CHEBOTAREV DENSITY THEOREM AND EXTREMAL PRIMES FOR NON-CM ELLIPTIC CURVES

AMITA MALIK AND NEHA PRABHU

Abstract. For a fixed non-CM elliptic curve $E$ over $\mathbb{Q}$ and a prime $\ell$, we prove an asymptotic formula on the number of primes $p \leq x$ for which the Frobenius trace $a_p(E)$ satisfies the congruence $a_p(E) \equiv [2\sqrt{p}] \pmod{\ell}$. In order to achieve this, we establish a joint distribution concerning the fractional part of $\alpha_p \theta$ for $\theta \in [0,1]$, $\alpha > 0$, and primes $p$ satisfying the Chebotarev condition. As a corollary, we also obtain upper bounds for the number of extremal primes. The results rely on GRH for Dedekind zeta functions for Galois extensions of number fields.

1. Introduction

Let $E$ denote an elliptic curve over $\mathbb{Q}$ without complex multiplication with conductor $N_E$. For a prime $p$ of good reduction, $E$ reduces to an elliptic curve over the finite field $\mathbb{F}_p$ and we denote by $a_p(E)$ the trace of the Frobenius automorphism acting on the points of $E$ over $\mathbb{F}_p$. Then, $a_p(E) = p + 1 - \#E(\mathbb{F}_p)$, and the Hasse bound $|a_p(E)| \leq 2\sqrt{p}$ holds. The last few decades have seen much research pertaining to the distribution of the sequence $a_p(E)/2\sqrt{p}$. Sato and Tate formulated a conjecture for the distribution of this sequence in the interval $[-1,1]$ around 1960 which was proven by Taylor, Clozel, Harris and Shepherd-Barron in [Tay08, CHT08, HSBT10].

Theorem (Sato-Tate conjecture). Let $E$ be a non-CM elliptic curve over $\mathbb{Q}$ with conductor $N_E$. Let $\alpha, \beta \in \mathbb{R}$ with $-1 \leq \alpha \leq \beta \leq 1$. Then, as $x \to \infty$,

$$\frac{1}{\pi(x)} \# \left\{ p \leq x, p \nmid N_E : \frac{a_p(E)}{2\sqrt{p}} \in (\alpha, \beta) \right\} \sim \frac{2}{\pi} \int_\alpha^\beta \sqrt{1-t^2} \, dt.$$

The measure $\mu_{ST}(\alpha, \beta) := \frac{2}{\pi} \int_\alpha^\beta \sqrt{1-t^2} \, dt$ is also known as the semicircle measure. The shape of the distribution clearly suggests fewer primes at the ends of the interval in comparison to those at the middle, so it is interesting to see if a precise statement can be made about the behaviour at the extremes. The objects of our study here are such primes, called extremal primes i.e. primes $p$ satisfying $a_p(E) = \pm[2\sqrt{p}]$, where $[\cdot]$ denotes the greatest integer function. These were first studied by James et al. [JTT+16] (see also [JP17]) who conjectured

Date: December 24, 2020.
2010 Mathematics Subject Classification. 11G05, 11N05.
Key words and phrases. Non-CM Elliptic curves, Extremal primes, Lang-Trotter conjecture, Chebotarev Density Theorem, Joint distribution, Fractional part of powers of primes.
that, as \( x \to \infty \),
\[
\# \{ p \leq x : p \nmid N_E, a_p(E) = \pm \sqrt{p} \} \sim \begin{cases} 
2 \frac{x^{3/4}}{3\pi \log x} & \text{if } E \text{ has complex multiplication (CM)}; \\
8 \frac{x^{1/4}}{3\pi \log x} & \text{if } E \text{ does not have CM}.
\end{cases}
\] (1.1)

The number of extremal primes is smaller for the case of non-CM curves since the measure of the interval at the ends of the Sato-Tate semi-circle distribution is smaller. On the other hand, for CM curves there is an excess of such primes since the measure for the distribution of \( a_p(E)/(2\sqrt{p}) \) in \([\alpha, \beta] \subseteq [-1, 1]/\{0\} \) is given by \( \frac{1}{2\pi} \int_\alpha^\beta \frac{dt}{\sqrt{1-t^2}} \). This is reminiscent of the Lang-Trotter conjecture where the trace is a fixed integer rather than being a function of the prime. More precisely,

**Conjecture 1.1 (Lang-Trotter conjecture).**

\[
\# \{ p \leq x : p \nmid N_E, a_p(E) = t \} \sim C_{E,t} \frac{x^{1/2}}{\log x}
\]

as \( x \to \infty \), where \( t \in \mathbb{Z} \) is fixed and \( C_{E,t} \) is a constant depending on the curve \( E \) and the integer \( t \). This conjecture is far from being proved and thus upper bounds remain of great interest.

The asymptotics in (1.1) for extremal primes for CM curves were proven by James and Pollack [JP17]. In a subsequent paper, Agwu, Harris, James, Kannan and Li [AHJ+18] studied asymptotic behavior of the primes where \( a_p(E) \) falls within a small range of the end of the Hasse interval. In the case of non-CM curves, the asymptotic was proved to be true on average in the Ph. D. thesis of Giberson [Gib17]. In contrast, the asymptotics (1.1) for a fixed non-CM curve seem to be out of reach with current techniques. In [DGM+20], along with David, Gafni, and Turnage-Butterbaugh, the authors established the following upper bounds for a single curve \( E/\mathbb{Q} \).

**Theorem (DGM+20).** Let \( E/\mathbb{Q} \) be a non-CM elliptic curve. Assume that for \( n \geq 0 \), the \( L \)-functions \( L(s; \text{Sym}^n(E)) \) have analytic continuation to the entire complex plane (except for a simple pole at \( s = 1 \) when \( n = 0 \), satisfy the expected functional equation and the Generalized Riemann Hypothesis (GRH). Then

\[
\#\{ x < p \leq 2x : p \nmid N_E, a_p(E) = \sqrt{p} \} \ll_{E} x^{1/2}.
\] (1.2)

**Remark 1.** Due to the recent breakthrough of Newton and Thorne [NT20], the only unproven hypothesis in the above result is GRH for symmetric powers of \( L \)-functions.

More recently, from Gafni, Thorner and Wong [GTW20] it follows that the bound in (1.2) can be made \( x(\log \log x)^2/(\log x)^2 \) unconditionally.

In this article, we follow a different approach to count extremal primes. Inspired by the work of Serre [Ser72] and Murty, Murty and Saradha [MMS88] on bounds for the Lang-Trotter conjecture, we investigate the number of primes up to \( x \) satisfying the extremality condition modulo a large prime \( \ell \). The distribution
of $a_p(E)$ modulo $\ell$ is known by the Chebotarev Density Theorem applied to the Galois extensions $\mathbb{Q}(E[\ell])/\mathbb{Q}$, the field obtained by adjoining the coordinates of $\ell$-torsion points of $E$ to $\mathbb{Q}$. A novelty in our application is the observation that studying primes $p$ at the end of the Sato-Tate distribution leads to studying the distribution of the fractional part of $2\sqrt{p}$. Balog \cite{Bal83} showed that the latter distribution is uniform. For our purpose, we require the joint distribution of rational primes satisfying a Chebotarev condition in the extensions $\mathbb{Q}(E[\ell])/\mathbb{Q}$ with this fractional part lying in certain interval. Most of the paper is devoted to proving this result for arbitrary finite Galois extensions over $\mathbb{Q}$, so as to be of independent interest.

We also give a version of this joint distribution in the case when the fractional part $\{\sqrt{p}\} < p^{-\lambda}$ for $\lambda < 1/4$. Note that for $\lambda = 1/2$, this concerns the infinitude of primes $p$ of the form $n^2 + 1$ for some $n \in \mathbb{N}$, also known as one of Landau’s four problems and is widely open.

Before stating our main results, we fix some notations. Throughout the paper, $p$ and $\ell$ denote primes, $\pi(x)$ denotes the number of primes up to $x$, and $\{y\}, [y]$ denote the fractional part and the integer part of $y$, respectively. For a finite Galois extension $L/\mathbb{Q}$ and $C$ a union of conjugacy classes in $\text{Gal}(L/\mathbb{Q})$, define

$$\pi_C(x, L) := \pi_C(x, L/\mathbb{Q}) := \#\{x < p \leq 2x : p \text{ unramified in } L, \sigma_p \in C\}$$

where $\sigma_p$ is the conjugacy class of the Frobenius automorphism associated with any prime lying above $p$. To simplify exposition, henceforth when we write $\sigma_p \in C$ we assume that $p$ is unramified in $L$ unless mentioned otherwise. We now state our main results.

**Theorem 1.1.** Consider a finite Galois extension $L/\mathbb{Q}$ with $n_L = [L : \mathbb{Q}]$. Let $\alpha > 0$, $\omega \geq 1$ and $0 \leq \delta_1 < \delta_2 \leq 1$ with $\delta := \delta_2 - \delta_1$. Let $\theta \in [0, 1]$ be fixed. Assume that GRH holds for the Dedekind zeta function $\zeta_L(s)$ and the parameters $n_L, \alpha, \omega$ and $\delta$ satisfy

$$\alpha^{1/4}(\omega n_L/\delta)^{1/2}(\log x)^2 \ll_\theta x^{(1-\theta)/4}.$$

Then the following holds uniformly for $\delta, \alpha$ and $\omega$.

$$\#\{x < p \leq 2x : \delta_1 \leq \{\alpha p^\theta\} < \delta_2 \text{ and } \sigma_p \in C\} - \delta \pi_C(x, L) \ll_\theta |C| n_L \log x \left(\frac{\delta \omega^{1/2} \alpha^{1/4}}{n_L^{1/2}} x^{(3+\theta)/4} + \frac{\delta \omega}{\alpha^{1/2}} x^{1-\theta/2} \log x \right) + (\delta n_L \omega)^{1/2} \alpha^{1/4} x^{(1+\theta)/4} \log x + \frac{|C| \delta x}{|G| \omega \log x}.$$

**Theorem 1.2.** Let $E/\mathbb{Q}$ be a non-CM elliptic curve. Assume that GRH holds for $\zeta_{E[\ell]}(s)$, where $\ell$ is a large prime. Then, for $\ell \ll x^{1/18} \omega^{-2/9} \log^{-8/9} x$, $\omega \geq 1$,

$$\#\{x < p \leq 2x : p \nmid N_E, a_p(E) \equiv [2\sqrt{p}] \mod \ell\} = \frac{\pi(x)}{\ell} + O_E \left(\frac{x}{\omega \ell \log x} + \omega^{1/2} \ell^{5/4} x^{7/8} \log x + \omega \ell^{7/2} x^{3/4} (\log x)^2\right).$$
Making the simple observation that
\[ \# \{ x < p \leq 2x : p \nmid N_E, a_p(E) = [2\sqrt{p}] \} \leq \# \{ x < p \leq 2x : p \nmid N_E, a_p(E) \equiv [2\sqrt{p}] \text{ mod } \ell \} \]
and setting \( \omega = 1 \) and \( \ell = x^{1/18} \log^{-8/9} x \) in Theorem 1.2, one obtains the following upper bounds for the number of extremal primes up to \( x \).

**Corollary 1.** Assume GRH as in Theorem 1.2. For a non-CM elliptic curve \( E/\mathbb{Q} \), and large \( x \),
\[ \{ x < p \leq 2x : p \nmid N_E, a_p(E) = [2\sqrt{p}] \} \ll_E x^{17/18} (\log x)^{-1/9}. \]

**Remark 2.** Similar results can be obtained for extremal primes with \( a_p(E) = -[2\sqrt{p}] \) using essentially the same arguments as presented here. Moreover, because of the generality in Theorem 1.1, one can write more general versions of Theorem 1.2 and Corollary 1 where \( \sqrt{p} \) is replaced by \( p^\theta \) for \( \theta \in [0, 1] \).

As in the case of upper bounds for the Lang-Trotter conjecture, we obtain better estimates for the joint distribution in the particular case of \( a_p(E) \equiv 0 \mod \ell \). To be precise, the following holds.

**Corollary 2.** Let \( E \) be a non-CM elliptic curve over \( \mathbb{Q} \). Assume that GRH holds for \( \zeta_{\mathbb{Q}(E[\ell])}(s) \) where \( \ell \) is a large prime with \( \ell \ll x^{1/14} (\log x)^{-8/7} \omega^{-2/7} \). Then
\[ \# \{ x < p \leq 2x : p \nmid N_E, a_p(E) \equiv [2\sqrt{p}] \equiv 0 \mod \ell \} = \frac{\pi(x)}{\ell^2} + O \left( \frac{x}{\ell^2 \omega \log x} + \frac{\omega^{1/2} x^{7/8} \log x}{\ell^{1/4}} + \omega \ell^{3/2} x^{3/4} (\log x)^2 \right). \]

In fact, using the same ideas as in Theorem 1.1, one can prove a more general result, stated below, where the bounds for the fractional part of the prime are themselves a function of the prime.

**Theorem 1.3.** Let \( \alpha, \lambda > 0 \) and \( \theta \in [0, 1] \) be fixed. For finite Galois extension \( L/K \), assume GRH for \( \zeta_L(s) \). Then
\[ \# \{ x < p \leq 2x : \{ \alpha p^\theta \} < p^{-\lambda} \text{ and } \sigma_p \in C \} - \sum_{x < p \leq 2x} p^{-\lambda} \ll \frac{|C|}{|G|} \frac{x^{1-\lambda}}{\omega \log x} + \frac{\omega^{1/2} x^{\theta/2} \log d_L \log^3 x}{\omega^{1/2} x^{1/2} \theta/2} + \frac{|C|}{|G|} \frac{\alpha^{1/2} x^{(1+\theta)/2} \log^3 x (\log d_L + n_L \log x) \left( \omega^2 + \frac{\omega x^{1/2 - \theta - \lambda}}{\alpha^{1/2}} \right)}{\omega^{1/2} x^{1/2 - \theta - \lambda}}, \]
where \( \omega \geq 1 \) is a parameter at our disposal.

Setting \( \theta = 1/2, \alpha = 1 \) and \( \lambda = 1/4 - \epsilon \) for any \( \epsilon > 0 \), we obtain the following asymptotic result, in spirit of the Landau’s prime counting problem where the primes satisfy \( \{ \sqrt{p} \} < p^{-1/2} \) i.e. \( p - 1 \) is a perfect square.
Corollary 3. For a finite Galois extension $L/\mathbb{Q}$, assume that GRH holds for $\zeta_L(s)$. Then, for a fixed $\varepsilon > 0$

$$\# \{ x < p \leq 2x : \{ \sqrt{p} \} < p^{-1/4+\varepsilon} \text{ and } \sigma_p \in C \} - \sum_{x < p \leq 2x \atop \sigma_p \in C} p^{-1/4+\varepsilon}$$

$$\ll \frac{|C|}{|G|} x^{3/4+\varepsilon} + \omega x^{1/4} \log d_L \log^3 x + \frac{|C|}{|G|} \omega^2 x^{3/4} \log^3 x (\log d_L + n_L \log x).$$

Setting $\alpha = 1, \theta = 1/2, \text{ and } \delta_1 = 0$ in Theorem 1.1, one obtains the following (conditional) generalization of [Bal85] that investigates the distribution of fractional parts of $p^\theta$ with $p \equiv a \mod q$.

Corollary 4. Assume the notations and hypotheses as in Theorem 1.1. Then

$$\# \{ x < p \leq 2x : \{ \sqrt{p} \} < \delta \text{ and } \sigma_p \in C \} - \delta \pi_C(x, L)$$

$$\ll \frac{|C|}{|G|} \left( \left( \delta \omega n_L \right)^{1/2} x^{7/8} \log x + n_L \delta \omega x^{3/4} (\log x)^2 + \frac{\delta x}{\omega \log x} \right).$$

Theorem 1.1 is also of a similar flavour as some other interesting joint distribution theorems such as asymptotics for the number of Charmichael numbers composed of primes satisfying the Chebotarev condition studied in [BGY13]. In [AG15], an asymptotic estimate for the number of Piatetski-Shapiro primes up to $x$ satisfying the Chebotarev condition is derived.

Remark 3. One can also write versions of Theorems 1.1 and 1.3 for general extensions $L/K$ where $K$ is a finite extension of $\mathbb{Q}$ and $L$ is a normal extension of $K$ with Galois group $G = G(L/K)$. For a fixed conjugacy class $C$ of $G$, here one would count primes $p \in K$ of norm $N_{K/\mathbb{Q}}p \leq x$ which are unramified in $L$ such that the Artin symbol satisfies $[L/K]_p = C$ and simultaneously have the fractional part $\{ \alpha (N_{K/\mathbb{Q}}p)^\theta \}$ lying in the interval $[\delta_1, \delta_2)$ of length $\delta$. The main term would then be $\delta \pi_C(x, L/K)$ and the error terms can be shown to be as in Theorems 1.1 and 1.3.

The structure of this paper is as follows. We begin Section 2 with some preliminaries and then prove Theorem 1.2 assuming Theorem 1.1. In Section 3, we first prove Theorem 1.1 adapting the ideas of Balog [Bal83] and Lagarias-Odlyzko [LO77]. The proofs of Theorems 1.3 and Corollary 2 are also presented in the same section. Lastly, in Section 4, we provide details of the results needed in the proof of Theorem 1.1.

Acknowledgements: The authors are grateful to Chantal David for suggesting the problem and for many fruitful discussions related to the paper. The first author is supported by NSF Grant DMS-1854398.

2. Preliminaries and proof of Theorem 1.2

Let $N_E$ denote the conductor of the elliptic curve (without complex multiplication) over $\mathbb{Q}$. For a given prime $\ell$, let $E[\ell]$ denote the $\ell$-torsion points subgroup
of $E[\mathbb{Q}]$. It is known that the Galois representation
\[ \rho_{E,\ell} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{Aut}_{\mathbb{F}_\ell}(E[\ell]) \cong \text{GL}_2(\mathbb{F}_\ell) \]
is unramified at all primes $p \nmid N_{E,\ell}$. The field $\mathbb{Q}(E[\ell])$, obtained by adjoining the coordinates of all the $\ell$-torsion points of $E$ to $\mathbb{Q}$, is the fixed field in $\overline{\mathbb{Q}}$ of $\ker \rho_{E,\ell}$. Serre [Ser72] showed that for all but finitely many primes $\ell$, the representation $\rho_{E,\ell}$ is surjective. Thus, using $\rho_{E,\ell}$ we see that for all but finitely many primes $\ell$, the Galois group $G_\ell := \text{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q})$ is equal to $\text{GL}_2(\mathbb{F}_\ell)$. Moreover, the characteristic polynomial of $\rho_{E,\ell}(\sigma_p)$ is given by
\[ x^2 - a_p(E)x + p \pmod{\ell}. \]
That is, $a_p(E)$ is the trace of the Frobenius automorphism at $p$. Therefore, for $a \in \mathbb{F}_\ell$, if $C_\ell(a)$ denotes the union of conjugacy classes in $\text{GL}_2(\mathbb{F}_\ell)$ of elements of trace $a$ modulo $\ell$, then
\[ a_p(E) \equiv a \pmod{\ell} \iff \sigma_p \in C_\ell(a). \]

We now review the structure of conjugacy classes in $\text{GL}_2(\mathbb{F}_\ell)$ for an odd prime $\ell$. This is well known, see for example [FH91, Section 5.2] and is listed below for the convenience of the reader.

| Class representative | No. of classes | Size of class |
|----------------------|----------------|--------------|
| $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$, $\lambda \in \mathbb{F}_\ell^\times$ | $\ell - 1$ | 1 |
| $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$, $\lambda \in \mathbb{F}_\ell^\times$ | $\ell - 1$ | $\ell^2 - 1$ |
| $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$, $\lambda_1 \neq \lambda_2, \lambda_1, \lambda_2 \in \mathbb{F}_\ell^\times$ | $\frac{1}{2}(\ell - 1)(\ell - 2)$ | $\ell(\ell + 1)$ |
| $\begin{pmatrix} \alpha & D \beta \\ \beta & \alpha \end{pmatrix}$, $\alpha, \beta \in \mathbb{F}_\ell, \beta \neq 0, D$ is a fixed non-square in $\mathbb{F}_\ell^\times$ | $\frac{\ell}{2}(\ell - 1)$ | $\ell(\ell - 1)$ |

Therefore,
\[ \frac{|C_\ell(a)|}{|G_\ell|} = \begin{cases} \frac{\ell^2 - \ell - 1}{(\ell - 1)^2(\ell + 1)} & \text{for } a \neq 0 \\ \frac{\ell}{(\ell - 1)(\ell + 1)} & \text{for } a = 0 \end{cases} \quad (2.1) \]

Moreover, for $a \neq 0$, $C_\ell(a)$ is a union of $\ell$ conjugacy classes, while $C_\ell(0)$ is a union of $\ell - 1$ conjugacy classes. We use the following effective Chebotarev density theorem of Lagarias-Odlyzko [LO77] which is sufficient for our purposes.

**Theorem** ([LO77]). Let $L/K$ be a finite Galois extension of number fields with Galois group $G$ and $C$ be a conjugacy class in $G$. There exists an effectively
computable positive absolute constant $c_1$ such that if $\zeta_L(s)$ satisfies the GRH, then for every $x \geq 2$

$$\pi_C(x, L/K) - \frac{|C|}{|G|} \pi(x) \leq c_1 \frac{|C|}{|G|} x^{1/2} \log d_L x^\alpha + \log d_L. \quad (2.2)$$

We now prove Theorem 1.2.

**Proof.** For each residue $a \in \{0, 1, \ldots, \ell - 1\}$, we have

$$[2\sqrt{p}] \equiv a \mod \ell \iff \left\{ \frac{2\sqrt{p}}{\ell} \right\} \in \left[ \frac{a}{\ell}, \frac{a + 1}{\ell} \right)$$

and

$$a_p(E) \equiv a \mod \ell \iff \sigma_p \in C_{\ell}(a) \subseteq G_{\ell}.$$ 

Therefore, by Theorem 1.1 with $\theta = 1/2$, $\alpha = 2/\ell$, and $\delta = 1/\ell$, we conclude

$$\# \{ p \leq x : a_p(E) \equiv [2\sqrt{p}] \equiv a \mod \ell \} = \frac{x}{\ell \log x} + O \left( \frac{x^{7/8} \log x}{\omega \ell^2 \log x} \right).$$

This gives us,

$$\# \{ p \leq x : a_p(E) \equiv [2\sqrt{p}] \mod \ell \}
= \sum_{a \mod \ell} \# \left\{ p \leq x : \sigma_p \in C_{\ell}(a) \text{ and } \left\{ \frac{2\sqrt{p}}{\ell} \right\} \in \left[ \frac{a}{\ell}, \frac{a + 1}{\ell} \right) \right\}
= \sum_{a \mod \ell} \frac{1}{\ell} \pi_{C_{\ell}(a)}(x, Q(E[\ell])) + O \left( x^{7/8} \ell^{1/4} \log x + \frac{x}{\omega \ell^2 \log x} \right)
= \pi_{C_{\ell}(a)}(x, Q(E[\ell])) + O \left( \omega^{1/2} \ell^{5/4} x^{7/8} \log x + \frac{x}{\omega \ell \log x} \right),$$

where we have used (2.1) and (2.2) to compute $\pi_{C_{\ell}(a)}(x, Q(E[\ell]))$. \hfill $\square$

3. **The Joint Distribution Theorem and Some Applications**

**Remark.** In what follows, we may assume that the parameters $\alpha$ and $\theta$ satisfy $\alpha x^\theta \geq 1$ since for $\alpha x^\theta < 1$, $\alpha x^\theta = \{\alpha x^\theta\} \in [\delta_1, \delta_2]$, and therefore the desired quantity can be computed using the Prime Number Theorem.

3.1. **Proof of Theorem 1.1**

**Proof.** To start with, we write the fractional part condition as follows:

$$[\alpha p^\theta - \delta_1] - [\alpha p^\theta - \delta_2] = \begin{cases} 1 & \text{if } \delta_1 \leq \{\alpha p^\theta\} < \delta_2; \\ 0 & \text{otherwise.} \end{cases}$$

First, we obtain the result when $x_j < p \leq x_{j+1}$ for $x_j := \lfloor x(1 + j/B) \rfloor + 1/2$ for $j = 0, \ldots, B$ and $B = \lfloor \omega \rfloor$. Summing over $j$ then establishes the result for $x < p \leq 2x$. 7
With $\delta = \delta_2 - \delta_1$, the length of the interval, we set
\[
U_- := \frac{\alpha x_j^\theta}{\delta}, \quad U_+ := \frac{\alpha x_{j+1}^\theta}{\delta}.
\]
Then for $x_j < p \leq x_{j+1}$, we have
\[
\alpha p^\theta \left( 1 - \frac{1}{U_-} \right) - \delta_1 \leq \alpha p^\theta - \delta_2 \leq \alpha p^\theta \left( 1 - \frac{1}{U_+} \right) - \delta_1.
\]
Note that we are interested in the sum
\[
S := \sum_{x_j < p \leq x_{j+1}} [\alpha p^\theta - \delta_1] - [\alpha p^\theta - \delta_2]
\]
in order to bound the number of primes $x_j < p \leq x_{j+1}$ such that $\sigma_p \in C$ and $\delta_1 \leq \{\alpha p^\theta\} < \delta_2$. This implies
\[
S \geq \sum_{x_j < p \leq x_{j+1}} [\alpha p^\theta - \delta_1] - [\alpha p^\theta \left( 1 - \frac{1}{U_+} \right) - \delta_1]
\]
and
\[
S \leq \sum_{x_j < p \leq x_{j+1}} [\alpha p^\theta - \delta_1] - [\alpha p^\theta \left( 1 - \frac{1}{U_-} \right) - \delta_1].
\]
Therefore, using
\[
\frac{\alpha p^\theta}{U_\pm} = \delta + O \left( \frac{\delta}{\omega} \right),
\]
in order to obtain the claimed asymptotics for $S$, it suffices to prove
\[
\sum_{x_j < p \leq x_{j+1}} [\alpha p^\theta - \delta_1] - [\alpha p^\theta \left( 1 - \frac{1}{U_\pm} \right) - \delta_1] - \frac{\alpha p^\theta}{U_\pm}
\]
\[
\ll \frac{|C|}{|G|} \log x \left( (\delta n_L/\omega)^{1/2} \alpha^{1/4} x^{(3+\theta)/4} + \frac{\delta n_L}{\alpha^{1/2}} x^{1-\theta/2} \log x \right)
\]
\[
+ (\delta n_L/\omega)^{1/2} \alpha^{1/4} x^{(1+\theta)/4} \log x.
\]
We may write the summand
\[
[\alpha p^\theta - \delta_1] - [\alpha p^\theta \left( 1 - \frac{1}{U_\pm} \right) - \delta_1] = \sum_{m \leq \alpha p^\theta - \delta_1} 1 - \sum_{m \leq \alpha p^\theta \left( 1 - \frac{1}{U_\pm} \right) - \delta_1} 1. \tag{3.2}
\]
Define the sequence $(a_m)_{m \in \mathbb{N}}$
\[
a_m := \begin{cases} 
1 & \text{if } \frac{1}{3} \alpha x^\theta - \delta_1 < m \leq 3 \alpha x^\theta - \delta_1 \\
0 & \text{otherwise}.
\end{cases}
\]
Set
\[
A_{\delta_1}(M) := \sum_{m \leq M - \delta_1} a_m = \sum_{m \geq 1} a_m f \left( \frac{m + \delta_1}{M} \right)
\]
where
\[ f(y) = \begin{cases} 
1 & \text{if } 0 < y < 1 \\
1/2 & \text{if } y = 1 \\
0 & \text{if } y > 1 
\end{cases} \]

Using the inverse Mellin transform, for \( \sigma > 0 \), we write
\[ f(y) = \frac{1}{2\pi i} \int_{\sigma-i\infty}^{\sigma+i\infty} \frac{y^{-s}}{s} \, ds. \]

For \( y = (m + \delta_1)/M \), this gives
\[ A_{\delta_1}(M) = \frac{1}{2\pi i} \int_{\sigma-i\infty}^{\sigma+i\infty} \sum_{m \geq 1} \frac{a_m}{(m + \delta_1)^s} \frac{M^s}{s} \, dx. \] (3.3)

Thus, using the definition of the sequence \( (a_m) \), we rewrite (3.2) as
\[
\left[ \alpha p^\theta - \delta_1 \right] - \left[ \alpha p^\theta \left( 1 - \frac{1}{U_{\pm}} \right) - \delta_1 \right] = \sum_{m \leq \alpha p^\theta - \delta_1} a_m - \sum_{m \leq (\alpha p^\theta) \left( 1 - \frac{1}{U_{\pm}} \right) - \delta_1} a_m
\]
\[ = A_{\delta_1}(\alpha p^\theta) - A_{\delta_1} \left( \alpha p^\theta \left( 1 - \frac{1}{U_{\pm}} \right) \right). \]

In order to estimate the integrals \( A_{\delta_1}(\alpha p^\theta) \) and \( A_{\delta_1}(\alpha p^\theta \left( 1 - \frac{1}{U_{\pm}} \right)) \), given by (3.3), we make use of the truncated Perron’s formula [Tit86, Lemma 3.12], and obtain
\[
\left[ \alpha p^\theta - \delta_1 \right] - \left[ \alpha p^\theta \left( 1 - \frac{1}{U_{\pm}} \right) - \delta_1 \right] = \frac{1}{2\pi i} \int_{1/2-iT_1}^{1/2+iT_1} L(s)H(s) \, p^{\theta s} \, ds + O \left( \sum_{\frac{1}{4} \alpha x^\theta < m + \delta_1 \leq 3 \alpha x^\theta} \min \left\{ 1, T_1^{-1} \left| \log \frac{\alpha p^\theta}{m + \delta_1} \right|^{-1} \right\} \right)
\]
\[ + O \left( \sum_{\frac{1}{4} \alpha x^\theta < m + \delta_1 \leq 3 \alpha x^\theta} \min \left\{ 1, T_1^{-1} \left| \log \frac{\alpha p^\theta}{m + \delta_1} \left( 1 - \frac{1}{U_{\pm}} \right)^{-1} \right|^{-1} \right\} \right)
\]
\[ = \frac{1}{2\pi i} \int_{1/2-iT_1}^{1/2+iT_1} L(s)H(s)p^{\theta s} \, ds + O \left( \frac{\alpha x^\theta}{T_1} \log(\alpha x^\theta) \right), \]

where
\[ H(s) := \frac{1}{s} \left( 1 - \left( 1 - \frac{1}{U_{\pm}} \right)^s \right) \ll \frac{1}{U_{\pm}} \]
and
\[ L(s) := \alpha^s \sum_{\frac{1}{4} \alpha x^\theta - \delta_1 < m \leq 3 \alpha x^\theta - \delta_1} \frac{1}{(m + \delta_1)^s}. \]
Summing over the primes, we find

\[
\sum_{x_j < p \leq x_{j+1} \atop \sigma_p \in \mathcal{C}} \left( \left[ \alpha p^\theta - \delta_1 \right] - \left[ \alpha p^\theta \left( 1 - \frac{1}{U_\pm} \right) - \delta_1 \right] \right)
\]

\[
= \frac{1}{2\pi i} \int_{1/2-iT_1}^{1/2+iT_1} L(s) H(s) F(-\theta s) \, ds + O \left( \frac{\alpha x^\theta}{T_1} \log(\alpha x^\theta) \pi_C(x_j, L) \right) \tag{3.4}
\]

where

\[
F(s) := \sum_{x_j < p \leq x_{j+1} \atop \sigma_p \in \mathcal{C}} p^{-s} \quad \text{and} \quad \pi_C(x_j, L) := \sum_{x_j < p \leq x_{j+1} \atop \sigma_p \in \mathcal{C}} 1.
\]

First, we compute the above integral in the smaller range, up to \( T_0 := \alpha x^\theta \).

Observe that in the range \( |t| \leq T_0 \), we have

\[
H(s) = \frac{1}{U_\pm} + O \left( \frac{|s - 1|}{U_\pm^2} \right)
\]

and

\[
L(s) = \alpha^s \left( 3\alpha x^\theta \right)^{1-s} - \left( \frac{\alpha x^\theta}{3} \right)^{1-s} \frac{1}{1-s} + O \left( x^{-\theta \Re(s)} \right)
\]

Therefore, for the integral in (3.4) in the range \( |t| \leq T_0 \), we have

\[
\frac{1}{2\pi i} \int_{1/2-iT_0}^{1/2+iT_0} L(s) H(s) F(-\theta s) \, ds
\]

\[
= \frac{1}{U_\pm} \sum_{x_j < p \leq x_{j+1} \atop \sigma_p \in \mathcal{C}} \alpha p^\theta \frac{1}{2\pi i} \int_{1/2-iT_0}^{1/2+iT_0} \left( \alpha p^\theta s^{-1} \left( 3\alpha x^\theta \right)^{1-s} - \left( \frac{\alpha x^\theta}{3} \right)^{1-s} \right) \frac{1}{1-s} \, ds \tag{3.5}
\]

\[
+ O \left( \frac{\delta}{\alpha} x^{-3\theta/2} \int_{-T_0}^{T_0} |F(-\theta/2 - i\theta t)| \, dt \right).
\]  \( \tag{3.6} \)

Using Cauchy-Schwarz inequality, the error term (3.6) is bounded by

\[
\ll \frac{\delta}{\alpha} x^{-3\theta/2} T_0^{1/2} \left( \int_{-T_0}^{T_0} |F(-\theta/2 - i\theta t)|^2 \, dt \right)^{1/2}. \tag{3.7}
\]

Also, by applying the mean value theorem for Dirichlet polynomials, we have

\[
\int_{-T_0}^{T_0} |F(-\theta/2 - i\theta t)|^2 \, dt \ll x^\theta \pi_C(x_j, L) \left( T_0 + x/\omega \right).
\]

Inserting this estimate in (3.7), the error term (3.6) is bounded by

\[
\ll \delta T_0^{1/2} \left( \alpha x^\theta \right)^{-1} \pi_C(x_j, L)^{1/2} \left( T_0^{1/2} + x^{1/2}/\omega^{1/2} \right)
\]

\[
\ll \delta \pi_C(x_j, L)^{1/2} \left( 1 + x^{(1-\theta)/2} \left( \alpha \omega \right)^{-1/2} \right), \tag{3.8}
\]
using $T_0 = \alpha x^\theta$. We now compute the integral in (3.5) to obtain the desired main term. The change of variable $w = 1 - s$ yields

$$
\frac{1}{U_{\pm}} \sum_{x_j < p \leq x_{j+1}} \alpha p^\theta \int_{1/2-iT_0}^{1/2+iT_0} \frac{1}{w} \left( \left( \frac{3x^\theta}{p^\theta} \right)^w - \left( \frac{x^\theta}{3p^\theta} \right)^w \right) \, dw.
$$

By Perron’s formula, for all values $x_j < p \leq x_{j+1},$

$$
\frac{1}{2\pi i} \int_{1/2-iT_0}^{1/2+iT_0} \frac{1}{w} \left( \left( \frac{3x^\theta}{p^\theta} \right)^w - \left( \frac{x^\theta}{3p^\theta} \right)^w \right) \, dw = 1 + O \left( \frac{1}{T_0^2} \right).
$$

Therefore (3.5) becomes

$$
\sum_{x_j < p \leq x_{j+1}} \alpha p^\theta \frac{1}{U_{\pm}} + O \left( \frac{1}{T_0 U_{\pm}} \sum_{x_j < p \leq x_{j+1}} \alpha p^\theta \right). \tag{3.9}
$$

Using $T_0 = \alpha x^\theta$ and collecting the terms from (3.4), (3.8) and (3.9), we obtain

$$
\sum_{x_j < p \leq x_{j+1}} \left( [\alpha p^\theta - \delta_1] - [\alpha p^\theta \left( 1 - \frac{1}{U_{\pm}} \right) - \delta_1] - \frac{\alpha p^\theta}{U_{\pm}} \right)
$$

$$
\ll \delta \pi C(x_j, L)^{1/2} \left( 1 + \frac{x^{(1-\theta)/2}}{(\alpha \omega)^{1/2}} \right) + \frac{\delta}{\alpha x^\theta} \pi C(x_j, L)
$$

$$
+ \frac{\alpha x^\theta}{T_1} \log(\alpha x^\theta) \pi C(x_j, L) + \frac{1}{U_{\pm}} \int_{T_0}^{T_1} |L(1/2 + it)||F(-\theta/2 - i\theta t)| \, dt \tag{3.10}
$$

In order to estimate the integral in the error term above, we use dyadic division, and bound the following integrals

$$
\frac{1}{2\pi i} \int_{1/2+iT'}^{1/2+i2T'} L(s)H(s)F(-s) \, ds \ll \frac{1}{U_{\pm}} \int_{T'}^{2T'} |L(1/2 + it)||F(-\theta/2 - i\theta t)| \, dt
$$

for $T_0 \leq T' \leq T_1/2$ using Cauchy-Schwarz inequality. This is obtained by obtaining the following uniform bound for $T' \leq \tau \leq 2T'$ and $[x_j, x_{j+1}] \subseteq [x, 2x]$ established in Proposition 4.2 for $K = \mathbb{Q}$

$$
F(-\theta/2 - i\theta \tau) \ll x^{\theta/2} \left( \log d_L + b + \frac{bx \log x}{T'} \right)
$$

$$
+ \frac{|C|}{|G|} x^{(1+\theta)/2} \left( \log d_L + n_L \log T' \right) \left( \log \frac{T'}{\log x} + x^{1/2} \right);
$$

and the mean value estimate below given by Lemma 4.1

$$
\int_{T'}^{2T'} |L(1/2 + it)|^2 \, dt \ll \alpha T' + \alpha^2 x^\theta (\log \alpha x^\theta).
$$
This gives us
\[
\int_{T'}^{2T'} |L(1/2 + it)||F(-\theta/2 - i\theta t)| \, dt \\
\ll (\alpha T'^2 + \alpha^2 x^\theta T' (\log \alpha x^\theta))^{1/2} \left\{ x^{\theta/2} \left( \log d_L + b + bx \frac{\log x}{T'} \right) \\
+ \frac{|C|}{|G|} x^{(1+\theta)/2} \left( \log d_L + n_L \log T' \right) \left( \frac{\log T'}{\log x} + \frac{x^{1/2}}{T'} \right) \right\}
\]
\[
\ll x^{\theta/2} (\log d_L + b) \left( \alpha T'^2 + \alpha^2 T' x^\theta \log (\alpha x^\theta) \right)^{1/2} \\
+ bx^{1+\theta/2} \log x \left( \alpha + \alpha^2 T'^{-1} x^\theta \log (\alpha x^\theta) \right)^{1/2} \\
+ \frac{|C|}{|G|} x^{(1+\theta)/2} (\log d_L + n_L \log T') \\
\left( \left( \alpha T'^2 + \alpha^2 T' x^\theta \log (\alpha x^\theta) \right)^{1/2} \frac{\log T'}{\log x} + \left( \alpha + \alpha^2 T'^{-1} x^\theta \log (\alpha x^\theta) \right)^{1/2} x^{1/2} \right).
\]

Recall that \( U_\pm \ll \frac{\alpha x^\theta}{\delta} \), \( \alpha x^\theta \leq T' < T_1 \), and \( \alpha x^\theta \log (\alpha x^\theta) < \delta T_1 \). Therefore,
\[
\frac{1}{U_\pm} \int_{T'}^{2T'} |L(1/2 + it)||F(-\theta/2 - i\theta t)| \, dt \\
\ll \frac{\delta}{(\alpha x^\theta)^{1/2}} \left\{ \frac{|C|}{|G|} x^{1/2} (\log d_L + n_L \log T_1) \left( T_1 \frac{\log T_1}{\log x} + x^{1/2} \right) \\
+ T_1 (\log d_L + b) + bx \log x \right\}.
\]

We now set
\[
T_1 = \frac{\alpha^{3/4}}{(n_L \delta \omega)^{1/2} \log x} x^{(1+\theta)/4}. 
\] (3.11)

Note that \( \log T_1 < \log x \) since we have assumed \( \alpha^{1/4}(\omega n_L/\delta)^{1/2}(\log x)^2 < x^{(1-\theta)/4} \). Thus, using \( \log d_L \ll n_L \log n_L \) (which follows from the discussion in Serre\cite{Ser72} Section I.3)), we conclude
\[
\frac{1}{U_\pm} \int_{T'}^{2T'} |L(1/2 + it)||F(-\theta/2 - i\theta t)| \, dt < (\delta n_L/\omega)^{1/2} x^{1/4} x^{(1+\theta)/4} \\
+ \frac{|C|}{|G|} \left( (\delta n_L/\omega)^{1/2} x^{3/4+\theta/4} + \frac{\delta n_L}{\alpha^{1/2} x^{1-\theta/2}} \log x \right).
\]

Given the value of \( T_1 \), since we use dyadic division of the interval \([T_0, T_1]\), the number of integrals that we need to add is \( O(\log x) \). With this, inserting the
above estimate in (3.10) gives us
\[
\sum_{x_j < p \leq x_{j+1}} \left( [\alpha p^\theta - \delta_1] - \left[ \alpha p^\theta \left( 1 - \frac{1}{U_\pm} \right) - \delta_1 \right] - \frac{\alpha p^\theta}{U_\pm} \right)
\]
\[\ll \delta \pi C(x_j, L)^{1/2} \left( 1 + \frac{x^{(1-\theta)/2}}{(\alpha \omega)^{1/2}} \right) + \delta \pi C(x_j, L) \]
\[+ \left| \frac{C}{G} \right| \log x \left( (\delta n_L / \omega)^{1/2} \alpha^{1/4} x^{(3+\theta)/4} + \frac{\delta n_L}{\alpha^{1/2} x^{1-\theta/2}} \log x \right) \]
\[+ (\delta n_L / \omega)^{1/2} \alpha^{1/4} x^{(1+\theta)/4} \log x. \tag{3.12} \]
Note that the error terms in (3.12) can be absorbed into (3.13). Invoking (3.1), this completes the proof of Theorem 1.1. \hfill \Box

3.2. Proof of Theorem 1.3. Since the proof is quite similar to that of Theorem 1.1, we point out only the main differences below and omit the details.

Proof. We proceed as in the proof of Theorem 1.1 with \( \delta_1 = 0, \quad \delta_2 = p^{-\lambda} \).

Note that in this case \( \delta = p^{-\lambda} \leq x_j^{-\lambda} \) and hence we can eliminate \( \delta \) from the error terms. We follow the proof above until (3.11) and choose \( T_1 = \alpha \omega x_j^{\theta+\lambda} \log x. \)

Following the reasoning after (3.11) in the proof of Theorem 1.1 with the above value of \( T_1 \), we obtain the asymptotics when \( x_j < p \leq x_{j+1} \). Lastly, summing over \( j \) gives the desired result claimed in Theorem 1.3. \hfill \Box

3.3. Proof of Corollary 2. We show
\[
\# \left\{ x < p \leq 2x : \sigma_p \in C_0 \text{ and } \left[ \frac{2 \sqrt{p}}{\ell} \right] \in \left[ 0, \frac{1}{\ell} \right] \right\} = \frac{x}{\ell^2 \log x} + O \left( \frac{x^{7/8}}{\ell^{1/4} \log x} \right),
\]
where \( C_0 \) denotes the union of conjugacy classes of trace zero in \( \text{Gal}(L/\mathbb{Q}) = \text{GL}_2(\mathbb{F}_\ell) \).

Before giving the proof, we first fix some notations. For a group \( G \) and \( C \subset G \), let \( \delta_C : G \to \{0,1\} \) denote the class function such that \( \delta_C(g) = 1 \) if and only if \( g \in C \). Then,
\[
\pi_C(x, L) = \sum_{p \text{ prime} \atop p \text{ unramified in } L \atop x < p \leq 2x} \delta_C(\sigma_p).
\]
Let
\[
\Phi_{C, [\delta_1, \delta_2]}(x, L, \alpha) := \sum_{p \text{ prime} \atop p \text{ unramified in } L \atop x < p \leq 2x \atop \delta_1 \leq (\alpha p^\theta) < \delta_2} \delta_C(\sigma_p).
\]
We now define an analogue of these functions that include contributions from ramified primes as well. Let $D_p$ and $I_p$ denote the decomposition and inertia subgroups of $G$, respectively at a chosen prime ideal $p$ lying above $p$. Consider $\text{Frob}_p \in D_p/I_p$, the Frobenius element at $p$. Then, for each integer $m \geq 1$, we define

$$
\delta_C(\sigma_p^m) := \frac{1}{|I_p|} \sum_{g \in D_p \mid I_p = \text{Frob}_p \in D_p/I_p} \delta_C(g).
$$

Note that $\delta_C(\sigma_p^m)$ is independent of the choice of $p$ and the above definition agrees with the usual definition of $\delta_C(\sigma_p^m)$ for primes $p$ that are unramified in $L$. Define

$$
\tilde{\pi}_C(x, L) := \sum_{p \text{ prime}, m \geq 1 \atop x < p^m \leq 2x} \frac{\delta_C(\sigma_p^m)}{m}
$$

and

$$
\tilde{\Phi}_{C, [\delta_1, \delta_2]}(x, L, \alpha) := \sum_{p \text{ prime}, m \geq 1 \atop x < p^m \leq 2x \atop \delta_1 \leq \{\alpha p^m\} < \delta_2} \frac{\delta_C(\sigma_p^m)}{m}.
$$

With these notations, we state two lemmas from [Zyw15] to be used later, and we state them for our case when the base field is $Q$.

**Lemma 3.1.** ([Zyw15] Lemma 2.7) For any subset $C$ of $G$ stable under conjugation,

$$
\tilde{\pi}_C(x, L) = \pi_C(x, L) + O\left(\frac{x^{1/2}}{\log x} + \log d_L\right). \tag{3.14}
$$

The following result follows from Proposition 8 of [Ser72].

**Lemma 3.2.** ([Zyw15] Lemma 2.6 (ii)) Let $N$ be a normal subgroup of $G$ and let $C$ be a subset of $G$ stable under conjugation that satisfies $NC \subseteq C$. Then

$$
\tilde{\pi}_C(x, L) = \tilde{\pi}_{C'}(x, L^N),
$$

where $C'$ is the image of $C$ in $G/N = \text{Gal}(L^N/Q)$.

We are now ready to prove Corollary 2.

**Proof.** Consider the extension $L/\mathbb{Q}$ with $L = \mathbb{Q}(E[\ell])$. Observe that $C_0$ is stable under multiplication by $H_\ell$, the subgroup of scalar matrices in $\text{GL}_2(\mathbb{F}_\ell)$. Moreover, it is the inverse image of $C'_0$, the subset of order two elements in $G'_\ell := G_\ell/H_\ell = \text{PGL}_2(\mathbb{F}_\ell)$. Applying Lemma 2 we obtain

$$
\tilde{\pi}_{C_0}(x, L) = \tilde{\pi}_{C'_0}(x, L^{H_\ell}).
$$
Therefore, using (3.14)

\[
\# \left\{ x < p \leq 2x : \sigma_p \in C_0, p \text{ unramified and } \left\{ \frac{2\sqrt{p}}{\ell} \right\} \in \left[ 0, \frac{1}{\ell} \right) \right\} 
= \Phi_{C_0,[0,\frac{1}{\ell}]}(x, L, \frac{2}{\ell})
= \Phi_{C_0,[0,\frac{1}{\ell}]}(x, L, \frac{2}{\ell}) + O \left( \frac{x^{1/2}}{\log x} + \log d_L \right)
= \Phi_{C_0,[0,\frac{1}{\ell}]}(x, LH_t, \frac{2}{\ell}) + O \left( \frac{x^{1/2}}{\log x} + \log d_L \right)
= \Phi_{C_0,[0,\frac{1}{\ell}]}(x, LH_t, \frac{2}{\ell}) + O \left( \frac{x^{1/2}}{\log x} + \log d_L \right).
\]

Using Theorem 1.1 and Chebotarev density theorem to the sub-extension \( L_{H_t}/\mathbb{Q} \),

\[
\Phi_{C_0,[0,\frac{1}{\ell}]}(x, LH_t, \frac{2}{\ell}) + O \left( \frac{x^{1/2}}{\log x} + \log d_L \right)
= \frac{\pi_{C_0}(x, LH_t)}{\ell} + O \left( \frac{x}{\ell^2 \omega \log x} + \omega^{1/2} \frac{x^{7/8}}{\ell^{1/4}} \log x + \omega \ell^{3/2} x^{3/4} (\log x)^2 \right)
= \frac{\pi(x)}{\ell^2} + O \left( \frac{x}{\ell^2 \omega \log x} + \omega^{1/2} \frac{x^{7/8}}{\ell^{1/4}} \log x + \omega \ell^{3/2} x^{3/4} (\log x)^2 \right)
\]

noting that \( \log d_L \ll [L_{H_t} : \mathbb{Q}] \ll \ell^3 \) and \( \ell \ll x^{1/4} \omega^{-2/7} \log^{-8/7} x \). This completes the proof. \( \square \)

4. Proofs of intermediate results

4.1. Mean value estimation of \( L(1/2 + it) \).

**Lemma 4.1.**
\[
\int_{T'}^{2T'} |L(1/2 + it)|^2 \, dt \ll \alpha T' + \alpha^2 x^\theta \log(x\alpha^\theta).
\]

**Proof.** We have
\[
\int_{T'}^{2T'} |L(1/2 + it)|^2 \, dt = \alpha \int_{T'}^{2T'} \left| \sum_{m + \delta_1 < \alpha \theta / 3 - \delta_1 < m \leq 3\alpha \theta - \delta_1} (m + \delta_1)^{-1/2-it} \right|^2 \, dt
= \alpha \int_{T'}^{2T'} \sum_{\alpha \theta / 3 - \delta_1 < m \leq 3\alpha \theta - \delta_1} (m + \delta_1)^{-1} + \sum_{\alpha \theta / 3 - \delta_1 < k \neq m \leq 3\alpha \theta - \delta_1} \frac{(k + \delta_1)^{-1/2-it}}{(m + \delta_1)^{1/2-it}} \, dt
= \sum_{\alpha \theta / 3 - \delta_1 < m \leq 3\alpha \theta - \delta_1} \frac{\alpha T'}{(m + \delta_1)} + O \left( \sum_{\alpha \theta / 3 - \delta_1 < m \leq 3\alpha \theta - \delta_1} \frac{\alpha((m + \delta_1)(k + \delta_1))^{-1/2}}{\log((m + \delta_1)/(k + \delta_1))} \right).
\]
Using $\delta_1 < \alpha x^\theta / 3$ and rewriting the sum in the error term, we obtain

$$
\sum_{\alpha x^\theta / 3 - \delta_1 < m \leq 3 \alpha x^\theta - \delta_1} (m + \delta_1)^{\alpha / 2} \frac{\alpha}{(m + \delta_1) \sqrt{1 - r/(m + \delta_1) \log (1 - r/(m + \delta_1))}} 
\ll \sum_{\alpha x^\theta / 3 - \delta_1 < m \leq 3 \alpha x^\theta - \delta_1} \frac{\alpha}{r} \ll \alpha^2 x^\theta \log (\alpha x^\theta).
$$

This gives us

$$
\int_{T'}^{2T'} |L(1/2 + it)|^2 dt = \alpha T' \sum_{\alpha x^\theta / 3 - \delta_1 < m \leq 3 \alpha x^\theta - \delta_1} (m + \delta_1)^{-1} + O \left( \alpha^2 x^\theta \log (\alpha x^\theta) \right)
\ll \alpha T' + \alpha^2 x^\theta \log (\alpha x^\theta).
$$

This completes the proof of the lemma. □

4.2. Estimation of $F(-\theta/2 - i\theta t)$. For each sub-interval $[x_j, x_{j+1}] \subset [x, 2x]$ we prove the following.

**Proposition 4.2.** Let $\theta \in [0, 1]$ be fixed. Given a Galois extension of number fields $L$ over $K$, and $C$ being a union of $b$ conjugacy class in $\text{Gal}(L/K)$, define

$$
F(-\theta/2 - i\theta t) = \sum_{\sigma_p \in C} (Np)^{\theta/2 + i\theta t}.
$$

Assume the Riemann Hypothesis for the Dedekind zeta function of the field extension $L/K$. Then

$$
F(-\theta/2 - i\theta t) \ll \frac{|C|}{|G|} x^{(1+\theta)/2} (\log d_L + n_L \log T') \left( \frac{\log T'}{\log x} + \frac{x^{1/2}}{T'} \right)
+x^{\theta/2} \left( \log d_L + bn_K + bn_K \frac{x \log x}{T'} \right)
$$

uniformly for $0 < T' \leq \tau \leq 2T'$.

The proof follows along the same lines as in [LO77]. The function $F(-\theta/2 - i\theta t)$ here is similar to that of $\pi_C(x, L/K)$ in [LO77], the main difference being a shift in the complex variable $s = \sigma + it$ by $\theta/2 + i\theta t$. While the shift in the real part by $\theta/2$ results in a factor of $x^{\theta/2}$ tagging along with the error terms obtained in [LO77], the shift in the imaginary part is where the saving is obtained. To be precise, we choose a contour that is a box which avoids the real axis, therefore the only poles in the interior are the non-trivial zeros of $L(s, \chi, L/E)$, and a pole at $-\theta/2 - i\theta t$. In particular, the residue from the pole at $s = 1$ that makes up the main term in the proof by Lagarias-Odlyzko [LO77] does not appear here, giving us a power saving under GRH.

We now provide details of the proof.
Proof. We first consider the function

$$
\Psi_C(-\theta/2 - i\theta \tau) := \sum_{Np^m \in (x_j, x_{j+1}] \atop p: \text{unramified}} \frac{\log Np}{Np^{m(-\theta/2 - i\theta \tau)}}
$$

for a single conjugacy class $C$ where $\Lambda$ denotes the von-Mangoldt function. We use partial summation to pass on to the bounds for $F(-\theta/2 - i\theta \tau)$. As in [LO77], in order to use Hecke $L$-functions, we need to consider the ramified primes as well, (which are later removed). For $\Re s > 1$, let

$$Z(s) := -\frac{|C|}{|G|} \sum_{\chi} \hat{\chi}(g) \frac{L'}{L}(s, \chi, L/E), \quad (4.1)$$

where $\chi$ runs over the irreducible characters of $H = Gal(L/E)$ and $E$ is the fixed field of $H$, the cyclic subgroup of $G$ generated by a chosen element $g \in C$. Note that

$$Z(s) = \sum_{p, m} \Theta(p^m) \log(Np)(Np)^{-ms}$$

where for an unramified prime $p \subseteq \mathcal{O}_K$,

$$\Theta(p^m) = \begin{cases} 1 & \text{if } \left(\frac{L/K}{p}\right)^m = C \\ 0 & \text{otherwise} \end{cases}$$

and $|\Theta(p^m)| \leq 1$ if $p$ ramifies in $L$. We use Perron’s formula to estimate $F(-\theta/2 - i\theta \tau)$ by considering partial sums of $Z(s)$, which include the ramified primes as well. Define

$$I(x_j, T) := I_C(x_j, T, \theta, \tau) = \frac{1}{2\pi i} \int_{\sigma_0 - iT}^{\sigma_0 + iT} Z(s - \theta/2 - i\theta \tau) \frac{x_j^{s+1} - x_j^s}{s} ds \quad (4.2)$$

where $T = \theta T'/2$ and $\sigma_0 = 1 + \theta/2 + 1/\log x$. Then,

$$|\Psi_C(-\theta/2 - i\theta \tau) - I(x_j, T)| \leq \left| I(x_j, T) - \sum_{p, m} \frac{\Theta(p^m) \log(Np)}{(Np)^{m(-\theta/2 - i\theta \tau)}} \right| + \sum_{p, m} \frac{\Theta(p^m) \log(Np)}{(Np)^{m(-\theta/2 - i\theta \tau)}}. \quad (4.3)$$
The two terms on the right hand side of the above equation are now estimated. Using Lemma 3.1 of [LO77], we have,

\[
\left| I(x_j, T) - \sum_{p, m \mid N p \leq x_j} \frac{\Theta(p^m) \log(N p)}{(N p)^{\nu - \theta/2 - i\theta \tau}} \right| \\
\leq \sum_{N p^m = x_j + 1 \text{ or } N p^m = x_j} \left( \frac{\log N p}{(N p)^{\nu - \theta/2}} \right) \\
+ \sum_{N p^m \neq x_j} \left( \frac{x_j}{N p^m} \right)^{\nu} \min \left( 1, T^{-1} \left| \frac{x_j}{N p^m} \right|^{-1} \right) \left( \frac{\log N p}{(N p)^{\nu - \theta/2}} \right)
\]

Following arguments from [LO77] to estimate the terms on the right side of the above inequality, and noting that \( x_j \leq 2x \) for each \( j = 0, \ldots, B \), we get

\[
I(x_j, T) - \sum_{x_j < N p \leq x_{j+1}} \frac{\Theta(p^m) \log(N p)}{(N p)^{\nu - \theta/2 - i\theta \tau}} \ll x^{\theta/2} n_K \log x + n_K \frac{\sigma_0}{T} + n_K x^{1+\theta/2} \log^2 x.
\]

Moreover,

\[
\sum_{x_j < N p \leq x_{j+1}} \frac{\Theta(p^m) \log(N p)}{(N p)^{\nu - \theta/2 - i\theta \tau}} \ll x^{\theta/2} \log x \log d_L.
\]

Putting (4.4) and (4.5) together in (4.3), we see that

\[
\Psi_C(-\theta/2 - i\theta \tau) = I(x_j, T) + O \left( x^{\theta/2} \log x \left( \log d_L + n_K + \frac{n_K x \log x}{T} \right) \right).
\]

Next, we estimate \( I(x_j, T) \). From (4.2) and (4.1), we have

\[
I(x_j, T) = -\frac{|C|}{|G|} \sum_{\chi} \tilde{\chi}(g) \frac{1}{2\pi i} \int_{\sigma_0 - iT}^{\sigma_0 + iT} \frac{L'}{L}(s - \theta/2 - i\theta \tau, \chi, L/E) \frac{x_j^{s+1} - x_j^s}{s} ds,
\]

where \( \chi \) runs through irreducible characters of \( H = \langle g \rangle \), \( T' \leq \tau \leq 2T' \) is fixed, and \( T = \theta T'/2 \). We make the change of variable \( s \leftrightarrow s - \frac{\theta}{2} - i\theta \tau \) to rewrite

\[
I(x_j, T) = -\frac{|C|}{|G|} \sum_{\chi} \tilde{\chi}(g) \frac{1}{2\pi i} \int_{1+\frac{\theta}{2} - iT - i\theta \tau}^{1+\frac{\theta}{2} + iT - i\theta \tau} \frac{L'}{L}(s, \chi, L/E) \frac{x_j^{s+1} - x_j^s}{s} ds.
\]
Abbreviating \( \frac{L'(s, \chi, L/E)}{L(s, \chi)} \) by \( L'(s, \chi) \), we evaluate for each character \( \chi \) of \( H \), the integral

\[
I_{\chi}(x_j, T) := \frac{1}{2\pi i} \int_{1+\frac{1}{\log x}+iT-i\theta \tau}^{1+\frac{1}{\log x}+iT+i\theta \tau} \frac{L'(s, \chi)}{L(s, \chi)} \frac{x_j^{s+\theta/2+i\theta \tau}}{s+\theta/2+i\theta \tau} \, ds
\]

for each \( j = 0, 1, \ldots, B \). We may assume that \( T + \theta \tau \) and \( T - \theta \tau \) don’t coincide with the imaginary part of a zero of any of the \( L(s, \chi) \). To estimate this integral, we move the line of integration and consider the integral over a rectangle and apply Cauchy’s theorem. More specifically, for \( J := m + \frac{1}{2} \) where \( m \) is a non-negative integer, let \( B_{T, J, \theta} \) be the positively oriented rectangle with vertices at

\[
1 + \frac{1}{\log x} - i(T + \theta \tau), \quad 1 + \frac{1}{\log x} + i(T - \theta \tau), \quad -J - \frac{\theta}{2} + i(T - \theta \tau) \quad \text{and} \quad -J - \frac{\theta}{2} - i(T + \theta \tau).
\]

Observe that this box does not intersect the real-axis, because \( T - \theta \tau < 0 \) for all \( \tau \in [T', 2T'] \). Define

\[
I_{\chi}(x_j, T, J) := \frac{x_j^{\theta/2+i\theta \tau}}{2\pi i} \int_{B_{T, J, \theta}} \frac{L'(s, \chi)}{L(s, \chi)} \frac{x_j^s}{s+\theta/2+i\theta \tau} \, ds.
\]

Now we estimate the error term

\[
R_{\chi}(x_j, T, J) := I_{\chi}(x_j, T, J) - I_{\chi}(x_j, T)
\]

uniformly for each \( j = 0, \ldots, B \). Here, the error \( R_{\chi}(x_j, T, J) \) consists of sum of one vertical integral \( V_{\chi}(x_j, T, J) \), and two horizontal integrals \( H_{\chi}(x_j, T, J) \) and \( H^*_{\chi}(x_j, T) \) which we now estimate, following the line of proof in [LO77, Section 6, Lemma 6.2]. We deduce

\[
V_{\chi}(x_j, T, J) := \frac{1}{2\pi i} \int_{-T}^{T} \frac{x_j^{-J+it}}{-J+it} \frac{L'(s, \chi)}{L(s, \chi)} \frac{x_j^s}{s+\theta/2+i\theta \tau} \, dt
\]

\[
\ll \frac{x^{-J}}{J} T (\log A(\chi) + n_E \log(|T + \theta \tau| + |J + \theta/2|));
\]

\[
H_{\chi}(x_j, T, J) := \frac{x_j^{\theta/2+i\theta \tau}}{2\pi i} \int_{-J-\theta/2}^{-1/4} \frac{x_j^{\sigma-i\tau}}{\sigma+\theta/2-i\tau} \frac{L'(s, \chi)}{L(s, \chi)} \, d\sigma
\]

\[
- \frac{x_j^{\theta/2+i\theta \tau}}{2\pi i} \int_{-J-\theta/2}^{-1/4} \frac{x_j^{\sigma+i\tau}}{\sigma+\theta/2+i\tau} \frac{L'(s, \chi)}{L(s, \chi)} \, d\sigma
\]

\[
\ll \frac{x^{-1/4+\theta/2}}{T \log x} (\log A(\chi) + n_E \log|T + \theta \tau|);
\]
and lastly

\[ H_\chi^*(x, T) := \frac{x^{\theta/2+i\theta T}}{2\pi i} \int_{-1/4}^{1+1/\log x} \frac{x_j^{\sigma-iT}}{\sigma + \theta/2 - iT} \frac{L'}{L}(\sigma - iT, \chi) \, d\sigma \]

\[ - \frac{x_j^{\theta/2+i\theta T}}{2\pi i} \int_{-1/4}^{1+1/\log x} \frac{x_j^{\sigma+iT}}{\sigma + \theta/2 + iT} \frac{L'}{L}(\sigma + iT, \chi) \, d\sigma \]

\[ = \frac{1}{2\pi i} \int_{-1/4}^{1+1/\log x} \frac{x_j^{\sigma+\theta/2-iT}}{\sigma + \theta/2 - iT} \sum_{\rho} \frac{d\sigma}{\sigma - iT + \theta T - \rho} \]

\[ - \frac{1}{2\pi i} \int_{-1/4}^{1+1/\log x} \frac{x_j^{\sigma+\theta/2+iT}}{\sigma + \theta/2 + iT} \sum_{\rho} \frac{d\sigma}{\sigma + iT - \theta T - \rho} \]

\[ + O \left( \frac{x^{1+\theta/2}}{T \log x} (\log A(\chi) + n_E \log|T + \theta T|) \right), \]

where the sum above is taken over the non-real zeros \( \rho \) of \( L(s, \chi) \) and \( A(\chi) = d_E N_{E/\ell}(f_\chi), f_\chi \) being the conductor of \( \chi \). The proof of Lemma 6.3 in [LO77] can be modified to show that

\[ 1 \int_{-1/4}^{1+1/\log x} \frac{x_j^{\sigma+\theta/2-iT}}{\sigma + \theta/2 - iT} \sum_{\rho} \frac{1}{\sigma - iT + \theta T - \rho} \, d\sigma \]

\[ \ll \frac{x^{1+1/\log x}}{T \log x} n_\chi(T + \theta T) \]

\[ \ll \frac{x^{1+\theta/2} \log x}{T} (\log A(\chi) + n_E \log|T + \theta T|). \]

Here \( n_\chi(t) \) denotes the number of zeros \( \rho = \beta + i\gamma \) of \( L(s, \chi) \) with \( 0 < \beta < 1 \) and \( |\gamma - t| \leq 1 \). A similar estimate holds for the sum over \( \rho \) with \( |\gamma + (T - \theta T)| \leq 1 \). Therefore, for each \( j = 0, 1, \ldots, B \),

\[ H_\chi^*(x_j, T) \ll \frac{x^{1+\theta/2} \log x}{T} (\log A(\chi) + n_E \log|T + \theta T|). \]

Note that the estimate for \( H_\chi(x_j, T) \) is bounded above by the estimate for \( H_\chi^*(x_j, T) \). Therefore, from (4.7),

\[ R_\chi(x, T, J) \ll \frac{x^{1+\theta/2} \log x}{T} (\log A(\chi) + n_E \log|T + \theta T|) + \frac{x^{-J}}{J} T (\log A(\chi) + n_E \log(|T - \theta T| + |J + \theta/2|)) \]

(4.8)

We remark here that one only needs to consider the first term above; the second term goes to zero as \( J \to \infty \). Next, by Cauchy’s theorem, \( I_\chi(x, T, J) \) is the sum of the residues at the poles of the integrand inside \( B_{t,J} \). For our specified contour,
the poles occur only at the non-real zeros of $L(s, \chi)$, and at $s = -\theta/2 - i\theta\tau$. This gives

$$I_\chi(x_j, T, J) = \sum_{|\gamma+\theta\tau|<T} \frac{x_j^{\rho+\theta/2+i\theta\tau}}{\rho+\theta/2+i\theta\tau} + \frac{L'}{L}(-\theta/2 - i\theta\tau).$$

(4.9)

The term $\frac{L'}{L}(-\theta/2 - i\theta\tau)$ is estimated using the following lemma which is a slightly general version of Lemma 6.2 in [LO77] and can be proved essentially using the same arguments, so we omit the details here.

**Lemma 4.3.** If $s = \sigma + it$ with $\sigma \leq -\theta/2$ and $|s+m| \geq \theta/2$ for all non-negative integers $m$, then

$$\frac{L'}{L}(s, \chi) \ll \log A(\chi) + n_E \log(|s|+2).$$

Applying these bounds, we get

$$\frac{L'}{L}(-\theta/2 - i\theta\tau) \ll \log A(\chi) + n_E \log(|\theta/2 + i\theta\tau|+2).$$

(4.10)

Using (4.10), (4.9) and (4.8) in (4.7), we have

$$I_\chi(x_j, T) = \sum_{|\gamma+\theta\tau|<T} \frac{x_j^{\rho+\theta/2+i\theta\tau}}{\rho+\theta/2+i\theta\tau} + O \left( \left( \frac{x^{1+\theta/2} \log x}{T} + 1 \right) (\log A(\chi) + n_E \log|T+\theta\tau|) \right).$$

We plug this into the definition of $I(x_j, T)$ to obtain

$$I(x_j, T) - S(x_{j+1}, T) + S(x_j, T)$$

$$\ll \left| \frac{C}{G} \right| \left( \frac{x^{1+\theta/2} \log x}{T} + 1 \right) \sum_{\chi} (\log A(\chi) + n_E \log|T+\theta\tau|)$$

$$\ll \left| \frac{C}{G} \right| \left( \frac{x^{1+\theta/2} \log x}{T} + 1 \right) (\log d_L + n_L \log|T+\theta\tau|),$$

(4.11)

where

$$S(y, T) := \left| \frac{C}{G} \right| \sum_{\chi} \bar{\chi}(g) \sum_{|\gamma+\theta\tau|<T} \frac{y^{\rho+\theta/2+i\theta\tau}}{\rho+\theta/2+i\theta\tau}.$$}

Under GRH, with slight modification to the calculation in the proof of Theorem 9.1 of [LO77], and summing over $\chi$, we get

$$S(x_j, T) \ll \left| \frac{C}{G} \right| x^{1/2+\theta/2} \log T (\log d_L + n_L \log|T+\theta\tau|)$$

Finally, using the above bounds in (4.11) and recalling (4.6), we conclude

$$\Psi_C(-\theta/2 - i\theta\tau) \ll \left| \frac{C}{G} \right| x^{1/2+\theta/2} (\log d_L + n_L \log|T+\theta\tau|) \left( \log T + \frac{x^{1/2}}{T} \log x \right)$$

$$+ x^{\theta/2} \log x \left( \log d_L + n_K + n_K \frac{x \log x}{T} \right).$$
Using partial summation and $\tau \leq 2T'$, and setting $T = \theta T'/2$, one gets the desired bounds for $F$ in the case of a fixed conjugacy class $C$.

Next, suppose $C = \bigcup_{m=1}^{b} C_m$ is a union of $b$ conjugacy classes for some integer $b \geq 1$. Then, using the estimates established for each conjugacy class $C_m$ and summing over $m$, we have

$$F(-\theta/2 - i\theta \tau) \ll \frac{\sum_{m=1}^{b} |C_m| x^{(1+\theta)/2}}{|G|} \left( \frac{\log d_L + n_L \log T'}{x} + \frac{x^{1/2}}{T'} \right) + x^{\theta/2} \left( \log d_L + bn_K + bn_K \frac{x \log x}{T'} \right)$$

$$= \frac{|C|}{|G|} x^{(1+\theta)/2} \left( \frac{\log d_L + n_L \log T'}{x} + \frac{x^{1/2}}{T'} \right) + x^{\theta/2} \left( \log d_L + bn_K + bn_K \frac{x \log x}{T'} \right),$$

noting that the error term in (4.5) that contributes $x^{\theta/2} \log d_L$ remains unchanged even if $C$ is a single class or a union of conjugacy classes. This completes the proof of the proposition. □

References

[AG15] Yildirim Akbal and Ahmet Muhtar Güloğlu. Piatetski-Shapiro meets Chebotarev. Acta Arith., 167(4):301–325, 2015.

[AHJ+18] Anthony Agwu, Phillip Harris, Kevin James, Siddarth Kannan, and Huixi Li. Frobenius distributions in short intervals for CM elliptic curves. J. Number Theory, 188:263–280, 2018.

[Bal83] A. Balog. On the fractional part of $p^\theta$. Arch. Math. (Basel), 40(5):434–440, 1983.

[Bal85] A. Balog. On the distribution of $p^\theta \mod 1$. Acta Math. Hungar., 45(1-2):179–199, 1985.

[BGY13] William D. Banks, Ahmet M. Güloğlu, and Aaron M. Yeager. Carmichael meets Chebotarev. Canad. Math. Bull., 56(4):695–708, 2013.

[CHT08] Laurent Clozel, Michael Harris, and Richard Taylor. Automorphy for some $l$-adic lifts of automorphic mod $l$ Galois representations. Publ. Math. Inst. Hautes Études Sci., (108):1–181, 2008. With Appendix A, summarizing unpublished work of Russ Mann, and Appendix B by Marie-France Vignéras.

[DGM+20] C. David, A. Gafni, A. Malik, N. Prabhu, and C. L. Turnage-Butterbaugh. Extremal primes for elliptic curves without complex multiplication. Proc. Amer. Math. Soc., 148(3):929–943, 2020.

[FH91] William Fulton and Joe Harris. Representation theory, volume 129 of Graduate Texts in Mathematics. Springer-Verlag, New York, 1991. A first course, Readings in Mathematics.

[Gib17] Luke M. Giberson. Average Frobenius Distributions for Elliptic Curves: Extremal Primes and Koblitz’s Conjecture. ProQuest LLC, Ann Arbor, MI, 2017. Thesis (Ph.D.)–Clemson University.

[GJ18] Luke Giberson and Kevin James. An average asymptotic for the number of extremal primes of elliptic curves. Acta Arith., 183(2):145–165, 2018.

[GTW20] Ayla Gafni, Jesse Thorner, and Peng-Jie Wong. Applications of the sato-tate conjecture, 2020.
[HSBT10] Michael Harris, Nick Shepherd-Barron, and Richard Taylor. A family of Calabi-Yau varieties and potential automorphy. *Ann. of Math. (2)*, 171(2):779–813, 2010.

[JP17] Kevin James and Paul Pollack. Extremal primes for elliptic curves with complex multiplication. *J. Number Theory*, 172:383–391, 2017.

[JTT+16] Kevin James, Brandon Tran, Minh-Tam Trinh, Phil Wertheimer, and Dania Zantout. Extremal primes for elliptic curves. *J. Number Theory*, 164:282–298, 2016.

[LO77] J. C. Lagarias and A. M. Odlyzko. Effective versions of the Chebotarev density theorem. pages 409–464, 1977.

[MMS88] M. Ram Murty, V. Kumar Murty, and N. Saradha. Modular forms and the Chebotarev density theorem. *Amer. J. Math.*, 110(2):253–281, 1988.

[NT20] James Newton and Jack A. Thorne. Symmetric power functoriality for holomorphic modular forms, 2020.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d’ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[Tay08] Richard Taylor. Automorphy for some $l$-adic lifts of automorphic mod $l$ Galois representations. II. *Publ. Math. Inst. Hautes Études Sci.*, (108):183–239, 2008.

[Tit86] E. C. Titchmarsh. *The theory of the Riemann zeta-function*. The Clarendon Press, Oxford University Press, New York, second edition, 1986. Edited and with a preface by D. R. Heath-Brown.

[Zyw15] David Zywina. Bounds for the Lang-Trotter conjectures. In *SCHOLAR—a scientific celebration highlighting open lines of arithmetic research*, volume 655 of *Contemp. Math.*, pages 235–256. Amer. Math. Soc., Providence, RI, 2015.

**American Institute of Mathematics, San Jose, California 95112**

*Email address:* amita.malik@aimath.org

**Indian Institute of Science Education and Research Pune, Dr. Homi Bhabha Road, Pune - 411008, Maharashtra, India**

*Email address:* neha.prabhu@acads.iiserpune.ac.in