J. Ramanujan Math. Soc. **33,** No.4 (2018) 399–426

The Chebotarev density theorem and the pair correlation conjecture

M. Ram Murty[1], V. Kumar Murty[2] and Peng-Jie Wong[3]

[1,3]*Department of Mathematics and Statistics, Queen's University, Kingston, Ontario K7L 3N6, Canada*
e-mail: murty@mast.queensu.ca; pjwong@mast.queensu.ca

[2]*Department of Mathematics, University of Toronto, Toronto, Ontario M5S 2E4, Canada*
e-mail: murty@math.utoronto.ca

Communicated by: Prof. Sanoli Gun

Received: May 11, 2017

Abstract. In this note, we formulate pair correlation conjectures and refine the effective version of the Chebotarev density theorem established by the first two authors. Also, we apply our result to study Artin's primitive root conjecture and the Lang-Trotter conjectures and obtain shaper error terms.

2010 Mathematics Subject Classification: 11M26, 11N45, 11R44.

1. Introduction

In order to study arithmetic problems via L-functions, the key is the location of the zeros and poles, originated from Riemann's remarkable insight of the connection between the distribution of primes and his zeta function. Such aspects also play a central role in studying the primes in number fields. Indeed, it has been shown 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 [15], which refines the previous works of Lagarias-Odlyzko [10] and Serre [23]. Moreover, in their unpublished paper written more than 20 years ago, the first two authors improved their result by assuming a certain pair correlation conjecture, which will be discussed in Section 3, and the Artin (holomorphy) conjecture.

Research of the first two authors is partially supported by NSERC Discovery grants.

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 conjectures have been studied by M. R. Murty with Perelli [16] and Zaharescu [17]. Nevertheless, the first two authors 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 for applications.

The primary purpose of this note is giving a refinement with a self-contained proof for the unpublished result of the first two authors. As shall be seen, our result allows one to derive a further "small" saving in powers of the main variable. Also, we shall demonstrate what this saving will yield.

1.1 The Chebotarev density theorem

Throughout this note, we will make use of some standard notation as follows. We shall always let K/k be a Galois extension of number fields with Galois group G. Let C be a union of conjugacy classes in G. For every unramified prime $\mathfrak{p}$ of k, $\sigma_{\mathfrak{p}}$ denotes the Artin symbol at $\mathfrak{p}$. Let us define $\pi_C(x) = \#\{\mathfrak{p} \mid \mathfrak{p} \text{ is unramified with } N\mathfrak{p} \leq x \text{ and } \sigma_{\mathfrak{p}} \subseteq C\}$. The celebrated Chebotarev density theorem states that

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

as $x \to \infty$, where $\pi_k(x) = \#\{\mathfrak{p} \mid \mathfrak{p} \text{ is a prime of } k \text{ with } N\mathfrak{p} \leq x\}$. If the generalised Riemann hypothesis (denoted GRH) for the Dedekind zeta function $\zeta_K(s)$ of K is assumed, an effective version of this theorem with explicit error terms was established by Lagarias and Odlyzko in their fundamental paper [10], and then refined by Serre [23]. In particular, under GRH, one has

$$\pi_C(x) = \frac{|C|}{|G|}\pi_k(x) + O\left(\frac{|C|}{|G|}x^{\frac{1}{2}}(\log d_K + n_K \log x)\right), \tag{1.1}$$

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 [23].

In [15], 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 for any union of conjugacy classes in G,

$$\pi_C(x) = \frac{|C|}{|G|}\pi_k(x) + O\big(|C|^{\frac{1}{2}}x^{\frac{1}{2}}n_k \log M(K/k)x\big), \tag{1.2}$$

where $n_k = [k : \mathbb{Q}]$,

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

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

If one writes the error term in (1.1) as

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

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 [15]), and the problem of primitive points on elliptic curves (cf. [7]).

1.2 The implication of pair correlation conjectures

A pair correlation conjecture (denoted PCC) of Artin L-functions was formulated by the first two authors in their unpublished work. A general formulation of PCC will be stated formally in Section 3. Also, it will be noticed that our conjectures are not as strong as the usual formulations as we only require a weak upper bound rather than a uniform asymptotic formula. Furthermore, under GRH, AC, and PCC, the first two authors proved the following (unpublished) result.

Theorem 1.1. *Under the assumption that GRH, AC, and PCC are valid for all Artin L-functions attached to irreducible characters of G. One has*

$$\pi_C(x) = \frac{|C|}{|G|}\pi_k(x) + O\left(n_k^{\frac{1}{2}}|C|^{\frac{1}{2}}\left(\frac{|G^{\#}|}{|G|}\right)^{\frac{1}{4}}x^{\frac{1}{2}}\log M(K/k)x\right), \quad (1.3)$$

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 $(|G^{\#}|/|G|)^{1/4}$ appears in the error term. Second, the n_k in (1.2) is replaced by $n_k^{1/2}$. From this, it is natural to expect significant gains in applications to "highly non-abelian" contexts (i.e., 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 PCC hold for all Artin L-functions of G, we have*

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

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

Remark. Clearly, the improvement over Theorem 1.2 lies in the factor $(|G^{\#}|/|G|)^{1/2}$. We shall, however, point out that PCC used in Theorem 1.2 is slightly stronger than Theorem 1.1. Indeed, the PCC in Theorem 1.2 requires a better spacing of zeros of associated Artin L-functions (cf. Theorem 5.1 and Corollary 5.2).

Also, as can be seen, our PCC does depend on the Galois extension K/k. Hence, for most arithmetic applications (see the next section), one, in fact, usually assumes a sequence of the pair correlation conjectures for associated Galois extensions.

1.3 Some applications

1.3.1 Artin's primitive root conjecture

Let us first consider Artin's primitive root conjecture. This conjecture asserts that for any non-zero integer a, which is not ± 1 nor 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

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

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].

We also note that the first two authors applied Theorem 1.1 instead of just GRH to derive

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

We shall improve this result later as the following. (We note that in Section 3, fixing a Galois extension K/k, for each irreducible character χ of $\mathrm{Gal}(K/k)$, we formulate a pair correlation hypothesis $PCC(\chi; m_\chi, c_\chi, r)$ where $m_\chi \in [1, \chi(1)]$, $c_\chi \in (0, 1]$ and $r \in [1, 2]$.)

Corollary 1.3. *Under the assumption that GRH and* $PCC(\chi; \chi(1), \chi(1)^{-1}, 1)$ *hold for all Artin L-functions of* $\mathrm{Gal}(K_m/\mathbb{Q})$*, we have*

$$N_a(x) = c(a)\,\mathrm{Li}\,x + O(x^{4/5}(\log ax)).$$

1.3.2 Elliptic analogues of Artin's primitive root conjecture

There are several related problems in the theory of elliptic curves to which our result 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 [4]). The following cyclicity problem was first considered by Serre [20]. Given an elliptic curve E over $\mathbb{Q}$ and of conductor N, one may ask about the number $f(x, E)$ of primes $p \le x$ such that $E(\mathbb{F}_p)$ is cyclic, where $E(\mathbb{F}_p)$ denotes the group of $\mathbb{F}_p$-rational points of $E/\mathbb{F}_p$. Under GRH Serre [20] (see also [14]) adapted Hooley's method to prove 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. (We remark that by the work of Gupta and M. R. Murty [7], one has an unconditional result concerning this problem.) This has been improved by Cojocaru and M. R. Murty [4, Theorem 1.1] that (under GRH)

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

Furthermore, applying (1.3) in this context and assuming GRH, AC, and PCC for all Artin L-functions of division fields of E, they derived

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

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

In this note, we shall apply Theorem 1.2 to derive the following estimate.

Corollary 1.4. *If GRH, AC, and* $PCC(\chi; \chi(1), \chi(1)^{-1}, 1)$ *hold for all Artin L-functions of all division fields of E, then*

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

1.3.3 The Lang-Trotter conjectures

In the later part of this note, we will consider the Lang-Trotter conjecture on Fourier coefficients of (non-CM) modular forms f of integral weight $k \geq 2$ and level N. Assume f is a normalised Hecke eigenform, and write its Fourier expansion as

$$f(z) = \sum_{n \geq 1} a_f(n) \exp(2\pi i n z).$$

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, the first two authors obtained an estimate of the form $O(x^{3/4})$. Moreover, if $a = 0$, they derived a bound of type $O(x^{2/3})$. From Theorem 1.2, one can improve their estimates as follows.

Corollary 1.5. *Assume GRH, AC, and* $PCC(\chi; \chi(1), \chi(1)^{-1}, 1)$ *are valid for all* χ *arising from all Galois extensions given by residual representations associated to* f *(see Section 8 for the precise description of such representations and Galois extensions). Then*

$$\pi_{f,a}(x) \ll \begin{cases} x^{2/3} (\log x)^{1/3} \text{ if } a \neq 0, \\ x^{1/2} \log x \text{ if } a = 0. \end{cases}$$

We remark that for the case that $a = 0$, the estimate is as predicted by Lang-Trotter (up to some log-saving). 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 $\mathbb{Q}$ and of conductor N. For any prime $p \nmid N$, we write

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

As Hasse's bound gives $|a_p(E)| \leq 2\sqrt{p}$, 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 $\mathbb{Q}$. 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)

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

and an effective Chebotarev density theorem to "obtain" $\theta = 9/10$ (again, no proof was given). The first proof, appearing in the literature, is due to Cojocaru, Fouvry, and M. R. Murty [3], who used the square sieve to show that under GRH, one has

$$\Pi_E(K, x) \ll_N x^{17/18} \log x,$$

where the estimate only depends on the conductor N of E and is uniform in K. Furthermore, the authors in [3] include new remarks made by Serre that under GRH, the mixed Galois representation method combining with a PGL_2-reduction would lead to

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

with an unspecified implicit constant.

In light of the above-mentioned works, Cojocaru and David [2] improved upon Serre's mixed Galois representation method, under GRH, that

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

Moreover, if AC and PCC are assumed, they gave

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

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)

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

(Although the power of x is $3/4$ in [2, Corollary 4], we, however, note that owing to a small arithmetic mistake, which will be seen in the last section, it should be $5/6$ as stated above.) As mentioned in [2], although such an estimate is not as good as the result obtained by using Serre's method, this, however, is independent of the number field K, which is essential for some applications. Last but not least, we remark that the authors of [2] did consider specific

fields associated to E and then used a sequence of GRH, AC, and PCC for the Artin L-functions of these fields. We shall call such fields "Frobenius fields" of E (see Section 9 for more details). At the end of this note, we shall apply Theorem 1.2 to derive the following improvement.

Corollary 1.6. *Assume GRH, AC, and* $PCC(\chi; \chi(1)^{1/2}, 1, 1)$ *hold for all Artin L-functions of all Frobenius fields of E, one has*

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

If $PCC(\chi; \chi(1), \chi(1)^{-1}, 1)$ *is further assumed, then*

$$\Pi_E(K, x) \ll_N x^{3/4} \log x,$$

and

$$\Pi_E(K, x) \ll_{N,K} x^{2/3} (\log x)^{1/2}.$$

2. Lemmata

In this section, we shall collect two lemmata developed in [15], which will play the main role in "saving power" later.

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

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

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.

To count primes, one also needs the estimate below.

Lemma 2.2 ([15]). *Let* χ *be an irreducible character of G. Then*

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

where $\mathfrak{f}(\chi)$ *denotes the (global) Artin conductor of irreducible character* χ.

3. Pair correlation functions

Let $\mathfrak{f}(\chi)$ denote the Artin conductor of an irreducible character χ of $G = \mathrm{Gal}(K/k)$, and let $A_\chi = d_K^{\chi(1)} N\mathfrak{f}(\chi)$ denote the conductor of χ. Let us further 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 $L(s, \chi, K/k)$. We define the pair correlation function for $L(s, \chi, K/k)$ as

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

where γ_1, γ_2 range over the imaginary parts of zeros of $L(s, \chi, K/k)$ on the critical line (counted according to multiplicity), and $\mathbf{e}(t) := \exp(2\pi i t)$. Let us also define $\mathcal{A}_\chi(T)$ by

$$\log \mathcal{A}_\chi(T) := \log A_\chi + \chi(1) n_k \log T.$$

By standard analytic number theory, we have the following estimate.

Proposition 3.1.

$$\mathcal{P}_T(X, \chi) \ll T(\log \mathcal{A}_\chi(T))^2.$$

Proof. First observe that

$$\mathcal{P}_T(X, \chi) = \sum_{j=0}^{2T} \sum_{\substack{-T \le \gamma_1, \gamma_2 \le T \\ j \le |\gamma_1 - \gamma_2| < j+1}} w(\gamma_1 - \gamma_2)\mathbf{e}((\gamma_1 - \gamma_2)X),$$

which is

$$\ll \sum_{|\gamma_1| \le T} \sum_{j=0}^{2T} \frac{1}{1+j^2} \left(\sum_{|\gamma_1 + j| \le \gamma_2 < |j+1+\gamma_1|} 1 + \sum_{|\gamma_1 + j| \ge -\gamma_2 > |j+1+\gamma_1|} 1 \right).$$

According to [15, 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

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

This is easily seen to be

$$\ll (\log A_\chi + \chi(1)n_k \log T) \sum_{|\gamma_1| \le T} 1 \ll T(\log A_\chi + \chi(1)n_k \log T)^2,$$

as desired. □

Now, we shall make the following pair correlation conjecture (for the Artin L-function $L(s, \chi, K/k)$) with respect to $1 \le m_\chi$, $0 < c_\chi \le 1$, and $1 \le r \le 2$, denoted $PCC(\chi; m_\chi, c_\chi, r)$.

Conjecture 3.2. Let $A > 0$. There exist $m_\chi \in [1, \chi(1)]$, $c_\chi \in (0, 1]$, and $r \in [1, 2]$ so that if

$$0 \le Y \le Am_\chi n_k \log T,$$

one has

$$\mathcal{P}_T(Y, \chi) \ll_A c_\chi T(\log \mathcal{A}_\chi(T))^r.$$

Remark. By Proposition 3.1, this pair correlation conjecture holds (under GRH) whenever $c_\chi = 1$ and $r = 2$, and it is easy to see that the content of this conjecture is in reducing the power of $\log \mathcal{A}_\chi(T)$ and the leading coefficient. Also, 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, the first two authors have conjectured that for $0 \le Y \le A\chi(1)n_k \log T$, one has

$$\mathcal{P}_T(Y, \chi) \ll_A T(\log \mathcal{A}_\chi(T)).$$

In our language, this is $PCC(\chi; \chi(1), 1, 1)$. We shall, however, show that one can use a weaker hypothesis $PCC(\chi; \chi(1)^{1/2}, 1, 1)$ to obtain the effective Chebotarev density theorem with the same error as in (1.1). Indeed, we will state our effective version of the Cheboatrev density theorem, i.e., Theorem 5.1, with respect to the parameters m_χ, c_χ, and r.

4. The sum $S(T, v, \chi, X)$

Now let us borrow some results of Heath-Brown [8]. Let γ run over an arbitrary countable set and consider

$$\sum_{0 < \gamma \le T} \mathbf{e}(\gamma(v + X)).$$

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

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

By the identity that

$$\int_{-\infty}^{\infty} k(\upsilon)\mathbf{e}(\upsilon x)d\upsilon = w(x),$$

a direct calculation gives

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

In light of [8, Lemma 4], the first two authors derived an estimate for $S(T, 0, \chi, X)$ for all irreducible characters of G. However, since their work is unpublished and we now use a slightly different PCC, we shall give a proof below.

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 $S(T, \upsilon) = S(T, \upsilon, \chi, X)$ as χ and X will be fixed. By Montgomery [13, Lemma 1.1], if f is a C^1-function on $[-1, 1]$,

$$f(0) \ll \int_{-1}^{1} |f'(\upsilon)|d\upsilon + \int_{-1}^{1} |f(\upsilon)|d\upsilon.$$

Hence, we have

$$|S(T, 0)|^2 \ll \int_{-1}^{1} |S(T, \upsilon)||S_\upsilon(T, \upsilon)|d\upsilon + \int_{-1}^{1} |S(T, \upsilon)|^2 d\upsilon,$$

where $S_\upsilon(T, \upsilon)$ denotes the partial derivative of $S(T, \upsilon)$ with respect to υ. Clearly,

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

Also, the Cauchy-Schwarz inequality yields

$$\int_{-1}^{1} |S(T, \upsilon)||S_\upsilon(T, \upsilon)|d\upsilon$$

$$\ll \left(\int_{-\infty}^{\infty} k(\upsilon)|S(T, \upsilon)|^2 d\upsilon\right)^{\frac{1}{2}} \left(\int_{-\infty}^{\infty} k(\upsilon) \left|\sum_{0<\gamma \leq T} \gamma\, \mathbf{e}(\gamma(\upsilon + X))\right|^2 d\upsilon\right)^{\frac{1}{2}}.$$

Applying the Abel summation formula, one has

$$\sum_{0<\gamma\leq T} \gamma\, \mathbf{e}(\gamma\,(\upsilon + X)) = T S(T, \upsilon) - \int_0^T S(t, \upsilon) dt$$

which implies that

$$\int_{-\infty}^{\infty} k(\upsilon) \left| \sum_{\gamma} \gamma\, \mathbf{e}(\gamma\,(\upsilon + X)) \right|^2 d\upsilon$$

$$\ll T^2 \int_{-\infty}^{\infty} k(\upsilon) |S(T, \upsilon)|^2 d\upsilon + T \int_0^T \int_{-\infty}^{\infty} k(\upsilon) |S(t, \upsilon)|^2 d\upsilon dt.$$

Finally, putting everything together gives

$$\begin{aligned} |S(T, 0, \chi, X)|^2 &\ll \mathcal{P}_T(X, \chi)^{\frac{1}{2}} \left(T^2 \mathcal{P}_T(X, \chi) + T \int_0^T \mathcal{P}_t(X, \chi) dt \right)^{\frac{1}{2}} \\ &\quad + \mathcal{P}_T(X, \chi) \\ &\ll T \max_{t \leq T} |\mathcal{P}_t(X, \chi)|, \end{aligned}$$

as required. □

Proposition 4.2. *Conjecture 3.2 implies that for any* $X \leq \frac{1}{2} A m_\chi n_k \log T$, *one has*

$$S(T, 0, \chi, X) \ll_A T^{\frac{3}{4}} \log \mathcal{A}_\chi(T) + \sqrt{c_\chi} T (\log \mathcal{A}_\chi(T))^{\frac{r}{2}}.$$

Proof. Observe that by Proposition 4.1,

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

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

$$X \leq \frac{1}{2} A m_\chi n_k \log T,$$

then clearly $X \leq A m_\chi n_k \log t$. In this range, we may apply the pair correlation conjecture to deduce the estimate

$$\max_{\sqrt{T} \leq t \leq T} \mathcal{P}_t(X, \chi) \ll_A \max_{\sqrt{T} \leq t \leq T} c_\chi t (\log \mathcal{A}_\chi(t))^r \leq c_\chi T (\log \mathcal{A}_\chi(T))^r$$

for the second term. Also, Proposition 3.1 tells us that

$$\max_{t\le\sqrt{T}} \mathcal{P}_t(X,\chi) \ll T^{\frac{1}{2}}(\log \mathcal{A}_\chi(T))^2,$$

which completes the proof. □

5. An effective version of the Chebotarev density theorem

As before, K/k denotes a Galois extension of number fields with Galois group G. Also, for any conjugate set C of G, let us define

$$\psi_C(x) := \sum_{\substack{N\mathfrak{p}^m\le x\\ \sigma_{\mathfrak{p}^m}\subseteq C}} \log N\mathfrak{p},$$

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

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

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

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.

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

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

In particular, $PCC(\chi; \chi(1)^{1/2}, 1, 1)$ *implies that*

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

Furthermore, if $PCC(\chi; \chi(1), \chi(1)^{-1}, 1)$ *is assumed, we have*

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

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

$$\psi(x, f) := \sum_{\substack{N\mathfrak{p}^m \le x \\ \sigma_{\mathfrak{p}}{}^m \subseteq C}} f(\sigma_{\mathfrak{p}}^m)\log N\mathfrak{p},$$

for any class function f on G. In particular, for the indicator function δ_C,

$$\psi(x, \delta_C) = \psi_C(x).$$

Theorem 5.3. *Under the same assumption as in the previous theorem. For* $A \ge \frac{1}{\pi n_k}$ *we have the estimate*

$$\psi(x, \chi) - \delta(\chi)x \ll_A x^{\frac{1}{2}}\log x\left((Am_\chi n_k)^{-1}\log \mathcal{A}_\chi(x) + \sqrt{c_\chi}(\log \mathcal{A}_\chi(x))^{\frac{r}{2}}\right),$$

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

Proof. We shall begin by developing an explicit formula as in [19], which has been established for general L-functions (under the holomorphy assumption) by V. K. Murty [18] applying a method based on [10]. For any $2 \le T \le x$, one has

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

where, as later, the sum is over the imaginary parts γ of the non-trivial zeros ρ of $L(s, \chi, K/k)$. Recall the associated pair correlation function is

$$S(T, \upsilon, \chi, X) = \sum_{0<\gamma\le T}\mathbf{e}(\gamma(\upsilon + X)),$$

where the sum runs over the imaginary parts (in absolute value) of non-trivial zeros of $L(s, \chi, K/k)$.

Now applying Abel's summation gives

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

which by integration by parts, is

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

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

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

where

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

Now we write $X = (\log x)/2\pi$. From Propositions 3.1 and 4.1, it follows that

$$\begin{aligned}\int_2^{x^{1/\pi A m_\chi n_k}} t^{-2}|S(t,\upsilon,\chi,X)|dt &\ll \int_2^{x^{1/\pi A m_\chi n_k}} t^{-1}(\log \mathcal{A}_\chi(t))dt \\ &\ll \frac{\log x}{A m_\chi n_k}\log \mathcal{A}_\chi(x).\end{aligned}$$

For the remaining range, Proposition 4.2 allows us to derive

$$\begin{aligned}&\int_{x^{1/\pi A m_\chi n_k}}^T t^{-2}|S(t,\upsilon,\chi,X)|dt \\ &\quad\ll \int_{x^{1/\pi A m_\chi n_k}}^T t^{-2}\left(t^{\frac{3}{4}}\log \mathcal{A}_\chi(t) + \sqrt{c_\chi}\,t(\log \mathcal{A}_\chi(t))^{\frac{r}{2}}\right)dt \\ &\quad\ll \left(x^{-1/4\pi A m_\chi n_k} + T^{-1/4}\right)\left(\log \mathcal{A}_\chi(T)\right) \\ &\qquad + (\log T)\sqrt{c_\chi}(\log \mathcal{A}_\chi(T))^{\frac{r}{2}}.\end{aligned}$$

Finally, choosing $T = x$, we deduce that $\psi(x, \chi) - \delta(\chi)x$ is

$$\begin{aligned}
&\ll x^{\frac{1}{2}}\big(\log \mathcal{A}_\chi(x) + \log \mathcal{A}_\chi(2)\big) \\
&\quad + x^{\frac{1}{2}}\left(\frac{\log x}{Am_\chi n_k}\log \mathcal{A}_\chi(x) + \big(x^{-1/4\pi Am_\chi n_k} + x^{\frac{-1}{4}}\big)\right. \\
&\qquad \left.\times\ (\log \mathcal{A}_\chi(x)) + (\log x)\sqrt{c_\chi}(\log \mathcal{A}_\chi(x))^{\frac{r}{2}}\right) \\
&\quad + \log x \log \mathcal{A}_\chi(x) + \chi(1)\log x\left(\frac{\log d_K}{|G|} + n_k x^{\frac{1}{2}}\right).
\end{aligned}$$

□

Now we are in a position to prove Theorem 5.1.

Proof of Theorem 5.1. By the estimate $\log A_\chi \ll \chi(1)n_k \log M(K/k)$, we have

$$\sum_{\chi\in\mathrm{Irr}(G)} c_\chi(\log \mathcal{A}_\chi(x))^r \ll \sum_{\chi\in\mathrm{Irr}(G)} c_\chi \chi(1)^r n_k^r (\log M(K/k)x)^r,$$

$$\sum_{\chi\in\mathrm{Irr}(G)} \big((Am_\chi n_k)^{-1}\log \mathcal{A}_\chi(x)\big)^2 \ll A^{-2}\sum_{\chi\in\mathrm{Irr}(G)} m_\chi^{-2}\chi(1)^2(\log M(K/k)x)^2.$$

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

$$\begin{aligned}
&\sum_{\chi\in\mathrm{Irr}(G)} |\psi(x, \chi) - \delta(\chi)x|^2 \\
&\quad \ll x(\log x)^2 n_k^r \sum_{\chi\in\mathrm{Irr}(G)} (c_\chi\chi(1)^r + m_\chi^{-2}\chi(1)^2)(\log M(K/k)x)^2.
\end{aligned}$$

This estimate and the Cauchy-Schwarz inequality yield that

$$\begin{aligned}
&\sum_C \frac{1}{|C|}\left|\psi(x, \delta_C) - \frac{|C|}{|G|}x\right|^2 \\
&\quad \le \sum_C \frac{2}{|C|}\left|\psi(x, \delta_C) - \frac{|C|}{|G|}\psi(x, 1_G)\right|^2 \\
&\qquad + \sum_C \frac{2}{|C|}\left|\frac{|C|}{|G|}\psi(x, 1_G) - \frac{|C|}{|G|}x\right|^2
\end{aligned}$$

$$= \frac{2}{|G|} \sum_{\chi \neq 1_G} |\psi(x, \chi)|^2 + \frac{2}{|G|}(\psi(x, 1_G) - x)^2$$

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

as desired. □

6. Artin's primitive root conjecture

Let $a \neq 0, \pm 1$ be a square-free integer, and consider

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

Artin's primitive root conjecture says that $N_a(x) \sim c(a) \operatorname{Li} x$, as $x \to \infty$, for some constant $c(a)$ only depending on a.

Following Artin, 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

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

We again note that the first two authors proved that if GRH and $PCC(\chi; \chi(1), 1, 1)$ are valid for all Artin L-functions attached to irreducible characters of $\mathrm{Gal}(L_m/\mathbb{Q})$, then one has

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

In light of their strategy, we shall prove Corollary 1.3.

Proof of Corollary 1.3. We first note that the Artin (holomorphy) conjecture holds in our consideration since $\mathrm{Gal}(K_m/\mathbb{Q})$ is metabelian. Denote by $\pi_m(x)$ the number of primes $p \leq x$ that split completely in K_m. Applying Corollary 5.2, we deduce that

$$\pi_m(x) = \frac{1}{n_m} \operatorname{Li} x + O\left(\left(\frac{x}{m}\right)^{1/2} (\log M_m x)\right),$$

where $n_m = [K_m : \mathbb{Q}]$ and $M_m = M(K_m/\mathbb{Q})$.

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

$$\log M_m x \ll \log(amx).$$

On the other hand, 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 K_m. Now the above estimate tells us that for $y \leq x$,

$$\sum_{m \leq y} \mu(m) \left(\pi_m(x) - \frac{1}{n_m} \operatorname{Li} x \right) \ll x^{1/2} y^{1/2} \log(ayx).$$

Thus, we have

$$\sum_{y \leq m \leq x} \pi_m(x) \ll \sum_{p \leq x} \sum_{\substack{y \leq m \leq x \\ m \mid (p-1) \\ p \mid a^{(p-1)/m} - 1}} 1,$$

where the summations on the right are bounded by

$$\sum_{v \leq x/y} \sum_{p \mid a^v - 1} 1 \ll (x/y)^2 (\log a).$$

Finally, choosing $y = x^{3/5}$ gives the desired result. □

We remark that the key estimates in the above proof are due to Hooley [9] and Gupta-M. R. Murty [6] (see also [14]).

7. Elliptic analogues of Artin's primitive root conjecture

As before, let E be an elliptic curve defined over $\mathbb{Q}$ and of conductor N, and set $f(x, E)$ to be the number of primes $p \leq x$ for which $p \nmid N$ and $E(\mathbb{F}_p)$ is cyclic. Under GRH, Serre [20] (see also [14]) adapted Hooley's method to prove 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 due to Gupta-M. R. Murty [7]. Moreover, applying their method and (1.3) and assuming GRH, AC, and the PCC for all Artin L-functions attached to irreducible characters of $\mathrm{Gal}(\mathbb{Q}(E[k])/\mathbb{Q})$'s, Cojocaru and M. R. Murty [4] derived

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

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

Before we prove our result, we shall borrow the following key ingredients from [4]. As discussed in [4, 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 [4], 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 that are divisors of $A(E)$ and k_2 composed of primes that are coprime to $A(E)$. Then [4, Proposition 3.6] asserts

$$n(k) \geq \phi(k_1)n(k_2) \gg \phi(k)k_2^3.$$

Moreover, by Hasse's inequality, they showed that

$$\sum_{\text{error}} \ll \frac{x^{3/2}}{y^2} + x^{1/2} \log \frac{x}{y} + \frac{x}{y}$$

unconditionally (see [4, Section 4]). Now we shall prove Corollary 1.4.

Proof of Corollary 1.4. In light of Cojocaru and M. R. Murty's method, we handle $\sum_{\text{main}}$ by our effective Chebotarev density theorem, Corollary 5.2. 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

$$\ll \sum_{\substack{k \leq y \\ \text{k square-free} \\ k = k_1 k_2}} \left(\frac{|\operatorname{Gal}(\mathbb{Q}(E[k])/\mathbb{Q})^{\#}|}{n(k)} \right)^{\frac{1}{2}} x^{\frac{1}{2}} (\log M(\mathbb{Q}(E[k])/\mathbb{Q})x).$$

Since the ramified primes of $\mathbb{Q}(E[k])/\mathbb{Q}$ are divisors of kN (see, for example, [4, Proposition 3.5]) and from [4, p. 615], one has

$$\frac{|\operatorname{Gal}(\mathbb{Q}(E[k])/\mathbb{Q})^{\#}|}{n(k)} \ll \frac{k_1^2}{k_2^2},$$

for $y \leq x$, the error $E(x)$ is

$$\ll x^{\frac{1}{2}} \sum_{\substack{k \leq y \\ \text{k square-free} \\ k=k_1k_2}} \left(\frac{k_1}{k_2}\right) (\log kNx) \ll x^{\frac{1}{2}} (\log Nx) \sum_{k_1} k_1 \sum_{k_2 \leq \frac{y}{k_1}} k_2^{-1}$$

As $\sum_{k_2 \leq \frac{y}{k_1}} k_2^{-1} \ll \log y$, we then have

$$E(x) \ll x^{\frac{1}{2}} (\log Nx)(\log y) A(E) 2^{\nu(A(E))} \ll x^{\frac{1}{2}} (\log Nx)(\log y) A(E)^2,$$

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

$$\sum_{\text{error}} \ll \frac{x^{3/2}}{y^2} + x^{1/2} \log \frac{x}{y} + \frac{x}{y},$$

and choosing $y = x^{1/2}$, we then deduce

$$f(x, E) = \left(\sum_{k \leq y} \frac{\mu(k)}{n(k)}\right) \operatorname{Li} x + O\big(x^{1/2} (\log Nx)(\log x) A(E)^2\big).$$

Finally, we further borrow an estimate for the "tail" from [4, Equation (18)]

$$\sum_{\substack{k > y \\ \text{k square-free} \\ k=k_1k_2}} \frac{1}{n(k)} \ll \frac{\log \log y}{y^3} A(E)^3$$

to deduce

$$f(x, E) = c(E) \operatorname{Li} x + O\big(x^{1/2} (\log Nx)(\log x) A(E)^2\big) + O\left(\frac{\log \log x}{x^{1/2} \log x} A(E)^3\right),$$

as required. □

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 ϵ for the congruence subgroup $\Gamma_0(N)$. Suppose that f is 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 $a_f(n)$'s over $\mathbb{Z}$. As in Serre [23], 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 is a family of λ-adic representations (à la Deligne [5])

$$\rho_{f,\lambda} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathcal{O}_\lambda)$$

where λ is a prime of K_f and $\mathcal{O}_\lambda$ denotes the completion of $\mathcal{O}$ at λ. Let $\ell = \ell(\lambda)$ be the rational prime underlying λ. Then $\rho_{f,\lambda}$ is unramified outside ℓN, and admits the property that for any prime p coprime to ℓN, 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 [12] and Ribet [21], for ℓ sufficiently large (as a function of f and N), there exists a subgroup H of finite index in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ 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 λ 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_ℓ of trace a has order

$$|C_a| \asymp \ell^3.$$

Thus, we deduce that

$$\pi_{C_a}(x) = \frac{1}{\ell}\frac{x}{\log x} + O(\ell^{\frac{1}{2}}x^{\frac{1}{2}}(\log \ell x)).$$

Now choosing $\ell \asymp x^{1/3}/(\log x)^{4/3}$, we then derive

$$\pi_{f,a}(x) \ll x^{\frac{2}{3}}(\log x)^{\frac{1}{3}},$$

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

$$\pi_{C_0}(x) = \frac{1}{\ell}\frac{x}{\log x} + O(x^{\frac{1}{2}}(\log \ell x)).$$

Choosing $\ell \asymp x^{\frac{1}{2}}$, we then have

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

These prove Corollary 1.5.

9. The Lang-Trotter conjecture

Let $E/\mathbb{Q}$ be a non-CM elliptic curve over $\mathbb{Q}$ and 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 $|a_p(E)| \leq 2\sqrt{p}$, 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 of class number h with w units, 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 $\mathbb{Q}$. The object of this section is to improve a result of Cojocaru and David [2] regarding the Lang-Trotter Conjecture on the behaviour of $\Pi_E(K, x)$ as stated in Corollary 1.6.

Following [2], we consider the mod ℓ representation associated to E:

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

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 ℓ 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

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

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_ℓ, where

$$PN_\ell := \left\{ \begin{pmatrix} 1 & 0 \\ 0 & b^{hw} \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ b^{hw} & 0 \end{pmatrix} \mid b \in (\mathbb{Z}/\ell\mathbb{Z})^\times \right\}.$$

In other words, we have an isomorphism

$$\hat{\rho}_{\ell,K} : \mathrm{Gal}(F_{\ell,K}/\mathbb{Q}) \to PN_\ell$$

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

$$\hat{\rho}_\ell : \mathrm{Gal}(F_{\ell,E}F_{\ell,K}/\mathbb{Q}) \to PGL_2(\mathbb{Z}/\ell\mathbb{Z}) \times PN_\ell$$

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

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_ℓ)

$$C_\ell = \left\{(g_1, g_2) \mid t(g_2) = P_{hw}(t(g_1)), g_2 = \begin{pmatrix} 1 & 0 \\ 0 & b^{hw} \end{pmatrix}, \left(\frac{(\mathrm{tr}\, g_1)^2 - 4\det g_1}{\ell}\right) = 1\right\},$$

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

$$t(g) := \frac{(\mathrm{tr}\, g)^2}{\det g}.$$

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

$$\Pi_E(K, x) \leq \pi_{C_\ell}(x, F_\ell/\mathbb{Q}).$$

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

$$\pi_{C_\ell}(x, F_\ell/\mathbb{Q}) \ll \frac{hx}{\ell \log x} + \ell^{3/2} x^{1/2} \log(\ell N x) + \ell \log(\ell N x).$$

Moreover, as discussed in [2, p. 1553], if one assumes PCC, which introduces an extra factor $1/\sqrt{\ell}$ in the error term, and leads to

$$\pi_{C_\ell}(x, F_\ell/\mathbb{Q}) \ll \frac{hx}{\ell \log x} + \ell x^{1/2} \log(\ell N x) + \ell \log(\ell N x).$$

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 PCC introduces an extra factor $1/\ell$ (instead of $1/\sqrt{\ell}$) which allows us to derive

$$\pi_{C_\ell}(x, F_\ell/\mathbb{Q}) \ll \frac{hx}{\ell \log x} + \ell^{1/2} x^{1/2} \log(\ell N x) + \ell \log(\ell N).$$

Choosing $\ell = \frac{h^{1/2} x^{1/3}}{\log x}$, we then have

$$\pi_{C_\ell}(x, F_\ell/\mathbb{Q}) \ll h^{1/2} x^{2/3} \left(1 + (\log x)^{1/2} \frac{\log(hNx)}{\log x}\right)$$

so that

$$\Pi_E(K, x) \ll_{N,h} x^{2/3} (\log x)^{1/2},$$

as desired.

To end this section, we shall derive a further estimate for $\Pi_E(K, x)$ that is uniform in K. As before, let $E/\mathbb{Q}$ 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

$$S_{\ell_1,\ell_2}(E, x) := \sum_{\substack{p \leq x \\ p \nmid \ell_1 \ell_2 N}} \left(\frac{4p - a_p(E)^2}{\ell_1 \ell_2}\right).$$

An upper estimate was obtained in [3] 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

$$S_{\ell_1,\ell_2}(E, x) = \sum_{\substack{p \leq x \\ p \nmid \ell_1 \ell_2 N \\ \left(\frac{4p - a_p(E)^2}{\ell_1}\right)\left(\frac{4p - a_p(E)^2}{\ell_2}\right) = 1}} 1 - \sum_{\substack{p \leq x \\ p \nmid \ell_1 \ell_2 N \\ \left(\frac{4p - a_p(E)^2}{\ell_1}\right)\left(\frac{4p - a_p(E)^2}{\ell_2}\right) = -1}} 1$$

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

where

$$C_1 := \left\{ (g_1, g_2) \mid \left(\frac{4 \det g_1 - (\operatorname{tr} g_1)^2}{\ell_1} \right) = \left(\frac{4 \det g_2 - (\operatorname{tr} g_2)^2}{\ell_2} \right) = 1 \right\},$$

$$C_2 := \left\{ (g_1, g_2) \mid \left(\frac{4 \det g_1 - (\operatorname{tr} g_1)^2}{\ell_1} \right) = \left(\frac{4 \det g_2 - (\operatorname{tr} g_2)^2}{\ell_2} \right) = -1 \right\},$$

$$C_3 := \left\{ (g_1, g_2) \mid \left(\frac{4 \det g_1 - (\operatorname{tr} g_1)^2}{\ell_1} \right) = -\left(\frac{4 \det g_2 - (\operatorname{tr} g_2)^2}{\ell_2} \right) = 1 \right\},$$

$$C_4 := \left\{ (g_1, g_2) \mid \left(\frac{4 \det g_1 - (\operatorname{tr} g_1)^2}{\ell_1} \right) = -\left(\frac{4 \det g_2 - (\operatorname{tr} g_2)^2}{\ell_2} \right) = -1 \right\}$$

are (conjugate) subsets of $PGL_2(\mathbb{Z}/\ell_1\ell_2\mathbb{Z})$ 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 showed that if $\ell_1 \equiv \ell_2 \pmod 4$, then

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

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

otherwise, one has

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

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

Since we are choosing ℓ_1 and ℓ_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

$$|PGL_2(\mathbb{Z}/\ell_1\ell_2\mathbb{Z})| = (\ell_1^3 - \ell_1)(\ell_2^3 - \ell_2).$$

Also, the number of conjugacy classes of $PGL_2(\mathbb{Z}/\ell_1\ell_2\mathbb{Z})$ is

$$|(PGL_2(\mathbb{Z}/\ell_1\ell_2\mathbb{Z}))^{\#}| \asymp \ell_1\ell_2.$$

We further note that

$$\left(\frac{|(PGL_2(\mathbb{Z}/\ell_1\ell_2\mathbb{Z}))^{\#}|}{|PGL_2(\mathbb{Z}/\ell_1\ell_2\mathbb{Z})|} \right)^{1/4} \asymp \ell_1^{-1/2}\ell_2^{-1/2}.$$

Thus, M. R. Murty-V. K. Murty's effective Chebotarev density theorem then allows one to deduce that (under GRH, AC, and $PCC(\chi; \chi(1), 1, 1)$)

$$\begin{aligned} S_{\ell_1,\ell_2}(E,x) &= \pi_{C_1\cup C_2}(x, F_{\ell_1\ell_2,E}/\mathbb{Q}) - \pi_{C_3\cup C_4}(x, F_{\ell_1\ell_2,E}/\mathbb{Q}) \\ &= \kappa_{\ell_1\ell_2}\pi(x) + O\left(\ell_1^{3/2}\ell_2^{3/2}\ell_1^{-1/2}\ell_2^{-1/2}x^{1/2}\log(\ell_1\ell_2 Nx)\right) \\ &= \kappa_{\ell_1\ell_2}\pi(x) + O\left(\ell_1\ell_2 x^{1/2}\log(\ell_1\ell_2 Nx)\right), \end{aligned}$$

where

$$\kappa_{\ell_1\ell_2} := \frac{|C_1\cup C_2| - |C_3\cup C_4|}{|PGL_2(\mathbb{Z}/\ell_1\ell_2\mathbb{Z})|}.$$

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

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

Now as in [2, p. 1554] (see also [3]), for $K = \mathbb{Q}(\sqrt{-D})$ and $z = z(x)$, the square sieve and the above estimates yield

$$\begin{aligned} \Pi_E(K,x) \ll{}& \frac{x\log z}{z\log x} + z^{2\theta}x^{1/2}\log(zNx) \\ &+ \frac{x\log z}{z\log x}\log D + \frac{x\log z}{z} \\ &+ \frac{x(\log z)^2}{z^2\log x}(\log D)^2 + \frac{x(\log z)^2}{z^2}\log D + \frac{x\log x(\log z)^2}{z^2}, \end{aligned}$$

where $\theta = 1$ (obtained by Cojocaru and David via M. R. Murty-V. K. Murty's result) or $\theta = 1/2$ (via our refinement). For $\theta = 1$, taking $z = x^{1/6}$, one then has

$$\Pi_E(K,x) \ll_N x^{5/6}\log x;$$

for $\theta = 1/2$, taking $z = x^{1/4}$, one obtains

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

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 an even shaper error term for the Chebotarev density theorem. We, however, note that as discussed in Section 8, our result 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 or seeking further improvement of the effective Chebotarev density theorem presented in this note, one shall search new ideas to move forward.

Acknowledgment

We would like to thank the referee for the careful reading and for making many helpful remarks on a previous version of this note.

References

[1] A. C. Cojocaru, Cyclicity of elliptic curves modulo p, Ph.D. Thesis, Queen's University (2002).
[2] A. C. Cojocaru and C. David, Frobenius fields for elliptic curves, *American Journal of Math.*, **130** (2008) no. 6, 1535–1560.
[3] A. C. Cojocaru, E. Fouvry and M. R. Murty, The square sieve and the Lang-Trotter conjecture, *Canadian Journal of Math.*, **57**, (2005) no. 6, 1155–1177.
[4] A. C. Cojocaru and M. R. Murty, Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linnik's problem, *Math. Annalen*, **330** (2004) no. 3, 601–625.
[5] P. Deligne, Formes modulaires et représentations ℓ-adiques, Sem. Bourbaki 355, Lecture Notes in Mathematics, Springer Verlag, Heidelberg, **179** (1971) 139–172.
[6] R. Gupta and M. R. Murty, A remark on Artin's conjecture, *Inventiones Math.*, **78** (1984) 127–130.
[7] R. Gupta and M. R. Murty, Cyclicity and generation of points mod p on elliptic curves, *Inventiones Math.*, **101** (1990) 225–235.
[8] D. R. Heath-Brown, Gaps between primes, and the pair correlation of zeros of the zeta-function, *Acta Arith.*, **41** (1982) 85–99.
[9] C. Hooley, On Artin's conjecture, *J. Reine Angew. Math.*, **225** (1967) 209–220.
[10] J. C. Lagarias and A. M. Odlyzko, Effective versions of the Chebotarev density theorem, Algebraic number fields: ζ-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London (1977) 409–464.
[11] S. Lang and H. Trotter, Frobenius distributions in GL_2-extensions, Lecture Notes in Mathematics, Springer-Verlag, **504** (1976).
[12] F. Momose, On the ℓ-adic representations attached to modular forms, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, **28**, (1981) no. 1, 89–109.
[13] H. L. Montgomery, Topics in Multiplicative Number Theory, Lecture Notes in Mathematics, Springer-Verlag, Berlin-New York, **227** (1971).
[14] M. R. Murty, On Artin's conjecture, *Journal of Number Theory*, **16** (1983) 147–168.
[15] M. R. Murty, V. K. Murty, and N. Saradha, Modular forms and the Chebotarev density theorem, *American Journal of Math.*, **110** (1988) 253–281.
[16] M. R. Murty and A. Perelli, The pair correlation of zeros of functions in the Selberg class, *International Math. Res. Notices*, **10** (1999) 531–545.
[17] M. R. Murty and A. Zaharescu, Explicit formulas for the pair correlation of zeros of functions in the Selberg class, *Forum Math.*, **14** (2002) no. 1, 65–83.

[18] V. K. Murty, Explicit formulae and the Lang-Trotter conjecture, *Rocky Mountain J. Math.*, **15(2)** (1985) 535–551.
[19] V. K. Murty, Modular forms and the Chebotarev density theorem II, Analytic Number Theory, Ed. Y. Motohashi, Cambridge University Press (1997) 287–308.
[20] J.-P. Serre, Résumé des cours de 1977–1978, Annuaire du Collège de France 1978, 67–70. (See also Collected Papers, Volume III, Springer-Verlag (1985)).
[21] K. Ribet, Galois representations attached to eigenforms with Nebentypus, Lecture Notes in Mathematics, Springer-Verlag, Heidelberg, **601** (1976) 17–52,
[22] K. Ribet, On ℓ-adic representations attached to modular forms II, *Glasgow J. Math.*, **27** (1985) 185–194.
[23] J.-P. Serre, Quelques applications du théorème de densité de Chebotarev, *Publ. Math. IHES*, **54** (1981) 123–201.