The average order of $M_E(n)$ is known to be $1/\log n$. In particular, it is known (see [13]) that

$$\sum_{n\le x} M_E(n) = \pi(x) + O(\sqrt{x}) \sim \frac{x}{\log x}. \tag{2.7}$$

We postulate an estimate of the following form.

Conjecture 4. *For $d \le x$, we have*

$$\sum_{\substack{n\le x\\ d|n}} M_E(n) \ll_E \frac{x(\log x)^C}{d},$$

for some $C = C(E) > 0$.

We are now in a position to state our main result, establishing a conditional equivalence between (2.2) and (2.3). More significantly, assuming the aforementioned conjectures, we are able to compute the explicit form of the refined Koblitz constant $C_{E,t}$ of Conjecture 2. This is the first result where the conjectured constant is conditionally determined. This validates existing heuristic predictions for the constant, which were hitherto supported by numerical evidence and average results over a family of elliptic curves. As we will show in Section 4, the expression derived by us for the constant agrees with that described by Zywina in [30, Proposition 2.4].

Theorem 2.2. *Let E be a fixed non-CM elliptic curve over $\mathbb{Q}$ with conductor N_E. Let $L = L(E)$ be the fixed positive integer given by Serre's result (Theorem 3.3) and let t be a fixed positive integer. Let N_p be the number of points on the curve E_p, where the curve $E_p := E$ modulo p. Suppose that the conjectures $\mathrm{EH}_{E,t}(x^\theta(\log x)^B)$, $\mathrm{EH}_{E,t,\mu}(x^{1-\theta})$ are true for some fixed $1/2 \le \theta < 1$ and a suitably large fixed $B > 0$. Suppose that Conjecture 4 holds. We then obtain the following:*

(a) Conjecture 3 is equivalent to the refined Koblitz conjecture. That is, the assertion (2.3) is equivalent to the assertion (2.2), with the refined Koblitz constant given by

$$C_{E,t} = \frac{\left(\sum_{r|tL} \frac{\mu(r)}{\omega(tr)}\right)}{\prod_{p|tL}\left(1-\frac{1}{p}\right)} \prod_{p\nmid tL}\left(1 - \frac{p^2-p-1}{(p-1)^3(p+1)}\right), \tag{2.8}$$

where ω is a function defined precisely in Section 3 (cf. (3.4)).

(b) We have

$$\sum_{\substack{p\le x, p\nmid N_E\\ N_p\equiv 0 \ (\mathrm{mod}\ t)}} \Lambda\left(\frac{N_p}{t}\right) \ge (1-o(1))C_{E,t}(1-\mathcal{A}_{E,L})\,\mathrm{Li}\,x,$$

where

$$\mathcal{A}_{E,L} = \left(1 - \frac{(\ell^4-2)}{(\ell^2-1)^2(\ell^2+1)}\right), \tag{2.9}$$

and ℓ is the least prime coprime to $L(E)$.

In what follows, we may at times drop the condition $N_p \equiv 0 \pmod t$ that appears in expressions of the form (2.3) and (2.2), taking it to be implied by the support of the arithmetical functions Λ and μ. The paper is organized as follows. In Section 3, we set things up in order to invoke the Chebotarev density theorem in our analysis. In Section 4, we compare our expression for the refined Koblitz constant with the expression conjectured by Zywina in [30]. In Section 6, we formulate the elliptic analogue of the Elliott-Halberstam conjecture. The proof of Theorem 2.2 is contained in Sections 8 and 9.

3. The Galois representation and the Chebotarev density theorem

Continuing with our previous notation, let E be an elliptic curve defined over $\mathbb{Q}$ with conductor N_E. For $d \geq 2$, let $E[d]$ denote the subgroup of d-torsion points inside $E(\overline{\mathbb{Q}})$. Let $K_d := \mathbb{Q}(E[d])$ be the finite Galois extension of $\mathbb{Q}$ obtained by adjoining the coordinates of the d-torsion points of E. Consider the natural group action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $E[d]$ given by

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[d]).$$

Let us assume $(d, N_E) = 1$ in which case we have $E[d] \simeq (\mathbb{Z}/d\mathbb{Z})^2$ and hence $\mathrm{Aut}(E[d]) \simeq \mathrm{GL}_2(\mathbb{Z}/d\mathbb{Z})$. Therefore the Galois representation ρ factors as follows:

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(K_d/\mathbb{Q}) \overset{\rho_d}{\hookrightarrow} \mathrm{GL}_2(\mathbb{Z}/d\mathbb{Z}).$$

For brevity, let us use the notation $G := \mathrm{Gal}(K_d/\mathbb{Q})$, $G(d) := \rho_d(G)$. Let p be a non-zero prime of $\mathbb{Q}$ such that E has good reduction at p, that is $p \nmid N_E$. If $p \nmid d$, then p is unramified in K_d (cf. Theorem 7.1, Chapter VII, [26]). Recall that to each prime ideal $\mathfrak{p}$ lying above p, we can associate what is called the Frobenius automorphism $\mathrm{Frob}_\mathfrak{p}$ of $\mathfrak{p}$ (cf. [17, ch. 11.3] for more details). Then, as $\mathfrak{p}$ ranges over the prime ideals above p, the Frobenius elements $\mathrm{Frob}_\mathfrak{p}$ comprise a conjugacy class of $\mathrm{Gal}(K_d/\mathbb{Q})$, which is called the Artin symbol of p. We denote it by σ_p. By abuse of notation, we will denote the image $\rho_d(\sigma_p) \subseteq \mathrm{GL}_2(\mathbb{Z}/d\mathbb{Z})$ as σ_p as well. It is known that the characteristic polynomial of $\rho_d(\mathrm{Frob}_\mathfrak{p})$ is

$$t^2 - \overline{a}_p t + \overline{p},$$

where $\overline{a}_p \equiv p + 1 - N_p \pmod{d}$ and $\overline{p} \equiv p \pmod{d}$. As a consequence, we have $N_p \equiv 0 \pmod{d}$ iff σ_p is contained in a conjugacy class of $G(d)$ consisting of elements having 1 as an eigenvalue.

More precisely, let us define

$$\Psi_0(d) := \{A \in \mathrm{Aut}(E[d]) \simeq \mathrm{GL}_2(\mathbb{Z}/d\mathbb{Z}) \mid \det(I - A) \equiv 0 \,(\mathrm{mod}\ d)\}, \tag{3.1}$$

and $C(d) := G(d) \cap \Psi_0(d)$. Then the primes $p \nmid dN_E$ such that $N_p \equiv 0 \,(\mathrm{mod}\ d)$ are precisely those for which $\sigma_p \subseteq C(d)$. By the Chebotarev density theorem, the natural density of such primes is the ratio

$$\frac{|C(d)|}{|G(d)|}. \tag{3.2}$$

In order to make the above ratio explicit, we will need the following properties of the set $\Psi_0(d)$.

Lemma 3.1. *If $(d_1, d_2) = 1$ then $\Psi_0(d_1 d_2) \simeq \Psi_0(d_1) \times \Psi_0(d_2)$.*

Proof. This follows upon using the isomorphism

$$\mathbb{Z}/d_1 d_2\mathbb{Z} \simeq \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}$$

to construct a well defined isomorphism $\psi : \Psi_0(d_1 d_2) \longrightarrow \Psi_0(d_1) \times \Psi_0(d_2)$. □

Lemma 3.2. *Let ℓ be a prime. Then $|\Psi_0(\ell)| = \ell^3 - 2\ell$.*

Proof. The cardinality $|\Psi_0(\ell)|$ counts all those matrices A in $\mathrm{GL}_2(\mathbb{Z}/d\mathbb{Z})$ which have 1 as an eigenvalue. This means that the characteristic polynomial char(A) is $(x-1)(x-a)$, where $a \in \mathbb{F}_\ell^*$. We recall the following result by Zywina [cf. Lemma 2.5, [30]]

$$\#\{A \in \mathrm{GL}_2(\mathbb{F}_\ell) : \text{eigen values of } A \text{ are 1 and } a\} = \begin{cases} \ell^2 + \ell, & \text{if } a \neq 1 \\ \ell^2, & \text{if } a = 1. \end{cases}$$

Hence $|\Psi_0(\ell)| = \ell^2 + (\ell - 2)(\ell^2 + \ell) = \ell^3 - 2\ell$, as required. □

We will also need to invoke the following important result of Serre [24] for non-CM elliptic curves.

Theorem 3.3 (Serre). *For a number field K, let E/K be an elliptic curve defined over K without complex multiplication. Then there exists a positive integer $L = L(E)$ such that if $d_1, d_2 \in \mathbb{N}$ with $(Ld_1, d_2) = 1$, then*

$$G(d_1 d_2) = G(d_1) \times \mathrm{Aut}(E[d_2]).$$

We will simplify the density (3.2) as follows. Let L be the integer appearing in Theorem 3.3. Given an integer d, we first uniquely write $d = d_1 d_2$, such that $\mathrm{rad}(d_1)|L$ and $(d_2, L) = 1$. Then using Lemma 3.1 and Theorem 3.3, we obtain

$$\frac{|C(d)|}{|G(d)|} = \frac{|G(d_1 d_2) \cap \Psi_0(d_1 d_2)|}{|G(d_1 d_2)|} = \frac{|G(d_1) \cap \Psi_0(d_1)|}{|G(d_1)|} \cdot \frac{|\mathrm{Aut}(E[d_2]) \cap \Psi_0(d_2)|}{|\mathrm{Aut}(E[d_2])|}.$$

$$=: \frac{1}{\omega(d_1)} \cdot \frac{1}{\delta(d_2)}, \tag{3.3}$$

where

$$\omega(d) = \frac{|G(d)|}{|G(d) \cap \Psi_0(d)|}, \quad \delta(d) = \frac{|\mathrm{Aut}(E[d])|}{|\mathrm{Aut}(E[d]) \cap \Psi_0(d)|}. \tag{3.4}$$

Keeping in mind that $\mathrm{Aut}(E[d]) \simeq \mathrm{GL}_2(\mathbb{Z}/d\mathbb{Z})$, we see from Lemma 3.1 that δ is a multiplicative function. Using Lemma 3.2, we see that on primes $\ell \nmid L$, it is given by

$$\delta(\ell) = \frac{(\ell - 1)(\ell^2 - 1)}{(\ell^2 - 2)}. \tag{3.5}$$

Furthermore, by a similar argument as in Lemma 3.2, it can be shown that

$$\delta(q) = \frac{(q - 1)(q^2 - 1)}{(q^2 - 2)}, \tag{3.6}$$

where $q = \ell^r$ for some $r \in \mathbb{N}$, and $\ell \nmid L$.
Let t be a fixed positive integer. Recall that the refined Koblitz conjecture is concerned with the number of primes $p \leq x$, $p \nmid N_E$, such that $\frac{N_p}{t}$ is prime. While trying to sieve out composite values of $\frac{N_p}{t}$, we will be led to estimate

$$\pi_E(x, d, t) := \#\left\{ p \leq x : p \nmid tdN_E, \ \frac{N_p}{t} \equiv 0 \ (\mathrm{mod}\ d) \right\}. \tag{3.7}$$

Since $N_p/t \equiv 0 \pmod d$ iff $\sigma_p \subseteq C(td)$, from the Chebotarev density theorem and the expressions (3.3) and (3.4), we immediately find that as $x \to \infty$,

$$\pi_E(x, d, t) \sim \frac{1}{\omega(td_1)} \frac{1}{\delta(d_2)} \,\mathrm{Li}(x), \tag{3.8}$$

where $d = d_1 d_2$ is the unique factorization of d such that $\mathrm{rad}(d_1)|tL$, and $(d_2, tL) = 1$.

Estimation of the error terms involved in (3.8) is a deep question. Effective versions of the Chebotarev density theorem have been given by Lagarias and Odlyzko [14], and Serre [25]. Refinements of these effective versions and applications to modular forms have been studied by M. R. Murty, V. K. Murty and N. Saradha [18]. Recently, Pierce, Turnage-Butterbaugh and Wood [21] established an unconditional effective version of the Chebotarev density theorem which holds for "almost all" number fields in a certain family of field extensions. Using the explicit versions of the Chebotarev density theorem given in [14] and [25], and assuming GRH for Artin L-functions, Steuding and Weng [28] obtained the estimate

$$\pi_E(x, d, t) = \frac{1}{\omega(td_1)} \cdot \frac{1}{\delta(d_2)} \,\mathrm{Li}(x) + O\left(d^{3/2} x^{1/2} \log (dN_E x) \right),$$

where $d = d_1 d_2$ with $\mathrm{rad}(d_1)|L$, and $(d_2, L) = 1$.

As pointed out by Cojocaru [5, Remark 12], one may also assume a more relaxed formulation of GRH using the results in [14]. More precisely, assuming that the Dedekind zeta functions of the division fields of E do not vanish for $\mathrm{Re}(s) > \theta$, for some $1/2 \leq \theta < 1$, we have

$$\pi_E(x, d, t) = \frac{1}{\omega(td_1)} \cdot \frac{1}{\delta(d_2)} \operatorname{Li}(x) + O\left(d^3 x^\theta \log\left(dN_E x\right)\right).$$

As stated in [5, Remark 13], from the results in [14], we have the following unconditional estimates for small d. For $d \ll \log\log x$, we have

$$\pi_E(x, d, t) = \frac{1}{\omega(td_1)} \cdot \frac{1}{\delta(d_2)} \operatorname{Li}(x) + O_A\left(d^3 \frac{x}{(\log x)^A}\right), \tag{3.9}$$

for any $A > 0$.

We conclude this section by recording a bound on $\frac{1}{\delta(n)}$, which will be of use to us in later sections.

Lemma 3.4. *Let L be the fixed positive integer appearing in Theorem* 3.3*. There exists an absolute constant $D > 0$ such that for $(n, L) = 1$, we have*

$$\frac{1}{\delta(n)} \ll \frac{(\log n)^D}{n}.$$

Proof. For a prime $\ell \nmid L$, may write (3.6) as

$$\frac{1}{\delta(\ell^r)} = \frac{1}{\ell^r} + O\left(\frac{1}{\ell^{2r}}\right). \tag{3.10}$$

Let n be an integer coprime to L, given by $n = \prod_{i=1}^{m} \ell_i^{\alpha_i}$, where $\alpha_i \in \mathbb{N}$. We then have,

$$\frac{1}{\delta(n)} = \prod_{i=1}^{m} \frac{1}{\ell_i^{\alpha_i}}\left(1 + O\left(\frac{1}{\ell_i^{\alpha_i}}\right)\right) = \frac{1}{n}\prod_{i=1}^{m}\left(1 + O\left(\frac{1}{\ell_i^{\alpha_i}}\right)\right) \leq \frac{1}{n}\exp\left(O\Big(\sum_{i=1}^{m}\frac{1}{\ell_i^{\alpha_i}}\Big)\right)$$

using the inequality $1 + x \leq \exp(x)$. Since $\alpha_i \geq 1$ for each i and

$$\sum_{i=1}^{m} \frac{1}{\ell_i^{\alpha_i}} \ll \sum_{\ell \leq n} \frac{1}{\ell} \ll \log\log n,$$

we obtain the desired bound. □

4. Comparison of (2.8) with the conjectured expression for $C_{E,t}$

In this section, we will compare the expression (2.8) for $C_{E,t}$ with that conjectured by Zywina in [30]. We first set up some notation and establish some essential lemmas.

For any integer m, let $R_m := \mathbb{Z}/m\mathbb{Z}$. Let d_1, d_2 be positive integers such that $(d_1, d_2) = 1$. Then by the Chinese remainder theorem we have the following isomorphism of rings

$$R_{d_1 d_2} \simeq R_{d_1} \times R_{d_2}.$$

Under the above isomorphism, the reduction modulo d_1 map from $R_{d_1 d_2}$ to R_{d_1} is given by the first projection

$$\begin{gathered} R_{d_1 d_2} \simeq R_{d_1} \times R_{d_2} \xrightarrow{\mathrm{pr}_1} R_{d_1} \\ x \longmapsto x \ (\mathrm{mod}\ d_1). \end{gathered}$$

This induces the isomorphism of groups

$$\mathrm{GL}_2(R_{d_1 d_2}) \simeq \mathrm{GL}_2(R_{d_1}) \times \mathrm{GL}_2(R_{d_2}).$$

Let I_m denote the identity matrix in $\mathrm{GL}_2(R_m)$. Under the above isomorphism, an element $A \in \mathrm{GL}_2(R_{d_1 d_2})$ can be represented as a tuple (A_1, A_2), where $A_1 \in \mathrm{GL}_2(R_{d_1})$ and $A_2 \in \mathrm{GL}_2(R_{d_2})$.

Recall that K_m is the finite field extension of $\mathbb{Q}$ obtained by adjoining the coordinates of the m-torsion points and $G(m)$ is the Galois group of the extension $K_m/\mathbb{Q}$, identified with a subset of $\mathrm{GL}_2(R_m)$. Consider the short exact sequence of groups

$$0 \to H \to G(d_1 d_2) \xrightarrow{f} G(d_1) \to 0, \tag{4.1}$$

where $f : G(d_1 d_2) \to G(d_1)$ is the natural surjection of Galois groups. Consider the subsets

$$G_{d_1}(d_1 d_2) := \{A \in G(d_1 d_2) | \det(I - A) \equiv 0 \pmod{d_1}\} \tag{4.2}$$

and

$$G_{d_1}(d_1) := \{A \in G(d_1) | \det(I - A) \equiv 0 \pmod{d_1}\}.$$

Then we have the following commutative diagram,

$$\begin{array}{ccccccccc}
 & & & & G_{d_1}(d_1 d_2) & \xrightarrow{f_{G_{d_1}(d_1 d_2)}} & G_{d_1}(d_1) & & \\
 & & & & \downarrow & & \downarrow & & \\
0 & \hookrightarrow & H & \longrightarrow & G(d_1 d_2) & \xrightarrow{f} & G(d_1) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow \rho_{d_1 d_2} & & \downarrow \rho_{d_1} & & \\
0 & \hookrightarrow & \mathrm{GL}_2(R_{d_2}) & \longrightarrow & \mathrm{GL}_2(R_{d_1 d_2}) & \xrightarrow[\mathrm{pr}_1]{} & \mathrm{GL}_2(R_{d_1}) & \longrightarrow & 0 \\
 & & & & \downarrow \wr & & & & \\
 & & & & \mathrm{GL}_2(R_{d_1}) \times \mathrm{GL}_2(R_{d_2}) & & & &
\end{array}$$

where we denote the restriction of f to $G_{d_1}(d_1 d_2)$ as $f_{G_{d_1}(d_1 d_2)}$.

Lemma 4.1. *The map*

$$f_{G_{d_1}(d_1 d_2)} : G_{d_1}(d_1 d_2) \to G_{d_1}(d_1)$$

is a surjection of sets.

Proof. Let $A_1 \in G_{d_1}(d_1) \hookrightarrow G(d_1)$. Since

$$f : G(d_1 d_2) \to G(d_1)$$

is a surjection, there exists $A \in G(d_1 d_2)$ such that $f(A) = A_1$. Since $A \in G(d_1 d_2) \hookrightarrow \mathrm{GL}_2(R_{d_1} d_2)$, A can be expressed as $A = (A_1, A_2)$, where $A_2 \in H$. Now A_1 satisfies

$$\det(I_{d_1} - A_1) \equiv 0 \pmod{d_1}.$$

But

$$\begin{aligned} \det(I_{d_1 d_2} - A) \pmod{d_1} &= \det(I_{d_1} - A_1) \pmod{d_1} \\ &\equiv 0 \pmod{d_1}. \end{aligned}$$

Hence $A = (A_1, A_2) \in G_{d_1}(d_1 d_2)$ and hence A is in the preimage of A_1 under $f_{G_{d_1}(d_1 d_2)}$. □

Lemma 4.2. *Let $A \in G_{d_1}(d_1 d_2)$ and let $B \in H$. Then $AB \in G_{d_1}(d_1 d_2)$.*

Proof. Let $A = (A_1, A_2) \in G_{d_1}(d_1 d_2)$, then it satisfies

$$\det(I_{d_1} - A_1) \equiv 0 \pmod{d_1}.$$

Let $B = (B_1, B_2) \in H \hookrightarrow G(d_1 d_2)$. Since $f(B) = I_{d_1} \in G(d_1)$, we have $B_1 = I_{d_1}$ and hence $B = (I_{d_1}, B_2)$. Now we have

$$AB = (A_1, A_2)(I_{d_1}, B_2) = (A_1, A_2 B_2)$$

which implies

$$\det(I_{d_1d_2} - AB) \pmod{d_1} = \det(I_{d_1} - A_1) \pmod{d_1} \equiv 0 \pmod{d_1}$$

since $A_1 \in G_{d_1}(d_1)$. Hence $AB \in G_{d_1}(d_1d_2)$ and we are done. □

Lemma 4.3. *For all $A_1 \in G_{d_1}(d_1)$, we have $f^{-1}_{G_{d_1}(d_1d_2)}(A_1) = AH$, where $A \in G_{d_1}(d_1d_2)$ is such that $f_{G_{d_1}(d_1d_2)}(A) = A_1$.*

Proof. Note that $f^{-1}_{G_{d_1}(d_1d_2)}(A_1) \subseteq AH$, since A lies in the preimage of A_1. For any $B \in H$, by Lemma 4.2 , $AB \in G_{d_1}(d_1d_2)$ and note that $f(AB) = A_1$, that is, AB is in the preimage of A_1. Hence $AH \subseteq f^{-1}_{G_{d_1}(d_1d_2)}(A_1)$. Therefore, $f^{-1}_{G_{d_1}(d_1d_2)}(A_1) = AH$ and we are done. □

Theorem 4.4. *For any d_1, d_2 satisfying $(d_1, d_2) = 1$, we have*

$$|G_{d_1}(d_1d_2)| = |G_{d_1}(d_1)||H|.$$

Proof. Let $n = |G_{d_1}(d_1)|$ and $G_{d_1}(d_1) = \{A_1, A_2, ..., A_n\}$. Consider

$$f_{G_{d_1}(d_1d_2)} : G_{d_1}(d_1d_2) \to G_{d_1}(d_1).$$

From Lemma 4.3, for any $A_i \in G_{d_1}(d_1)$, we have $f^{-1}_{G_{d_1}(d_1d_2)}(A_i) = AH$ for some $A \in G_{d_1}(d_1d_2)$. Since $f_{G_{d_1}(d_1d_2)}$ is a surjection, we have

$$G_{d_1}(d_1d_2) = \bigsqcup_{i=1}^{n} f^{-1}_{G_{d_1}(d_1d_2)}(A_i).$$

Therefore, we obtain

$$|G_{d_1}(d_1d_2)| = \sum_{i=1}^{n} \left|f^{-1}_{G_{d_1}(d_1d_2)}(A_i)\right| = |G_{d_1}(d_1)||H|.$$

□

Corollary 4.5. *For all d_1, d_2 such that $(d_1, d_2) = 1$, we obtain*

$$\frac{|G_{d_1}(d_1d_2)|}{|G(d_1d_2)|} = \frac{|G_{d_1}(d_1)|}{|G(d_1)|}.$$

Proof. From the short exact sequence (4.1), we get

$$|G(d_1d_2)| = |G(d_1)||H|.$$

By Theorem 4.4 , we have

$$|G_{d_1}(d_1d_2)| = |G_{d_1}(d_1)||H|.$$

Hence combining the above we obtain our result. □

4.1. The constant $C_{E,t}$.

The constant $C_{E,t}$ described by Zywina [30, Proposition 2.4] is given by

$$C_{E,t} = \frac{\delta_{E,t}\left(t \prod_{\ell | tL} \ell\right)}{\prod_{\ell | tL} (1 - 1/\ell)} \prod_{\ell \nmid tL} \left(1 - \frac{\ell^2 - \ell - 1}{(\ell - 1)^3(\ell + 1)}\right), \tag{4.3}$$

where

$$\delta_{E,t}(m) := \frac{|G(m) \cap \Psi_t(m)|}{|G(m)|}, \tag{4.4}$$

$$\Psi_t(m) := \{A \in \mathrm{Aut}(E[m]) \simeq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \mid \det(I - A) \in t(\mathbb{Z}/m\mathbb{Z})^*\}.$$

Let $m = t\text{rad}(tL)$. As discussed in Section 2.1 of [30], we have $N_p \equiv \det(I - \rho_m(\sigma_p)) \pmod m$. Moreover, $\delta_{E,t}$ is the natural density of primes for which N_p/t is an integer that is coprime to $\text{rad}(tL)$.

For a given divisor d of m, consider the set

$$G_{td}(m) = G(m) \cap \{A \in \text{Aut}(E[m]) \simeq \text{GL}_2(\mathbb{Z}/m\mathbb{Z}) \mid \det(I - A) \equiv 0 \pmod{td}\}. \tag{4.5}$$

Thus, for a prime $p \nmid N_E$, $N_p \equiv 0 \pmod{td}$ if and only if $\rho_m(\sigma_p) \subseteq G_{td}(m)$. By the Chebotarev density theorem, the natural density of the primes for which N_p/t is an integer divisible by d is thus $|G_{td}(m)|/|G(m)|$.

Since $\delta_{E,t}$ is the complement of the natural density of primes for which N_p/t is divisible by *some* non-trivial divisor d of m, we see that inclusion-exclusion gives us

$$\delta_{E,t} = 1 - \sum_{\substack{d|m \\ d>1}} \mu(d) \frac{|G_{td}(m)|}{|G(m)|} = \sum_{d|\text{rad}(tL)} \mu(d) \frac{|G_{td}(m)|}{|G(m)|}.$$

Now, for each divisor d of $\text{rad}(tL)$ consider the factorization $t = t_1t_2$, where where $\text{rad}(t_1) = (d, t)$ and $(t_2, d) = 1$. Then for the integer N_p/t, we have

$$\frac{N_p}{t} \equiv 0 \pmod d \iff \left(\frac{N_p}{t}\right) t_2 \equiv 0 \pmod d, \tag{4.6}$$

since $(t_2, d) = 1$. Since the latter congruence above occurs if and only if $\rho_m(\sigma_p) \subseteq G_{t_1d}(m)$, we may replace the density $|G_{td}(m)|/|G(m)|$ by $|G_{t_1d}(m)|/|G(m)|$. We thus obtain

$$\delta_{E,t}(m) = \sum_{d|\text{rad}(tL)} \mu(d) \frac{|G_{t_1d}(m)|}{|G(m)|}.$$

Writing $\text{rad}(tL) = dd'$, we see that $m = t_1t_2dd'$, where $(t_1d, t_2d') = 1$. Using Corollary 4.5 twice gives

$$\frac{|G_{t_1d}(m))|}{|G(m)|} = \frac{|G_{t_1d}(t_1d)|}{|G(t_1d)|} = \frac{|G_{t_1d}(td)|}{|G(td)|}.$$

Again, using (4.6), we may replace $|G_{t_1d}(td)|/|G(td)|$ by the density $|G_{td}(td)|/|G(td)|$, which is simply $1/\omega(td)$ (see (3.4)). This gives

$$\delta_{E,t}(t\text{rad}(tL)) = \sum_{d|\text{rad}(tL)} \frac{\mu(d)}{\omega(td)}, \tag{4.7}$$

so that the expression (2.8) does indeed agree with (4.3).

5. Preliminaries

In this section, we state some lemmas that will be useful to us later in the paper. Let $\nu(L)$ denote the number of distinct prime factors of L.

Lemma 5.1. *Let L be a fixed positive integer. As $x \to \infty$, we have*

$$\sum_{\substack{n \le x \\ rad(n)|L}} 1 \ll (2\log x)^{\nu(L)}.$$

Proof. Let $\mathrm{rad}(L) = p_1 p_2 ... p_k$. Then the required sum counts atmost the number of integers n of the form $p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ with $0 \le \alpha_i \le \frac{\log x}{\log p_i}$. Thus,

$$\sum_{\substack{n \le x \\ \mathrm{rad}(n) | L}} 1 \quad \le \quad \prod_{i=1}^{k} \left(1 + \frac{\log x}{\log p_i} \right) \ll \prod_{i=1}^{k} (2 \log x) \ll (2 \log x)^{\nu(L)}.$$

□

Lemma 5.2. *Let L be a fixed positive integer. We have*

$$\sum_{\substack{n \le x \\ rad(n) | L}} (\tau_3(n))^2 \ll (2 \log x)^{12\nu(L)}.$$

Proof. It is easy to see that $\tau_3(n) \ll (\tau(n))^3$. Hence,

$$\sum_{\substack{n \le x \\ \mathrm{rad}(n) | L}} (\tau_3(n))^2 \ll \sum_{\substack{n \le x \\ \mathrm{rad}(n) | L}} (\tau(n))^6 \ll \left(\sum_{\substack{n \le x \\ \mathrm{rad}(n) | L}} \tau(n) \right)^6. \tag{5.1}$$

Now,

$$\sum_{\substack{n \le x \\ \mathrm{rad}(n) | L}} \tau(n) = \sum_{\substack{n \le x \\ \mathrm{rad}(n) | L}} \sum_{d | n} 1 \quad = \quad \sum_{\substack{d \le x \\ \mathrm{rad}(d) | L}} \sum_{\substack{m \le x/d \\ \mathrm{rad}(m) | L}} 1$$
$$\ll \quad (2 \log x)^{2\nu(L)},$$

using Lemma 5.1. Putting this into (5.1) completes the proof. □

6. An elliptic analogue of the Elliott-Halberstam conjecture

In Section 3, we discussed the asymptotic (3.8) for $\pi_E(x, d, t)$ that follows from the Chebotarev density theorem. In the context of the Koblitz conjecture, we will need (3.8) with the error term controlled on *average* over moduli d in a certain range. This can be thought of as an elliptic analogue of the Elliott-Halberstam conjecture given in (2.4).

Conjecture EH$_{E,t}(x^\theta)$: Elliptic analogue of the Elliott-Halberstam Conjecture. *Let $L = L(E)$ be the fixed positive integer given by Serre's result (Theorem 3.3) and let t be a fixed positive integer. Define*

$$\Delta_E(y, d, t) := \pi_E(y, d, t) - \frac{\mathrm{Li}(y)}{\omega(d_1 t) \delta(d_2)}, \tag{6.1}$$

where $d = d_1 d_2$ is the unique factorization of d such that $rad(d_1) | tL$ and $(d_2, tL) = 1$. Then we have as $x \to \infty$,

$$\sum_{d \le x^\theta} \max_{y \le x} \left| \Delta_E(y, d, t) \right| \ll_A \frac{x}{(\log x)^A} \tag{6.2}$$

for any $A > 0$.

A pivotal step in the proof of our main result is the derivation of a variant of Conjecture $\mathrm{EH}_{E,t}(x^\theta)$. Assuming the elliptic analogue of the Elliott-Halberstam Conjecture given above, we derive an equidistribution result for primes p with $\frac{N_p}{t}$ in an arithmetic progression, satisfying the additional constraint that $\frac{N_p}{t}$ is squarefree. Towards this goal, we consider

$$\pi_E^*(x, d, t) := \# \left\{ p \le x : p \nmid dt N_E, \, \frac{N_p}{t} \equiv 0 \pmod{d}, \, \mu^2 \left(\frac{N_p}{t} \right) \ne 0 \right\}. \tag{6.3}$$

We obtain the following conditional result for $\pi_E^*(x,d,t)$, with the error term controlled on average in the range $d \le x^\theta$.

Theorem 6.1. *Assume that Conjecture 4 holds. Suppose that Conjecture* $\mathrm{EH}_{E,t}\left(x^\theta(\log x)^B\right)$ *is true for some fixed* $0<\theta<1$, *and a suitably large absolute constant* B. *Let* $L = L(E)$ *be the fixed positive integer given by Theorem 3.3. Let*

$$\Delta_{\mu^2}(y,d,E,t) = \pi_E^*(y,d,t) - \mathrm{Li}(y)\sum_{e=1}^{\infty}\frac{\mu(e)}{\omega(t[d_1,e_1^2])\delta([d_2,e_2^2])},$$

where $d = d_1d_2$ *is the unique factorization of* d *such that* $rad(d_1)|tL$, *and* $(d_2,tL)=1$. *Similarly for* $e = e_1e_2$. *Then, as* $x\to\infty$, *we have*

$$\sum_{d\le x^\theta}\mu^2(d)\max_{y\le x}\left|\Delta_{\mu^2}(y,d,E,t)\right| \ll_A \frac{x}{(\log x)^A}, \tag{6.4}$$

for any $A>0$.

The remainder of this section will be devoted towards completing the proof of Theorem 6.1.

Proof of Theorem 6.1. Recall the identity

$$\sum_{e^2|n}\mu(e) = \begin{cases}1, & \text{if } n \text{ is squarefree}\\ 0, & \text{otherwise.}\end{cases} \tag{6.5}$$

Using this we may write,

$$\pi_E^*(x,d,t) = \sum_{\substack{p\le x\\ p\nmid tdN_E\\ \frac{N_p}{t}\equiv 0 \ (\mathrm{mod}\ d)}}\mu^2\left(\frac{N_p}{t}\right) = \sum_{\substack{p\le x\\ p\nmid tdN_E\\ \frac{N_p}{t}\equiv 0 \ (\mathrm{mod}\ d)}}\ \sum_{e^2|\frac{N_p}{t}}\mu(e). \tag{6.6}$$

Let $z\le x$ be a function of x, to be chosen later. We write,

$$\pi_E^*(x,d,t) = \pi_E^*(x,d,t;z) + \widetilde{\pi}_E(x,d,t;z), \tag{6.7}$$

where,

$$\pi_E^*(x,d,t;z) = \sum_{\substack{p\le x\\ p\nmid tdN_E\\ \frac{N_p}{t}\equiv 0 \ (\mathrm{mod}\ d)}}\ \sum_{\substack{e^2|\frac{N_p}{t}\\ e\le z}}\mu(e) \tag{6.8}$$

and

$$\widetilde{\pi}_E(x,d,t;z) = \sum_{\substack{p\le x\\ p\nmid tdN_E\\ \frac{N_p}{t}\equiv 0 \ (\mathrm{mod}\ d)}}\ \sum_{\substack{e^2|\frac{N_p}{t}\\ e> z}}\mu(e). \tag{6.9}$$

We expect the tail sum $\widetilde{\pi}_E(x,d,t;z)$ to be negligible as $z\to\infty$. Indeed, we prove the following.

Proposition 6.2. *Suppose Conjecture 4 holds. Let* $z = (\log x)^B$, *where* B *is a sufficiently large absolute constant. Then for any* $A>0$,

$$\sum_{d\le x^\theta}\mu^2(d)\max_{y\le x}\left|\widetilde{\pi}_E(y,d,t;z)\right| \ll_A \frac{x}{(\log x)^A}.$$

Proof. We have

$$\begin{aligned}\widetilde{\pi}_E(y,d,t;z) &= \sum_{\substack{p\le y\\ p\nmid tdN_E\\ \frac{N_p}{t}\equiv 0 \ (\mathrm{mod}\ d)}} \sum_{\substack{e^2|\frac{N_p}{t}\\ e>z}} \mu(e)\\ &= \sum_{z<e\le\sqrt{y}+1} \mu(e) \sum_{\substack{p\le y\\ p\nmid tdN_E\\ N_p\equiv 0\ (\mathrm{mod}\ t([d,e^2]))}} 1,\end{aligned}$$

upon changing the order of summation and using the Hasse bound $|a_p|\le 2\sqrt{p}$. Hence,

$$\max_{y\le x}|\widetilde{\pi}_E(y,d,t;z)| \le \sum_{z<e\le\sqrt{x}+1} \sum_{\substack{p\le x\\ N_p\equiv 0\ (\mathrm{mod}\ t([d,e^2]))}} 1 \tag{6.10}$$

For the inner sum above, we will first run over possible values n of N_p and then bound the number of primes p for which $N_p=n$. Using Conjecture 4, we obtain

$$\begin{aligned}\sum_{\substack{p\le x\\ N_p\equiv 0\ (\mathrm{mod}\ t[d,e^2])}} 1 &\le \sum_{\substack{n\le x+2\sqrt{x}+1\\ n\equiv 0\ (\mathrm{mod}\ (t[d,e^2]))}} \sum_{p:N_p=n} 1\\ &= \sum_{\substack{n\le x+2\sqrt{x}+1\\ n\equiv 0\ (\mathrm{mod}\ (t[d,e^2]))}} M_E(n)\\ &\ll \frac{x(\log x)^C}{t[d,e^2]},\end{aligned} \tag{6.11}$$

for some $C>0$. We write $d=d'r, e=e'r$, where $r=(d,e)$. As d is squarefree, we have $[d,e^2]=d'e'^2r^2$. We then have

$$\begin{aligned}\sum_{d\le x^\theta}\mu^2(d)\sum_{z<e\le\sqrt{x}+1}\frac{x(\log x)^C}{t[d,e^2]} &\ll x(\log x)^C\sum_{r\le x^\theta}\frac{1}{tr^2}\sum_{d'\le x^\theta}\frac{1}{d'}\sum_{z/r<e'\le\sqrt{x}+1}\frac{1}{e'^2}\\ &\ll x(\log x)^C\sum_{r\le x^\theta}\sum_{d'\le x^\theta}\frac{1}{td'rz} \ll \frac{x(\log x)^{C_1}}{z},\end{aligned} \tag{6.12}$$

for some absolute constant $C_1=C_1(E)>0$. Combining (6.10), (6.11), (6.12) and choosing $z=(\log x)^{C_1+A}$, for A sufficiently large completes the proof. $\square$

Let us now turn to the sum $\pi^*(x,d,t;z)$, which is expected to contribute to the main term in (6.7). We will denote it as π_z^* for the remainder of the section. Upon interchanging the order of summation, we have

$$\pi_z^* := \sum_{\substack{p\le x\\ p\nmid tdN_E\\ \frac{N_p}{t}\equiv 0\ (\mathrm{mod}\ d)}} \sum_{\substack{e^2|\frac{N_p}{t}\\ e\le z}} \mu(e) = \sum_{e\le z}\mu(e) \sum_{\substack{p\le x\\ p\nmid tdN_E\\ \frac{N_p}{t}\equiv 0\ (\mathrm{mod}\ [d,e^2])}} 1.$$

Let us note that if $p\mid[d,e^2]$, then the inner sum is atmost

$$\sum_{\substack{p\le x\\ p|[d,e^2]\\ p\nmid d}} 1 \le \sum_{n|e^2}\Lambda(n) = \log(e^2).$$

Thus, the contribution of primes $p \mid [d, e^2]$ to π_z^* is of the order

$$\sum_{e \le z} \log(e^2) \ll z \log(z^2). \tag{6.13}$$

recall that we chose $z = (\log x)^B$ with B sufficiently large in Proposition 6.2. The contribution (6.13) is hence negligible and we may assume $p \nmid [d, e^2]$ henceforth. In other words, as $x \to \infty$,

$$\begin{aligned} \pi_z^* \quad &\sim \quad \sum_{e \le z} \mu(e) \sum_{\substack{p \le x \\ p \nmid t[d,e^2]N_E \\ \frac{N_p}{t} \equiv 0 \ (\mathrm{mod}\ [d,e^2])}} 1 \\ &= \quad \sum_{e \le z} \mu(e) \pi_E(x, [d, e^2], t), \end{aligned}$$

where $\pi_E(x, [d, e^2], t)$ is as defined in (3.7). Let $[d, e^2] = [d, e^2]_1 [d, e^2]_2$ be the unique factorization of $[d, e^2]_2$ with $\mathrm{rad}([d, e^2]_1) | tL$, and $[d, e^2]_2$ coprime to tL. It is easy to see that $[d, e^2]_i = [d_i, e_i^2]$, for $i = 1, 2$, where $d = d_1 d_2$, $\mathrm{rad}(d_1) | tL, (d_2, L) = 1$, and similarly for $e = e_1 e_2$. Therefore, applying (6.1) we have

$$\begin{aligned} \pi_z^* &\sim \sum_{e \le z} \mu(e) \frac{\mathrm{Li}(x)}{\omega(t[d, e^2]_1)\delta([d, e^2]_2)} + O\Bigg(\sum_{e \le z} \mu^2(e) \left| \Delta_E(x, [d, e^2], t) \right| \Bigg) \\ &= M(x, d, t; z) + E(x, d, t; z) \qquad \text{(say)}. \end{aligned} \tag{6.14}$$

We now proceed towards simplifying the main term $M(x, d, t; z)$ in (6.14). A natural step is to get rid of the dependence on z. Let us write,

$$\begin{aligned} M(x, d, t; z) &= \mathrm{Li}(x) \sum_{e=1}^{\infty} \frac{\mu(e)}{\omega(t[d_1, e_1^2])\delta([d_2, e_2^2])} - \mathrm{Li}(x) \sum_{e > z} \frac{\mu(e)}{\omega(t[d_1, e_1^2])\delta([d_2, e_2^2])} \\ &= M(x, d, t) - \widetilde{M}(x, d, t; z) \qquad \text{(say)}. \end{aligned} \tag{6.15}$$

As our next step, we show that the tail sum $\widetilde{M}$ above is negligible *on average* over d, as $z \to \infty$.

Proposition 6.3. *Let $z = (\log x)^B$, where $B > 0$ is a sufficiently large constant. Then for any $A > 0$,*

$$\sum_{d \le x^\theta} \mu^2(d) \max_{y \le x} \left| \widetilde{M}(y, d, t; z) \right| \ll_A \frac{x}{(\log x)^A}.$$

Proof. We have from (6.15),

$$\sum_{d \le x^\theta} \mu^2(d) \max_{y \le x} |\widetilde{M}| \ll \mathrm{Li}(x) \sum_{d \le x^\theta} \mu^2(d) \sum_{e > z} \frac{\mu^2(e)}{\delta([d_2, e_2^2])},$$

since $\omega(n) \ge 1$ for all $n \in \mathbb{N}$. As $e = e_1 e_2$ is squarefree with $\mathrm{rad}(e_1) | tL$, in the above sum over e, we have $e_2 > \frac{e}{tL} > \frac{z}{tL}$ and e_1 ranging over divisors of tL. Hence,

$$\begin{aligned} \sum_{d \le x^\theta} \mu^2(d) \max_{y \le x} |\widetilde{M}| \quad &\ll \quad \mathrm{Li}(x)\tau(tL) \sum_{d \le x^\theta} \mu^2(d) \sum_{e_2 > \frac{z}{tL}} \frac{1}{\delta([d_2, e_2^2])} \\ &\ll \quad \mathrm{Li}(x)\tau(tL) \sum_{d_1 | tL} 1 \sum_{d_2 \le x^\theta} \mu^2(d_2) \sum_{e_2 > \frac{z}{tL}} \frac{(\log[d_2, e_2^2])^D}{[d_2, e_2^2]}, \end{aligned}$$

using the factorization $d = d_1 d_2$ and applying Lemma 3.4. Writing $d_2 = d_2' r, e_2 = e_2' r$, where $r = (d_2, e_2)$, we have $[d_2, e_2^2] = d_2'^2 e_2'^2 r^2$. This gives

$$\sum_{d \le x^\theta} \max_{y \le x} |\widetilde{M}| \ll \mathrm{Li}(x)(\tau(tL))^2 \sum_{r \le x^\theta} \sum_{d_2' \le x^\theta} \sum_{e_2' > \frac{z}{tLr}} \frac{\log(d_2'^2 e_2'^2 r^2)}{d_2'^2 e_2'^2 r^2}.$$

As done in the proof of Proposition 6.2, one can show that the inner triple sum over r, d_2' and e_2' is $\ll_{t,L} \frac{(\log x)^C}{z}$ for some absolute constant $C > 0$. Choosing $z = (\log x)^{A+C}$ for A sufficiently large completes the proof. □

Coming back to (6.14), we now show that if we assume $\mathrm{EH}_{E,t}(x^\theta)$ for some $0 < \theta < 1$, then the error term $E(x, d, t; z)$ can be controlled on average in almost the same range of d, conditional upon Conjecture 4.

Proposition 6.4. *Let $z = (\log x)^B$, where $B > 0$ is a sufficiently large constant. Suppose Conjecture 4 and Conjecture $\mathrm{EH}_{E,t}(x^\theta z^2)$ hold. Then for any $A > 0$, we have*

$$\sum_{d \le x^\theta} \mu^2(d) \max_{y \le x} \big|E(y, d, t; z)\big| \ll \frac{x}{(\log x)^A}.$$

Proof. We will denote $E(y, d, t; z)$ as $E(y)$ in this proof. Put $r = [d, e^2]$. It can be shown that the number of d and e such that $[d, e^2] = r$ is atmost $\tau_3(r)$. From the definition of $E(y)$ in (6.14) we get

$$\sum_{d \le x^\theta} \mu^2(d) \max_{y \le x} \big|E(y)\big| \quad \ll \quad \sum_{r \le x^\theta z^2} \tau_3(r) \max_{y \le x} |\Delta_E(y, r, t)|.$$

Now using the Cauchy- Schwarz inequality we have,

$$\sum_{d \le x^\theta} \mu^2(d) \max_{y \le x} |E(y)| \ll \left(\sum_{r \le x^\theta z^2} (\tau_3(r))^2 \max_{y \le x} |\Delta_E(y, r, t)| \right)^{\frac{1}{2}} \left(\sum_{r \le x^\theta z^2} \max_{y \le x} |\Delta_E(y, r, t)| \right)^{\frac{1}{2}} \tag{6.16}$$

The hypothesis $\mathrm{EH}_{E,t}(x^\theta z^2)$ yields that the second term on the right hand side of (6.16) is

$$\ll_A \left(\frac{x}{(\log x)^A} \right)^{1/2},$$

for any $A > 0$. Thus, in order to complete the proof, it suffices to show that the first term on the right hand side of (6.16) is of the order

$$(x(\log x)^C)^{1/2} \tag{6.17}$$

for some absolute constant $C > 0$. Let us observe that by definition (6.1),

$$\max_{y \le x} \big|\Delta_E(y, r, t)\big| \le \Bigg| \sum_{\substack{p \le x,\, p \nmid trN_E \\ N_p \equiv 0 \ (\mathrm{mod}\ tr)}} 1 \Bigg| + \left| \frac{\mathrm{Li}(x)}{\omega(tr_1)\delta(r_2)} \right|.$$

We estimate the contribution of the final term above to (6.16) as follows. Upon using Lemma 3.4 followed by Lemma 5.2, we have

$$\begin{aligned} \mathrm{Li}(x) \sum_{r \le x^\theta z^2} \frac{(\tau_3(r))^2}{\omega(tr_1)\delta(r_2)} \quad &\ll \quad \mathrm{Li}(x) \sum_{\substack{r_1 \le x^\theta \\ \mathrm{rad}(r_1) | tL}} (\tau_3(r_1))^2 \sum_{r_2 \le x^\theta z^2} \frac{(\tau_3(r_2))^2 (\log r_2)^D}{r_2} \\ &\ll \quad \mathrm{Li}(x)(2\log x)^{12\nu(L)}(\log x)^C, \end{aligned}$$

for some absolute constant $C > 0$. Hence in order to show (6.17), we are left to estimate the sum

$$\sum_{r \le x^\theta z^2} (\tau_3(r))^2 \left| \sum_{\substack{p \le x,\, p \nmid trN_E \\ N_p \equiv 0 \pmod{tr}}} 1 \right|.$$

On running over values n of N_p and then over primes p such that $N_p = n$, Conjecture 4 yields that the above sum is

$$\begin{aligned} \le \sum_{r \le x^\theta z^2} (\tau_3(r))^2 \sum_{\substack{n \le x+2\sqrt{x}+1, \\ n \equiv 0 \pmod{tr}}} M_E(n) &\ll x(\log x)^C \sum_{r \le x^\theta z^2} \frac{(\tau_3(r))^2}{tr} \\ &\ll x(\log x)^{C_1} \end{aligned}$$

for some absolute constant $C_1 = C_1(E) > 0$. This gives (6.17) and thus completes the proof. □

We are now ready to obtain Theorem 6.1 as follows. From equations (6.7), (6.14) and (6.15), it is clear that

$$\pi_E^*(x,d,t) \sim M(x,d,t) - \widetilde{M}(x,d,t;z) + E(x,d,t;z) + \widetilde{\pi}(x,d,t;z).$$

Then

$$\begin{aligned} \Delta_{\mu^2}(y,d,E,t) &= \pi_E^*(y,d,t) - M(y,d,t) \\ &= \widetilde{\pi}(y,d,t;z) + E(y,d,t;z) - \widetilde{M}(y,d,t;z). \end{aligned} \tag{6.18}$$

Applying Propositions 6.2, 6.3, and 6.4 to (6.18), we obtain Theorem 6.1.

7. Preliminary computations for the Koblitz constant

The following special case of the Wiener-Ikehara Tauberian theorem due to D. J. Newman [20] will be instrumental in our calculations for the constant $C_{E,t}$.

Theorem 7.1 (Newman)**.** *Let $|a_n| \le 1$. We consider the series*

$$F(s) := \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

which is absolutely convergent for $\mathrm{Re}(s) > 1$. If $F(s)$ can be analytically continued to $\mathrm{Re}(s) \ge 1$, then the series $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ converges for $\mathrm{Re}(s) \ge 1$. Moreover, for $\mathrm{Re}(s) \ge 1$, we have $\sum_{n=1}^{\infty} \frac{a_n}{n^s} = F(s)$.

We prove the following preliminary lemmas.

Lemma 7.2. *Let L be any fixed positive integer. Let $\delta(\ell)$ be as given in* (3.5) *for primes $\ell \nmid L$. Then as $x \to \infty$, we have*

$$\sum_{d \le x, (d,L)=1} \frac{\mu(d)}{\delta(d)} \ll e^{-c\sqrt{\log x}} \tag{7.1}$$

for some $c > 0$.

Proof. Let $s = \sigma + it$, $\sigma > 0$. Consider the series

$$f(s) := \sum_{\substack{d=1 \\ (d,L)=1}}^{\infty} \frac{\mu(d)}{\delta(d) d^s}. \tag{7.2}$$

Using Lemma 3.4 we see $f(s)$ is absolutely convergent for $\mathrm{Re}(s) > 0$. Using (3.5), we have the following Euler product for $f(s)$ in this region:

$$f(s) = \prod_{\ell \nmid L} \left(1 - \frac{(\ell^2 - 2)}{(\ell - 1)(\ell^2 - 1)\ell^s}\right).$$

Multiplying and dividing by the factor $\prod_{\ell}\left(1-\frac{1}{\ell^{s+1}}\right)$, we write

$$f(s)=\zeta(s+1)^{-1}G(s), \tag{7.3}$$

where $\zeta(s)$ is the Riemann-zeta function and

$$G(s)=\prod_{\ell|L}\left(1-\frac{1}{\ell^{s+1}}\right)^{-1}\prod_{\ell\nmid L}\left(1-\frac{1}{\ell^{s+1}}\right)^{-1}\left(1-\frac{(\ell^2-2)}{(\ell-1)(\ell^2-1)\ell^s}\right).$$

Writing the denominator of the last term in parentheses as $\ell^s(\ell^2-2)\ell(1-x_\ell)$, where

$$x_\ell=\frac{\ell^2-\ell-1}{\ell(\ell^2-2)},$$

we have

$$G(s)=\prod_{\ell|L}\left(1-\frac{1}{\ell^{s+1}}\right)^{-1}\prod_{\ell\nmid L}\left(1-\frac{1}{\ell^{s+1}}\right)^{-1}\left(1-\frac{1}{\ell^{s+1}(1-x_\ell)}\right). \tag{7.4}$$

Since $x_\ell=O(\frac{1}{\ell})$, we have

$$\begin{aligned}G(s) &= \prod_{\ell|L}\left(1-\frac{1}{\ell^{s+1}}\right)^{-1}\prod_{\ell\nmid L}\left(1-\frac{1}{\ell^{s+1}}\right)^{-1}\left(1-\frac{1}{\ell^{s+1}}+\frac{O(1/\ell)}{\ell^{s+1}}\right)\\ &= \prod_{\ell|L}\left(1-\frac{1}{\ell^{s+1}}\right)^{-1}\prod_{\ell\nmid L}\left(1+\frac{O(1/\ell)}{\ell^{s+1}}\left(1-\frac{1}{\ell^{s+1}}\right)^{-1}\right)\\ &= \prod_{\ell|L}\left(1-\frac{1}{\ell^{s+1}}\right)^{-1}\prod_{\ell\nmid L}\left(1+O\left(\frac{1}{\ell^{s+2}}\right)+O\left(\frac{1}{\ell^{2s+3}}\right)\right).\end{aligned}$$

Thus, we see that $G(s)$ is absolutely convergent for $\mathrm{Re}(s)>-1$.

We now apply a quantitative version of Perron's formula (cf. [10, Section 3], [29, Lemma 3.12]) to get

$$\sum_{\substack{d\le x\\(d,L)=1}}\frac{\mu(d)}{\delta(d)}=\frac{1}{2\pi i}\int_{b-iT}^{b+iT}\frac{G(s)}{\zeta(s+1)}\frac{x^s}{s}ds+O\left(\frac{(\log x)^2}{T}\right), \tag{7.5}$$

with $b=\frac{1}{\log x}$. Let us denote $\mathrm{Re}(s)$ by σ. Since we have the zero-free region (cf. [29, Theorem 3.8])

$$\sigma\ge 1-\frac{c_0}{\log(|t|+2)},\qquad t\in\mathbb{R},$$

for some $c_0>0$, we can shift the above integral to the left, to the path $[\gamma-iT,\gamma+iT]$, where $\gamma=\gamma(t)=-\frac{c_0}{\log(|t|+2)}$. This gives

$$\sum_{\substack{d\le x\\(d,L)=1}}\frac{\mu(d)}{\delta(d)}=\frac{1}{2\pi i}\left(\int_{b-iT}^{\gamma-iT}+\int_{\gamma-iT}^{\gamma+iT}+\int_{\gamma+iT}^{b+iT}\right)+O\left(\frac{(\log x)^2}{T}\right), \tag{7.6}$$

where the integrands are the same as in (7.5). We will obtain the required bound by estimating each of the above integrals and choosing T suitably in terms of x.

We first estimate the upper horizontal integral. Using the bounds (cf. [29, (3.11.8)])

$$G(s)\ll 1,\qquad \zeta(s)^{-1}\ll\log(|t|+2)$$

in the region $\sigma \geq 1 - \frac{c_0}{\log(|t|+2)}$, we have

$$\int_{\gamma+iT}^{b+iT} \frac{G(s)}{\zeta(s+1)} \frac{x^s}{s} ds \ll \frac{\log(T+2)}{T} \int_{\gamma}^{b} x^{\sigma} \, d\sigma \ll \frac{\log(T+2)}{T} x^{\frac{1}{\log x}} (\log x)$$
$$\ll \frac{\log(T+2)}{T} \log x. \tag{7.7}$$

The lower horizontal can be bounded in exactly the same way. Finally, we have

$$\int_{\gamma-iT}^{\gamma+iT} \frac{G(s)}{\zeta(s+1)} \frac{x^s}{s} ds \quad \ll \quad \int_0^T x^{-\frac{c_0}{\log(t+2)}} \log(t+2) \frac{dt}{\sqrt{\gamma^2+t^2}}.$$

Choosing T_1 such that $\log(T_1+2) = \frac{\sqrt{c_0 \log x}}{2}$, we split the above integral as $\int_0^{T_1} + \int_{T_1}^{T}$, to obtain

$$\int_{\gamma-iT}^{\gamma+iT} \frac{G(s)}{\zeta(s+1)} \frac{x^s}{s} ds \ll \int_0^{T_1} x^{-\frac{c_0}{\log(t+2)}} \log(t+2) \, dt + \int_{T_1}^{T} x^{-\frac{c_0}{\log(t+2)}} \log(t+2) \frac{dt}{t}$$
$$\ll e^{-2\sqrt{c_0 \log x}} \sqrt{\log x} \int_0^{T_1} dt + e^{-\frac{c_0 \log x}{\log(T+2)}} (\log T)^2$$
$$\ll e^{-c_1\sqrt{\log x}} + e^{-\frac{c_2 \log x}{\log T}}, \tag{7.8}$$

for some constants $c_1, c_2 > 0$. Choosing $\log T = \sqrt{\log x}$ and putting together (7.6), (7.7) and (7.8), we have obtained

$$\sum_{\substack{d \leq x \\ (d,L)=1}} \frac{\mu(d)}{\delta(d)} \ll e^{-c\sqrt{\log x}}$$

for some $c > 0$, as needed. □

Lemma 7.3. *Let $L = L(E)$ be as given in the statement of Theorem* 3.3 *and δ be as in* (3.5). *Let*

$$F(s) = \sum_{(d,L)=1} \frac{\mu(d)}{\delta(d) d^s} g(d),$$

where $g(d)$ is a multiplicative function of d, satisfying $g(\ell) = 1 + O\left(\frac{1}{\ell}\right)$ on primes ℓ dividing d, with an absolute implied constant. Then $F(s)$ is absolutely convergent for $\mathrm{Re}(s) > 0$ *and can be analytically continued to* $\mathrm{Re}(s) = 0$. *Moreover,*

$$\sum_{(d,L)=1} \frac{\mu(d)}{\delta(d)} g(d) \log(1/d) = \prod_{\ell \mid L} \left(1 - \frac{1}{\ell}\right)^{-1} \prod_{\ell \nmid L} \left(1 - \frac{1}{\ell}\right)^{-1} \left(1 - \frac{g(\ell)}{\delta(\ell)}\right).$$

Proof. From Lemma 3.4, $F(s)$ is clearly absolutely convergent for $\mathrm{Re}(s) > 0$. In this region, we have the Euler product

$$F(s) \quad = \quad \prod_{\ell \nmid L} \left(1 - \frac{(\ell^2-2)g(\ell)}{(\ell-1)(\ell^2-1)\ell^s}\right) = \prod_{\ell \nmid L} \left(1 - \frac{1 + O\left(\frac{1}{\ell}\right)}{\ell^{s+1}(1-x_\ell)}\right)$$

where

$$x_\ell = \frac{\ell^2 - \ell - 1}{\ell(\ell^2-2)},$$

as done in (7.4). As done in the proof of Lemma 7.2, we may write

$$F(s) = \zeta(s+1)^{-1} H(s), \tag{7.9}$$

where

$$H(s) = \prod_{\ell | L} \left(1 - \frac{1}{\ell^{s+1}}\right)^{-1} \prod_{\ell \nmid L} \left(1 - \frac{1}{\ell^{s+1}}\right)^{-1} \left(1 - \frac{(\ell^2 - 2) g(\ell)}{(\ell - 1)(\ell^2 - 1)\ell^s}\right) \tag{7.10}$$

can be simplified to

$$H(s) = \prod_{\ell | L} \left(1 - \frac{1}{\ell^{s+1}}\right)^{-1} \prod_{\ell \nmid L} \left(1 + O\left(\frac{1}{\ell^{s+2}}\right)\right).$$

Thus, $H(s)$ is absolutely convergent for $\mathrm{Re}(s) > -1$. From the expression (7.9), we see that $F(s)$ can be analytically continued to $\mathrm{Re}(s) \geq 0$.

In particular, (7.9) gives us

$$F'(s) = -\frac{\zeta'(s+1)}{\zeta(s+1)} \frac{1}{\zeta(s+1)} H(s) + \zeta(s+1)^{-1} H'(s),$$

in the region $\mathrm{Re}(s) \geq 0$. As $\zeta(s)$ and $-\frac{\zeta'}{\zeta}(s)$ have simple poles at $s = 1$ with residue 1, we find that

$$F'(0) = H(0) = \prod_{\ell | L} \left(1 - \frac{1}{\ell}\right)^{-1} \prod_{\ell \nmid L} \left(1 - \frac{1}{\ell}\right)^{-1} \left(1 - \frac{(\ell^2 - 2) g(\ell)}{(\ell - 1)(\ell^2 - 1)}\right), \tag{7.11}$$

from (7.10). Using Theorem 7.1 of Newman, we see that the series representation

$$F'(s) = \sum_{(d,L)=1} \frac{\mu(d)}{\delta(d) d^s} g(d) \log(1/d) \tag{7.12}$$

for $\mathrm{Re}(s) > 0$ must also hold for $\mathrm{Re}(s) \geq 0$, and the expressions (7.11) and (7.12) agree at $s = 0$. □

Lemma 7.4. *Let t, L be fixed positive integers and ω be any arithmetical function. Then we have*

$$\sum_{d|L,\, e|L} \frac{\mu(d)\mu(e)}{\omega(t[d, e^2])} = \sum_{d|L} \frac{\mu(d)}{\omega(td)}. \tag{7.13}$$

Proof. Since d and e are squarefree, we have $[d, e^2] = d'e^2$, where $d' = d/r$ and $r = (d, e)$. Note that d' is coprime to r and e. If we fix divisors d' and e of L, with $(d', e) = 1$, then r can range over any divisor of e. Each such choice of r yields a unique d, given by $d = d'r$. The sum in question is thus given by

$$\sum_{e|L} \sum_{d|L} \frac{\mu(d)\mu(e)}{\omega(t[d, e^2])} = \sum_{e|L} \sum_{\substack{d'|L \\ (d',e)=1}} \frac{\mu(e)\mu(d')}{\omega(td'e^2)} \sum_{r|e} \mu(r).$$

The innermost sum is supported only on $e = 1$ by the fundamental property of the Möbius function, thus completing the proof. □

We will now use the above lemmas to complete our computation of the refined Koblitz constant from certain sums involving the functions δ and ω given in (3.4). These sums will come up in a natural way in subsections 8.1 and 8.2, and play an important role in the proof of Theorem 2.2.

Lemma 7.5. *Let t be a fixed positive integer. Let $L = L(E)$ be the integer appearing in Theorem 3.3. We have*

$$\sum_{(d,tL)=1} \sum_{(e,tL)=1} \frac{\mu(d)\mu(e) \log\left(\frac{1}{d}\right)}{\delta([d, e^2])} = \prod_{\ell | tL} \left(1 - \frac{1}{\ell}\right)^{-1} \prod_{\ell \nmid tL} \left(1 - \frac{\ell^2 - \ell - 1}{(\ell - 1)^3(\ell + 1)}\right). \tag{7.14}$$

Proof. We use the identity $f([m,n])f((m,n)) = f(m)f(n)$, which holds for any multiplicative function f and $m, n \in \mathbb{N}$ (cf. Selberg [23]). Then the innermost sum above can be written as

$$\sum_{(e,tL)=1} \frac{\mu(e)\delta((d,e))}{\delta(e^2)\delta(d)}.$$

The double sum over d and e in (7.14) is thus given by

$$\sum_{(d,tL)=1} \frac{\mu(d)\log(1/d)}{\delta(d)} h(d), \tag{7.15}$$

where

$$h(d) = \sum_{(e,tL)=1} \frac{\mu(e)\delta((d,e))}{\delta(e^2)}.$$

We write

$$h(d) = \prod_{\substack{p\nmid tL \\ p\nmid d}} \left(1 - \frac{1}{\delta(p^2)}\right) \prod_{\substack{p\nmid tL \\ p\mid d}} \left(1 - \frac{\delta(p)}{\delta(p^2)}\right) = \prod_{p\nmid tL} \left(1 - \frac{1}{\delta(p^2)}\right) g(d), \tag{7.16}$$

where $g(d)$ is a multiplicative function of d, given on primes $\ell | d$ by

$$g(\ell) = \left(1 - \frac{\delta(\ell)}{\delta(\ell^2)}\right)\left(1 - \frac{1}{\delta(\ell^2)}\right)^{-1}. \tag{7.17}$$

Observe that g satisfies the hypothesis of Lemma 7.3 by invoking (3.5). Applying Lemma 7.3, and using (7.16), we see that the sum (7.15) simplifies to

$$\prod_{\ell | tL} \left(1 - \frac{1}{\ell}\right)^{-1} \prod_{\ell\nmid tL} \left(1 - \frac{1}{\ell}\right)^{-1} \left(1 - \frac{1}{\delta(\ell^2)}\right)\left(1 - \frac{g(\ell)}{\delta(\ell)}\right).$$

Simplifying the above product using (7.17) and the expression (3.6) for δ, we see that (7.15) is given by

$$\prod_{\ell | tL} \left(1 - \frac{1}{\ell}\right)^{-1} \prod_{\ell\nmid tL} \left(1 - \frac{\ell^2 - \ell - 1}{(\ell-1)^3(\ell+1)}\right)$$

as needed. □

Lemma 7.6. *Let t be a fixed positive integer. Let $L = L(E)$ be the integer appearing in Theorem* 3.3. *We have*

$$\sum_{\substack{d_1 | tL \\ e_1 | tL}} \frac{\mu(d_1)\mu(e_1)}{\omega(t[d_1, e_1^2])} \sum_{\substack{(d_2,tL)=1 \\ (e_2,tL)=1}} \frac{\mu(d_2)\mu(e_2)\log(1/d_2)}{\delta([d_2, e_2^2])} = C_{E,t},$$

where the constant $C_{E,t}$ is as given by (2.8).

Proof. Using Lemma 7.4, we see that the sum over d_1, e_1 reduces to

$$\sum_{r | tL} \frac{\mu(r)}{\omega(tr)}. \tag{7.18}$$

Using Lemma 7.5 for the sum over d_2, e_2, we obtain the required expression for our sum. □

We also have the following expression for $C_{E,t}$ in terms of another sum.

Lemma 7.7. *Let t be a fixed positive integer. Let $L = L(E)$ be the integer appearing in Theorem 3.3. We have*

$$\sum_{e_1|tL}\frac{\mu(e_1)}{\omega(te_1)}\sum_{(e_2,tL)=1}\frac{\mu(e_2)\log(1/e_2)}{\delta(e_2)} = C_{E,t},$$

where $C_{E,t}$ is as defined in (2.8).

Proof. It is enough to show that

$$\sum_{(e,tL)=1}\frac{\mu(e)\log(1/e)}{\delta(e)} = \prod_{\ell|tL}\left(1-\frac{1}{\ell}\right)^{-1}\prod_{\ell\nmid tL}\left(1-\frac{\ell^2-\ell-1}{(\ell-1)^3(\ell+1)}\right). \tag{7.19}$$

For the sum on the left hand side, we are in a position to apply Lemma 7.3 with $g \equiv 1$. This gives

$$\sum_{(e,tL)=1}\frac{\mu(e)\log(1/e)}{\delta(e)} = \prod_{\ell|tL}\left(1-\frac{1}{\ell}\right)^{-1}\prod_{\ell\nmid tL}\left(1-\frac{1}{\ell}\right)^{-1}\left(1-\frac{1}{\delta(\ell)}\right),$$

which upon simplification using (3.5), yields (7.19). □

8. Decomposition of Λ

Let t be a fixed positive integer. In this section, we want to estimate the number of primes $p \le x$ with $p \nmid N_E$, such that $\frac{N_p}{t}$ is a prime. Consider the sum

$$S_{E,t}(x) := \sum_{\substack{p\le x\\ p\nmid N_E\\ N_p\equiv 0 \pmod t}} \mu^2\left(\frac{N_p}{t}\right)\Lambda\left(\frac{N_p}{t}\right). \tag{8.1}$$

Note that $N_p \le x + 2\sqrt{x} + 1$ by the Hasse bound. We find that

$$\Lambda\left(\frac{N_p}{t}\right) = \mu^2\left(\frac{N_p}{t}\right)\Lambda\left(\frac{N_p}{t}\right),$$

except when $\frac{N_p}{t}$ is a prime power. However on considering the sum

$$\sum_{\substack{p\le x,\alpha\ge 2,\\ \frac{N_p}{t}=q^\alpha\\ q \text{ prime}}}\Lambda\left(\frac{N_p}{t}\right) \le \sum_{\substack{n\le x+2\sqrt{x}+1,\\ \alpha\ge 2,\frac{n}{t}=q^\alpha}} M_E(n)\Lambda\left(\frac{n}{t}\right) \le \sum_{\substack{n\le x^{\frac{2}{3}},\\ \alpha\ge 2,\frac{n}{t}=q^\alpha}} M_E(n)\Lambda\left(\frac{n}{t}\right) + \sum_{\substack{x^{\frac{2}{3}}<n\le(\sqrt{x}+1)^2,\\ \alpha\ge 2,\frac{n}{t}=q^\alpha}} M_E(n)\Lambda\left(\frac{n}{t}\right),$$

by (2.7), we have

$$\sum_{\substack{n\le x^{\frac{2}{3}},\\ \alpha\ge 2,\frac{n}{t}=q^\alpha}} M_E(n)\Lambda\left(\frac{n}{t}\right) = O(x^{\frac{2}{3}}).$$

We now observe there must exist a power of q, say q^{β_q} with $\beta_q \ge 2$, such that $q^{\beta_q} \mid n$ and $q^{\beta_q} \ge x^{\frac{2}{3}}/t$ for all $x^{\frac{2}{3}} < n \le x + 2\sqrt{x} + 1$ which are of the form tq^α with $\alpha \ge 2$. This shows that

$$\sum_{\substack{x^{\frac{2}{3}}<n\le(\sqrt{x}+1)^2,\\ \alpha\ge 2,\frac{n}{t}=q^\alpha}} M_E(n)\Lambda\left(\frac{n}{t}\right) \le \sum_{q\le\sqrt{x}+1}\sum_{\substack{x^{\frac{2}{3}}<n\le(\sqrt{x}+1)^2,\\ q^{\beta_q}|n}} M_E(n)\Lambda\left(\frac{n}{t}\right).$$

By Conjecture 4, it follows that

$$\sum_{q\le\sqrt{x}+1}\ \sum_{\substack{x^{\frac{2}{3}}<n\le(\sqrt{x}+1)^2,\\ q^{\beta_q}\mid n}} M_E(n)\Lambda\left(\frac{n}{t}\right)=O\left(\log x\sum_{\substack{q\le\sqrt{x}+1,\\ q^{\beta_q}>\frac{x^{\frac{2}{3}}}{t}}}\frac{x(\log x)^C}{q^{\beta_q}}\right)=O_t(x^{\frac{5}{6}}(\log x)^C),$$

for some $C>0$. This yields

$$\sum_{\substack{p\le x\\ p\nmid N_E\\ N_p\equiv 0 \pmod t}}\Lambda\left(\frac{N_p}{t}\right)=\sum_{\substack{p\le x\\ p\nmid N_E\\ N_p\equiv 0 \pmod t}}\mu^2\left(\frac{N_p}{t}\right)\Lambda\left(\frac{N_p}{t}\right)+O_t(x^{\frac{5}{6}}(\log x)^C).$$

Thus it is enough to work with the sum (8.1).
Recall (cf. Ex 1.1.6, [16]) that

$$\Lambda(n)=\sum_{d\mid n}\mu(d)\log(1/d).$$

For some fixed $y>0$, we may write $\Lambda(n)=\Lambda_y(n)+\widetilde{\Lambda}_y(n)$, where

$$\Lambda_y(n):=\sum_{d\mid n,d\le y}\mu(d)\log(1/d),\qquad \widetilde{\Lambda}_y(n):=\sum_{d\mid n,d>y}\mu(d)\log(1/d).$$

Applying this decomposition of Λ we break the sum $S_{E,t}(x)$ into two sub-sums $S_{1,t}(y)$ and $S_{2,t}(y)$, where

$$S_{1,t}(y):=\sum_{\substack{p\le x\\ p\nmid N_E\\ N_p\equiv 0 \pmod t}}\mu^2\left(\frac{N_p}{t}\right)\sum_{\substack{d\mid\frac{N_p}{t}\\ d\le y}}\mu(d)\log(1/d), \tag{8.2}$$

and

$$S_{2,t}(y):=\sum_{\substack{p\le x\\ p\nmid N_E\\ N_p\equiv 0 \pmod t}}\mu^2\left(\frac{N_p}{t}\right)\sum_{\substack{d\mid\frac{N_p}{t}\\ d>y}}\mu(d)\log(1/d). \tag{8.3}$$

We treat the two sums above separately. Henceforth, we consider $y=y(x)$ as a parameter which will be chosen suitably later.

We have thus obtained, for some $C>0$

$$\sum_{\substack{p\le x\\ p\nmid N_E\\ N_p\equiv 0 \pmod t}}\Lambda\left(\frac{N_p}{t}\right)=S_{1,t}(y)+S_{2,t}(y)+O(x^{5/6}(\log x)^C). \tag{8.4}$$

In order to prove Theorem 2.2, we derive an asymptotic formula for $S_{1,t}(y)$ and show that the main contribution to $S_{E,t}(x)$ comes from the sum $S_{1,t}(y)$.

8.1. **Contribution from $S_{1,t}(y)$.** We will first estimate $S_{1,t}(y)$ in terms of a sum involving the functions ω and δ defined in (3.4).

Lemma 8.1. *Let $L=L(E)$ be the fixed positive integer appearing in Theorem 3.3. Let $y=x^\theta$ for some fixed $0<\theta<1$, and $B>0$ be a suitably large absolute constant. Assume that Conjecture 4 and Conjecture $\mathrm{EH}_{E,t}\left(x^\theta(\log x)^B\right)$ are true. Then for any $A>0$, we have*

$$S_{1,t}(y)=\mathrm{Li}(x)\sum_{d\le y}\sum_{e=1}^{\infty}\frac{\mu(d)\mu(e)\log(1/d)}{\omega(t[d_1,e_1^2])\delta([d_2,e_2^2])}+O_A\left(\frac{x}{(\log x)^A}\right),$$

where $d = d_1 d_2$ is the unique factorization of d such that rad$(d_1)|tL$, $(d_2, tL) = 1$ and similarly for e.

Proof. After interchanging the order of summation in (8.2), we may rewrite $S_{1,t}(y)$ as

$$S_{1,t}(y) := \sum_{d \leq y} \mu(d) \log(1/d) \sum_{\substack{p \leq x \\ p \nmid N_E \\ N_p \equiv 0 \ (\mathrm{mod}\ td)}} \mu^2\left(\frac{N_p}{t}\right) \tag{8.5}$$

Note that if $p|td$, then the inner sum can contribute at most

$$\sum_{\substack{p \leq x \\ p|td}} \mu^2\left(\frac{N_p}{t}\right) \ll \sum_{n|td} \Lambda(n) \ll \log(td).$$

Therefore, the contribution to the sum (8.5) when $(p, td) \neq 1$ is $\ll y(\log y)^2$, which is negligible. So, we may assume that $(p, td) = 1$. We now consider the sum

$$\sum_{d \leq y} \mu(d) \log(1/d) \sum_{\substack{p \leq x \\ p \nmid tdN_E \\ N_p \equiv 0 \ (\mathrm{mod}\ td)}} \mu^2\left(\frac{N_p}{t}\right).$$

The inner sum above is $\pi_E^*(x, d, t)$ as defined in (6.3). Under the assumption of Conjecture 4 and Conjecture $\mathrm{EH}_{E,t}\left(x^\theta (\log x)^B\right)$, Theorem 6.1 gives

$$S_{1,t}(y) = \mathrm{Li}(x) \sum_{d \leq y} \sum_{e=1}^{\infty} \frac{\mu(d)\mu(e)\log(1/d)}{\omega(t[d_1, e_1^2])\delta([d_2, e_2^2])} + \Delta_{1,t}(y),$$

where

$$\begin{aligned} \Delta_{1,t}(y) &:= \sum_{d \leq y} \mu(d) \log(1/d) \Delta_{\mu^2}(y, d, E, t) \\ &\ll \log y \sum_{d \leq y} \mu^2(d) |\Delta_{\mu^2}(y, d, E, t)| \ll \frac{x}{(\log x)^A}, \end{aligned}$$

for any $A > 0$, using (6.4). This completes the proof. □

We are now left to study the sum in the main term

$$M_t(y) := \sum_{d \leq y} \sum_{e=1}^{\infty} \frac{\mu(d)\mu(e)\log(1/d)}{\omega(t[d_1, e_1^2])\delta([d_2, e_2^2])}, \tag{8.6}$$

as $y \to \infty$. Writing $\log(1/d)$ as $\log(1/d_1) + \log(1/d_2)$, we have

$$M_t(y) = M_{1,t}(y) + M_{2,t}(y),$$

where

$$M_{1,t}(y) := \sum_{\substack{d_1|tL \\ e_1|tL}} \frac{\mu(d_1)\mu(e_1)\log(1/d_1)}{\omega\left(t[d_1, e_1^2]\right)} \sum_{(e_2, tL)=1} \sum_{\substack{d_2 \leq \frac{y}{d_1} \\ (d_2, tL)=1}} \frac{\mu(d_2)\mu(e_2)}{\delta([d_2, e_2^2])} \tag{8.7}$$

and

$$M_{2,t}(y) := \sum_{\substack{d_1|tL \\ e_1|tL}} \frac{\mu(d_1)\mu(e_1)}{\omega\left(t[d_1, e_1^2]\right)} \sum_{(e_2, tL)=1} \sum_{\substack{d_2 \leq \frac{y}{d_1} \\ (d_2, tL)=1}} \frac{\mu(d_2)\mu(e_2)}{\delta([d_2, e_2^2])} \log(1/d_2). \tag{8.8}$$

The following two propositions summarize the contribution of each of the above components of the main term.

Proposition 8.2. *Let $L = L(E)$ be the positive integer given in Theorem 3.3. As $y \to \infty$, we have*

$$M_{1,t}(y) \ll_{t,L} e^{-c\sqrt{\log y}},$$

for some absolute $c > 0$.

Proof. Consider the double sum

$$\sum_{(e,tL)=1} \sum_{\substack{d \le y \\ (d,\,tL)=1}} \frac{\mu(d)\mu(e)}{\delta\left([d, e^2]\right)} \tag{8.9}$$

Since d, e are squarefree, putting $r = (d, e)$, we see that $[d, e^2] = d'e^2$, where $d' = d/r$. Given any e coprime to tL, r can range over all divisors of e. Thus, (8.9) equals

$$\sum_{(e,tL)=1} \frac{\mu(e)}{\delta(e^2)} \sum_{r|e} \mu(r) \sum_{\substack{d' \le y/r \\ (d',\,ertL)=1}} \frac{\mu(d')}{\delta(d')} \quad \ll \quad e^{-c_1\sqrt{\log y}} \sum_{(e,tL)=1} \frac{\mu^2(e)}{\delta(e^2)} \sum_{r|e} \mu^2(r)$$

for some constant $c_1 > 0$, using Lemma 7.2. Since

$$\sum_{(e,tL)=1} \frac{\mu^2(e)\tau(e)}{\delta(e^2)}$$

is absolutely convergent using Lemma 3.4, the sum in (8.9) is $\ll \exp(-c\sqrt{\log y})$ for some $c > 0$.

The inner double sum of $M_{1,t}(y)$ in (8.7) is precisely (8.9) with y/d_1 instead of y. Hence, for some $c > 0$,

$$M_{1,t}(y) \quad \ll \quad e^{-c\sqrt{\log y}} \sum_{d_1,\, e_1|tL} \frac{\mu^2(d_1)\mu^2(e_1)\log(d_1)}{|\omega(t[d_1, e_1^2])|} \ll e^{-c\sqrt{\log y}} \log(tL)\tau(tL)^2,$$

which completes the proof. □

Proposition 8.3. *We have, as $y \to \infty$,*

$$M_{2,t}(y) = (1 + o(1))C_{E,t},$$

where $C_{E,t}$ is the constant defined in (2.8).

Proof. This follows immediately from Lemma 7.6. □

We obtain the following asymptotic formula for $S_{1,t}(y)$.

Lemma 8.4. *Let $y = x^\theta$ for a fixed $0 < \theta < 1$, and $B > 0$ be a suitably large absolute constant. Assume that Conjecture 4 and Conjecture $\mathrm{EH}_{E,t}\left(x^\theta(\log x)^B\right)$ are true. Then as $x \to \infty$, we have*

$$S_{1,t}(y) = (1 + o(1))C_{E,t}\,\mathrm{Li}(x),$$

where $C_{E,t}$ is as defined in (2.8).

Proof. The result follows upon putting together Lemma 8.1, (8.6), and Propositions 8.2 and 8.3. □

8.2. **Contribution from $S_{2,t}(y)$:** We recall from (8.3) that

$$S_{2,t}(y) := \sum_{\substack{p \le x \\ p \nmid N_E \\ N_p \equiv 0 \ (\mathrm{mod}\ t)}} \mu^2\left(\frac{N_p}{t}\right) \sum_{\substack{d | \frac{N_p}{t} \\ d > y}} \mu(d)\log(1/d).$$

Let $\frac{N_p}{t} = de$. Since $p \leq x$, the Hasse bound gives $dte \leq x+1+2\sqrt{x}$. We write the sum over divisors e of N_p/t, instead of d, to get

$$S_{2,t}(y) = \sum_{\substack{p \leq x \\ p \nmid N_E \\ N_p \equiv 0 \ (\mathrm{mod}\ t)}} \mu^2\left(\frac{N_p}{t}\right) \sum_{\substack{e \mid \frac{N_p}{t} \\ e \leq \frac{(x+1+2\sqrt{x})}{yt}}} \mu\left(\frac{N_p}{et}\right) \log\left(\frac{et}{N_p}\right).$$

Since $\frac{N_p}{t}$ is squarefree in the above sum, we may write $\mu\left(\frac{N_p}{et}\right) = \mu\left(\frac{N_p}{t}\right)\mu(e)$. Therefore,

$$S_{2,t}(y) = \sum_{\substack{p \leq x \\ p \nmid N_E \\ N_p \equiv 0 \ (\mathrm{mod}\ t)}} \sum_{\substack{e \mid \frac{N_p}{t} \\ e \leq \frac{(x+1+2\sqrt{x})}{yt}}} \mu\left(\frac{N_p}{t}\right) \mu(e) \log\left(\frac{et}{N_p}\right).$$

Using this we rewrite

$$S_{2,t}(y) = S_{2,t}^{(1)}(y) - S_{2,t}^{(2)}(y),$$

where,

$$S_{2,t}^{(1)}(y) := \sum_{\substack{p \leq x \\ p \nmid N_E \\ N_p \equiv 0 \ (\mathrm{mod}\ t)}} \sum_{\substack{e \mid \frac{N_p}{t} \\ e \leq \frac{(x+1+2\sqrt{x})}{yt}}} \mu\left(\frac{N_p}{t}\right) \mu(e) \log e \tag{8.10}$$

and,

$$S_{2,t}^{(2)}(y) := \sum_{\substack{p \leq x \\ p \nmid N_E \\ N_p \equiv 0 \ (\mathrm{mod}\ t)}} \sum_{\substack{e \mid \frac{N_p}{t} \\ e \leq \frac{(x+1+2\sqrt{x})}{yt}}} \mu(e)\mu\left(\frac{N_p}{t}\right) \log\left(\frac{N_p}{t}\right) \tag{8.11}$$

We evaluate $S_{2,t}^{(1)}(y)$ and $S_{2,t}^{(2)}(y)$ in the following propositions.

Proposition 8.5. *Let $y = x^\theta$ for some fixed $0 < \theta < 1$. Assume Conjecture $\mathrm{EH}_{E,t,\mu}(x^{1-\theta})$holds. Then for any $A > 0$, we have*

$$S_{2,t}^{(1)}(y) = (-C_{E,t} + o(1)) \sum_{\substack{p \leq x \\ p \nmid N_E}} \mu\left(\frac{N_p}{t}\right) + O\left(\frac{x}{(\log x)^A}\right),$$

where $C_{E,t}$ is as defined in (2.8).

Proof. After interchanging the order of summation, we rewrite the sum in (8.10) as

$$S_{2,t}^{(1)}(y) = \sum_{e \leq \frac{(x+1+2\sqrt{x})}{yt}} \mu(e) \log(e) \sum_{\substack{p \leq x \\ p \nmid N_E \\ N_p \equiv 0 \ (\mathrm{mod}\ et)}} \mu\left(\frac{N_p}{t}\right)$$

Note that the contribution to the sum (8.5) when $p | et$ is $\ll x^{1-\theta}(\log x)^2$, which is negligible. Hence we may assume that $(p, et) = 1$ and consider the sum

$$\sum_{e \leq \frac{(x+1+2\sqrt{x})}{yt}} \mu(e) \log(e) \sum_{\substack{p \leq x \\ p \nmid etN_E \\ N_p \equiv 0 \ (\mathrm{mod}\ et)}} \mu\left(\frac{N_p}{t}\right)$$

Let $e = e_1e_2$ be the unique factorization of e such that $\mathrm{rad}(e_1)|tL$, and $(e_2, tL) = 1$. Using Conjecture $\mathrm{EH}_{E,t,\mu}(x^{1-\theta})$ in the above expression, we have

$$S_{2,t}^{(1)}(y) = \sum_{e_1|tL} \sum_{e_2 \le \frac{(x+1+2\sqrt{x})}{yte_1}} \frac{\mu(e_1)\mu(e_2)}{\omega(te_1)\delta(e_2)} \log(e_1e_2) \sum_{\substack{p\le x \\ p\nmid N_E}} \mu\left(\frac{N_p}{t}\right) + O\left(\frac{x}{(\log x)^A}\right), \tag{8.12}$$

for any $A > 0$. The double sum over e_1 and e_2 is independent of the sum over primes p above. We observe that

$$\sum_{e_1|tL} \frac{\mu(e_1)}{\omega(te_1)} \log(e_1) \sum_{e_2 \le \frac{(x+1+2\sqrt{x})}{yte_1}} \frac{\mu(e_2)}{\delta(e_2)} \ll_{t,L} e^{-c\sqrt{\log x}},$$

using Lemma 7.2. From this and Lemma 7.7, we see that the aforementioned double sum in (8.12) equals

$$-(1 + o(1))C_{E,t} + O\big(\exp(-c\sqrt{\log x})\big).$$

Putting this into (8.12) completes the proof. □

In order to show that $S_{2,t}^{(2)}(y)$ is negligible, we need the following logarithmically weighted version of $\mathrm{EH}_{E,t,\mu}\left(x^{\theta}\right)$.

Proposition 8.6. *Assume that Conjecture* $\mathrm{EH}_{E,t,\mu}(x^{\theta})$ *holds. Let*

$$\tilde{\Delta}_{E,\mu}(x, e, t) := \sum_{\substack{p\le x,\, p\nmid teN_E \\ N_p\equiv 0 \ (\mathrm{mod}\ te)}} \mu\left(\frac{N_p}{t}\right) \log\left(\frac{N_p}{t}\right) - \frac{1}{\omega(te_1)\delta(e_2)} \sum_{\substack{p\le x \\ p\nmid N_E}} \mu\left(\frac{N_p}{t}\right) \log\left(\frac{N_p}{t}\right), \tag{8.13}$$

where $e = e_1e_2$ *is the unique factorization of* e *such that* $\mathrm{rad}(e_1)|L$, *and* $(e_2, tL) = 1$. *Then given any* $A > 0$, *there exists* $B = B(A) > 0$ *such that*

$$\sum_{e \le \frac{x^{\theta'}}{(\log x)^B}} |\tilde{\Delta}_{E,\mu}(x, e, t)| \ll_A \frac{x}{(\log x)^A},$$

for any $\theta' \le \min\{\theta, 1/2\}$.

Proof. We will rephrase Conjecture $\mathrm{EH}_{E,t,\mu}(x^{\theta})$ using an indicator function which detects integers (with multiplicity) of the form $\frac{N_p}{t}$ for some prime $p \nmid etN_E$. More precisely, we define

$$\mathbb{1}_{E,t}(n) := \#\{p \nmid etN_E : N_p/t = n\}. \tag{8.14}$$

Let us define the function $b(y) = y + 2\sqrt{y} + 1$. Then for any y sufficiently large, we have

$$\sum_{\substack{n \le \frac{b(y)}{t} \\ n\equiv 0 \ (\mathrm{mod}\ e)}} \mu(n)\mathbb{1}_{E,t}(n) = \sum_{\substack{p\le y,\, p\nmid teN_E \\ N_p\equiv 0 \ (\mathrm{mod}\ te)}} \mu\left(\frac{N_p}{t}\right) + O(\sqrt{y}), \tag{8.15}$$

where the O-term takes into account the possible contribution from N_p' s with p lying in the interval $(y, y + 4\sqrt{y} + 4]$, to the sum on the left hand side of (8.15). By (2.6), we have that (8.15) equals

$$\frac{1}{\omega(te_1)\delta(e_2)} \sum_{\substack{p \le y \\ p \nmid N_E}} \mu\left(\frac{N_p}{t}\right) + O(\sqrt{y}) + \Delta_{E,\mu}(y, e, t)$$
$$= \frac{1}{\omega(te_1)\delta(e_2)} \sum_{\substack{p \le y \\ p \nmid etN_E}} \mu\left(\frac{N_p}{t}\right) + O(\sqrt{y}) + \Delta_{E,\mu}(y, e, t) + O\bigg(\frac{1}{\delta(e_2)} \sum_{p \mid et} 1\bigg).$$

Using (8.14) again, we obtain that Conjecture $\mathrm{EH}_{E,t,\mu}(x^\theta)$ can be formulated as follows:

$$\sum_{\substack{n \le \frac{b(y)}{t} \\ n \equiv 0 \ (\mathrm{mod}\ e)}} \mu(n) \mathbb{1}_{E,t}(n) = \frac{1}{\omega(te_1)\delta(e_2)} \sum_{n \le \frac{b(y)}{t}} \mu(n) \mathbb{1}_{E,t}(n) + \Delta_{E,\mu}(y, e, t) + O(\sqrt{y}). \tag{8.16}$$

We now apply partial summation to the sum

$$\sum_{\substack{n \le \frac{b(x)}{t} \\ n \equiv 0 \ (\mathrm{mod}\ e)}} \mu(n) \mathbb{1}_{E,t}(n) \log n,$$

to get

$$\Bigg(\sum_{\substack{n \le \frac{b(x)}{t} \\ n \equiv 0 \ (\mathrm{mod}\ e)}} \mu(n) \mathbb{1}_{E,t}(n) \Bigg) \log(b(x)/t) - \int_1^{b(x)/t} \Bigg(\sum_{\substack{n \le u \\ n \equiv 0 \ (\mathrm{mod}\ e)}} \mu(n) \mathbb{1}_{E,t}(n) \Bigg) \frac{1}{u} du$$
$$= \frac{1}{\omega(te_1)\delta(e_2)} \Bigg[\Bigg(\sum_{n \le \frac{b(x)}{t}} \mu(n) \mathbb{1}_{E,t}(n) \Bigg) \log(b(x)/t) - \int_1^{b(x)/t} \Bigg(\sum_{n \le u} \mu(n) \mathbb{1}_{E,t}(n) \Bigg) \frac{1}{u} du \Bigg]$$
$$+ O_t(\sqrt{x} \log x) + \Bigg(\max_{y \le x} |\Delta_{E,\mu}(y, e, t)| \log x \Bigg),$$

where the last expression follows from (8.16). Notice that the expression inside the square brackets is exactly what one would obtain on applying partial summation to

$$\sum_{n \le \frac{b(x)}{t}} \mu(n) \mathbb{1}_{E,t}(n) \log n.$$

Hence, we have

$$\sum_{\substack{n \le \frac{b(x)}{t} \\ n \equiv 0 \ (\mathrm{mod}\ e)}} \mu(n) \mathbb{1}_{E,t}(n) \log n = \frac{1}{\omega(te_1)\delta(e_2)} \sum_{n \le \frac{b(x)}{t}} \mu(n) \mathbb{1}_{E,t}(n) \log(n) + \Delta'_{E,\mu}(x, e, t), \tag{8.17}$$

where

$$\Delta'_{E,\mu}(x, e, t) := \max_{y \le x} |\Delta_{E,\mu}(y, e, t)| \log x + O_t(\sqrt{x} \log x). \tag{8.18}$$

Making the transition from sums over n to those over primes p using (8.14), we have

$$\sum_{\substack{p \le x,\, p \nmid teN_E \\ N_p \equiv 0 \ (\mathrm{mod}\ te)}} \mu\left(\frac{N_p}{t}\right) \log\left(\frac{N_p}{t}\right) = \frac{1}{\omega(te_1)\delta(e_2)} \sum_{p \le x,\, p \nmid N_E} \mu\left(\frac{N_p}{t}\right) \log\left(\frac{N_p}{t}\right) + \tilde{\Delta}_{E,\mu}(x, e, t),$$

where

$$\tilde{\Delta}_{E,\mu}(x,e,t) = \Delta'_{E,\mu}(x,e,t) + O\bigg(\frac{1}{\delta(e_2)}\sum_{p|et}\log x\bigg).$$

Since the last term above is $\ll 1$, (8.18) yields the desired bound on $\tilde{\Delta}_{E,\mu}(x,e,t)$. □

This result allows us to bound $S_{2,t}^{(2)}(y)$ as follows.

Proposition 8.7. *Suppose that Conjecture* $\mathrm{EH}_{E,t,\mu}(x^{1-\theta})$ *holds for some* $\theta \geq 1/2$. *Then given* $A > 0$, *there exists* $B = B(A) > 0$, *such that*

$$S_{2,t}^{(2)}(x^\theta(\log x)^B) \ll_A \frac{x}{(\log x)^A}.$$

Proof. Let $y = x^\theta(\log x)^{B(A)}$. Recall from (8.11) that

$$S_{2,t}^{(2)}(y) := \sum_{e\leq\frac{(x+1+2\sqrt{x})}{yt}} \mu(e) \sum_{\substack{p\leq x,\, p\nmid N_E\\ N_p\equiv 0 \pmod{te}}} \mu\left(\frac{N_p}{t}\right)\log\left(\frac{N_p}{t}\right).$$

As in Proposition 8.5, the contribution to the above sum when $p|te$ is $\ll x^{1-\theta}(\log x)^2$, which is negligible and we will be considering

$$\sum_{e\leq\frac{(x+1+2\sqrt{x})}{yt}} \mu(e) \sum_{\substack{p\leq x,\, p\nmid teN_E\\ N_p\equiv 0 \pmod{te}}} \mu\left(\frac{N_p}{t}\right)\log\left(\frac{N_p}{t}\right).$$

From Proposition 8.6 , we get

$$\begin{aligned} S_{2,t}^{(2)}(y) &= \sum_{e\leq\frac{(x+1+2\sqrt{x})}{yt}} \frac{\mu(e)}{\omega(te_1)\delta(e_2)} \sum_{\substack{p\leq x\\ p\nmid N_E}} \mu\left(\frac{N_p}{t}\right)\log\left(\frac{N_p}{t}\right) + O\left(\frac{x}{(\log x)^A}\right) \\ &= \sum_{e_1|tL}\frac{\mu(e_1)}{\omega(te_1)} \sum_{e_2\leq\frac{(x+1+2\sqrt{x})}{yte_1}} \frac{\mu(e_2)}{\delta(e_2)} \sum_{\substack{p\leq x\\ p\nmid N_E}} \mu\left(\frac{N_p}{t}\right)\log\left(\frac{N_p}{t}\right) + O\left(\frac{x}{(\log x)^A}\right). \end{aligned}$$

A crucial observation at this point is that the sums over e_1, e_2 and p in the main term are independent of each other. The sum over p is trivially bounded by $x\log x$ and we bound the former sums using Lemma 7.2 to get

$$\sum_{e_1|tL}\frac{\mu(e_1)}{\omega(te_1)} \sum_{e_2\leq\frac{(x+1+2\sqrt{x})}{yte_1}} \frac{\mu(e_2)}{\delta(e_2)} \ll \tau(tL)\exp(-c\sqrt{\log x}),$$

for some $c > 0$. This completes the proof. □

From Propositions 8.5 and 8.7, we have obtained the following estimate for $S_{2,t}(y)$.

Lemma 8.8. *Suppose that Conjecture* $\mathrm{EH}_{E,t,\mu}(x^{1-\theta})$ *holds for some* $\theta \geq 1/2$. *Given* $A > 0$, *there exists* $B = B(A) > 0$ *such that*

$$S_{2,t}(x^\theta(\log x)^B) = (-C_{E,t} + o(1))\sum_{\substack{p\leq x\\ p\nmid N_E}} \mu\left(\frac{N_p}{t}\right) + O\left(\frac{x}{(\log x)^A}\right),$$

where $C_{E,t}$ *is the constant defined in* (2.8).

9. Proof of the Theorem 2.2

Let $B = B(A)$ as in Lemma 8.8. Choosing $y = x^\theta(\log x)^B$ for some fixed $1/2 \leq \theta < 1$, we first note that Lemma 8.4 holds with this choice of y as well, provided we assume $\mathrm{EH}_{E,t}(y(\log x)^C)$, for some sufficiently large C.

Using (8.4), and Lemmas 8.4, 8.8, we obtain

$$\sum_{\substack{p\leq x\\ p\nmid N_E\\ N_p\equiv 0 \pmod t}} \Lambda\left(\frac{N_p}{t}\right) = (C_{E,t}+o(1))\,\mathrm{Li}(x) + (-C_{E,t}+o(1)) \sum_{\substack{p\leq x,\, p\nmid N_E\\ N_p\equiv 0 \pmod t}} \mu\left(\frac{N_p}{t}\right)$$

$$= C_{E,t}\left(\mathrm{Li}(x) - \sum_{p\leq x,\, p\nmid N_E} \mu\left(\frac{N_p}{t}\right)\right) + o(\mathrm{Li}(x)), \tag{9.1}$$

under the conjectures $\mathrm{EH}_{E,t}(x^\theta(\log x)^C)$, $\mathrm{EH}_{E,t,\mu}(x^{1-\theta})$ and Conjecture 4, for C sufficiently large. Here $C_{E,t}$ is as in (2.8). This shows that (2.2) and (2.3) are equivalent to each other.

From (9.1), part $b)$ of the result follows if we have

$$\left|\sum_{p\leq x,\, p\nmid N_E} \mu\left(\frac{N_p}{t}\right)\right| \leq \mathcal{A}_{E,L}\,\mathrm{Li}(x) + o(\mathrm{Li}(x)). \tag{9.2}$$

We prove this as follows.

$$\begin{aligned}\left|\sum_{p\leq x,\, p\nmid N_E} \mu\left(\frac{N_p}{t}\right)\right| &\leq \sum_{\substack{p\leq x,\, p\nmid N_E\\ N_p \text{ is squarefree}}} 1\\ &= \sum_{\substack{p\leq x\\ p\nmid N_E}} 1 - \sum_{\substack{p\leq x,\, p\nmid N_E\\ N_p \text{ is divisible by a square}}} 1.\end{aligned}$$

Take ℓ to be the smallest prime coprime to L. Then the right hand side above is

$$\leq \quad (1+o(1))\,\mathrm{Li}(x) - \sum_{\substack{p\leq x,\, p\nmid N_E\\ N_p\equiv 0 \pmod{\ell^2}}} 1.$$

Using (3.9), we have for any $A > 0$,

$$\sum_{\substack{p\leq x,\, p\nmid N_E\\ N_p\equiv 0 \pmod{\ell^2}}} 1 = \frac{1}{\delta(\ell^2)}\,\mathrm{Li}(x) + O_A\left(\ell^6 \frac{x}{(\log x)^A}\right).$$

Therefore,

$$\left|\sum_{\substack{p\leq x,\, p\nmid N_E\\ N_p\equiv 0 \pmod t}} \mu\left(\frac{N_p}{t}\right)\right| \leq \mathrm{Li}(x)\left(1-\frac{1}{\delta(\ell^2)}\right) + O_A\left(\ell^6\frac{x}{(\log x)^A}\right) + o(\mathrm{Li}(x)).$$

Since $\mathcal{A}_{E,L} = \left(1-\frac{1}{\delta(\ell^2)}\right)$, this completes the proof of part $b)$ of the result.

Acknowledgments. The authors express their sincere gratitude to Prof. M. Ram Murty for suggesting this project to them as well as for his insightful discussions. The second author was supported by the SERB-DST grant SRG/2020/002248. The fourth author was supported by the SERB-DST grant ECR/2018/001566 and the DST INSPIRE Faculty Award Program.

REFERENCES

1. A. Akbary, D. Ghioca, and V. Kumar Murty, *Reductions of points on elliptic curves*, Math. Ann. **347** (2010), no. 2, 365–394. MR 2606941
2. A. Balog, A-C. Cojocaru, and C. David, *Average twin prime conjecture for elliptic curves*, Amer. J. Math. **133** (2011), no. 5, 1179–1229. MR 2843097
3. T. Bandman, F. Grunewald, and B. Kunyavskiĭ, *Geometry and arithmetic of verbal dynamical systems on simple groups*, Groups Geom. Dyn. **4** (2010), no. 4, 607–655, With an appendix by Nathan Jones. MR 2727656
4. A-C. Cojocaru, *Questions about the reductions modulo primes of an elliptic curve*, Number theory, CRM Proc. Lecture Notes, vol. 36, Amer. Math. Soc., Providence, RI, 2004, pp. 61–79. MR 2076566
5. ———, *Reductions of an elliptic curve with almost prime orders*, Acta Arith. **119** (2005), no. 3, 265–289. MR 2167436
6. ———, *Primes, elliptic curves and cyclic groups*, Analytic methods in arithmetic geometry, Contemp. Math., vol. 740, Amer. Math. Soc., [Providence], RI, [2019] ©2019, With an appendix by Cojocaru, Matthew Fitzpatrick, Thomas Insley and Hakan Yilmaz, pp. 1–69. MR 4033729
7. C. David and E. Smith, *Elliptic curves with a given number of points over finite fields*, Compos. Math. **149** (2013), no. 2, 175–203. MR 3020306
8. C. David and J. Wu, *Almost prime values of the order of elliptic curves over finite fields*, Forum Math. **24** (2012), no. 1, 99–119. MR 2879973
9. L. Giberson, *Koblitz's conjecture on average for elliptic curves over abelian number fields of square-free conductor*, J. Number Theory **185** (2018), 449–478. MR 3734359
10. D. A. Goldston and C. Y. Yıldırım, *Higher correlations of divisor sums related to primes. I. Triple correlations*, Integers **3** (2003), A5, 66. MR 1985667
11. H. Iwaniec and J. Jiménez Urroz, *Orders of CM elliptic curves modulo p with at most two primes*, Ann. Sc. Norm. Super. Pisa Cl. Sci. (5) **9** (2010), no. 4, 815–832. MR 2789476
12. N. Koblitz, *Primality of the number of points on an elliptic curve over a finite field*, Pacific J. Math. **131** (1988), no. 1, 157–165. MR 917870
13. E. Kowalski, *Analytic problems for elliptic curves*, J. Ramanujan Math. Soc. **21** (2006), no. 1, 19–114. MR 2226355
14. 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), 1977, pp. 409–464. MR 0447191
15. S. A. Miri and V. Kumar Murty, *An application of sieve methods to elliptic curves*, Lecture Notes in Comput. Sci., vol. 2247, Springer, Berlin, 2001. MR 1934487
16. M. R. Murty, *Problems in analytic number theory*, second ed., Graduate Texts in Mathematics, vol. 206, Springer, New York, 2008, Readings in Mathematics. MR 2376618
17. M. R. Murty and J. Esmonde, *Problems in algebraic number theory*, second ed., Graduate Texts in Mathematics, vol. 190, Springer-Verlag, New York, 2005. MR 2090972
18. M. R. Murty, V. Kumar Murty, and N. Saradha, *Modular forms and the Chebotarev density theorem*, Amer. J. Math. **110** (1988), no. 2, 253–281. MR 935007
19. M. R. Murty and A. Vatwani, *Twin primes and the parity problem*, J. Number Theory **180** (2017), 643–659. MR 3679820
20. D. J. Newman, *Simple analytic proof of the prime number theorem*, Amer. Math. Monthly **87** (1980), no. 9, 693–696. MR 602825
21. L. B. Pierce, C. L. Turnage-Butterbaugh, and M. M. Wood, *An effective Chebotarev density theorem for families of number fields, with an application to ℓ-torsion in class groups*, Invent. Math. **219** (2020), no. 2, 701–778. MR 4054810
22. Atle Selberg, *Lectures on sieves, Collected papers. II*, Springer Collected Works in Mathematics, Springer, Heidelberg, 2014, Reprint of the 1991 edition [MR1295844], With a foreword by K. Chandrasekharan. MR 3308963
23. ———, *Remarks on multiplicative functions, Collected papers. I*, Springer Collected Works in Mathematics, Springer, Heidelberg, 2014, With a foreword by K. Chandrasekharan, Reprint of the 1989 edition [MR1117906]. MR 3287209
24. J. P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent Math **15** (1972), 259–331.
25. Jean-Pierre Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. (1981), no. 54, 323–401. MR 644559
26. J. H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR 2514094
27. J. Steuding and A. Weng, *Erratum: "On the number of prime divisors of the order of elliptic curves modulo p" [Acta Arith.* **117** *(2005), no. 4, 341–352; mr2140162]*, Acta Arith. **119** (2005), no. 4, 407–408. MR 2189069
28. ———, *On the number of prime divisors of the order of elliptic curves modulo p*, Acta Arith. **117** (2005), no. 4, 341–352. MR 2140162
29. E. C. Titchmarsh, *The theory of the Riemann zeta-function*, second ed., The Clarendon Press, Oxford University Press, New York, 1986, Edited and with a preface by D. R. Heath-Brown. MR 882550
30. D. Zywina, *A refinement of Koblitz's conjecture*, Int. J. Number Theory **7** (2011), no. 3, 739–769. MR 2805578

Department of Mathematics, Indian Institute of Technology Gandhinagar, Gandhinagar, Gujarat 382355, India
Email address: sampa.d@iitgn.ac.in

Department of Mathematics, Indian Institute of Technology Gandhinagar, Gandhinagar, Gujarat 382355, India
Email address: arnab.saha@iitgn.ac.in

Department of Mathematics, Chennai Mathematical Institute, H1, SIPCOT IT Park, Siruseri, Kelambakkam, Chennai, Tamil Nadu 603103, India
Email address: jyothsnaas@cmi.ac.in

Department of Mathematics, Indian Institute of Technology Gandhinagar, Gandhinagar, Gujarat 382355, India
Email address: akshaa.vatwani@iitgn.ac.in