ACTA ARITHMETICA
Online First version

Supercharacters and the Chebotarev density theorem

by

Peng-Jie Wong (Lethbridge)

1. Introduction. Almost one hundred years ago, Emil Artin introduced his L-functions and made the following famous conjecture.

Conjecture. *Let K/k be a Galois extension of number fields with Galois group G, and let χ be a character of G. If χ does not contain the trivial character of G, then the Artin L-function $L(s, \chi, K/k)$ attached to χ can be extended to an entire function.*

From Artin reciprocity, this conjecture follows if χ is monomial, i.e., χ is induced from a character of degree 1. After Artin's work, Brauer [3] proved his induction theorem and then derived that all Artin L-functions extend meromorphically over $\mathbb{C}$. By the works of Langlands and many others (see, for example, [6, 8, 9, 11, 14]), we know that Artin's conjecture holds for certain irreducible characters of degree 2 and 4. From these results, the author [15] recently showed that Artin's conjecture holds if K/k is *nearly supersolvable*, i.e., $G = \mathrm{Gal}(K/k)$ admits a normal subgroup N with G/N supersolvable such that all irreducible characters of N are of degree at most 2. Furthermore, in [16, 17], Artin's conjecture is established for all solvable Galois groups of degree at most 200, with a single exceptional group of order 108. However, in general, Artin's conjecture is still open.

Like Dirichlet L-functions leading to the prime number theorem for arithmetic progressions, Artin L-functions lead to a proof of the Chebotarev density theorem. Indeed, the theorem follows from Artin reciprocity, the Brauer induction theorem, and the theory of Hecke L-functions. (For the convenience of the reader, let us recall the Chebotarev density theorem. As above, K/k denotes a Galois extension of number fields with Galois group G. For every unramified prime ideal $\mathfrak{p}$ in $\mathcal{O}_k$, $\sigma_\mathfrak{p}$ denotes the Artin symbol at $\mathfrak{p}$.

2010 *Mathematics Subject Classification*: 11M26, 11N45, 20C15.
Key words and phrases: supercharacters, Chebotarev density theorem, Artin's conjecture.
Received 20 March 2018; revised 9 June 2018.
Published online *.

Let C be a subset of G stable under conjugation, and denote

$$\pi_C(x) = \#\{\mathfrak{p} \mid \mathfrak{p} \text{ is unramified with } \mathrm{N}\,\mathfrak{p} \leq x \text{ and } \sigma_{\mathfrak{p}} \subseteq C\}.$$

The *Chebotarev density theorem* asserts that, as $x \to \infty$,

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

where $\mathrm{Li}\,x$ is the usual offset logarithmic integral function.)

To study arithmetic problems, it is crucial to know the error term for the Chebotarev density theorem. This was studied, with and without the generalised Riemann hypothesis (denoted GRH), by Lagarias and Odlyzko [7] as well as Serre [13]. Moreover, under the further assumption of Artin's conjecture, M. R. Murty, V. K. Murty, and Saradha [10] gave the following refinement.

THEOREM 1.1 ([10, Proposition 3.6]). *Suppose that all Artin L-functions attached to irreducible characters of $G = \mathrm{Gal}(K/k)$ are holomorphic at $s \neq 1$, and that the GRH holds for the Dedekind zeta function $\zeta_K(s)$ of K. Then*

$$\sum_C \frac{1}{|C|}\left|\pi_C(x) - \frac{|C|}{|G|}\,\mathrm{Li}\,x\right|^2 \ll x n_k^2 \big(\log(M(K/k)x)\big)^2,$$

where the sum on the left runs over conjugacy classes C of G, $\pi_C(x)$ is defined as above, n_k is the degree of $k/\mathbb{Q}$, and $M(K/k)$ is a computable constant depending only on K/k (see (2.1) *below for a precise description of $M(K/k)$). In particular,*

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

In a completely different vein, in order to study matrix groups, Diaconis and Isaacs [4] introduced the theory of supercharacters as follows.

DEFINITION 1 ([4, Section 2]). Let G be a finite group. Let $\mathcal{K}$ be a partition of G and let $\mathcal{X}$ be a partition of $\mathrm{Irr}(G)$. The ordered pair $(\mathcal{X}, \mathcal{K})$ is a *supercharacter theory* if

SC1. $\{1\} \in \mathcal{K}$,
SC2. $|\mathcal{X}| = |\mathcal{K}|$, and
SC3. for each $X \in \mathcal{X}$, the character $\sigma_X = \sum_{\psi \in X} \psi(1)\psi$ is constant on each $K \in \mathcal{K}$.

The characters σ_X are called *supercharacters*, and the elements K in $\mathcal{K}$ are called *superclasses*. In addition, if $f : G \to \mathbb{C}$ is constant on each superclass in G, then we say f is a *superclass function* on G. (Here, $\mathrm{Irr}(G)$ denotes the set of irreducible characters of G, and 1 stands for the identity element of G.)

The irreducible characters and conjugacy classes of G give a supercharacter theory of G, which will be referred to as the *classical theory* of G. Indeed, Diaconis and Isaacs showed their theory enjoys properties similar to the classical character theory. For example, every superclass is a union of conjugacy classes in G [4, Theorem 2.2]. Also, as noted in [4], every group G admits a non-classical theory with only two supercharacters 1_G and $\mathrm{Reg}_G - 1_G$ and superclasses $\{1\}$ and $G \setminus \{1\}$, where 1_G denotes the trivial character of G and $\mathrm{Reg}_G = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\chi$ is the character of the regular representation of G. This theory will be called the *maximal theory* of G.

We note that from the definition, every supercharacter is a character. Also, as shown in [4, Theorem 2.2], if $(\mathcal{X}, \mathcal{K})$ is a supercharacter theory of G, some member of $\mathcal{X}$ consists of just the trivial character 1_G of G. In other words, the trivial character is always a supercharacter in any theory. Following the convention of the classical character theory, for $X \in \mathcal{X}$, if $\sigma_X \neq 1_G$, we shall call σ_X *non-trivial.*

As the supercharacter theory generalises the (irreducible) character theory, it may be of interest to study Artin L-functions attached to supercharacters. For instance, if $G = \mathrm{Gal}(K/k)$ is equipped with the maximal theory, then the Artin L-functions attached to supercharacters with respect to such a theory are

$$L(s, 1_G, K/k) = \zeta_k(s) \quad \text{and} \quad L(s, \mathrm{Reg}_G - 1_G, K/k) = \zeta_K(s)/\zeta_k(s).$$

By a result of Aramata and Brauer [2], we know that $\zeta_K(s)/\zeta_k(s)$ is entire. This can be interpreted as Artin's conjecture being valid for all Artin L-functions attached to supercharacters of the maximal theory. In light of the above observation, we consider the following conjecture, which may be seen as a supercharacter-theoretic variant of Artin's conjecture.

Conjecture 1. *Let K/k be a Galois extension of number fields with Galois group G. Let $(\mathcal{X}, \mathcal{K})$ be a supercharacter theory of G and let* $\mathrm{Sup}(G)$ *denote the set of supercharacters with respect to $(\mathcal{X}, \mathcal{K})$. Then for every non-trivial $\sigma \in \mathrm{Sup}(G)$, the Artin L-function $L(s, \sigma, K/k)$ attached to σ extends to an entire function. For such an instance, we shall say that Artin's conjecture holds for G with respect to $(\mathcal{X}, \mathcal{K})$.*

We note that if $(\mathcal{X}, \mathcal{K})$ is the classical theory, then Conjecture 1 is equivalent to Artin's conjecture. In general, Conjecture 1 follows from Artin's conjecture since every non-trivial supercharacter is a character that does not contain the trivial character. Furthermore, as discussed above, Conjecture 1 is valid whenever the theory $(\mathcal{X}, \mathcal{K})$ of G is maximal.

The object of this paper is to show the following effective version of the Chebotarev density theorem for *any* supercharacter theory.

Theorem 1.2. *Let $G = \mathrm{Gal}(K/k)$ and let $(\mathcal{X}, \mathcal{K})$ be a supercharacter theory of G. Suppose that Conjecture* 1 *is true for K/k with respect to $(\mathcal{X}, \mathcal{K})$, and that the GRH holds for $\zeta_K(s)$. Then*

$$\sum_{C} \frac{1}{|C|} \left| \pi_C(x) - \frac{|C|}{|G|} \operatorname{Li} x \right|^2 \ll x n_k^2 \big(\log(M(K/k)x)\big)^2,$$

where the sum on the left runs over superclasses $C \in \mathcal{K}$, and $\pi_C(x)$, n_k, and $M(K/k)$ are defined in the same way as in Theorem 1.1.

Applying the Cauchy–Schwarz inequality, we have the following.

Corollary 1.3. *Under the same assumption and notation as above, one has*

$$\pi_D(x) = \frac{|D|}{|G|} \operatorname{Li} x + O\big(|D|^{1/2} x^{1/2} n_k \log(M(K/k)x)\big)$$

for an arbitrary union D of superclasses in $\mathcal{K}$.

Note that if $(\mathcal{X}, \mathcal{K})$ is the classical theory, our theorem is exactly Theorem 1.1. Also, from the above discussion (à la Aramata–Brauer), if $(\mathcal{X}, \mathcal{K})$ is maximal, then the holomorphy assumption on Artin L-functions in Theorem 1.2 can be removed. With these and Conjecture 1 in mind, in Section 4, we shall further study the relation between supercharacters and Artin's conjecture. In particular, by invoking the "$*$-product" constructed by Hendrickson [5], we give a simple criterion, Proposition 4.2, to check Artin's conjecture for certain supercharacter theories. As a consequence, we obtain the following two effective versions of the Chebotarev density theorem, Propositions 1.4 and 1.5, without assuming Artin's conjecture, by applying Corollaries 4.3 and 4.4, respectively.

Proposition 1.4. *In the notation of Theorem* 1.2, *let N be a normal subgroup of G contained in the centre $\mathbf{Z}(G)$ of G. Suppose that the GRH holds for $\zeta_K(s)$. Then*

$$\sum_{C} \frac{1}{|C|} \left| \pi_C(x) - \frac{|C|}{|G|} \operatorname{Li} x \right|^2 \ll x n_k^2 \big(\log(M(K/k)x)\big)^2,$$

where the sum on the left runs over $G \setminus N$ and all conjugacy classes of N. In particular, if C is $G \setminus N$, a conjugacy class of N, or a union of such sets, one has

$$\pi_C(x) = \frac{|C|}{|G|} \operatorname{Li} x + O\big(|C|^{1/2} x^{1/2} n_k \log(M(K/k)x)\big).$$

Proposition 1.5. *In the notation of Theorem* 1.2, *let N be a normal subgroup of G with G/N nearly supersolvable. Suppose that the GRH holds* *for $\zeta_K(s)$. Then*

$$\sum_C \frac{1}{|C|}\left|\pi_C(x) - \frac{|C|}{|G|}\operatorname{Li} x\right|^2 \ll x n_k^2 \big(\log(M(K/k)x)\big)^2,$$

where the sum on the left runs over $\{1\}$, $N \setminus \{1\}$, and all sets of the form ND for some non-trivial conjugacy class D in G/N. In particular, if C is $\{1\}$, $N \setminus \{1\}$, a set of the form ND for some non-trivial conjugacy class D in G/N, or a union of such sets, one has

$$\pi_C(x) = \frac{|C|}{|G|}\operatorname{Li} x + O\big(|C|^{1/2} x^{1/2} n_k \log(M(K/k)x)\big).$$

As demonstrated in [10], the above estimates are versatile enough for studying several arithmetic objects and related problems. We shall give two applications of our results to elliptic curves and modular forms.

First of all, let f be a normalised Hecke eigenform of integral weight $k \geq 2$ for $\Gamma_0(N)$, and let ϵ be its nebentypus character. Write $f(z) = \sum_{n\geq 1} a_f(n) e^{2\pi i n z}$ for its Fourier expansion at $i\infty$, and for simplicity of discussion, suppose that the $a_f(n)$'s are all rational. By a celebrated result of Deligne, for each prime ℓ, there is a representation

$$\rho_{f,\ell} : \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{GL}_2\big(\mathbb{Z}_\ell\big)$$

such that for any p not dividing ℓN, one has

$$\operatorname{tr} \rho_{f,\ell}(\sigma_p) = a_p \quad \text{and} \quad \det \rho_{f,\ell}(\sigma_p) = p^{k-1}\epsilon(p),$$

where σ_p stands for a Frobenius element at p. Denote by $\widetilde{\rho}_{f,\ell}$ the reduction (mod ℓ) of $\rho_{f,\ell}$ (into $\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$), and let K_ℓ be the fixed field of the kernel of $\widetilde{\rho}_{f,\ell}$. For the sake of simplicity, we assume the reduction is surjective, i.e., $\operatorname{Gal}(K_\ell/\mathbb{Q}) = \operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. It may be of interest to study the prime-counting function $\pi_f(x, \ell, a)$ defined as

$$\pi_f(x,\ell,a) = \#\{p \leq x \mid p \nmid \ell N \text{ is a prime such that } \det \widetilde{\rho}_{f,\ell}(\sigma_p) = a\}$$

for any given $a \in (\mathbb{Z}/\ell\mathbb{Z})^*$. We now recall that the determinant of $\rho_{f,\ell}$ is, in fact, the mod ℓ cyclotomic character χ_ℓ. (For the details of the above discussion of modular forms and their Galois representations, we refer the interested reader to Ribet's beautiful article [12].) From this connection, the above prime-counting function $\pi_f(x, \ell, a)$ may be seen as a non-abelian generalisation of the usual prime-counting function $\pi(x, \ell, a)$ for the primes congruent to a modulo ℓ, and should have a similar distribution. Indeed, we shall show this is the case below.

With the notation used in Proposition 1.5, we shall consider $G = \operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ and let $N = \operatorname{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$, which is normal (as the determinant gives a natural homomorphism from $\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ to $(\mathbb{Z}/\ell\mathbb{Z})^*$ with kernel $\operatorname{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$). Now let D_a denote the class consisting of matrices with determinant a in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})/\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \simeq (\mathbb{Z}/\ell\mathbb{Z})^*$. It is clear that $|ND_a| = |\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})|$ and that the condition $\det \widetilde{\rho}_{f,\ell}(\sigma_p) = a$ is nothing but $\widetilde{\rho}_{f,\ell}(\sigma_p) \in ND_a$. Thus, the Chebotarev density theorem tells us that, as $x \to \infty$,

$$\pi_f(x,\ell,a) \sim \frac{1}{\phi(\ell)} \operatorname{Li} x,$$

where ϕ is Euler's totient function. Furthermore, under the GRH and with the same notation as above, Proposition 1.5 yields

$$\pi_f(x,\ell,a) = \frac{1}{\phi(\ell)} \operatorname{Li} x + O(|\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})|^{1/2} x^{1/2} \log(\ell N x)).$$

(We remark that this can also be derived from Theorem 1.1 under the further assumption of Artin's conjecture on $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$-extensions. Also, one may drop the assumption of rationality of $a_f(n)$ by replacing $\mathbb{Z}$ in the above discussion by $\mathcal{O}_f$, the ring of integers of the algebraic number field obtained by adjoining the Fourier coefficients $a_f(n)$ to $\mathbb{Q}$.)

Secondly, we shall apply Proposition 1.4 to the geometric variant of the Titchmarsh problem considered by Akbary and Ghioca [1]. In particular, we refine their result, [1, Theorem 1.5], by removing the use of Artin's conjecture for the case of elliptic curves as follows.

Corollary 1.6. *Let E be an elliptic curve over $\mathbb{Q}$, and let $\delta \in [0,1)$ be a real number. For each $m \in \mathbb{N}$, we let C_m be a union of conjugacy classes in $G_m = \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$, where $E[m]$ denotes the set of m-torsion points of E, such that*

(1) *$|C_m| \ll m^\delta$, and*
(2) *each $\sigma \in C_m$ acts on $E[m]$ via a scalar matrix $a\mathrm{I}_2 = \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$.*

For each prime p, we further define $\tau_{\mathcal{E},\mathcal{C}}(p) = \#\{m \in \mathbb{N} \mid \sigma_p \in C_m\}$. Assume the GRH is valid for each extension $\mathbb{Q}(E[m])/\mathbb{Q}$. Then

$$\sum_{p \le x} \tau_{\mathcal{E},\mathcal{C}}(p) - \sum_{m=1}^{\infty} \frac{|C_m|}{|G_m|} \operatorname{Li} x \ll \begin{cases} x^{\frac{10+3\delta}{12+2\delta}} (\log x)^{\frac{4}{6+\delta}} & \text{for } \delta \in [0,2/3), \\ (x/\log x)^{\frac{5+2\delta}{6+\delta}} & \text{for } \delta \in [2/3,1). \end{cases}$$

(We recall that $G_m = \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$ embeds into $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ canonically. We will fix such an embedding throughout our discussion. In addition, by abuse of notation, we shall write I_2 for the identity matrix of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ for any m.)

The paper is arranged as follows. In the next section, we shall collect the preliminaries for the proof of our effective version of the Chebotarev density theorem. The proofs of Theorem 1.2 and of Propositions 1.4 and 1.5 will be given in Sections 3 and 4, respectively. Finally, in Section 5, we discuss how to derive Corollary 1.6 from Proposition 1.4.

2. Preliminaries. Throughout this paper, we make use of some standard notation. We write $f \ll g$ or equivalently $f = O(g)$ if there is a constant M such that $|f(x)| \leq Mg(x)$ for all x sufficiently large. (We remark that all implied constants in estimates presented in this section are absolute.) Also, we write $f \sim g$ if $f(x)/g(x) \to 1$ as $x \to \infty$. In addition, $n_k = [k : \mathbb{Q}]$ is the degree of k over $\mathbb{Q}$, and $n = [K : k]$. Let d_k and d_K denote the absolute discriminants of $k/\mathbb{Q}$ and $K/\mathbb{Q}$, respectively. Let $P(K/k)$ denote the set of rational primes p for which there is a prime $\mathfrak{p}$ of k with $\mathfrak{p} \mid p$ and $\mathfrak{p}$ is ramified in K. We then set

$$M(K/k) = n d_k^{1/n_k} \prod_{p \in P(K/k)} p. \tag{2.1}$$

Let $\mathfrak{f}(\chi)$ denote the Artin conductor of a character χ of $G = \mathrm{Gal}(K/k)$, and let $A_\chi = d_k^{\chi(1)} \,\mathrm{N}\,\mathfrak{f}(\chi)$ denote the conductor of χ.

To obtain a sharp error term for the Chebotarev density theorem, M. R. Murty, V. K. Murty, and Saradha [10] first derived the two estimates stated below.

Proposition 2.1 ([10, Section 3.5]). *For each unramified prime $\mathfrak{p}$ of k, let $\sigma_\mathfrak{p}$ denote the Artin symbol at $\mathfrak{p}$. Let χ be a character of G and let $\pi(x,\chi) = \sum_{\mathrm{N}\,\mathfrak{p} \leq x} \chi(\sigma_\mathfrak{p})$, where the sum is over unramified primes $\mathfrak{p}$ of k. Let $\delta(\chi)$ denote the multiplicity of the trivial character in χ. Suppose that the Artin L-function $L(s,\chi)$ is holomorphic for all $s \neq 1$ and is non-zero for $\Re(s) \neq 1/2$ and $0 < \Re(s) < 1$. Then*

$$\pi(x,\chi) = \delta(\chi) \,\mathrm{Li}\, x + O\big(x^{1/2}(\log A_\chi + \chi(1) n_k \log x) + \chi(1) n_k \log M(K/k)\big).$$

Lemma 2.2 ([10, Proposition 2.5]). *Let χ be an irreducible character of G. Then*

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

From these estimates, one can derive the effective version of the Chebotarev density theorem stated in Theorem 1.1.

As mentioned earlier, effective versions of the Chebotarev density theorem with explicit error terms were first established by Lagarias and Odlyzko [7] and were refined by Serre [13]. In particular, if the GRH for $\zeta_K(s)$ is assumed, one has

$$\pi_C(x) = \frac{|C|}{|G|} \,\mathrm{Li}\, x + O\big(|C| x^{1/2} n_k \log(M(K/k)x)\big). \tag{2.2}$$

(We remark that there are unconditional versions, and refer the reader to

[7] and [13].) We further note that by Theorem 1.1, one has

$$\pi_C(x) = \frac{|C|}{|G|} \operatorname{Li} x + O\big(|C|^{1/2} x^{1/2} n_k \log(M(K/k)x)\big). \tag{2.3}$$

It is clear that (2.3) is a better estimate because the factor $|C|$ in (2.2) is now replaced by $|C|^{1/2}$. Such an estimate is more versatile for many applications such as the Lang–Trotter conjecture on Fourier coefficients of modular forms (see [10]) and the Titchmarsh divisor problem for abelian varieties (cf. [1] and Section 5).

3. An effective Chebotarev density theorem. In this section, we will make use of notation introduced in the previous section, and we shall fix a supercharacter theory $(\mathcal{X}, \mathcal{K})$ for $G = \operatorname{Gal}(K/k)$. Also, $\operatorname{Sup}(G)$ will stand for the set of supercharacters of G with respect to $(\mathcal{X}, \mathcal{K})$.

Following the strategy developed in [10], in order to extend Theorem 1.1 to superclasses of G, we need the following lemmata.

Lemma 3.1. *For any superclass $C \in \mathcal{K}$,*

$$\delta_C = \frac{|C|}{|G|} \sum_{\sigma \in \operatorname{Sup}(G)} \frac{\overline{\sigma(g_C)}\sigma}{\sigma(1)},$$

where δ_C denotes the indicator function of C, and g_C is a representative of C.

Proof. We recall that from the orthogonality property of $\operatorname{Irr}(G)$, Diaconis and Isaacs deduced that the set $\operatorname{Sup}(G)$ forms an orthogonal basis for the inner product space of all superclass functions on G with respect to the usual inner product. Thus,

$$\delta_C = \sum_{\sigma \in \operatorname{Sup}(G)} (\delta_C, \sigma) \frac{\sigma}{(\sigma, \sigma)},$$

where $(\sigma, \sigma) = \sigma(1)$. Since for any representative g_C of C,

$$(\delta_C, \sigma) = \frac{1}{|G|} \sum_{g \in G} \delta_C(g)\overline{\sigma(g)} = \frac{|C|}{|G|}\overline{\sigma(g_C)},$$

the claim follows. ∎

Lemma 3.2. *Let π be a complex-valued linear function defined on the vector space of superclass functions of G (with respect to $(\mathcal{X}, \mathcal{K})$). Then*

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

where the sum on the left runs over superclasses $C \in \mathcal{K}$, and the sum on the right runs over the non-trivial supercharacters in $\operatorname{Sup}(G)$.

Proof. Since π is linear, by Lemma 3.1, one can write

$$\pi(\delta_C) - \frac{|C|}{|G|}\pi(1_G) = \frac{|C|}{|G|}\sum_{\sigma\neq 1_G}\frac{\overline{\sigma(g_C)}\pi(\sigma)}{\sigma(1)},$$

where g_C is a representative of C. Therefore,

$$\begin{aligned}\left|\pi(\delta_C) - \frac{|C|}{|G|}\pi(1_G)\right|^2 &= \left(\frac{|C|}{|G|}\sum_{\sigma\neq 1_G}\frac{\overline{\sigma(g_C)}\pi(\sigma)}{\sigma(1)}\right)\overline{\left(\frac{|C|}{|G|}\sum_{\tau\neq 1_G}\frac{\overline{\tau(g_C)}\pi(\tau)}{\tau(1)}\right)}\\ &= \frac{|C|^2}{|G|^2}\sum_{\sigma,\tau\neq 1_G}\pi(\sigma)\overline{\pi(\tau)}\frac{\overline{\sigma(g_C)}\tau(g_C)}{\sigma(1)\tau(1)}.\end{aligned}$$

Dividing both sides by $|C|$ and then summing over all superclasses of G on both sides, one has

$$\begin{aligned}\sum_C \frac{1}{|C|}\left|\pi(\delta_C) - \frac{|C|}{|G|}\pi(1_G)\right|^2 &= \sum_C \frac{|C|}{|G|^2}\sum_{\sigma,\tau\neq 1_G}\pi(\sigma)\overline{\pi(\tau)}\frac{\overline{\sigma(g_C)}\tau(g_C)}{\sigma(1)\tau(1)}\\ &= \frac{1}{|G|}\sum_{\sigma,\tau\neq 1_G}\pi(\sigma)\overline{\pi(\tau)}\frac{1}{|G|}\sum_C |C|\frac{\overline{\sigma(g_C)}\tau(g_C)}{\sigma(1)\tau(1)}.\end{aligned}$$

As one can write the inner sum as

$$\frac{1}{|G|}\sum_C |C|\frac{\overline{\sigma(g_C)}\tau(g_C)}{\sigma(1)\tau(1)} = \frac{1}{|G|}\sum_{g\in G}\frac{\overline{\sigma(g)}\tau(g)}{\sigma(1)\tau(1)} = \frac{(\sigma,\tau)}{\sigma(1)\tau(1)},$$

the orthogonality property of $\mathrm{Sup}(G)$ then implies that

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

as desired. ∎

For the purpose of counting primes, we also need to rewrite the estimates stated in Proposition 2.1 and Lemma 2.2 in the context of supercharacters. As before, for each unramified prime $\mathfrak{p}$ of k, let $\sigma_{\mathfrak{p}}$ denote the Artin symbol at $\mathfrak{p}$. Let χ be a superclass function on G and let $\pi(x,\chi) = \sum_{\mathrm{N}\,\mathfrak{p}\leq x}\chi(\sigma_{\mathfrak{p}})$, where the sum is over unramified primes $\mathfrak{p}$ of k. In particular, we have $\pi(x,\delta_C) = \pi_C(x)$ for any superclass C. Together with the definition of supercharacters, Proposition 2.1 gives:

Proposition 3.3. *Assuming the GRH for the Dedekind zeta function of k, one has*

$$\pi(x,1_G) = \mathrm{Li}\,x + O\big(x^{1/2}(\log d_k + n_k\log x) + n_k\log M(K/k)\big),$$

where $M(K/k)$ is defined as in (2.1).

For any non-trivial supercharacter $\sigma \in \mathrm{Sup}(G)$, if the Artin L-function $L(s,\sigma,K/k)$ is entire and is non-zero for $\Re(s) \neq 1/2$ and $0 < \Re(s) < 1$, then

$$\pi(x,\sigma) = O\big(x^{1/2}(\log A_\sigma + \sigma(1) n_k \log x) + \sigma(1) n_k \log M(K/k)\big),$$

where $A_\sigma = d_k^{\sigma(1)} \mathrm{N}\,\mathfrak{f}(\sigma)$ denotes the conductor of σ.

By the properties of Artin conductors, we have a variant of Lemma 2.2 as follows.

Lemma 3.4. *Let $\sigma \in \mathrm{Sup}(G)$ be a supercharacter of G. Then*

$$\log \mathrm{N}\,\mathfrak{f}(\sigma) \leq 2\sigma(1) n_k \Big(\sum_{p \in P(K/k)} \log p + \log n \Big).$$

Proof. One can write any supercharacter σ as

$$\sigma = \sum_{\chi \in \mathrm{Irr}(G,\sigma)} \chi(1)\chi,$$

where $\mathrm{Irr}(G,\sigma)$ is the subset of $\mathrm{Irr}(G)$ consisting of all irreducible characters appearing in σ. Since, for any characters χ_1 and χ_2, $\mathfrak{f}(\chi_1+\chi_2) = \mathfrak{f}(\chi_1)\mathfrak{f}(\chi_2)$, and the (absolute) norm N is completely multiplicative, one has

$$\log \mathrm{N}\,\mathfrak{f}(\sigma) = \sum_{\chi \in \mathrm{Irr}(G,\sigma)} \chi(1) \log \mathrm{N}\,\mathfrak{f}(\chi).$$

Therefore, Lemma 2.2 implies that

$$\log \mathrm{N}\,\mathfrak{f}(\sigma) \leq \sum_{\chi \in \mathrm{Irr}(G,\sigma)} \chi(1) \Big(2\chi(1) n_k \Big(\sum_{p \in P(K/k)} \log p + \log n \Big)\Big).$$

Now the assertion follows from the identity $\sigma(1) = \sum_{\chi \in \mathrm{Irr}(G,\sigma)} \chi^2(1)$. ∎

Using these estimates, we can now prove our main results.

Proof of Theorem 1.2 and Corollary 1.3. First, observe that

$$\sum_C \frac{1}{|C|} \left| \frac{|C|}{|G|}\pi(x,1_G) - \frac{|C|}{|G|} \mathrm{Li}\,x \right|^2 = \frac{1}{|G|^2} \sum_C |C| (\pi(x,1_G) - \mathrm{Li}\,x)^2 = \frac{1}{|G|}(\pi(x,1_G) - \mathrm{Li}\,x)^2. \tag{3.1}$$

Applying Lemma 3.2 and noticing that $\pi_C(x) = \pi(x,\delta_C)$, one has

$$\sum_C \frac{1}{|C|} \left| \pi_C(x) - \frac{|C|}{|G|}\pi(x,1_G) \right|^2 = \frac{1}{|G|} \sum_{\sigma \neq 1_G} \frac{|\pi(x,\sigma)|^2}{\sigma(1)}. \tag{3.2}$$

Also, for any $\sigma \in \mathrm{Sup}(G)$, Proposition 3.3 and Lemma 3.4 give

$$\pi(x,\sigma) - \delta(\sigma)\,\mathrm{Li}\,x \ll x^{1/2} \sigma(1) n_k \log\big(M(K/k)x\big),$$

where $\delta(\sigma)$ denotes the indicator function of 1_G.

Now, from the Cauchy–Schwarz inequality, (3.1), (3.2), and the above estimate for $\pi(x,\sigma)$, it follows that

$$\begin{aligned}
&\sum_C \frac{1}{|C|}\left|\pi_C(x) - \frac{|C|}{|G|}\operatorname{Li} x\right|^2 \\
&\qquad \le \sum_C \frac{2}{|C|}\left|\pi_C(x) - \frac{|C|}{|G|}\pi(x,1_G)\right|^2 + \sum_C \frac{2}{|C|}\left|\frac{|C|}{|G|}\pi(x,1_G) - \frac{|C|}{|G|}\operatorname{Li} x\right|^2 \\
&\qquad = \frac{2}{|G|}\sum_{\sigma\neq 1_G}\frac{|\pi(x,\sigma)|^2}{\sigma(1)} + \frac{2}{|G|}(\pi(x,1_G) - \operatorname{Li} x)^2 \\
&\qquad \ll \frac{1}{|G|}\sum_{\sigma\in \operatorname{Sup}(G)} x\sigma(1)n_k^2\big(\log(M(K/k)x)\big)^2.
\end{aligned}$$

We then conclude by using $|G| = \sum_{\chi\in\operatorname{Irr}(G)}\chi^2(1) = \sum_{\sigma\in\operatorname{Sup}(G)}\sigma(1)$.

Furthermore, by the Cauchy–Schwarz inequality and Theorem 1.2, for any union D of superclasses in G, one has

$$\begin{aligned}
\left|\pi(x,\delta_D) - \frac{|D|}{|G|}\operatorname{Li} x\right| &= \left|\sum_{C\subseteq D}\left(\pi(x,\delta_C) - \frac{|C|}{|G|}\operatorname{Li} x\right)\frac{|C|^{1/2}}{|C|^{1/2}}\right| \\
&\le \left(\sum_{C\subseteq D}\frac{1}{|C|}\left|\pi(x,\delta_C) - \frac{|C|}{|G|}\operatorname{Li} x\right|^2\right)^{1/2}\Big(\sum_{C\subseteq D}|C|\Big)^{1/2} \\
&\ll \big(xn_k^2\big(\log(M(K/k)x)\big)^2\big)^{1/2}|D|^{1/2},
\end{aligned}$$

where the sums run over all superclasses $C\subseteq D$. ■

4. The $*$-product and proofs of Propositions 1.4 and 1.5. As we now have a variant of Theorem 1.1 in the context of supercharacter theory, it seems possible to refine Theorem 1.1 by removing the use of Artin's conjecture for certain cases. Indeed, in this section, we shall find some supercharacter theories of $G = \operatorname{Gal}(K/k)$ satisfying Conjecture 1. We first recall that the Aramata–Brauer theorem asserts that the quotient $\zeta_K(s)/\zeta_k(s)$ is entire for any Galois extension K/k with Galois group G. In other words, Artin's conjecture holds for the Artin L-functions attached to the supercharacters $\operatorname{Reg}_G - 1_G$ and 1_G. (We note that $\{\operatorname{Reg}_G - 1_G, 1_G\}$ together with $\{G\setminus\{1\},\{1\}\}$ gives the maximal theory of G.)

In [5], Hendrickson introduced the $*$-product of supercharacter theories, which produces a supercharacter theory of G from its normal subgroup N and the quotient group $H = G/N$ as follows. Let G be a finite group and N be a normal subgroup of G. We equip N and G/N with supercharacter theories $(\mathcal{X},\mathcal{K})$ and $(\mathcal{Y},\mathcal{J})$, respectively. Following [5], $(\mathcal{X},\mathcal{K})$ is said to be *G-invariant* if for each $g\in G$ and $n\in N$, both n and $g^{-1}ng$ belong to the same superclass. Assuming that $(\mathcal{X},\mathcal{K})$ is G-invariant, let $(\mathcal{Z},\mathcal{M})$ denote the pair with

$$\begin{aligned}\mathcal{Z} &= \{\operatorname{Ind}_N^G \sigma_X \mid X \in \mathcal{X}\setminus\{1_N\}\} \cup \{\operatorname{Inf}_{G/N}^G \sigma_Y \mid Y \in \mathcal{Y}\},\\ \mathcal{M} &= \mathcal{K} \cup \{NJ \mid J \in \mathcal{J}\setminus\{1\}\}.\end{aligned}$$

Hendrickson [5, Theorem 4.3] then proved the following assertion.

Proposition 4.1. *The pair $(\mathcal{Z},\mathcal{M})$ defines a supercharacter theory of G.*

This supercharacter theory is referred to as the $*$-*product* of $(\mathcal{X},\mathcal{K})$ and $(\mathcal{Y},\mathcal{J})$. From the construction of $*$-product, we derive the following criterion.

Proposition 4.2. *Let $G = \operatorname{Gal}(K/k)$, and let N and G/N be equipped with $(\mathcal{X},\mathcal{K})$ and $(\mathcal{Y},\mathcal{J})$, respectively, where $(\mathcal{X},\mathcal{K})$ is G-invariant. Suppose that Conjecture* 1 *holds for both $(\mathcal{X},\mathcal{K})$ and $(\mathcal{Y},\mathcal{J})$. Then Artin's conjecture is valid for G with respect to the $*$-product $(\mathcal{Z},\mathcal{M})$ of $(\mathcal{X},\mathcal{K})$ and $(\mathcal{Y},\mathcal{J})$.*

Proof. By the construction, any supercharacter σ of G (equipped with $(\mathcal{Z},\mathcal{M})$) is either $\operatorname{Ind}_N^G \tau$ for some supercharacter τ of $(\mathcal{X},\mathcal{K})$, or $\operatorname{Inf}_{G/N}^G \psi$ for some supercharacter ψ of $(\mathcal{Y},\mathcal{J})$. For the former instance, the induction invariance property of Artin L-functions gives

$$L(s,\sigma,K/k) = L(s,\operatorname{Ind}_N^G \tau, K/k) = L(s,\tau,K/K^N).$$

For the latter case, we have

$$L(s,\sigma,K/k) = L(s,\operatorname{Inf}_{G/N}^G \psi, K/k) = L(s,\psi,K^N/k).$$

Now the holomorphy of $L(s,\sigma,K/k)$ follows from our assumption that Artin's conjecture holds for $L(s,\tau,K/K^N)$ and $L(s,\psi,K^N/k)$. ∎

From this proposition, we immediately have the following corollary.

Corollary 4.3. *Let $G = \operatorname{Gal}(K/k)$. Let N and G/N be equipped with $(\mathcal{X},\mathcal{K})$ and $(\mathcal{Y},\mathcal{J})$, respectively. Assume further that N is* central, *i.e. contained in $\mathbf{Z}(G)$, and that $(\mathcal{Y},\mathcal{J})$ is the maximal theory. Then Artin's conjecture holds for G with respect to the $*$-product $(\mathcal{Z},\mathcal{M})$ of $(\mathcal{X},\mathcal{K})$ and $(\mathcal{Y},\mathcal{J})$.*

Proof. Firstly, the Aramata–Brauer theorem asserts that Artin's conjecture holds for G/N equipped with maximal $(\mathcal{Y},\mathcal{J})$.

On the other hand, as N is central, it is clear that for any $n \in N$ and $g \in G$, one has

$$g^{-1}ng = n,$$

which means that any supercharacter theory $(\mathcal{X},\mathcal{K})$ is automatically G-invariant. Furthermore, N is abelian since N is central. Thus, Artin's conjecture is valid for $(\mathcal{X},\mathcal{K})$ and hence the corollary follows from Proposition 4.2. ∎

Proof of Proposition 1.4. Assume the GRH, and let N be normal and contained in $\mathbf{Z}(G)$. By Theorem 1.2 and Corollary 1.3, it suffices to check that Conjecture 1 for the $*$-product $(\mathcal{Z},\mathcal{M})$ of $(\mathcal{X},\mathcal{K})$ and $(\mathcal{Y},\mathcal{J})$ holds, where $(\mathcal{X},\mathcal{K})$ is the classical theory of N, and $(\mathcal{Y},\mathcal{J})$ is the maximal theory of G/N. However, this follows immediately from Corollary 4.3. Note that the collection of superclasses of $(\mathcal{Z},\mathcal{M})$ is

$$\mathcal{K}\cup\{NJ \mid J\in\mathcal{J}\setminus\{1\}\},$$

which consists of all conjugacy classes in N and of the set $G\setminus N$. ∎

We now equip N with the maximal theory of N and note that for any $n\in N$ and $g\in G$, $g^{-1}ng=1$ if and only if $n=1$. Since in such an instance, there are only two superclasses, namely $\{1\}$ and $N\setminus\{1\}$, a moment's reflection shows that the maximal theory of N is always G-invariant. As mentioned in the introduction, Artin's conjecture for all nearly supersolvable Galois extensions was established by the author [15, Section 6.1]. Thus, Proposition 4.2 yields the following.

Corollary 4.4. *Let $G=\mathrm{Gal}(K/k)$, and let N and G/N be equipped with $(\mathcal{X},\mathcal{K})$ and $(\mathcal{Y},\mathcal{J})$, respectively. Assume $(\mathcal{X},\mathcal{K})$ is the maximal theory. If G/N is nearly supersolvable, then Artin's conjecture holds for G with respect to the $*$-product of $(\mathcal{X},\mathcal{K})$ and $(\mathcal{Y},\mathcal{J})$.*

From this corollary, it is easy to deduce Proposition 1.5 as follows.

Proof of Proposition 1.5. Let N be normal in G and equipped with maximal $(\mathcal{X},\mathcal{K})$, and let G/N be nearly supersolvable with classical $(\mathcal{Y},\mathcal{J})$. By Corollary 4.4, Artin's conjecture holds for G with respect to the $*$-product of $(\mathcal{X},\mathcal{K})$ and $(\mathcal{Y},\mathcal{J})$.

Thus, under the GRH, the proposition follows from Theorem 1.2 and Corollary 1.3. Note that for such a $*$-product, the collection of superclasses consists of $\{1\}$, $N\setminus\{1\}$, and sets of the form NJ for some non-trivial conjugacy class J in G/N. ∎

5. An application to the Titchmarsh divisor problem for elliptic curves. In their paper [1], Akbary and Ghioca formulated a geometric analogue of the Titchmarsh divisor problem in the context of abelian varieties defined over $\mathbb{Q}$ and proved several theorems concerning the asymptotic distribution of the primes with certain splitting properties in the division fields of a given abelian variety. For the sake of simplicity, we shall only consider the case of elliptic curves. Following [1], for any elliptic curve $E/\mathbb{Q}$, we consider the family $\mathcal{E}=\{\mathcal{E}_m=\mathbb{Q}(E[m])\mid m\in\mathbb{N}\}$ of division fields of E. Let C_m be a union of conjugacy classes in $G_m=\mathrm{Gal}(\mathcal{E}_m/\mathbb{Q})$ and let $\mathcal{C}=\{C_m\}$. Setting $\tau_{\mathcal{E},\mathcal{C}}(p)=\#\{m\in\mathbb{N}\mid\sigma_p\in C_m\}$, one may want to study the behaviour of $\sum_{p\le x}\tau_{\mathcal{E},\mathcal{C}}(p)$ as $x\to\infty$.

This question was studied and answered by Akbary and Ghioca in [1, Theorem 1.5], who gave the estimate described in Corollary 1.6 under the further assumption of Artin's conjecture for every G_m. We shall give a sketch of their proof below. First, let us recall the conditions imposed in their theorem:

1. There is a number $\delta \in [0,1)$ such that for any m, $|C_m| \ll m^\delta$.
2. Each $\sigma \in C_m$ acts on $E[m]$ via a scalar matrix $a\mathrm{I}_2$.

As discussed in [1, proof of Theorem 1.5], by the second condition, in order to study $\sum_{p\le x} \tau_{\mathcal{E},\mathcal{C}}(p)$, it suffices to estimate $\sum_{p\le x} \pi_{\mathcal{E},\mathcal{C}}(x,m)$, where

$$\pi_{\mathcal{E},\mathcal{C}}(x,m) = \#\{p \le x \mid p \text{ is a prime of good reduction so that } \sigma_p \in C_m\}.$$

(Indeed, condition 2 forces that $p \equiv a^2 \pmod m$, and hence $m \le x$ whenever $x > a^2$, which justifies the range of the new summatory function above.)

For the summatory function over the initial range $m \le (x/\log x)^{2/(\delta+6)}$, Theorem 1.1 is applied to get

$$\pi_{\mathcal{E},\mathcal{C}}(x,m) = \frac{|C_m|}{[\mathcal{E}_m:\mathbb{Q}]}\operatorname{Li} x + O(|C_m|^{1/2}x^{1/2}\log(mx)). \tag{5.1}$$

This is the only step in the proof that requires the GRH and Artin's conjecture. Furthermore, because of the nature of sieving process (cf. [1, equations (5.1)–(5.5)]), condition 1 is needed for bounding the summatory function over the initial range.

On the other hand, in order to obtain a good estimate for the remaining range, one needs to invoke condition 2 again. (Indeed, such a condition allows one to further reduce the sum to the range $m \le 2x^{1/2}$.)

Now we are in a position to prove Corollary 1.6. As remarked in [1], condition 2 above is equivalent to the condition that C_m consists of scalar matrices in $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. For each m, we let N_m stand for the subgroup consisting of all scalar matrices in G_m. Noticing that any scalar matrix (in G_m) forms a conjugacy class in N_m, applying Proposition 1.4 (with $G = G_m$ and $N = N_m$) yields the key estimate (5.1), even without using Artin's conjecture. In other words, we can remove the assumption of Artin's conjecture from [1, Theorem 1.5] and deduce Corollary 1.6.

Acknowledgements. The core of this paper is based on Chapter 4 of [15]. The author would like to thank Professor Ram Murty for his kind guidance and encouragement and to express his appreciation to Professors Amir Akbary and Wen-Ching Winnie Li for their careful reading and helpful suggestions. Also, the author wishes to thank the referee for the detailed and useful comments.

The author is currently a PIMS Post-Doctoral Fellow at the University of Lethbridge.

References

[1] A. Akbary and D. Ghioca, *A geometric variant of Titchmarsh divisor problem*, Int. J. Number Theory 8 (2012), 53–69.

[2] R. Brauer, *On the zeta-functions of algebraic number fields*, Amer. J. Math. 69 (1947), 243–250.

[3] R. Brauer, *On Artin's L-series with general group characters*, Ann. of Math. (2) 48 (1947), 502–514.

[4] P. Diaconis and I. M. Isaacs, *Supercharacters and superclasses for algebra groups*, Trans. Amer. Math. Soc. 360 (2008), 2359–2392.

[5] A. O. F. Hendrickson, *Supercharacter theory constructions corresponding to Schur ring products*, Comm. Algebra 40 (2012), 4420–4438.

[6] C. Khare and J.-P. Wintenberger, *Serre's modularity conjecture (I)*, Invent. Math. 178 (2009), 485–504.

[7] J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem*, in: Algebraic Number Fields: L-functions and Galois Properties (Durham, 1975), Academic Press, London, 1977, 409–464.

[8] R. P. Langlands, *Base Change for* GL(2), Ann. of Math. Stud. 96, Princeton Univ. Press, Princeton, NJ, and Univ. of Tokyo Press, Tokyo, 1980.

[9] K. Martin, *A symplectic case of Artin's conjecture*, Math. Res. Lett. 10 (2003), 483–492.

[10] M. R. Murty, V. K. Murty, and N. Saradha, *Modular forms and the Chebotarev density theorem*, Amer. J. Math. 110 (1988), 253–281.

[11] D. Ramakrishnan, *Modularity of solvable Artin representations of* GO(4)*-type*, Int. Math. Res. Notices 2002, 1–54.

[12] K. A. Ribet, *Galois representations and modular forms*, Bull. Amer. Math. Soc. (N.S.) 32 (1995), 375–402.

[13] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. 54 (1981), 323–401.

[14] J. Tunnell, *Artin's conjecture for representations of octahedral type*, Bull. Amer. Math. Soc. (N.S.) 5 (1981), 173–175.

[15] P.-J. Wong, *Character theory and Artin L-functions*, Ph.D. thesis, Queen's Univ., 2017.

[16] P.-J. Wong, *Langlands reciprocity for certain Galois extensions*, J. Number Theory 178 (2017), 126–145.

[17] P.-J. Wong, *Applications of group theory to conjectures of Artin and Langlands*, Int. J. Number Theory 14 (2018), 881–898.

Peng-Jie Wong
Department of Mathematics and Computer Science
University of Lethbridge
Lethbridge, Alberta T1K 3M4, Canada
E-mail: pengjie.wong@uleth.ca

Abstract (will appear on the journal's web site only)

We employ the theory of supercharacters introduced by Diaconis and Isaacs to refine the previous work of M. R. Murty, V. K. Murty, and Saradha by deriving effective versions of the Chebotarev density theorem for certain unions of conjugacy classes without using Artin's conjecture. As an application, we remove the assumption of Artin's conjecture from a result of Akbary and Ghioca on the Titchmarsh divisor problem for elliptic curves.