THE CHEBOTAREV DENSITY THEOREM AND THE PAIR CORRELATION CONJECTURE

M. RAM MURTY, V. KUMAR MURTY, AND PENG-JIE WONG

Abstract. In this note, we formulate the pair correlation conjecture and give a refinement of the effective version of the Chebotarev density theorem established by M. R. Murty and V. K. Murty in their unpublished work. We also apply this result to study Artin’s primitive root conjecture and the Lang-Trotter conjecture and then obtain sharper error terms.

1. Introduction

In order to study arithmetical problems via L-functions, the key is the location of the zeros and poles, which originates from Riemann’s remarkable insight of the connection between the distribution of primes and his zeta function. For instance, both aspects play a main role in studying the primes in number fields; and it has been established that the holomorphy of Artin L-functions enables one to derive an effective version of the Chebotarev density theorem with a sharper error term by the first two authors and Saradha [18], which refines the previous works of Lagarias-Odlyzko [10] and Serre [24]. Moreover, in their unpublished paper [17] written more than 20 years ago, M. R. Murty and V. K. Murty improve their result under the assumption of the pair correlation conjecture, which will be discussed in Section 3, and the Artin (holomorphy) conjecture. Their saving in powers of the main variable has a dramatic effect on several famous problems of number theory.

For general L-functions belonging to the Selberg class, the pair correlation conjecture has been studied by M. R. Murty and Perelli [19] and M. R. Murty and Zaharescu [20]. However, M. R. Murty and V. K. Murty departed from these works by tracing the dependence of error terms on various constants associated to the involved L-functions. As one will see, such uniform estimates are crucial in applications.

The main purpose of this note is giving a refinement with a self-contained proof for the unpublished result of M. R. Murty and V. K. Murty, which allows one to derive a further “small” saving in powers of the main variable. Also we shall demonstrate what this saving will lead to in much the same spirit as in [17].

1.1. The Chebotarev Density Theorem. Throughout this note, we will make use of some notation introduced in this section as follows. We shall always let $K/k$ be a Galois extension of number fields with Galois group $G$. Let $C$ be a subset of $G$ which is stable under conjugation. Thus, $C$ is a union of conjugacy classes.

Date: December 13, 2016.

Key words and phrases. Artin L-functions, Chebotarev density theorem, pair correlation conjecture.

Research of the first two authors is partially supported by NSERC Discovery grants.
in $G$. For every unramified prime $p$ of $k$, $\sigma_p$ denotes the Artin symbol at $p$. Let us define $\pi_C(x) = \#\{p \mid p$ is unramified with $Np \leq x$ and $\sigma_p \subseteq C\}$. The celebrated Chebotarev density theorem states that

$$\pi_C(x) \sim \frac{|C|}{|G|} \pi_k(x),$$

as $x \to \infty$, where $\pi_k(x) = \#\{p \mid p$ is a prime with $Np \leq x\}$. Effective versions of this theorem with explicit error terms were first established by Lagarias and Odlyzko in their fundamental paper [10]. If the generalised Riemann hypothesis (denoted GRH) for the Dedekind zeta function $\zeta_K(s)$ is assumed, Serre [24] showed that

$$\pi_C(x) = \frac{|C|}{|G|} \pi_k(x) + O\left(\frac{|C|}{|G|} x^{\frac{1}{2}} \log d_K + n_K \log x\right),$$

(1.1) where $n_K = [K : \mathbb{Q}]$, $d_K$ is the absolute discriminant of $K$, and the big-O symbol is absolute. We also remark that there are unconditional versions, and refer the reader to [10] and [24].

In [18], the authors derive a stronger version under the assumption of the Artin conjecture on the holomorphy of all Artin L-functions attached to non-trivial irreducible characters of $G$. More precisely, if the Artin conjecture (denoted AC) holds and $\zeta_K(s)$ satisfies GRH, then

$$\pi_C(x) = \frac{|C|}{|G|} \pi_k(x) + O\left(\frac{|C|}{|G|} x^{\frac{1}{2}} n_k \log M(K/k)x\right),$$

(1.2) where $C$ is a conjugacy class in $G$, $n_k = [k : \mathbb{Q}]$,

$$M(K/k) = nd_K^{\frac{1}{n_k}} \prod_{p \in P(K/k)} p,$$

$n = [K : k]$, and $P(K/k)$ denotes the set of rational primes $p$ for which there is $p$ of $k$ with $p|p$ such that $p$ is ramified in $K$.

If one writes the error term in (1.1) as

$$O\left(\frac{|C|}{|G|} x^{\frac{1}{2}} n_k \left(\log d_K \frac{n_K}{n_K} + \log x\right)\right),$$

one can see that (1.2) is a better estimate as the factor $|C|$ in (1.1) is now replaced by $|C|^{\frac{1}{2}}$. These estimates are more versatile for many applications such as Artin’s primitive root conjecture, the Lang-Trotter conjecture on Fourier coefficients of modular forms (see [18]), and the problem of primitive points on elliptic curves (see [7]).

1.2. The Implication of a Pair Correlation Conjecture. A pair correlation conjecture (denoted PCC) of Artin L-functions was formulated by M. R. Murty and V. K. Murty in [17]. It will be stated formally in Section 3. Also it will be noticed that this conjecture is not as strong as the usual formulations as here we only require a weak upper bound rather than a uniform asymptotic formula.

In [17], the authors derived the following.
Theorem 1.1. [17] Under the assumption that GRH, AC and the pair correlation conjecture are valid for all Artin L-functions attached to irreducible characters of $G$. One has

$$(1.3) \quad \pi_C(x) = \frac{|C|}{|G|} \pi_k(x) + O \left( n_k^\frac{1}{2} |C|^{\frac{1}{2}} \left( \frac{|G^\#|}{|G|} \right)^{\frac{1}{2}} x^{\frac{3}{2}} \log M(K/k)x \right),$$

where $G^\#$ is the set of all conjugacy classes in $G$ and $M(K/k)$ is defined as before.

This is a significant improvement in two aspects. First and foremost, the factor $\left( \frac{|G^\#|}{|G|} \right)^{1/4}$ appears in the error term. Second, the $n_k$ in (1.2) is replaced by $n_k^{1/2}$. As mentioned in [17], the authors expect significant gains in applications to “highly non-abelian” contexts, i.e., to Galois extensions whose Galois groups have few and large conjugacy classes. Indeed, it has been shown that this improvement leads to dramatic results on several arithmetical problems.

Before we demonstrate how this saving plays a role in helping one derive better estimates for some problems of number theory, we shall state here our main theorem so that the reader may immediately compare the refinement to (1.1), (1.2) and (1.3) in this note.

Theorem 1.2. Under the assumption that GRH, AC and the pair correlation conjecture hold for all Artin L-functions of $G$, we have

$$\pi_C(x) = \frac{|C|}{|G|} \pi_k(x) + O \left( n_k^\frac{1}{2} |C|^{\frac{1}{2}} \left( \frac{|G^\#|}{|G|} \right)^{\frac{1}{2}} x^{\frac{3}{2}} \log M(K/k)x \right),$$

where $C$ is a conjugacy class in $G$ and $G^\#$ is defined as above.

The improvement over Theorem 1.3 lies in the factor $\left( \frac{|G^\#|}{|G|} \right)^{1/2}$.

1.3. Some Applications.

1.3.1. Artin’s Primitive Root Conjecture. Let us first consider the Artin primitive root conjecture. This conjecture asserts that for any non-zero integer $a$, which is not a perfect square, there are infinitely many primes $p$ such that $a$ is a primitive root modulo $p$. If we set

$$N_a(x) := \# \{ p \leq x \mid a \text{ is a primitive root mod } p \},$$

then, assuming GRH for all $K_m = \mathbb{Q}(\zeta_m, a^{1/m})$, Hooley [9] showed that

$$N_a(x) = c(a) \text{Li} x + O(x(\log \log x)^2/(\log x)^2),$$

where $c(a)$ is a positive constant. We remark that there is an unconditional result due to Gupta and M. R. Murty, and we refer the interested reader to [6].

In [17], the authors apply Theorem 1.1 instead of just GRH to derive

$$N_a(x) = c(a) \text{Li} x + O(x^{10/11}(\log x)^2(\log a)).$$

We will improve this result later as the following.

$$N_a(x) = c(a) \text{Li} x + O(x^{4/5}(\log a x)).$$
1.3.2. Elliptic analogues of Artin’s Primitive Root Conjecture. As mentioned in [17], there are several related problems in the theory of elliptic curves to which their Theorem 1.1 can be applied. For instance, an elliptic analogue of Artin’s primitive root conjecture, formulated by Lang and Trotter, can be treated along a similar line (see, for example, [1] and [3]). The following cyclicity problem was first considered by Serre [23]. Given an elliptic curve $E$ over $\mathbb{Q}$ of conductor $N$, one may be curious about the number $f(x, E)$ of primes $p \leq x$ such that $E(\mathbb{F}_p)$ is cyclic. Serre [23] (see also [16]) adapted Hooley’s method to prove under GRH that

$$f(x, E) = c_E \frac{x}{\log x} + O \left( \frac{x \log \log x}{(\log x)^2} \right),$$

where $c_E$ is a constant depending on $E$. Also, Serre showed that $c_E > 0$ if $E$ has an irrational 2-division point. This has been improved by Cojocaru and M. R. Murty [3, Theorem 1.1] that (under GRH)

$$f(x, E) = c_E \mathrm{Li} x + O \left( x^{5/6}(\log x)^{2/3} \right).$$

We also remark that by the work of Gupta and M. R. Murty [7], one has an unconditional result concerning this problem.

Furthermore, applying (1.3) in this context and assuming GRH, AC and the pair correlation conjecture for all Artin L-functions of division fields of $E$, Cojocaru and M. R. Murty [3] derived

$$f(x, E) = c_E \mathrm{Li} x + O \left( x^{7/10}(\log Nx)^{4/5}A(E) \right),$$

where $A(E)$ is Serre’s constant associated to $E$.

In this note, we shall apply our Theorem 1.2 to get

$$f(x, E) = c(E) \mathrm{Li} x + O \left( x^{1/2}(\log Nx)A(E)^2 \right).$$

1.3.3. The Lang-Trotter Conjecture. In the later part of this note, we will consider the Lang-Trotter conjecture on coefficients of (non-CM) modular forms $f$ of integral weight $k \geq 2$ and level $N$. Let $f$ be a normalised Hecke eigenform, and let us write

$$f(z) = \sum_{n \geq 1} a_f(n) \exp(2\pi inz), \quad a_f(n) \in \mathbb{Z}.$$ 

Lang and Trotter conjectured that given an integer $a$, the number of primes $p \leq x$ such that $a_f(p) = a$ is $O(x^{1/2})$. Several results are already established for this conjecture. Under PCC, M. R. Murty and V. K. Murty obtained the estimate of the form $O(x^{3/4})$. Moreover, if $a = 0$, they derived a bound of type $O(x^{2/3})$. We will show that if Theorem 1.2 is assumed, one can get the estimate of the type $O(x^{2/3})$. Also for $a = 0$, we derive the estimate $O(x^{1/2})$ as predicted by Lang-Trotter. From this consistency, our effective version of Chebotarev density theorem seems to be the best possible.

Now let us consider $E/\mathbb{Q}$, a non-CM elliptic curve over $\mathbb{Q}$ of conductor $N$. For any prime $p \nmid N$, we let $E(\mathbb{F}_p)$ denote the group of $\mathbb{F}_p$-rational points of $E/\mathbb{F}_p$, and write

$$|E(\mathbb{F}_p)| = p + 1 - a_p(E).$$
By Hasse’s bound that $|a_p(E)| < 2\sqrt{p}$, one can see that the characteristic polynomial $T^2 - a_p(E)T + p$ has two complex conjugate roots $\pi_p(E)$ and $\bar{\pi}_p(E)$ with $|\pi_p(E)| = \sqrt{p}$.

Let $K$ be an imaginary quadratic field, and set

$$\Pi_E(K, x) := \#\{p \leq x \mid p \nmid N, Q(\pi_p(E)) = K\},$$

where $Q(\pi_p(E))$ is the field generated by $\pi_p(E)$ over $\mathbb{Q}$.

In 1976, Lang and Trotter conjectured that there exists a positive constant $c(E, K)$, depending on $E$ and $K$, such that

$$\Pi_E(K, x) \sim c(E, K) \frac{x^{1/2}}{\log x}$$
as $x \to \infty$. This was first investigated by Serre, who stated (without proof) that if GRH is assumed, one may apply the Selberg sieve to derive

$$\Pi_E(K, x) \ll x^\theta$$
for some (unspecified) $\frac{1}{2} \leq \theta < 1$. Also Serre remarked that one could use a mixed Galois representation (associated to $E$ and $K$)

$$\rho_\ell : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Z}_\ell) \times GL_2(\mathbb{Z}_\ell)$$

and an effective Chebotarev density theorem to “obtain” $\theta = \frac{9}{10}$ (again, no proof was given). The first proof, appearing in literature, is due to Cojocaru, Fouvry and M. R. Murty [4], who used the square sieve to show that under GRH, one has

$$\Pi_E(K, x) \ll_N x^{\frac{17}{12}} \log x,$$

where the estimate only depends on the conductor $N$ of $E$ and is uniform in $K$.

Furthermore, the authors in [4] include new remarks made by Serre that the mixed Galois representation method combining with a $PGL_2$-reduction would lead to, under GRH,

$$\Pi_E(K, x) \ll_{E,K} x^{\frac{7}{8}},$$

with an unspecified implicit constant.

Inspired by the above-mentioned works, Cojocaru and David [2] improved upon Serre’s mixed Galois representation method, under GRH,

$$\Pi_E(K, x) \ll_{E,K} x^{\frac{4}{7}}/(\log x)^{1/5}.$$ 

Moreover, if AC and PCC are assumed, they gave

$$\Pi_E(K, x) \ll_{E,K} x^{\frac{3}{4}}.$$ 

Also in [2], the authors presented a new method of estimating a character sum associated to $E$, which together with the square sieve gives (under GRH, AC, and PCC)

$$\Pi_E(K, x) \ll_N x^{\frac{5}{6}} \log x.$$ 

(Although in [2, Corollary 4] the power of $x$ is $3/4$, we however note that owing to a small arithmetic mistake, which will be noticed in the last section, it should be $5/6$ as we state above.) As mentioned in [2], although such an estimate is not as good as the above result obtained by using Serre’s method, this however is independent of the number field $K$, which is essential for some applications.
At the end of this note, we shall show that assuming Theorem 1.2, one can improve the above results as follows.

$$\Pi_{E,K}(K,x) \ll_{E,K} x^{\frac{2}{3}},$$

and

$$\Pi_{E,K}(K,x) \ll_N x^{3/4} \log x.$$

2. Lemmata

In this section, we shall collect several lemmata developed in [18], which will play a main role in “saving power” later.

**Lemma 2.1.** Let $\pi$ be a complex-valued linear function defined on the vector space of class functions of $G$. Then

$$\sum_C \frac{1}{|C|} \left| \pi(\delta_C) - |G| \pi(1_G) \right|^2 = \frac{1}{|G|} \sum_{\chi \neq 1_G} |\pi(\chi)|^2$$

where the sum on the left runs over conjugacy classes $C$ of $G$, and the sum on the right is over non-trivial irreducible characters of $G$.

For the purpose of counting primes, one also needs below the estimate.

**Theorem 2.2.** [18] Let $\chi$ be an irreducible character of $G$. Then

$$\log Nf(\chi) \leq 2\chi(1)n_k \left( \sum_{p \in \mathcal{P}(K/k)} \log p + \log n \right),$$

where $f(\chi)$ denotes the (global) Artin conductor of irreducible character $\chi$.

3. The Pair Correlation Function

Let $f(\chi)$ denote the Artin conductor of an irreducible character $\chi$ of $G = \text{Gal}(K/k)$, and let $A_\chi = d_K^{(1)} Nf(\chi)$ denote the conductor of $\chi$.

Let us also set

$$w(u) := \frac{4}{4 + u^2}.$$

Consider the Artin L-function $L(s, \chi, K/k)$ and assume the Artin conjecture and GRH for $L(s, \chi, K/k)$. Following [17], we define the pair correlation function for $L(s, \chi, K/k)$ as

$$\mathcal{P}_T(X, \chi) := \sum_{-T \leq \gamma_1, \gamma_2 \leq T} w(\gamma_1 - \gamma_2)e((\gamma_1 - \gamma_2)X),$$

where $\gamma_1, \gamma_2$ range over the imaginary parts of zeros of $L(s, \chi, K/k)$ on the critical line (counted according to multiplicity), and $e(t) := \exp(2\pi it)$. Let us also define $A_\chi(T)$ by

$$\log A_\chi(T) = \log A_\chi + \chi(1)n_k \log T.$$

Adapting the method developed in [17], we have the following estimate.
Proposition 3.1.

\[ \mathcal{P}_T(X, \chi) \ll T(\log A_\chi(T))^2. \]

Proof. First observe that

\[
\mathcal{P}_T(X, \chi) = \sum_{j=0}^{2T} \sum_{-T \leq \gamma_1, \gamma_2 \leq T \atop j \leq |\gamma_1 - \gamma_2| < j + 1} w(\gamma_1 - \gamma_2) e((\gamma_1 - \gamma_2)X),
\]

which is

\[
\ll \sum_{|\gamma_1| \leq T} \sum_{j=0}^{2T} \frac{1}{1 + j^2} \left( \sum_{|\gamma_1 + j| \leq |\gamma_1 + j_1 + 1 + \gamma_1|} 1 + \sum_{|\gamma_1 + j| \geq |\gamma_1 + j_1 + 1 + \gamma_1|} 1 \right).
\]

According to [18, 3.5.5], the number of zeros (of \( L(s, \chi, K/k) \)) with imaginary part in the interval \([t, t + 1)\) is \( \ll \log A_\chi + \chi(1)n_k \log |t| \). Thus, the above estimate becomes

\[
\ll \sum_{|\gamma_1| \leq T} \sum_{j=0}^{2T} \frac{1}{1 + j^2} (\log A_\chi + \chi(1)n_k \log T).
\]

This is easily seen to be

\[
\ll (\log A_\chi + \chi(1)n_k \log T) \sum_{|\gamma_1| \leq T} 1.
\]

As the sum is clearly \( T(\log A_\chi + \chi(1)n_k \log T) \), the result follows. \( \square \)

In light of [17], we shall make the following pair correlation conjecture (for the Artin L-function \( L(s, \chi, K/k) \)) with respect to \( 0 < m_\chi, 0 < c_\chi \leq 1 \) and \( 1 \leq r \leq 2 \), denoted PCC\((m_\chi, c_\chi, r)\).

**Conjecture 3.2.** Let \( A > 0 \). There exist \( 0 < m_\chi \leq \chi(1), 0 < c_\chi \leq 1 \) and \( 1 \leq r \leq 2 \) such that for

\[
0 \leq Y \leq Am_\chi n_k \log T,
\]

one has

\[
\mathcal{P}_T(Y, \chi) \ll_A c_\chi T(\log A_\chi(T))^r.
\]

**Remark.** By Proposition 3.1, this pair correlation conjecture holds (under GRH) when \( c_\chi = 1 \) and \( r = 2 \), and it is easy to see that the content of this conjecture is in reducing the power of \( \log A_\chi(T) \) and the leading coefficient. Also, as mentioned in [17], the contribution of terms with \( \gamma_1 = \gamma_2 \) shows that one cannot expect \( r < 1 \). On the other hand, as the usual formulations of the pair correlation conjecture require an asymptotic formula, the above conjecture is much weaker.

Furthermore, in [17], the authors conjecture that for \( 0 \leq Y \leq A\chi(1)n_k \log T \), one has

\[
\mathcal{P}_T(Y, \chi) \ll_A A (\log A_\chi(T)).
\]

In our language, this is PCC\((\chi(1), 1, 1)\). We shall, however, show that one can use a weaker hypothesis PCC\((\chi(1)^{1/2}, \chi(1)^{-1}, 2)\) to obtain the effective Chebotarev density theorem with the same error as in (1.1). Indeed, we will state our effective version of the Chebotarev density theorem, i.e., Theorem 5.1, with respect to the parameters \( m_\chi, c_\chi, r \).
4. The Sum $S(T, v, \chi, X)$

Now let us borrow some results of Heath-Brown [8]. Let $\gamma$ run over an arbitrary countable set and define

$$S(T, v, X) := \sum_{0 < \gamma \leq T} e(\gamma(v + X)).$$

In the case that $\gamma$ ranges over the imaginary parts of the zeros of $L(s, \chi, K/k)$, we will write $S(T, v, \chi, X)$ to indicate this. Following Heath-Brown, we set

$$k(v) = 2\pi \exp(-4\pi|v|).$$

By the identity that

$$\int_{-\infty}^{\infty} k(v)e(vx)dv = w(x),$$

a direct calculation gives

$$\int_{-\infty}^{\infty} k(v)|S(T, v, \chi, X)|^2 = \mathcal{P}_T(X, \chi).$$

In light of [8, Lemma 4], M. R. Murty and V. K. Murty derived an estimate for $S(T, 0, \chi, X)$ for all irreducible characters of $G$. However, since [17] is unpublished and we now use a slightly different PCC, we shall give a proof based on their method.

**Proposition 4.1.** For any $T \geq 1$, one has

$$S(T, 0, \chi, X) \ll T^{\frac{1}{2}} \left( \max_{t \leq T} \mathcal{P}_t(X, \chi) \right)^{\frac{1}{2}}.$$  

**Proof.** In the following discussion, we shall write $S(T, v) = S(T, v, \chi, X)$ as $\chi$ and $X$ will be fixed. By Montgomery [15, Lemma 1.1], if $f$ is a $C^1$-function on $[-1, 1], \ f(0) \ll \int_{-1}^{1} |f'(v)|dv + \int_{-1}^{1} |f(v)|dv.$

Hence,

$$|S(T, 0)|^2 \ll \int_{-1}^{1} |S(T, v)||S_v(T, v)|dv + \int_{-1}^{1} |S(T, v)|^2dv,$$

where $S_v(T, v)$ denotes the first derivative of $S(T, v)$ with respect to the $v$ variable. Clearly, one has

$$\int_{-1}^{1} |S(T, v)|^2dv \ll \int_{-1}^{1} e^{-4\pi|v|}|S(T, v)|^2dv$$

so that

$$\int_{-1}^{1} |S(T, v)|^2dv \ll \int_{-\infty}^{\infty} k(v)|S(T, v)|^2dv.$$

A similar reasoning together with the Cauchy-Schwarz inequality then yields

$$\int_{-1}^{1} |S(T, v)||S_v(T, v)|dv.$$
\[
\ll \left( \int_{-\infty}^{\infty} k(v) |S(T, v)|^2 dv \right)^{\frac{1}{2}} \left( \int_{-\infty}^{\infty} k(v) \left| \sum_{0<\gamma \leq T} \gamma e(\gamma + X) \right|^2 dv \right)^{\frac{1}{2}}.
\]

Applying the Abel summation formula, one has
\[
\sum_{0<\gamma \leq T} \gamma e(\gamma + X) = TS(T, v) - \int_0^T S(t, v) dv
\]
which implies that
\[
\int_{-\infty}^{\infty} k(v) \left| \sum_\gamma \gamma e(\gamma + X) \right|^2
\ll T^2 \int_{-\infty}^{\infty} k(v) |S(T, v)|^2 dv + T \int_0^T \int_{-\infty}^{\infty} k(v) |S(t, v)|^2 dv dt.
\]

Finally, putting everything together gives
\[
|S(T, 0, \chi, X)|^2 \ll \mathcal{P}_T(X, \chi)^{\frac{1}{2}} \left( T^2 \mathcal{P}_T(X, \chi) + T \int_0^T \mathcal{P}_t(X, \chi) dt \right)^{\frac{1}{2}} + \mathcal{P}_T(X, \chi)
\ll T^{\max_{t \leq T} |\mathcal{P}_t(X, \chi)|}
\]
as desired. \hfill \Box

**Proposition 4.2.** Conjecture 3.2 implies that for any \( X \leq \frac{1}{2} Am_\chi n_k \log T \), one has
\[
S(T, 0, \chi, X) \ll_A T^{\frac{3}{4}} \log A_\chi(T) + \sqrt{c_\chi T} (\log A_\chi(T))^{\frac{1}{2}}.
\]

**Proof.** Observe that
\[
\max_{t \leq T} \mathcal{P}_t(X, \chi) \leq \max_{t \leq \sqrt{T}} \mathcal{P}_t(X, \chi) + \max_{\sqrt{T} \leq t \leq T} \mathcal{P}_t(X, \chi).
\]
In the range \( \sqrt{T} \leq t \leq T \), it is clear that \( \frac{1}{2} \log T \leq \log t \leq \log T \). Thus, if
\[
X \leq \frac{1}{2} Am_\chi n_k \log T,
\]
then clearly \( X \leq Am_\chi n_k \log t \). In this range, we may apply the pair correlation conjecture to deduce the estimate
\[
\max_{\sqrt{T} \leq t \leq T} \mathcal{P}_t(X, \chi) \ll_A \max_{\sqrt{T} \leq t \leq T} c_\chi t (\log A_\chi(t))^r \leq c_\chi T (\log A_\chi(T))^r
\]
for the second term. Also Proposition 3.1 tells us that
\[
\max_{t \leq \sqrt{T}} \mathcal{P}_t(X, \chi) \ll T^{\frac{1}{4}} (\log A_\chi(T))^2,
\]
which completes the proof. \hfill \Box
5. An Effective Version of the Chebotarev Density Theorem

Let $K/k$ be a Galois extension of number fields with Galois group $G$. Also, for any conjugate set $C$ of $G$, let us define

$$
\psi_C(x) := \sum_{Np^m \leq x \atop \sigma_p \subseteq C} \log Np,
$$

where the sum runs over all unramified primes $p$ of $k$, and $\sigma_p$ denotes the Artin symbol at $p$. The main result of this section is the following estimate.

**Theorem 5.1.** Assume GRH, AC and PCC($\chi, c_\chi, r$) for all Artin L-functions attached to irreducible characters $\chi$ of $G$. Then, one has the estimate

$$
\sum_{C} \frac{1}{|C|} \left( \psi_C(x) - \frac{|C|}{|G|} x \right)^2 \ll x (\log x)^2 (\log M(K/k)x)^2 \frac{n_k}{|G|} \sum_{\chi \in \text{Irr}(G)} (c_\chi \chi(1)^r + m_\chi^{-2} \chi(1)^2)
$$

where, as later, the sum is over all conjugacy classes of $G$, $G^#$ is the set of all classes of $G$, and $M(K/k)$ is defined as before.

From this, one can immediately derive an estimate for any conjugacy class $C$ of $G$.

**Corollary 5.2.** Under the assumption in the above theorem, we have

$$
\psi_C(x) - \frac{|C|}{|G|} x \ll x^{\frac{1}{2}} (\log x)(\log M(K/k)x)n_k^\frac{1}{2} \left( \frac{|G^#|}{|G|} \frac{1}{4} x^{\frac{1}{2}} \log M(K/k)x \right)^{\frac{1}{2}} \left( \sum_{\chi \in \text{Irr}(G)} c_\chi \chi(1)^r + m_\chi^{-2} \chi(1)^2 \right)^{\frac{1}{2}}.
$$

In particular, either PCC($\chi(1)^{1/2}, \chi(1)^{-1}, 2$) or PCC($\chi(1), 1, 1$) implies

$$
\pi_C(x) = \frac{|C|}{|G|} \pi_k(x) + O \left( n_k^\frac{1}{2} |C| \frac{1}{2} \left( \frac{|G^#|}{|G|} \right)^{\frac{1}{4}} x^{\frac{1}{2}} \log M(K/k)x \right);
$$

and if either PCC($\chi(1), \chi(1)^{-2}, 2$) or PCC($\chi(1), \chi(1)^{-1}, 1$) is assumed, we have

$$
\pi_C(x) = \frac{|C|}{|G|} \pi_k(x) + O \left( n_k^\frac{1}{2} |C| \frac{1}{2} \left( \frac{|G^#|}{|G|} \right)^{\frac{1}{4}} x^{\frac{1}{2}} \log M(K/k)x \right).
$$

To prove our main result, we shall prove the following estimate by adapting the method developed by the first two authors. Now let us set

$$
\psi(x, f) := \sum_{Np^m \leq x \atop \sigma_p \subseteq C} f(\sigma_p^m) \log Np,
$$

for any class function $f$ on $G$. In particular, for the characteristic function $\delta_C$,

$$
\psi(x, \delta_C) = \psi_C(x).
$$
Theorem 5.3. Under the assumption in the previous theorem. Then, for \( A \geq \frac{1}{\pi n_k} \) we have the estimate

\[
\psi(x, \chi) - \delta(\chi)x \ll_A x^{\frac{1}{2}} \left( \frac{\log x}{Am\chi n_k} \log A\chi(x) + (\log x)\left( \frac{1}{\sqrt{A\chi n_k}} \log A\chi(x) \right)^{\frac{1}{2}} \right)
\]

where \( \delta(\chi) \) denotes the multiplicity of the trivial character in \( \chi \).

Proof. We shall begin by developing an explicit formula as in [22] and [17], which has been established for general L-functions (under the holomorphy assumption) by V. K. Murty [21] applying a method based on [10]. For any \( 2 \leq T \leq x \), one has

\[
\psi(x, \chi) - \delta(\chi)x + \sum_{|\gamma| \leq T} \frac{x^\rho}{\rho} \ll \frac{x \log x}{T} - \log A\chi(T) + \chi(1) \log x \left( \frac{\log d_K}{|G|} + n_k x^{\frac{1}{2}} \right),
\]

where, as later, the sum is over the imaginary parts \( \gamma \) of the non-trivial zeros of \( L(s, \chi, K/k) \). Recall the pair correlation function we introduced previously is

\[
S(T, v) = S(T, v, \chi, X) = \sum_{0 < \gamma \leq T} e(\gamma(v + X)),
\]

where the sum runs over the imaginary parts \( \gamma \) of zeros of \( L(s, \chi, K/k) \).

Now applying Abel’s summation gives

\[
\sum_{|\gamma| \leq T} \frac{x^{i\gamma}}{\frac{1}{2} + i\gamma} = \int_0^T \frac{dS(t, 0, (\log x)/2\pi)}{\frac{1}{2} + it},
\]

which by integration by parts, is

\[
\ll T^{-1} S(T, 0, (\log x)/2\pi) + N(\chi, 2) + \int_2^T \frac{S(t, 0, (\log x)/2\pi)}{t^2} dt,
\]

where \( N(\chi, 2) \) denotes the number of zeros of \( L(s, \chi, K/k) \) with imaginary part less than 2. Applying this then makes \( \psi(x, \chi) - \delta(\chi)x \) become

\[
\ll x^{\frac{1}{2}} \left( T^{-1} S(T, 0, (\log x)/2\pi) + \log A\chi(2) + \int_2^T \frac{S(t, 0, (\log x)/2\pi)}{t^2} dt \right) + E,
\]

where

\[
E \ll \frac{x \log x}{T} - \log A\chi(T) + \chi(1) \log x \left( \frac{\log d_K}{|G|} + n_k x^{\frac{1}{2}} \right).
\]

Now we write \( X = (\log x)/2\pi \). By using Propositions 3.1 and 4.1, we first have

\[
\int_{2}^{x^{1/\pi Am\chi n_k}} t^{-2} |S(t, v, \sigma, X)| dt \ll \int_{2}^{x^{1/\pi Am\chi n_k}} t^{-1} (\log A\sigma(t)) dt.
\]

This is

\[
\ll \frac{\log x}{Am\chi n_k} \log A\chi(x).
\]
Moreover, Proposition 4.2 allows us to derive

\[
\int_{x^{1/π Am_n k}}^{T} t^{-2} |S(t, β, X)| dt \ll \int_{x^{1/π Am_n k}}^{T} t^{-2} \{t^{2} \log A_β(t) + \sqrt{c_β} t (\log A_β(t))^{2}\} dt
\]

\[
\ll (x^{-1/4π Am_n k} + T^{-1/4})(\log A_β(T)) + (\log T)(\sqrt{c_β} \log A_β(T))^{2}.
\]

Finally, choosing \(T = x\), we deduce that \(ψ(x, β) - δ(β) x\) is

\[
\ll x^{\frac{1}{2}} \left( x^{-\frac{1}{4}} \log A_β(x) + \sqrt{c_β} (\log A_β(x))^{2} + \log A_β(2) \right)
\]

\[
+ x^{\frac{1}{2}} \left( \log x \frac{\log A_β(x)}{Am_n k} + (x^{-1/4π Am_n k} + x^{-1})(\log A_β(x)) + (\log x)(\sqrt{c_β} \log A_β(x))^{2} \right)
\]

\[
+ \log x \log A_β(x) + (1) \log x \left( \frac{\log C_k}{|G|} + n_k x^{\frac{1}{2}} \right).
\]

**Proof of Theorem 5.1.** By the estimate

\[
\log A_β \ll χ(1)n_k \log M(K/k),
\]

we have

\[
\sum_{β ∈ Irr(G)} c_β (\log A_β(x))^r \ll \sum_{β ∈ Irr(G)} c_β χ(1)^r n_k^{r} (\log M(K/k)x)^r.
\]

Also, one has

\[
\sum_{β ∈ Irr(G)} \left( \frac{\log x}{Am_n k} \log A_β(x) \right)^2 \ll (\log x)^2 A^{-2} \sum_{β ∈ Irr(G)} m_β^{-2} χ(1)^2 (\log M(K/k)x)^2.
\]

Hence, applying Theorem 5.3 with \(A = 1\) (note that \(r \leq 2\)),

\[
\sum_{β ∈ Irr(G)} |ψ(x, β) - δ(β) x|^2 \ll x(\log x)^2 n_k \sum_{β ∈ Irr(G)} (c_β χ(1)^r + m_β^{-2} χ(1)^2)(\log M(K/k)x)^2.
\]

Now this estimate and the Cauchy-Schwarz inequality tell us that

\[
\sum_{C} \frac{1}{|C|} \left| \psi(x, δ_C) - \frac{|C|}{|G|} x \right|^2
\]

\[
\leq \sum_{C} \frac{1}{|C|} \left| \psi(x, δ_C) - \frac{|C|}{|G|} \psi(x, 1_G) + \frac{|C|}{|G|} \psi(x, 1_G) - \frac{|C|}{|G|} x \right|^2
\]

\[
\leq \sum_{C} \frac{2}{|C|} \left| \psi(x, δ_C) - \frac{|C|}{|G|} \psi(x, 1_G) \right|^2 + \sum_{C} \frac{2}{|C|} \left| \frac{|C|}{|G|} \psi(x, 1_G) - \frac{|C|}{|G|} x \right|^2
\]

\[
= \frac{2}{|G|} \sum_{χ ≠ 1_G} \frac{|ψ(x, χ)|^2}{χ(1)} + \frac{2}{|G|} (ψ(x, 1_G) - x)^2
\]

\[
\ll x(\log x)^2 (\log M(K/k)x)^2 n_k \sum_{χ ∈ Irr(G)} (c_χ χ(1)^r + m_χ^{-2} χ(1)^2)
\]
6. Artin’s Primitive Root Conjecture

Let \( a \neq 0, 1 \) be a square-free integer, and set
\[
N_a(x) := \# \{ p \leq x \mid a \text{ is a primitive root mod } p \}.
\]
Artin’s primitive root conjecture asserts that
\[
N_a(x) \sim c(a) \text{Li} x
\]
for some constant \( c(a) \) only depending on \( a \).

Let us consider the Kummer extension \( K_m = \mathbb{Q}(\zeta_m, a^{1/m}) \).
As mentioned earlier, assuming GRH for all \( K_m \), Hooley [9] showed that
\[
N_a(x) = c(a) \text{Li} x + O(x(\log \log x)^2/(\log x)^2).
\]
In [17], the authors proved that if GRH and PCC(\( \chi(1), 1, 1 \)) are assumed for all Artin L-functions attached to all irreducible characters of \( \text{Gal}(L_m/\mathbb{Q}) \), then one has
\[
N_a(x) = c(a) \text{Li} x + O(x^{10/11}(\log x)^2(\log a)).
\]
In light of their strategy, we give below an improvement.

**Theorem 6.1.** Under the assumption that GRH and the pair correlation conjecture hold for all Artin L-functions of \( \text{Gal}(K_m/\mathbb{Q}) \), we have
\[
N_a(x) = c(a) \text{Li} x + O(x^{4/5}(\log ax)).
\]

**Proof.** We first note that the Artin conjecture holds as \( \text{Gal}(K_m/\mathbb{Q}) \) is metabelian. Denote by \( \pi_m(x) \) the number of primes \( p \leq x \) which split completely in \( K_m \). Applying Corollary 5.2, we deduce that
\[
\pi_m(x) = \frac{1}{n_m} \text{Li} x + O \left( \sqrt{\frac{x}{m}(\log M_m x)} \right),
\]
where \( n_m = [K_m : \mathbb{Q}] = m\phi(m) \) and \( M_m = M(L_m/\mathbb{Q}) \).

In addition, since the absolute discriminant of \( \mathbb{Q}(a^{1/m}) \) is \( a^{m-1}m^m \) and the discriminant of \( \mathbb{Q}(\zeta_m) \) divides \( m^{\phi(m)} \), a moment’s reflection shows that
\[
M_m = \prod_{p|am} p \leq am,
\]
and hence
\[
\log M_m x \ll \log am x.
\]

Also by the inclusion-exclusion principle,
\[
N_a(x) = \sum_{m=1}^{\infty} \mu(m)\pi_m(x),
\]
as \( a \) is a primitive root mod \( p \) if and only if \( p \) does not split completely in any \( L_m \).

Now the above estimate tells us that for \( y \leq x \),
\[
\sum_{m \leq y} \mu(m) \left( \pi_m(x) - \frac{1}{n_m} \text{Li} x \right) \ll x^{1/2} y^{1/2}(\log ay x).
\]
Also,
\[ \sum_{y \leq m \leq x} \pi_m(x) \leq \sum_{p \leq x} \sum_{y \leq m \leq x \atop m \mid (p-1)} \sum_{p \mid (p-1)/m-1} 1, \]
where the later summations are bounded by
\[ \sum_{v \leq x/y} \sum_{p \mid a^v-1} \ll (x/y)^2 (\log a). \]

Finally, choosing \( y = x^{3/5} \) gives the desired result. \( \square \)

We remark that the key estimates in the above proof are duo to Hooley [9] and Gupta-M. R. Murty [6], and we also indicate the reader to [16].

7. Elliptic analogues of Artin’s Primitive Root Conjecture

As before, let \( E \) be an elliptic curve defined over \( \mathbb{Q} \) of conductor \( N \), and set \( f(x, E) \) to be the number of primes \( p \leq x \) such that \( E(\mathbb{F}_p) \) is cyclic. As mentioned above, Serre [23] (see also [16]) adapted Hooley’s method to prove under GRH that
\[ f(x, E) = c_E \frac{x}{\log x} + O \left( \frac{x \log \log x}{(\log x)^2} \right), \]
where \( c_E \) is a constant depending on \( E \). Also Serre showed that \( c_E > 0 \) if \( E \) has an irrational 2-division point.

As mentioned earlier, one has an unconditional result duo to Gupta-M. R. Murty [7]. Moreover, applying their method and (1.3) and assuming GRH, Artin’s conjecture and the pair correlation conjecture for all Artin L-functions attached to all irreducible characters of \( \text{Gal}(\mathbb{Q}(E[k])/\mathbb{Q}) \), Cojocaru and M. R. Murty [3] derived
\[ f(x, E) = c_E \text{Li}(x) + O \left( \frac{x^{7/10} (\log N x)^{4/5} A(E)}{\log x} \right), \]
where \( A(E) \) is Serre’s constant associated to \( E \).

Before we state and prove our result, we borrow below key ingredients from [3]. As discussed in [3, Section 2],
\[ f(x, E) = \sum_{k \leq 2\sqrt{x}} \mu(k) \pi_1(x, \mathbb{Q}(E[k]) / \mathbb{Q}), \]
where \( \pi_1(x, \mathbb{Q}(E[k]) / \mathbb{Q}) \) denotes the number of primes \( p \leq x \) that split completely in \( \mathbb{Q}(E[k]) / \mathbb{Q} \). Following Cojocaru and M. R. Murty [3], we shall consider the splitting
\[ f(x, E) = \sum_{k \leq y} \mu(k) \pi_1(x, \mathbb{Q}(E[k]) / \mathbb{Q}) + \sum_{y < k \leq 2\sqrt{x}} \mu(k) \pi_1(x, \mathbb{Q}(E[k]) / \mathbb{Q}) \]
\[ =: \sum_{\text{main}} + \sum_{\text{error}} \]
for some parameter \( y = y(x) \) to be chosen later. For any positive integer \( k \), let us set \( n(k) = [\mathbb{Q}(E[k]) : \mathbb{Q}] \), and write \( k = k_1 k_2 \) with \( k_1 \) composed of primes which are
divisors of \( A(E) \) and \( k_2 \) composed of primes which are coprime to \( A(E) \). Then [3, Proposition 3.6] asserts
\[
n(k) \geq \phi(k_1)n(k_2) \gg \phi(k)k_2^3.
\]
Moreover, Cojocaru and M. R. Murty showed by Hasse’s inequality that
\[
\sum_{\text{error}} \ll \frac{x^{3/2}}{y^2} + x^{1/2} \log \frac{x}{y} + \frac{x}{y}
\]
unconditionally (see [3, Section 4]).

Now we shall prove the following.

**Theorem 7.1.** If GRH and the pair correlation conjecture hold for all Artin L-functions of \( \text{Gal}(\mathbb{Q}(E[k])/\mathbb{Q}) \) is assumed, we have
\[
f(x, E) = c(E) \operatorname{Li} x + O \left( x^{\frac{3}{2}} (\log N x) A(E)^2 \right).
\]

**Proof.** In light of Cojocaru and M. R. Murty’s method, we handle \( \sum_{\text{main}} \) by our effective Chebotarev density theorem, Corollary 5.2, together with the above estimates. We first have
\[
\sum_{\text{main}} = \sum_{k \leq y} \frac{\mu(k)}{n(k)} \operatorname{Li} x + E(x),
\]
where the error \( E(x) \) is
\[
\sum_{\substack{k \leq y \\ k \text{ square-free} \\ k = k_1k_2}} O \left( \left( \frac{|\text{Gal}(\mathbb{Q}(E[k])/\mathbb{Q})|}{n(k)} \right)^{\frac{1}{2}} x^{\frac{3}{2}} (\log M(\mathbb{Q}(E[k])/\mathbb{Q})x) \right).
\]

Since
\[
\frac{|\text{Gal}(\mathbb{Q}(E[k])/\mathbb{Q})|}{n(k)} \ll \frac{k_1^2}{k_2^2},
\]
(see [3, pp. 615]) and the ramified primes of \( \mathbb{Q}(E[k])/\mathbb{Q} \) are divisors of \( kN \) (see, for example, [3, Proposition 3.5]), for \( y \leq x \) the error \( E(x) \) becomes
\[
E(x) \ll x^{\frac{3}{2}} \sum_{\substack{k \leq y \\ k \text{ square-free} \\ k = k_1k_2}} \left( \frac{k_1}{k_2} \right) (\log kN x)
\]
\[
\ll x^{\frac{3}{2}} (\log N x) \sum_{k_1} k_1 \sum_{k_2 \leq \frac{x}{k_1}} k_2^{-1}
\]
\[
\ll x^{\frac{3}{2}} (\log N x) \log y \sum_{k_1} k_1.
\]
We then have
\[ E(x) \ll x^{\frac{1}{2}}(\log Nx)(\log y) \sum_{k_1} \nu(k_1) \ll x^{\frac{1}{2}}(\log Nx)(\log y)A(E)^2 \nu(A(E)) \ll x^{\frac{1}{2}}(\log Nx)(\log y)A(E)^2, \]
where \( \nu(n) \) denotes the number of prime divisors of \( n \) and the last estimate is due to the inequality \( \nu(n) \leq \frac{\log n}{\log 2} \). Thus, by recalling that
\[ \sum_{\text{error}} \ll x^{3/2}/y^2 + x^{1/2} \log x/y + x/y, \]
and choosing \( y = x^{1/2} \), we then deduce
\[ f(x, E) = \left( \sum_{k \leq y} \frac{\mu(k)}{n(k)} \right) \operatorname{Li} x + O \left( x^{\frac{1}{2}}(\log Nx)(\log x)A(E)^2 \right). \]
Finally, we further borrow below an estimate of the “tail” from [3, Equation (18)]
\[ \sum_{k > y} \frac{1}{n(k)} \ll \frac{\log \log y}{y^3} A(E)^3 \]
to deduce
\[ f(x, E) = c(E) \operatorname{Li} x + O \left( x^{\frac{1}{2}}(\log Nx)(\log x)A(E)^2 \right) + O \left( \frac{\log \log x}{x^{1/2} \log x} A(E)^3 \right), \]
as desired. \( \square \)

8. Fourier Coefficients of Modular Forms

In this section, we consider non-CM holomorphic modular forms \( f \) of integral weight \( k \geq 2 \) and character \( \epsilon \) for the congruence subgroup \( \Gamma_0(N) \). Let \( f \) be a normalised Hecke eigenform, and let us write
\[ f(z) = \sum_{n \geq 1} a_f(n)q^n \]
for the Fourier expansion at infinity, where \( q = \exp(2\pi i z) \). Let \( \mathcal{O} \) denote the ring generated by \( a_f \) over \( \mathbb{Z} \). As in Serre [24], we first note that this ring is contained in the ring of integers of a number field \( K_f \) associated to \( f \). Moreover, associated to \( f \) are a family of \( \lambda \)-adic representations (à la Deligne [5])
\[ \rho_{f,\lambda} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow GL_2(\mathcal{O}_\lambda) \]
where \( \lambda \) is a prime of \( K_f \) and \( \mathcal{O}_\lambda \) denotes the completion of \( \mathcal{O} \) at \( \lambda \). Let \( \ell = \ell(\lambda) \) be the rational prime underlying \( \lambda \). Then \( \rho_{f,\lambda} \) is unramified outside \( \ell N \), and admits the property that for any prime \( p \) coprime to \( \ell N \), the characteristic polynomial of the Frobenius at \( p \) is
\[ T^2 - a_f(p)T + \epsilon(p)p^{k-1}. \]
By the work of Momose [14] and Ribet [11], for \( \ell \) sufficiently large (as a function of \( f \) and \( N \)), there exists a subgroup \( H \) of finite index in \( Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \) such that the image of \( \rho_{f,\lambda} \) on \( H \) is equal to

\[
\{ g \in GL_2(\mathcal{O}_\lambda) \mid \det g \in \mathcal{O}_\lambda^{\times(k-1)} \}.
\]

In particular, if we reduce the representation modulo a prime \( \lambda \) of degree one, and such that \((\ell(\lambda), k-1) = 1\), then the image of such a residual representation is

\[
G_\ell = GL_2(\mathbb{Z}/\ell\mathbb{Z}).
\]

In this case, the number of conjugacy classes is

\[
|G_\ell^\#| \asymp \ell^2.
\]

Also, the conjugacy set \( C_a \) consisting of elements in \( G_\ell \) of trace \( a \) has order

\[
|C_a| \asymp \ell^3.
\]

Thus, we deduce that

\[
\psi_{C_a}(x) = \frac{1}{\ell} x + O(\ell^{\frac{1}{2}} x^{\frac{1}{2}}(\log \ell x)).
\]

Now choosing \( \ell = x^{1/3} \), we then derive

\[
\pi_{f,a}(x) \ll x^{\frac{2}{3}},
\]

where \( \pi_{f,a}(x) \) denotes the number of primes \( p \leq x \) with \( a_f(p) = a \). In the case \( a = 0 \), we can get a better estimate by passing to \( PGL_2(\mathbb{Z}/\ell\mathbb{Z}) \), which allows us to deduce

\[
\psi_{C_a}(x) = \frac{1}{\ell} x + O(x^{\frac{1}{2}}(\log \ell x)).
\]

Choosing \( \ell = x^{\frac{1}{2}} \), we then have

\[
\pi_{f,0}(x) \ll x^{\frac{1}{2}}.
\]

9. THE LANG-TROTTER CONJECTURE

Let \( E/\mathbb{Q} \) be a non-CM elliptic curve over \( \mathbb{Q} \) of conductor \( N \). For any prime \( p \nmid N \), we let \( E(\mathbb{F}_p) \) denote the group of \( \mathbb{F}_p \)-rational points of \( E/\mathbb{F}_p \), and write

\[
|E(\mathbb{F}_p)| = p + 1 - a_p(E).
\]

By Hasse’s bound that \( |a_p(E)| < 2\sqrt{p} \), one can see that the characteristic polynomial \( T^2 - a_p(E)T + p \) has two complex conjugate roots \( \pi_p(E) \) and \( \overline{\pi_p(E)} \) with \( |\pi_p(E)| = \sqrt{p} \).

Let \( K \) be an imaginary quadratic field, and set

\[
\Pi_E(K, x) := \# \{ p \leq x \mid p \nmid N, \mathbb{Q}(\pi_p(E)) = K \},
\]

where \( \mathbb{Q}(\pi_p(E)) \) is the field generated by \( \pi_p(E) \) over \( \mathbb{Q} \).

Following Cojocaru and David, we let \( K \) be an imaginary quadratic field of class number \( h \) and number of unit \( w \). On one hand, we consider the mod \( \ell \) representation associated to \( E \):

\[
\rho_{\ell,E} : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Z}/\ell\mathbb{Z}).
\]

Thanks to Serre’s theorem on the image of the absolute group acting on the subgroup of torsion of \( E(\overline{\mathbb{Q}}) \), we may further assume that \( \ell \) is sufficiently large so that
\( \rho_{\ell,E} \) is surjective and \( \mathbb{Q}(E[\ell]) \cap K = \mathbb{Q} \). Thus, we can now consider the projection of \( \rho_{\ell,E} \) in \( PGL_2(\mathbb{Z}/\ell\mathbb{Z}) \) and obtain a bijective representation

\[
\hat{\rho}_{\ell,E} : \text{Gal}(F_{\ell,E}/\mathbb{Q}) \to PGL_2(\mathbb{Z}/\ell\mathbb{Z}),
\]

where \( F_{\ell,E} \) denotes the extension of \( \mathbb{Q} \) that makes the representation injective. As with \( \rho_{\ell,E} \), one can consider the projection of \( \hat{\rho}_{\ell,K} \) into \( PGL_2(\mathbb{Z}/\ell\mathbb{Z}) \). By [2, Lemma 6], we know that the image of \( \hat{\rho}_{\ell,K} \) (in \( PGL_2(\mathbb{Z}/\ell\mathbb{Z}) \)) is \( PN_{\ell} \), where

\[
PN_{\ell} := \left\{ \left( \begin{array}{cc} 1 & 0 \\ 0 & b^h \end{array} \right), \left( \begin{array}{cc} 0 & 1 \\ b^h & 0 \end{array} \right) \mid b \in (\mathbb{Z}/\ell\mathbb{Z})^\times \right\}.
\]

In other words, we have an isomorphism

\[
\rho_{\ell,K} : \text{Gal}(F_{\ell,K}/\mathbb{Q}) \to PN_{\ell}
\]

for some extension \( F_{\ell,K}/ \mathbb{Q} \). We then consider the product representation

\[
\hat{\rho} : \text{Gal}(F_{\ell,E}F_{\ell,K}/\mathbb{Q}) \to PGL_2(\mathbb{Z}/\ell\mathbb{Z}) \times PN_{\ell}
\]

sending \( g \) to \((\hat{\rho}_{\ell,E}(g), \hat{\rho}_{\ell,K}(g))\). As discussed in [2], if \( \ell \) is a sufficiently large rational prime splitting in \( K \) such that \( F_{\ell,E} \cap F_{\ell,K} = \mathbb{Q} \), then

\[
G_{\ell} \simeq PGL_2(\mathbb{Z}/\ell\mathbb{Z}) \times PN_{\ell},
\]

where \( G_{\ell} := \text{Im}(\hat{\rho}) = \text{Gal}(F_{\ell,E}F_{\ell,K}/\mathbb{Q}) \). We remark that in [2, Proposition 8], the authors gave a sufficient condition so that \( \ell \) splits in \( K \) and \( F_{\ell,E} \cap F_{\ell,K} = \mathbb{Q} \). Now let us fix a prime \( \ell \) which satisfies this property, and is sufficient large so that \( \rho_{\ell,E} \) is surjective and that \( Q(E[\ell]) \cap K = \mathbb{Q} \).

We also recall that for any independent variables \( a \) and \( b \), and any natural number \( n \), there is a polynomial \( P_n(X) \in \mathbb{Z}[X] \) such that

\[
\frac{(a^n + b^n)^2}{(ab)^n} = p_n \left( \frac{(a + b)^2}{ab} \right)
\]

(see, for example, [2, Lemma 14]). Now let us consider the conjugate set (in \( G_{\ell} \))

\[
C_{\ell} = \left\{ (g_1, g_2) \mid t(g_2) = P_{hw}(t(g_1)), g_2 = \left( \begin{array}{cc} 1 & 0 \\ 0 & b^h \end{array} \right), \left( \frac{(\text{tr} \ g_1)^2 - 4 \det \ g_1}{\ell} \right) = 1 \right\},
\]

where for any \( g \in GL_2(\mathbb{Z}/\ell\mathbb{Z}) \),

\[
t(g) := \frac{(\text{tr} \ g)^2}{\det \ g}.
\]

We note that \( t(g) \) and the Legendre symbol condition in the above definition are well-defined on \( PGL_2(\mathbb{Z}/\ell\mathbb{Z}) \). From this, Cojocaru and David showed that for \( \ell \) splitting in \( K \), one has

\[
\Pi_{E}(K, x) \leq \pi_{C_{\ell}}(x, F_{\ell}).
\]

Now applying a reduction method introduced in [18], Cojocaru and David (see [2, Equations (14) and (15)]) derived that under GRH,

\[
\pi_{C_{\ell}}(x, F_{\ell}/\mathbb{Q}) \ll \frac{h_x}{\ell \log x} + \ell^{3/2}x^{1/2} \log(\ell N x) + \ell \log(\ell N).
\]
Moreover, as discussed in [2, pp. 1553], if one assumes the pair correlation conjecture, which introduces an extra factor $1/\sqrt{\ell}$ in the error term, and leads to
\[
\pi_{C_1}(x, F_{\ell}/Q) \ll \frac{hx}{\ell \log x} + \ell x^{1/2} \log(\ell N x) + \ell \log(\ell N).
\]
As we discussed in the very beginning, our result improves M. R. Murty-V. K. Murty’s effective Chebotarev density theorem by replacing the power $1/4$ of the factor $|G^\#|/|G|$ by $1/2$, where $G^\#$ denotes the set of conjugacy classes in $G$. Now the pair correlation conjecture introduces an extra factor $1/\ell$ (instead of $1/\sqrt{\ell}$) which allows us to derive
\[
\pi_{C_1}(x, F_{\ell}/Q) \ll \frac{hx}{\ell \log x} + \ell^{1/2} x^{1/2} \log(\ell N x) + \ell \log(\ell N).
\]
Choosing $\ell = \frac{h^{1/2} x^{1/3}}{\log x}$, we then have
\[
\pi_{C_1}(x, F_{\ell}/Q) \ll h^{1/2} x^{2/3} \left( 1 + \frac{\log(h N x)}{\log x} \right)
\]
so that
\[
\Pi_E(K, x) \ll_{N, h} x^{2/3},
\]
as desired.

As before, let $E/Q$ be a non-CM elliptic curve of conductor $N$. Let $\ell_1 \neq \ell_2$ be rational primes such that the mod $\ell_1 \ell_2$ Galois representation associated to $E$ is surjective. Let us consider the character sum
\[
S_{\ell_1, \ell_2}(E, x) := \sum_{p \leq x \atop p \not| \ell_1 \ell_2 N} \left( \frac{4p - a_p(E)^2}{\ell_1 \ell_2} \right).
\]
An upper estimate is obtained in [4] as an application of effective versions of Chebotarev density theorem of Lagarias-Odlyzko (under GRH), M. R. Murty-V. K. Murty-Saradha (under GRH and AC), and M. R. Murty-V. K. Murty (under GRH, AC, and PCC). This has been improved by Cojocaru and David [2] as follows.

First we decompose the character sum as
\[
S_{\ell_1, \ell_2}(E, x) = 1 + \sum_{p \leq x \atop p \not| \ell_1 \ell_2 N} \left( \frac{4p}{\ell_1} \right) \left( \frac{4p - a_p(E)^2}{\ell_2} \right) + \sum_{p \leq x \atop p | \ell_1 \ell_2 N} \left( \frac{4p}{\ell_1} \right) \left( \frac{4p - a_p(E)^2}{\ell_2} \right) = -1
\]
where
\[
C_1 := \left\{ (g_1, g_2) \mid \left( \frac{4 \det g_1 - (\text{tr} g_2)^2}{\ell_1} \right) = 1 \right\},
\]
\[
C_2 := \left\{ (g_1, g_2) \mid \left( \frac{4 \det g_1 - (\text{tr} g_2)^2}{\ell_1} \right) = -1 \right\}.
\]
are (conjugate) subsets of $\text{PGL}_2(\mathbb{Z}/\ell_1\ell_2\mathbb{Z})$ (i.e. $(g_1, g_2) \in \text{PGL}_2(\mathbb{Z}/\ell_1\ell_2\mathbb{Z})$ in our setting), and $F_{\ell_1, \ell_2, E}$ is the extension $F_{\ell_1, E}F_{\ell_2, E}$ introduced as above.

In [2], the authors then give that if $\ell_1 \equiv \ell_2 \pmod{4}$, then

$$|C_1 \cup C_2| = \frac{(\ell_1^3 - \ell_2^3)(\ell_1^3 - \ell_2^3)}{2} - \frac{\ell_1^3(\ell_1^2 - \ell_2^2)}{2} - \frac{\ell_2^3(\ell_1^2 - \ell_2^2)}{2} + \ell_1\ell_2,$$

$$|C_3 \cup C_4| = \frac{(\ell_1^3 - \ell_2^3)(\ell_1^3 - \ell_2^3)}{2} - \frac{\ell_1^3(\ell_1^2 - \ell_2^2)}{2} - \frac{\ell_2^3(\ell_1^2 - \ell_2^2)}{2};$$

otherwise, one has

$$|C_1 \cup C_2| = \frac{(\ell_1^3 - \ell_2^3)(\ell_1^3 - \ell_2^3)}{2} - \frac{\ell_1^3(\ell_1^2 - \ell_2^2)}{2} - \frac{\ell_2^3(\ell_1^2 - \ell_2^2)}{2},$$

$$|C_3 \cup C_4| = \frac{(\ell_1^3 - \ell_2^3)(\ell_1^3 - \ell_2^3)}{2} - \frac{\ell_1^3(\ell_1^2 - \ell_2^2)}{2} - \frac{\ell_2^3(\ell_1^2 - \ell_2^2)}{2} + \ell_1\ell_2.$$

Since we are choosing $\ell_1$ and $\ell_2$ such that the mod $\ell_1\ell_2$ Galois representation associated to $E$ is surjective, the size of the image of this representation is

$$|\text{PGL}_2(\mathbb{Z}/\ell_1\ell_2\mathbb{Z})| = (\ell_1^3 - \ell_2^3)(\ell_1^3 - \ell_2^3).$$

Also the number of conjugacy classes of $\text{PGL}_2(\mathbb{Z}/\ell_1\ell_2\mathbb{Z})$ is

$$|\langle \text{PGL}_2(\mathbb{Z}/\ell_1\ell_2\mathbb{Z})\rangle^\#| \asymp \ell_1\ell_2.$$

Thus, M. R. Murty-V. K. Murty’s effective Chebotarëv density theorem then allows one to deduce that (under GRH, AC, and $\text{PCC}(\chi(1), 1, 1)$)

$$S_{\ell_1, \ell_2}(E, x) = \pi_{C_1 \cup C_2}(x, F_{\ell_1, \ell_2, E}/\mathbb{Q}) - \pi_{C_3 \cup C_4}(x, F_{\ell_1, \ell_2, E}/\mathbb{Q})$$

$$= \kappa_{\ell_1, \ell_2}\pi(x) + O \left( \ell_1^{3/2}\ell_2^{1/2}\ell_1^{-1/2}\ell_2^{-1/2}x^{1/2}\log(\ell_1\ell_2Nx) \right)$$

$$= \kappa_{\ell_1, \ell_2}\pi(x) + O \left( \ell_1\ell_2x^{1/2}\log(\ell_1\ell_2Nx) \right),$$

as

$$\left( \frac{|\langle \text{PGL}_2(\mathbb{Z}/\ell_1\ell_2\mathbb{Z})\rangle^\#|}{|\text{PGL}_2(\mathbb{Z}/\ell_1\ell_2\mathbb{Z})|} \right)^{1/2} \asymp \ell_1^{-1/2}\ell_2^{-1/2}.$$

If one would like to apply Corollary 5.2, then the power $1/4$ can be replaced by $1/2$, and hence

$$S_{\ell_1, \ell_2}(E, x) = \kappa_{\ell_1, \ell_2}\pi(x) + O \left( \ell_1^{1/2}\ell_2^{1/2}x^{1/2}\log(\ell_1\ell_2Nx) \right),$$

where

$$\kappa_{\ell_1, \ell_2} := \frac{|C_1 \cup C_2| - |C_3 \cup C_4|}{|\text{PGL}_2(\mathbb{Z}/\ell_1\ell_2\mathbb{Z})|}.$$
Now following Cojocaru and David [2, pp. 1554], applying the square sieve and the above estimates, one has

\[
\Pi_E(K, x) \ll \frac{x \log z}{z \log x} + z^{2\theta} x^{1/2} \log(zN^2)
\]

\[
\quad + \frac{x \log z}{z \log x} \log D + \frac{x \log z}{z}
\]

\[
\quad + \frac{x(\log z)^2}{z^2 \log x} (\log D)^2 + \frac{x(\log z)^2}{z^2} \log D + \frac{x \log x (\log z)^2}{z^2},
\]

where \( K = \mathbb{Q}(\sqrt{-D}) \), \( z = z(x) \) is a positive number depending on \( x \), and where \( \theta = 1 \) (obtained by Cojocaru and David via M. R. Murty-V. K. Murty’s theorem), and \( \theta = 1/2 \) (obtained by applying our refinement).

Then by taking

\[ z = x^{1/6}, \]

one has

\[ \Pi_E(K, x) \ll x^{5/6} \log x; \]

by taking

\[ z = x^{1/4}, \]

we have

\[ \Pi_E(K, x) \ll x^{3/4} \log x. \]

10. CONCLUDING REMARKS

As shown in the previous sections, our effective Chebotarev density theorem yields sharp error terms for several arithmetical problems. We expect that there will be more applications of our result. On the other hand, it seems to be a natural desire for one to impose a stronger pair correlation conjecture to obtain another effective version of the Chebotarev density theorem with a shaper error term. We, however, note that as discussed in Section 8, our effective Chebotarev density theorem already gives the error term predicted by Lang and Trotter (up to some log-saving) via a projection method. Thus, we believe that instead of expecting further improvement of effective Chebotarev density theorem, one shall search new ideas to move forward.

REFERENCES