

CONSTANTS FOR ARTIN-LIKE PROBLEMS IN KUMMER AND DIVISION FIELDS

AMIR AKBARY AND MILAD FAKHARI

ABSTRACT. We apply the character sums method of Lenstra, Moree, and Stevenhagen to explicitly compute the constants in the Titchmarsh divisor problem for Kummer fields and division fields of Serre curves. We derive our results as special cases of a general result on the product expressions for the sums in the form

$$\sum_{n=1}^{\infty} \frac{g(n)}{\#G(n)}$$

in which $g(n)$ is a multiplicative arithmetic function and $\{G(n)\}$ is a certain family of Galois groups. Our results extend the application of the character sums method to the evaluation of constants, such as the Titchmarsh divisor constants, that are not density constants.

1. INTRODUCTION

Throughout this paper, let a be a non-zero integer that is not ± 1 . Let h be the largest integer for which a is a perfect h -th power. In 1927, Emil Artin proposed a conjecture for the density of primes q for which a given integer a is a primitive root modulo q . More precisely, Artin conjectured that the density is

$$(1.1) \quad A_a = \prod_{p \text{ prime}} \left(1 - \frac{1}{\#G(p)}\right) = \prod_{p \text{ prime}} \left(1 - \frac{1}{p-1}\right) \prod_{p \text{ prime}} \left(1 - \frac{1}{p(p-1)}\right),$$

where $G(p)$ is the Galois group of $\mathbb{Q}(\zeta_p, a^{1/p})$ over \mathbb{Q} . Here ζ_p is a primitive p -th root of unity. Note that $G(p)$ depends on a , but we suppress the dependence on a in our notation for simplicity. Also, observe that $A_a = 0$ if a is a perfect square as $G(2) = \{1\}$ for such a .

In 1957, computer calculations of the density for various values of a by D. H. Lehmer and E. Lehmer revealed some discrepancies from the conjectured value A_a . The reason for these inconsistencies is the dependency between the splitting conditions in *Kummer fields* $\mathbb{Q}(\zeta_p, a^{1/p})$.

To deal with these dependencies, Artin suggested an *entanglement correction factor* that appears when $a_{sf} \equiv 1 \pmod{4}$, where a_{sf} , the square-free part of a , is the largest square-free factor of a (see preface to Artin's collected works [3]). More precisely, the corrected conjectured density δ_a is

$$(1.2) \quad \delta_a = \begin{cases} A_a & \text{if } a_{sf} \not\equiv 1 \pmod{4}, \\ E_a \cdot A_a & \text{if } a_{sf} \equiv 1 \pmod{4}, \end{cases}$$

where

$$(1.3) \quad E_a = 1 - \mu(|a_{sf}|) \prod_{\substack{p|h \\ p|a_{sf}}} \frac{1}{p-2} \prod_{\substack{p|h \\ p|a_{sf}}} \frac{1}{p^2 - p - 1}.$$

Date: June 21, 2023.

2020 Mathematics Subject Classification. 11N37, 11A07.

Key words and phrases. Generalized Artin problem, character sums, Titchmarsh divisor problems in the family of number fields.

Here, $\mu(\cdot)$ is the Möbius function. Hooley proved the modified conjecture [9] in 1967 under the assumption of the *Generalized Riemann Hypothesis* (GRH) for the *Kummer fields* $K_n = \mathbb{Q}(\zeta_n, a^{1/n})$ for square-free values of n . For any n , let $G(n)$ be the Galois group of K_n/\mathbb{Q} . Hooley proved, under the GRH, that the primitive root density is

$$(1.4) \quad \sum_{n=1}^{\infty} \frac{\mu(n)}{\#G(n)},$$

and then showed that the above sum equals the corrected conjectured density δ_a in (1.2).

In [14], Lenstra, Moree, and Stevenhagen introduced their character sums method in finding product expressions for densities in Artin-like problems. Their method directly studies the primes that do not split completely in a Kummer family attached to a , without considering the summation expressions such as (1.4) for the constants. In [14, Theorem 4.2], they express the correction factor (1.3), when a is non-square and the discriminant d of $K_2 = \mathbb{Q}(a^{1/2})$ is odd, as

$$(1.5) \quad E_a = 1 + \prod_{p|2d} \frac{-1}{\#G(p) - 1}.$$

The authors of [14] achieve this by constructing a quadratic character $\chi = \prod_p \chi_p$ of a certain profinite group $A = \prod_p A_p$ such that $\ker \chi = \text{Gal}(K_\infty/\mathbb{Q})$, where $K_\infty = \bigcup_{n \geq 1} K_n$ (see Section 2 for details). They derive (1.2) as a special case of the following general theorem ([14, Theorem 3.3]) in the context of profinite groups.

Theorem 1.1 (Lenstra-Moree-Stevenhagen). *Let $A = \prod_p A_p$, with Haar measure $\nu = \prod_p \nu_p$, and the quadratic character $\chi = \prod_p \chi_p$ be as above. Then for $G = \ker \chi$ and $S = \prod_p S_p$, a product of ν_p -measurable subsets $S_p \subset A_p$ with $\nu_p(S_p) > 0$, we have*

$$\delta(S) = \frac{\nu(G \cap S)}{\nu(G)} = \left(1 + \prod_p \frac{1}{\nu_p(S_p)} \int_{S_p} \chi_p d\nu_p \right) \cdot \frac{\nu(S)}{\nu(A)}.$$

The above theorem shows that if $\frac{\nu(G \cap S)}{\nu(G)} \neq \frac{\nu(S)}{\nu(A)}$, then the density of S in A can be corrected to give the density of the elements of S in G . Moreover, the correction factor can be written explicitly in terms of the average of local characters χ_p over S_p .

Our goals in this paper are two-fold. In one direction, in Theorem 1.6 and Corollary 4.1, we will show how the character sums method of [14] can be adapted to directly deal with the general sums similar to (1.4). This is an approach different from the one given in Theorem 1.1 in which a density given as a product, i.e., $\nu(S)/\nu(A)$, is corrected to another density, i.e., $\nu(G \cap S)/\nu(G)$, which is not explicitly given as an infinite sum. In another direction, we describe how the method of [14] can be adapted to derive product expressions for the general sums similar to (1.4) in which $\mu(n)$ is replaced by a multiplicative arithmetic function that could be supported on non-square free integers (all the examples given in [14] are dealing with arithmetical functions supported on square-free integers). Such arithmetic sums appear naturally on many Artin-like problems. In addition, some of them, such as Titchmarsh divisor problems for families of number fields, are not problems related to the natural density of subsets of integers. In this direction, our Theorem 1.2 provides a product formula for the constant appearing in the Generalized Artin Problem for multiplicative functions f (see Problem 1.5) in full generality.

We continue with our general setup. Let $a = \pm a_0^e$, where e is the largest positive integer such that $|a|$ is a perfect e -th power, and $\text{sign}(a_0) = \text{sign}(a)$. In our arguments, the integer a is fixed, so we suppress the dependency on a in most of our notations. We fix a solution of the equation $x^2 - a_0 = 0$ and denote it by $a_0^{1/2}$. The quadratic field $K = \mathbb{Q}(a_0^{1/2})$, the so-called *entanglement field*, plays an important role in our arguments. We denote the discriminant of K by D . Observe

that for an integer $a (\neq 0, \pm 1)$, we have three different cases based on the parity of the exponent e and the sign of a : (i) *Odd exponent case*, in which e is odd; (ii) *Square case*, in which e is even and $a > 0$; (iii) *Twisted case*, in which e is even and $a < 0$. We refer to cases (i) and (ii) as *untwisted cases*. Note that for odd exponent case $K = K_2$, for square case $K_2 = \mathbb{Q}$ and $K \neq K_2$, and for twisted case $K_2 = \mathbb{Q}(i)$ and $K \neq K_2$.

For a Kummer family $\{K_n\}$, the Galois elements in $G(n) = \text{Gal}(K_n/\mathbb{Q})$ are determined by their actions on the n -th roots of a and the n -th roots of unity. Thus, any Galois automorphism can be realized as a group automorphism of the multiplicative group

$$R_n = \{\alpha \in \overline{\mathbb{Q}}^\times; \alpha^n \in \langle a \rangle\},$$

the group of n -radicals of a . This yields the injective homomorphisms

$$(1.6) \quad r_n : G(n) \rightarrow A(n) := \text{Aut}_{\mathbb{Q}^\times \cap R_n}(R_n),$$

where $A(n)$ is the group of automorphisms of R_n fixing elements of \mathbb{Q}^\times . For $n = \prod_{p^k \parallel n} p^k$ we have $A(n) \cong \prod_{p^k \parallel n} A(p^k)$. Let $\nu_p(e)$ denote the multiplicity of p in e . Let $\Phi(n)$ be the Euler totient function. For odd p ,

$$\#A(p^k) = p^{k - \min\{k, \nu_p(e)\}} \Phi(p^k)$$

and for $p = 2$,

$$\#A(2^k) = \begin{cases} 2^{k - \min\{k, s-1\}} \Phi(2^k) & \text{if } e \text{ is odd or } a > 0, \\ 2^{k - \min\{k, s-1\}} \Phi(2^{k+1}) & \text{if } e \text{ is even and } a < 0, \end{cases}$$

where

$$(1.7) \quad s = \begin{cases} \nu_2(e) + 1 & \text{if } e \text{ is odd or } a > 0, \\ \nu_2(e) + 2 & \text{if } e \text{ is even and } a < 0. \end{cases}$$

(see Proposition 3.1 for a proof.)

The following theorem, related to the family of Kummer fields K_n , gives us the product expressions of a large family of summations involving the orders of the Galois groups of K_n/\mathbb{Q} .

Theorem 1.2. *Let $a = \pm a_0^e$, where a_0 and e are defined as above, $K = \mathbb{Q}(a_0^{1/2})$, and let D be the discriminant of K . Let g be a multiplicative arithmetic function such that*

$$\sum_{n \geq 1} \frac{|g(n)|}{\#G(n)} < \infty,$$

where $\{G(n)\}$ is the family of Galois groups of the Kummer family $\{\mathbb{Q}(\zeta_n, a^{1/n})\}$. Let $A(n)$ be as defined above. Then,

$$(1.8) \quad \sum_{n=1}^{\infty} \frac{g(n)}{\#G(n)} = \prod_p \sum_{k \geq 0} \frac{g(p^k)}{\#A(p^k)} + \prod_p \sum_{k \geq \ell(p)} \frac{g(p^k)}{\#A(p^k)},$$

where

$$\ell(p) = \begin{cases} 0 & \text{if } p \text{ is odd and } p \nmid D, \\ 1 & \text{if } p \text{ is odd and } p \mid D, \\ s & \text{if } p = 2 \text{ and } D \text{ is odd,} \\ \max\{2, s\} & \text{if } p = 2 \text{ and } 4 \parallel D, \\ 2 & \text{if } p = 2, 8 \parallel D, \text{ and } (\nu_2(e) = 1 \text{ and } a < 0), \\ \max\{3, s\} & \text{if } p = 2, 8 \parallel D, \text{ and } (\nu_2(e) \neq 1 \text{ or } a > 0). \end{cases}$$

Remarks 1.3. (i) In the summation (1.4) appearing in Artin's primitive root conjecture, we have $g(n) = \mu(n)$. In this case, formula (1.8) for $g(n) = \mu(n)$ provides a unified way of expressing the constant in Artin's primitive root conjecture. Note that if e is even and $a > 0$, i.e., a is a perfect square, we have

$$\sum_{k \geq 0} \frac{\mu(2^k)}{\#A(2^k)} = 0 \quad \text{and} \quad \sum_{k \geq \ell(2)} \frac{\mu(2^k)}{\#A(2^k)} = 0.$$

(The first sum is zero since $\#A(2) = 1$ and the second sum is zero since $\ell(2) \geq 2$.) Hence, (1.8) vanishes. Also, if e is even and $a < 0$, then $\ell(2) \geq 2$. Thus, (1.8) reduces to (1.1). If e is odd and D is even, then again $\ell(2) \geq 2$ and (1.8) reduces to (1.1). The only remaining case is when e is odd and D is odd (equivalently e odd and $a_{sf} \equiv 1 \pmod{4}$), where (1.8) reduces to $E_a \cdot A_a$ given in (1.2).

(ii) As a consequence of Theorem 1.1, we can derive necessary and sufficient conditions for the vanishing of

$$(1.9) \quad \sum_{n=1}^{\infty} \frac{g(n)}{\#G(n)}.$$

More precisely, (1.9) vanishes if and only if one of the following holds:

(a) For a prime $p \nmid 2D$, we have $\sum_{k \geq 0} \frac{g(p^k)}{\#A(p^k)} = 0$.

(b) We have

$$\prod_{p|2D} \sum_{k \geq 0} \frac{g(p^k)}{\#A(p^k)} + \prod_{p|2D} \sum_{k \geq \ell(p)} \frac{g(p^k)}{\#A(p^k)} = 0.$$

In the case of Artin's conjecture, (a) is never satisfied and (b) holds if and only if a is a perfect square.

(iii) If $\#G(n)$ was a multiplicative function, then the sum in (1.8) would have been equal to the product $\prod_p \sum_{k \geq 0} \frac{g(p^k)}{\#G(p^k)}$. However, this is not the case for the Kummer family, and thus the sum in (1.8) may differ from the above naive product. If the sum and the product are not equal, then a complex number $E_{a,g}$ is called a *correction factor* if

$$\sum_{n=1}^{\infty} \frac{g(n)}{\#G(n)} = E_{a,g} \prod_p \sum_{k \geq 0} \frac{g(p^k)}{\#G(p^k)}.$$

The expression (1.8) provides precise information on the correction factor $E_{a,g}$. In fact, if

$\sum_{k \geq 0} \frac{g(p^k)}{\#G(p^k)} \neq 0$ for all primes $p \mid 2D$, we have

$$\sum_{n=1}^{\infty} \frac{g(n)}{\#G(n)} = \left(\frac{\prod_{p|2D} \sum_{k \geq 0} \frac{g(p^k)}{\#A(p^k)} + \prod_{p|2D} \sum_{k \geq \ell(p)} \frac{g(p^k)}{\#A(p^k)}}{\prod_{p|2D} \sum_{k \geq 0} \frac{g(p^k)}{\#G(p^k)}} \right) \prod_p \sum_{k \geq 0} \frac{g(p^k)}{\#G(p^k)}.$$

Also, if $\sum_{k \geq 0} \frac{g(p^k)}{\#G(p^k)} = 0$ for some prime $p \mid 2D$, and $\sum_{n \geq 1} \frac{g(n)}{\#G(n)} \neq 0$, then the product $\prod_p \sum_{k \geq 0} \frac{g(p^k)}{\#G(p^k)}$ cannot be corrected.

It should be noted that for $K = \mathbb{Q}(\sqrt{\pm 2})$ the above correction factor is slightly different from the one given in Theorem 1.1 for the density problems since in these cases $\#G(2^k) \neq \#A(2^k)$ for some positive integers k .

(iv) For integer $a (\neq 0, \pm 1)$, let $n_a = \prod_{p|2D} p^{\ell(p)}$, where D and $\ell(p)$ are as in Theorem 1.2. Then, by taking $g(n) = 1/n^s$, for $\Re(s) > 0$, in Theorem 1.2 and comparing the coefficients of $1/n^s$ in both sides of (1.8), we get

$$[\mathbb{Q}(\zeta_n, a^{1/n}) : \mathbb{Q}] = \begin{cases} \#A(n) & \text{if } n_a \nmid n, \\ \frac{1}{2}\#A(n) & \text{if } n_a \mid n. \end{cases}$$

The formula (1.8) can be used to study the constants in many Artin-like problems. We next apply this formula in the computation of the average value of a specific arithmetic function attached to a Kummer family. More precisely, for $\{K_n := \mathbb{Q}(\zeta_n, a^{1/n})\}_{n \geq 1}$, we define

$$\tau_a(p) = \# \{n \in \mathbb{N}; p \text{ splits completely in } K_n/\mathbb{Q}\}.$$

The Titchmarsh divisor problem attached to a Kummer family concerns the behaviour of $\sum_{p \leq x} \tau_a(p)$ as $x \rightarrow \infty$ (see [1] for the motivation behind this problem and its relation with the classical Titchmarsh divisor problem on the average value of the number of divisors of shifted primes). Under the assumption of the GRH for the Dedekind zeta function of K_n/\mathbb{Q} for $n \geq 1$, Felix and Murty [8, Theorem 1.6] proved that

$$(1.10) \quad \sum_{p \leq x} \tau_a(p) \sim \left(\sum_{n \geq 1} \frac{1}{[K_n : \mathbb{Q}]} \right) \cdot \text{li}(x),$$

as $x \rightarrow \infty$, where $\text{li}(x) = \int_2^x \frac{1}{\log t} dt$. They do not provide an Euler product expression for the constant appearing in the main term of (1.10). As a direct consequence of Theorem 1.2 with $g(n) = 1$, we readily find an explicit product formula for the constant appearing in (1.10).

Proposition 1.4. *Let $a = \pm a_0^e$ with $e = \prod_p p^{\nu_p(e)}$, and let D be the discriminant of $K = \mathbb{Q}(a_0^{1/2})$. Then, if e is odd or $a > 0$,*

$$(1.11) \quad \sum_{n \geq 1} \frac{1}{[K_n : \mathbb{Q}]} = \left(1 + \frac{c_0}{3 \cdot 2^{\nu_2(e)} - 2} \prod_{p|2D} \frac{p^{\nu_p(e)+2} + p^{\nu_p(e)+1} - p^2}{p^{\nu_p(e)+3} + p^{\nu_p(e)} - p^2} \right) \\ \times \prod_p \left(1 + \frac{p^{\nu_p(e)+2} + p^{\nu_p(e)+1} - p^2}{p^{\nu_p(e)}(p-1)(p^2-1)} \right),$$

where

$$c_0 = \begin{cases} 1/4 & \text{if } 4 \parallel D \text{ and } \nu_2(e) = 0, \text{ or if } 8 \parallel D \text{ and } \nu_2(e) = 1, \\ 1/16 & \text{if } 8 \parallel D \text{ and } \nu_2(e) = 0, \\ 1 & \text{otherwise.} \end{cases}$$

If e is even and $a < 0$ (i.e., the twisted case)

$$(1.12) \quad \sum_{n \geq 1} \frac{1}{[K_n : \mathbb{Q}]} = \left(1 + \frac{c_0}{3 \cdot 2^{\nu_2(e)+2} - 2} \prod_{\substack{p|D \\ p \neq 2}} \frac{p^{\nu_p(e)+2} + p^{\nu_p(e)+1} - p^2}{p^{\nu_p(e)+3} + p^{\nu_p(e)} - p^2} \right) \\ \times \left(1 + \frac{2^{\nu_2(e)+2} - 2^{\nu_2(e)} - 1}{3 \cdot 2^{\nu_2(e)}} \right) \prod_{\substack{p \\ p \neq 2}} \left(1 + \frac{p^{\nu_p(e)+2} + p^{\nu_p(e)+1} - p^2}{p^{\nu_p(e)}(p-1)(p^2-1)} \right),$$

where

$$c_0 = \begin{cases} 4 & \text{if } 8 \parallel D \text{ and } \nu_2(e) = 1, \\ 1 & \text{otherwise.} \end{cases}$$

Let c_a denote the constant given in (1.11) and (1.12). It is evident that $c_a = q_a \cdot u$, where q_a is a rational number depending on a , and u is the *universal constant*

$$(1.13) \quad \sum_{n=1}^{\infty} \frac{1}{n\Phi(n)} = \prod_p \left(1 + \frac{p}{(p-1)(p^2-1)} \right) = 2.203856 \dots,$$

where $\Phi(n)$ is the Euler totient function. Observe that if $\nu_p(e) = 0$ for all p , the expressions for naive products (products over all primes p) given in (1.11) and (1.12) reduce to (1.13). This is in accordance with [2, Theorem 1.4] in which (1.13) appears as the average constant while varying a . Thus, on average over a , a smooth version of (1.11) and (1.12), i.e., the universal constant, appears.

The product expressions of Proposition 1.4 provide a convenient way of computing the numerical value of c_a for a given value of a . We record a sample of such values in the following table.

a	-13	-10	-8	-5	-3	-2	2	3	5	8	10	13
c_a	2.205	2.206	2.972	2.214	2.343	2.258	2.258	2.238	2.247	2.972	2.206	2.209

The classical Artin conjecture and the Titchmarsh divisor problem for a Kummer family are instances of a more general problem that we now describe. For an integer $a (\neq 0, \pm 1)$ and a prime $p \nmid a$, the *residual index* of $a \bmod p$, denoted by $i_a(p)$ is the index of the subgroup $\langle a \rangle$ in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$. There is a vast amount of literature on the study of asymptotics of functions of $i_a(p)$ as p varies over primes. In [16, p. 377], the following problem is proposed.

Problem 1.5 (Generalized Artin Problem). *For certain integers a and arithmetic functions $f(n)$, establish the asymptotic formula*

$$\sum_{p \leq x} f(i_a(p)) \sim c_{f,a} \operatorname{li}(x),$$

as $x \rightarrow \infty$, where

$$(1.14) \quad c_{f,a} := \sum_{n \geq 1} \frac{g(n)}{[K_n : \mathbb{Q}]}.$$

Here $g(n) = \sum_{d|n} \mu(d) f(n/d)$ is the Möbius inverse of $f(n)$, where $\mu(n)$ is the Möbius function.

Note that by setting $f(n)$ as the characteristic function of the set $S = \{1\}$ and $g(n) = \mu(n)$ in Problem 1.5, we get the Artin conjecture, and $f(n) = d(n)$ (the divisor function) and $g(n) = 1$ give the Titchmarsh divisor problem for a Kummer family, this is true since $\tau_a(p) = d(i_a(p))$ (see [8, Lemma 2.1] for details). Also, a conjecture of Laxton from 1969 [13] predicts that for $f(n) = 1/n$, the generalized Artin problem determines the density of primes in the sequence given by the recurrence $w_{n+2} = (a+1)w_{n+1} - aw_n$, where $a > 1$ is a fixed integer. Another instance of Problem 1.5 appears in a conjecture of Bach, Lukes, Shallit, and Williams [4] in which the constant $c_{f,2}$ for $f(n) = \log n$ appears in the main term of the asymptotic formula for $\log P_2(x)$, where $P_2(x)$ is the smallest x -pseudopower of the base 2.

A notable result on Generalized Artin Problem, due to Felix and Murty [8, Theorem 1.7], establishes, under the assumption of GRH, the asymptotic

$$(1.15) \quad \sum_{p \leq x} f(i_a(p)) = c_{f,a} \operatorname{li}(x) + O_a \left(\frac{x}{(\log x)^{2-\epsilon-\alpha}} \right),$$

for $\epsilon > 0$. Here $f(n)$ is an arithmetic function whose Möbius inverse $g(n)$ satisfies

$$|g(n)| \ll d_k(n)^r (\log n)^\alpha,$$

with $k, r \in \mathbb{N}$ and $0 \leq \alpha < 1$ all fixed, where $d_k(n)$ denotes the number of representations of n as product of k positive integers. Observe that the identity (1.8) in Theorem 1.2 conveniently furnish a product formula in full generality for the constant $c_{f,a}$ in (1.15) when f (equivalently g) is a multiplicative function. This product formula is valuable for studying the vanishing criteria for $c_{f,a}$ and their numerical evaluations for different f .

We now comment on the proof of Theorem 1.2. Observe that corresponding to the Kummer family $\{K_n\}$, we can consider the inverse systems $((G(n))_{n \in \mathbb{N}}, (i_{n_1, n_2})_{n_1 | n_2})$ and $((A(n))_{n \in \mathbb{N}}, (j_{n_1, n_2})_{n_1 | n_2})$ ordered by divisibility relation on \mathbb{N} , where $G(n)$ and $A(n)$ are as defined before and i_{n_1, n_2} and j_{n_1, n_2} , for $n_1 | n_2$, are restriction maps. By taking the inverse limits on both sides of (1.6) we have the injective continuous homomorphism

$$r : G = \varprojlim G(n) \rightarrow A = \varprojlim A(n)$$

of profinite groups, where $G = \text{Gal}(K_\infty/\mathbb{Q})$ and $A = \text{Aut}_{\mathbb{Q}^\times \cap R_\infty}(R_\infty)$ with $K_\infty = \bigcup_{n \geq 1} K_n$ and $R_\infty = \bigcup_{n \geq 1} R_n$. As profinite groups, both G and A are endowed with compact topologies and thus can be equipped by Haar measures. We will show that Theorem 1.2 is a corollary of the following theorem attached to a general setting of profinite groups G and A .

Theorem 1.6. *Let $((G(n))_{n \in \mathbb{N}}, (i_{n_1, n_2})_{n_1 | n_2})$ and $((A(n))_{n \in \mathbb{N}}, (j_{n_1, n_2})_{n_1 | n_2})$ be inverse systems of finite groups ordered by divisibility relation on \mathbb{N} . Moreover, for $n \geq 1$, assume that there are injective maps $r_n : G(n) \rightarrow A(n)$ compatible by i_{n_1, n_2} and j_{n_1, n_2} , i.e., for $n_1 | n_2$, the diagram*

$$\begin{array}{ccc} G(n_2) & \xrightarrow{r_{n_2}} & A(n_2) \\ \downarrow i_{n_1, n_2} & & \downarrow j_{n_1, n_2} \\ G(n_1) & \xrightarrow{r_{n_1}} & A(n_1) \end{array}$$

commutes. Let $r : G = \varprojlim G(n) \rightarrow A = \varprojlim A(n)$ be the resulting injective continuous homomorphism of profinite groups. Let μ_m be the multiplicative group of m -th roots of unity for a fixed m . Suppose there exists an exact sequence

$$(1.16) \quad 1 \rightarrow G \xrightarrow{r} A \xrightarrow{\chi} \mu_m \rightarrow 1,$$

where χ is a continuous homomorphism. Let g be an arithmetic function such that

$$\sum_{n \geq 1} \frac{|g(n)|}{\#G(n)} < \infty.$$

Consider the natural projections $\pi_{A,n} : A \rightarrow A(n)$ and let

$$(1.17) \quad \tilde{g} = \sum_{n \geq 1} g(n) 1_{\ker \pi_{A,n}},$$

where $1_{\ker \pi_{A,n}}$ denotes the characteristic function of $\ker \pi_{A,n}$. Let ν_A be the normalized Haar measure attached to A . Then, $\tilde{g} \in L^1(\nu_A)$ (the space of ν_A -integrable functions) and

$$\sum_{n \geq 1} \frac{g(n)}{\#G(n)} = \sum_{i=0}^{m-1} \int_A \tilde{g} \chi^i d\nu_A.$$

Observe that Theorem 1.6 is quite general and can be applied in the evaluation of sums of the form $\sum_{n \geq 1} g(n)/\#G(n)$ for any family $\{G(n)\}$ of finite groups satisfying the assumptions of the theorem. The Kummer family is an instance of such families. Another example is the family of division fields attached to a *Serre elliptic curve* E (see Section 7 for the definition). Following

[14, Section 8], in Section 7, we show that the family of division fields $\{\mathbb{Q}(E[n])\}$ attached to a Serre curve E satisfies the conditions of Theorem 1.6 and so as a consequence of it the following holds.

Proposition 1.7. *Let $\mathbb{Q}(E[n])$ denote the n -division field of a Serre elliptic curve defined over \mathbb{Q} by a Weierstrass equation $y^2 = x^3 + ax + b$. Let Δ be the discriminant of the cubic equation $x^3 + ax + b = 0$ and let D be the discriminant of the quadratic field $K = \mathbb{Q}(\Delta^{1/2})$. Let $g(n)$ be a multiplicative arithmetic function such that*

$$\sum_{n \geq 1}^{\infty} \frac{|g(n)|}{[\mathbb{Q}(E[n]) : \mathbb{Q}]} < \infty.$$

Then,

$$(1.18) \quad \sum_{n=1}^{\infty} \frac{g(n)}{[\mathbb{Q}(E[n]) : \mathbb{Q}]} = \prod_p \sum_{k \geq 0} \frac{g(p^k)}{p^{4k-3}(p^2-1)(p-1)} + \prod_p \sum_{k \geq \ell(p)} \frac{g(p^k)}{p^{4k-3}(p^2-1)(p-1)},$$

where

$$\ell(p) = \begin{cases} 0 & \text{if } p \text{ is odd and } p \nmid D, \\ 1 & \text{if } p \text{ is odd and } p \mid D, \\ 1 & \text{if } p = 2 \text{ and } D \text{ is odd,} \\ 2 & \text{if } p = 2 \text{ and } 4 \parallel D, \\ 3 & \text{if } p = 2 \text{ and } 8 \parallel D. \end{cases}$$

Observe that the above proposition for $g(n) = 1$ reduces to the product expression of the Titchmarsh divisor problem for the family of division fields attached to a Serre curve E . We note that the product expression for this constant and two other constants corresponding to different $g(n)$'s for such families are given in [5, Theorem 5] by determining the value of $[\mathbb{Q}(E[n]) : \mathbb{Q}]$ for a Serre curve E (see [5, Proposition 17 (iv)]) and employing [11, Lemma 3.12]. It is worth mentioning that a similar approach in finding the expression (1.11) using the exact formulas for $[K_n : \mathbb{Q}]$ as given in [20, Proposition 4.1] will result in the tedious case by case computations that does not appear to be straightforward. Especially when $a < 0$, this approach seems to be intractable. The method of [14] as described above provides an elegant approach to establishing identities similar to (1.11) and (1.12).

The structure of the paper is as follows. We describe our adaptation of the character sums method of [14] in Sections 2 and 3 and prove Proposition 3.3 that plays a crucial role in our explicit computation of the constants in the Kummer case. Section 4 is dedicated to a proof of Theorem 1.6. The proofs of Theorem 1.2 and its consequence, Proposition 1.4, are given respectively in Sections 5 and 6. Finally, a brief discussion on Serre curves and the proof of Proposition 1.7 are provided in Section 7.

Notations 1.8. The following notations are used throughout the paper. The letter p denotes a prime number, k denotes a non-negative integer, the letter n denotes a positive integer, the multiplicity of the prime p in the prime factorization of n is denoted by $\nu_p(n)$, the cardinality of a finite set S is denoted by $\#S$, 1_S is the characteristic function of a set S , $\overline{\mathbb{Q}}$ is an algebraic closure of \mathbb{Q} , ζ_n denotes a primitive root of unity, and $\Phi(n)$ is the Euler totient function. In Sections 2, 3, 5, and 6, $a = \pm a_0^e$ is a non-zero integer other than ± 1 , the collection $\{K_n = \mathbb{Q}(\zeta_n, a^{1/n})\}_{n \in \mathbb{N}}$ is the family of Kummer fields and $K = \mathbb{Q}(a_0^{1/2})$ is the entanglement field attached to this family, D is the discriminant of K , the Galois group of K_n over \mathbb{Q} is denoted by $G(n)$, the inverse limit of the directed family $\{G(n)\}$ is denoted by G , μ_∞ denotes the group of all roots of unity, and $\mathbb{Q}_{ab} = \mathbb{Q}(\mu_\infty)$ is the maximal abelian extension of \mathbb{Q} . The group of n -radicals of the integer $a = \pm a_0^e$ is denoted by R_n and $R_\infty = \bigcup_{n \geq 1} R_n$. The group of automorphisms of R_n (respectively R_∞) that fix \mathbb{Q}^\times is denoted

by $A(n)$ (respectively A). The inverse limit of the system $\{A(p^k)\}_{k \geq 1}$ is denoted by A_p . The map $\pi_{A,n}$ (respectively $\pi_{G,n}$ and φ_{p^k}) is the projection map from A (respectively G and A_p) to $A(n)$ (respectively $G(n)$ and $A(p^k)$). The profinite completion of \mathbb{Z} is denoted by $\widehat{\mathbb{Z}}$ and \mathbb{Z}_p is the ring of p -adic integers. The normalized Haar measures on G , A , and A_p are denoted respectively by ν_G , ν_A , and ν_{A_p} . The space of ν -integrable functions is denoted by $L^1(\nu)$. In Section 4, $G(n)$, $A(n)$, $A(p^k)$, G , A , A_p , $\pi_{A,n}$, φ_{p^k} , ν_G , ν_A , and ν_{A_p} are used in the general setting of profinite groups. Finally, in Section 7, $E[n]$ denotes the group of n -division points of an elliptic curve E defined over \mathbb{Q} given by a Weierstrass equation with discriminant Δ , and $K = \mathbb{Q}(\Delta^{1/2})$ of discriminant D is the entanglement field attached to the family of division fields of a Serre elliptic curve.

2. THE ASSOCIATED CHARACTER TO A KUMMER FAMILY

Recall that for an integer $a (\neq 0, \pm 1)$, we set $a = \pm a_0^e$, where $\text{sign}(a) = \text{sign}(a_0)$ and e is the largest such integer. We fix a solution of the equation $x^2 - a_0 = 0$, denote it by $a_0^{1/2}$, and set $K = \mathbb{Q}(a_0^{1/2})$.

We next define a quadratic character which describes the entanglements inside a given Kummer family $\{K_n\}$. Let $\mu_\infty = \bigcup_{n \geq 1} \mu_n(\overline{\mathbb{Q}})$ be the group of all roots of unity in $\overline{\mathbb{Q}}$. Then, μ_∞ is contained in $K_\infty = \bigcup_{n \geq 1} K_n$. In addition, the infinite extension K_∞/\mathbb{Q} is the compositum of $\mathbb{Q}(a_0^{\mathbb{Q}})$ and \mathbb{Q}_{ab} (the maximal abelian extension of \mathbb{Q}), where

$$(2.1) \quad \mathbb{Q}(a_0^{\mathbb{Q}}) \cap \mathbb{Q}_{ab} = \mathbb{Q}(a_0^{1/2})$$

(see [14, Lemma 2.5]). Note that $a_0^{\mathbb{Q}} = \{a_0^b; b \in \mathbb{Q}\}$. In [14, Page 494] it is proved that

$$(2.2) \quad A = \text{Aut}_{\mathbb{Q}^\times \cap R_\infty}(R_\infty) \cong \text{Hom}(a_0^{\mathbb{Q}}/a_0^{\mathbb{Z}}, \mu_\infty) \rtimes \text{Aut}(\mu_\infty),$$

where $a_0^{\mathbb{Z}} = \{a_0^b; b \in \mathbb{Z}\}$, and for $(\phi_1, \sigma_1), (\phi_2, \sigma_2) \in A$ we have

$$(\phi_1, \sigma_1)(\phi_2, \sigma_2) = (\phi_1 \cdot (\sigma_1 \circ \phi_2), \sigma_1 \circ \sigma_2).$$

Note that $G = \text{Gal}(K_\infty/\mathbb{Q})$ can be embedded in A . Thus, if $(\phi, \sigma) \in \text{Hom}(a_0^{\mathbb{Q}}/a_0^{\mathbb{Z}}, \mu_\infty) \rtimes \text{Aut}(\mu_\infty) \cong A$ is an element of G , then, by (2.1), the action of ϕ and σ on $\mathbb{Q}(a_0^{1/2})$ must be the same. One can show that $(\phi, \sigma) \in A$ is in G if and only if ϕ and σ act in a compatible way on $a_0^{1/2}$, i.e.,

$$(2.3) \quad \phi(a_0^{1/2}) = \frac{\sigma(a_0^{1/2})}{a_0^{1/2}} \in \mu_2$$

(see [14, Page 494]). (For simplicity, we used $\phi(a_0^{1/2})$ instead of $\phi(a_0^{1/2} a_0^{\mathbb{Z}})$.) We elaborate on (2.3) by considering two distinct quadratic characters ψ_K and χ_D on A which are related to the entanglement field $K = \mathbb{Q}(a_0^{1/2})$ of discriminant D . The quadratic character $\psi_K : A \rightarrow \mu_2$ corresponds to the action of ϕ -component of $(\phi, \sigma) \in A$ on $a_0^{1/2}$, i.e.,

$$\psi_K(\phi, \sigma) = \phi(a_0^{1/2}) \in \mu_2.$$

This is a *non-cyclotomic character*, i.e., ψ_K does not factor via the natural map $A \rightarrow \text{Aut}(\mu_\infty)$ (see [14, Page 495]). The other quadratic character,

$$\chi_D : A \rightarrow \text{Aut}(\mu_\infty) \cong \widehat{\mathbb{Z}}^\times \rightarrow \mu_2,$$

corresponds to the action of the cyclotomic component $\text{Aut}(\mu_\infty)$ of A on $K = \mathbb{Q}(a_0^{1/2})$ of discriminant D , i.e.,

$$\chi_D(\phi, \sigma) = \frac{\sigma(a_0^{1/2})}{a_0^{1/2}} \in \mu_2.$$

Hence, by [6, Proposition 5.16 and Corollary 5.17], χ_D is the lift of the Kronecker symbol $\left(\frac{D}{\cdot}\right)$ to $\text{Aut}(\mu_\infty) \cong \widehat{\mathbb{Z}}^\times$.

The characters χ_D and ψ_K are not the same on A since one is cyclotomic, and the other is not. Moreover, by (2.3), an element $x \in A$ is in G if and only if $\psi_K(x) = \chi_D(x)$. Thus, the image of the homomorphism $G \rightarrow A$ is the kernel of the non-trivial quadratic character $\chi = \psi_K \cdot \chi_D : A \rightarrow \mu_2$. In other words, the sequence

$$1 \longrightarrow G \xrightarrow{r} A \xrightarrow{\chi = \psi_K \cdot \chi_D} \mu_2 \longrightarrow 1$$

is an exact sequence (see [14, Theorem 2.9] for more details).

Let $A(p^k) = \text{Aut}_{\mathbb{Q}^\times \cap R_{p^k}}(R_{p^k})$ and $A_p = \varprojlim A(p^k)$. Since an element of A can be determined by its action on prime power radicals, then $A \cong \prod_p A_p$ (see [14, formula (2.10), p. 495] and [15, p. 20]). The character χ_D is the lift of the Kronecker symbol $\left(\frac{D}{\cdot}\right)$ to A via the maps

$$A \cong \left(\prod_p A_p \right) \xrightarrow{\text{proj}} \text{Aut}(\mu_\infty) \left(\cong \prod_p \mathbb{Z}_p^\times \right) \xrightarrow{\text{proj}} (\mathbb{Z}/|D|\mathbb{Z})^\times,$$

where the first projection comes via (2.2). Since D is a fundamental discriminant, $\chi_D = \prod_{p|D} \chi_{D,p}$, where $\chi_{D,p}$ is the lift of the Legendre symbol modulo p to A_p for odd p , and $\chi_{D,2}$ is the lift of one of the Dirichlet characters mod 8 to A_2 (see [7, Chapter 5]). More precisely, if D is odd, then $\chi_{D,2} = 1$; if $4 \parallel D$, then $\chi_{D,2}$ is the lift to A_2 of $\left(\frac{-4}{\cdot}\right)$, the unique Dirichlet character mod 8 of conductor 4; and if $8 \parallel D$, then $\chi_{D,2}$ is the lift to A_2 of $\left(\frac{\pm 8}{\cdot}\right)$, one of the two Dirichlet characters mod 8 of conductor 8. For the case $8 \parallel D = 2^a \prod_{i=1}^k p_i$, if $D > 0$ and the number of $1 \leq i \leq k$ with $p_i \equiv 3 \pmod{4}$ is even, or $D < 0$ and the number of $1 \leq i \leq k$ with $p_i \equiv 3 \pmod{4}$ is odd, then $\chi_{D,2}$ is the lift to A_2 of $\left(\frac{8}{\cdot}\right)$. Otherwise, $\chi_{D,2}$ is the lift to A_2 of $\left(\frac{-8}{\cdot}\right)$.

Next, we show that χ can be written as a product of local characters $\chi_p : A_p \rightarrow \mu_2$. Note that ψ_K factors via A_2 . Let $\psi_{K,2} : A_2 \rightarrow \mu_2$ be the corresponding homomorphism obtained from factorization of ψ_K via A_2 . For odd primes $p \nmid D$, set $\chi_p = 1$. Let $\chi_p = \chi_{D,p}$ for odd primes $p \mid D$ and for prime 2 let $\chi_2 = \chi_{D,2} \cdot \psi_{K,2}$. Therefore, by the above construction of χ , we have the decomposition $\chi = \prod_p \chi_p$.

3. THE LOCAL CHARACTERS χ_p

In this section, we find the smallest values of k , as a function of p and a , for which the local character χ_p factors via $A(p^k)$. In other words, we will determine the values of k for which χ_p is trivial on $\ker \varphi_{p^k}$ and it is nontrivial on $\ker \varphi_{p^{k-1}}$, where φ_{p^i} is the projection map from A_p to $A(p^i)$. The values are recorded in the statements of Theorem 1.2 and Proposition 3.3. We start by giving a concrete description of the groups $A(2^k)$, for positive integers k , as subgroups of matrices $\begin{pmatrix} 1 & 0 \\ b & d \end{pmatrix}$, where $b \in \mathbb{Z}/2^k\mathbb{Z}$ and $d \in (\mathbb{Z}/2^k\mathbb{Z})^\times$. We achieve this by choosing a certain compatible system of generators for the groups R_{2^k} , where $k \geq 1$.

Proposition 3.1. (i) Let $\Phi(n)$ be the Euler totient function and s be as defined in (1.7). For odd p ,

$$\#A(p^k) = p^{k - \min\{k, \nu_p(e)\}} \Phi(p^k)$$

and for $p = 2$,

$$\#A(2^k) = \begin{cases} 2^{k - \min\{k, s-1\}} \Phi(2^k) & \text{if } e \text{ is odd or } a > 0, \\ 2^{k - \min\{k, s-1\}} \Phi(2^{k+1}) & \text{if } e \text{ is even and } a < 0. \end{cases}$$

(ii) If e is even and $a < 0$, we have

$$A(2^k) \cong \left\{ \begin{pmatrix} 1 & 0 \\ b & d \end{pmatrix}; b \in \mathbb{Z}/2^k\mathbb{Z}, d \in (\mathbb{Z}/2^k\mathbb{Z})^\times, \text{ and } 2b + 1 \equiv d \pmod{2^{\min\{k, s-1\}}} \right\}.$$

(iii) If e is odd or $a > 0$, we have

$$A(2^k) \cong \left\{ \begin{pmatrix} 1 & 0 \\ b & d \end{pmatrix}; b \in \mathbb{Z}/2^k\mathbb{Z}, d \in (\mathbb{Z}/2^k\mathbb{Z})^\times, \text{ and } b + 1 \equiv d \pmod{2^{\min\{k, s-1\}}} \right\}.$$

Proof. (i) For odd primes p , it is known that $A(p^k) \cong G(p^k) = \text{Gal}(K_{p^k}/\mathbb{Q})$ (see [14, Remarks 2.12. (b), p. 496]). Also if $K \neq \mathbb{Q}(\sqrt{\pm 2})$, then $A(2^k) \cong G(2^k)$. Since the size of $A(2^k)$ is independent of K , we get the formulas for the size of $A(p^k)$ from the ones for $G(p^k)$ as given in [20, Proposition 4.1].

(ii) Let $a = -a_0^e$ as before and $e = 2^{\nu_2(e)}e_1$, where $\nu_2(e) \geq 1$ and e_1 is odd. We denote a primitive m -th root of unity by ζ_m . Recall that R_{2^k} is the group of 2^k -radicals. We have

$$R_{2^k} = \langle \zeta_{2^{k+1}}^{e_1} (a_0^{e_1})^{1/2^{k-\nu_2(e)}}, \zeta_{2^k} \rangle = \langle \beta, \zeta_{2^k} \rangle.$$

An automorphism $\tau \in A(2^k)$ is determined by its action on these generators of R_{2^k} , i.e., β and ζ_{2^k} . We have $\tau(\beta) = \beta \zeta_{2^k}^{b(\tau)}$ and $\tau(\zeta_{2^k}) = \zeta_{2^k}^{d(\tau)}$, where $b(\tau) \in \mathbb{Z}/2^k\mathbb{Z}$ and $d(\tau) \in (\mathbb{Z}/2^k\mathbb{Z})^\times$. We consider two cases.

Case 1: $k \geq s - 1 = \nu_2(e) + 1$. We have

$$a_0^{e_1} \tau(\zeta_{2^{k+1}}^{2^{k-\nu_2(e)}}) = \tau(\beta^{2^{k-\nu_2(e)}}) = (\beta \zeta_{2^k}^{b(\tau)})^{2^{k-\nu_2(e)}} = a_0^{e_1} \zeta_{2^{k+1}}^{2^{k-\nu_2(e)}} \zeta_{2^k}^{b(\tau)2^{k-\nu_2(e)}}.$$

From here we get

$$\zeta_{2^k}^{d(\tau)2^{k-\nu_2(e)-1}} = \zeta_{2^k}^{2^{k-\nu_2(e)-1} + b(\tau)2^{k-\nu_2(e)}}.$$

This implies $2b(\tau) + 1 \equiv d(\tau) \pmod{2^{s-1}}$.

Case 2: $k < s - 1 = \nu_2(e) + 1$. We have

$$(a_0^{e_1})^{2/2^{k-\nu_2(e)}} \tau(\zeta_{2^{k+1}}^2) = \tau(\beta^2) = (\beta \zeta_{2^k}^{b(\tau)})^2 = (a_0^{e_1})^{2/2^{k-\nu_2(e)}} \zeta_{2^{k+1}}^2 \zeta_{2^k}^{2b(\tau)}.$$

From here we get

$$\zeta_{2^k}^{d(\tau)} = \zeta_{2^k}^{1+2b(\tau)}.$$

This implies $2b(\tau) + 1 \equiv d(\tau) \pmod{2^k}$.

So any $\tau \in A(2^k)$ corresponds to a matrix $\begin{pmatrix} 1 & 0 \\ b(\tau) & d(\tau) \end{pmatrix}$ in the affine group of matrices given in part (ii) of the proposition. Since, in each case, the number of such matrices is equal to the cardinality of $A(2^k)$ given in part (i), then the claimed isomorphism in part (ii) holds.

(iii) The proof is analogous to the proof of (ii) by considering $R_{2^k} = \langle \zeta_{2^k} (a_0^{e_1})^{1/2^{k-\nu_2(e)}}, \zeta_{2^k} \rangle$, where $(e_1, 2) = 1$. □

The following proposition indicates the significance of the integer s defined in (1.7).

Proposition 3.2. *The number s defined in (1.7) is the smallest integer k for which $\psi_{K,2}$ factors via $A(2^k)$.*

Proof. For integers $k \geq 0$, let $\varphi_{p^k} : A_p \rightarrow A(p^k)$ be the projection map. It is enough to show that $\psi_{K,2}$ is non-trivial on $\ker \varphi_{2^{s-1}}$ and is trivial on $\ker \varphi_{2^s}$. We write the proof for the twisted case, where $s = \nu_2(e) + 2$. The proof for the untwisted case is similar.

Assume that $a = -(a_0^{e_1})^{2^{\nu_2(e)}}$ as in part (iii) of Proposition 3.1. Let $\alpha \in A_2$ be such that

$$\tau_2 = \varphi_{2^{\nu_2(e)+2}}(\alpha) = \begin{pmatrix} 1 & 0 \\ 0 & 1 + 2^{\nu_2(e)+1} \end{pmatrix} \in A(2^{\nu_2(e)+2}).$$

Observe that $\alpha \in \ker \varphi_{2^{\nu_2(e)+1}}$ and since $R_{2^{\nu_2(e)+2}} = \langle \zeta_{2^{\nu_2(e)+3}} (a_0^{e_1})^{1/4}, \zeta_{2^{\nu_2(e)+2}} \rangle$, we have

$$(3.1) \quad \tau_2(\zeta_{2^{\nu_2(e)+3}} (a_0^{e_1})^{1/4}) = \zeta_{2^{\nu_2(e)+3}} (a_0^{e_1})^{1/4}.$$

Raising both sides of (3.1) to power 2 and observing that $\zeta_{2^{\nu_2(e)+2}}$ and $(a_0^{e_1})^{1/2} \in R_{2^{\nu_2(e)+2}}$, we get

$$(3.2) \quad \tau_2(\zeta_{2^{\nu_2(e)+2}})\tau_2((a_0^{e_1})^{1/2}) = \zeta_{2^{\nu_2(e)+2}}(a_0^{e_1})^{1/2}.$$

Now since $\tau_2(\zeta_{2^{\nu_2(e)+2}}) = \zeta_{2^{\nu_2(e)+2}}^{1+2^{\nu_2(e)+1}}$, the equation (3.2) implies that

$$\tau_2(a_0^{e_1/2}) = -a_0^{e_1/2}.$$

We have $e_1 = 2m + 1$ for some integer m . Hence,

$$\tau_2(a_0^{1/2}a_0^m) = -a_0^{1/2}a_0^m.$$

Thus for $\alpha \in \ker \varphi_{2^{\nu_2(e)+1}}$, we have $\psi_{K,2}(\alpha) = -1$. Hence, $\psi_{K,2}$ is non-trivial on $\ker \varphi_{2^{\nu_2(e)+1}}$.

Next, let $\alpha \in A_2$ be such that $\alpha \in \ker \varphi_{2^{\nu_2(e)+2}}$. Hence,

$$\tau_3 = \varphi_{2^{\nu_2(e)+3}}(\alpha) = \begin{pmatrix} 1 & 0 \\ b & d \end{pmatrix} \in A(2^{\nu_2(e)+3})$$

and

$$(3.3) \quad \begin{pmatrix} 1 & 0 \\ b & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{2^{\nu_2(e)+2}}.$$

Hence, $b = 2^{\nu_2(e)+2}b_1$ for some integer b_1 . We have

$$\tau_3(\zeta_{2^{\nu_2(e)+4}}(a_0^{e_1})^{1/8}) = \zeta_{2^{\nu_2(e)+4}}(a_0^{e_1})^{1/8} \zeta_{2^{\nu_2(e)+3}}^{2^{\nu_2(e)+2}b_1}.$$

Squaring both sides of this identity yields

$$\tau_3(\zeta_{2^{\nu_2(e)+3}})\tau_3((a_0^{e_1})^{1/4}) = \zeta_{2^{\nu_2(e)+3}}(a_0^{e_1})^{1/4}.$$

This implies

$$(3.4) \quad \tau_3((a_0^{e_1})^{1/4}) = \frac{\zeta_{2^{\nu_2(e)+3}}}{\zeta_{2^{\nu_2(e)+3}}^d}(a_0^{e_1})^{1/4}.$$

Now observe, from (3.3), that

$$(3.5) \quad d = 1 + 2^{\nu_2(e)+2}d_1$$

for some integer d_1 . Raising both sides of (3.4) to power 2 and employing (3.5) yield

$$\tau_3((a_0^{e_1})^{1/2}) = (a_0^{e_1})^{1/2}.$$

Hence,

$$\tau_3(a_0^{1/2}a_0^m) = a_0^{1/2}a_0^m,$$

where $e_1 = 2m + 1$. Thus, $\psi_{K,2}$ is trivial on $\ker \varphi_{2^{\nu_2(e)+2}}$. □

The following proposition is essential in proving Theorem 1.2.

Proposition 3.3. *Let $\ell(p)$ be the smallest integer k for which χ_p factors via $A(p^k)$. Then*

$$\ell(p) = \begin{cases} 0 & \text{if } p \text{ is odd and } p \nmid D, \\ 1 & \text{if } p \text{ is odd and } p \mid D, \\ s & \text{if } p = 2 \text{ and } D \text{ is odd,} \\ \max\{2, s\} & \text{if } p = 2 \text{ and } 4 \parallel D, \\ 2 & \text{if } p = 2, 8 \parallel D, \text{ and } (\nu_2(e) = 1 \text{ and } a < 0), \\ \max\{3, s\} & \text{if } p = 2, 8 \parallel D, \text{ and } (\nu_2(e) \neq 1 \text{ or } a > 0). \end{cases}$$

Proof. If $p \nmid 2D$, by the definition of χ_p , we have that χ_p is constantly equal to 1. Thus, the assertion holds.

If p is an odd integer dividing D , then χ_p is the Legendre symbol mod p , so the result follows.

If $p = 2$ and D is odd, then $\chi_2 = \psi_{K,2}$. Thus, the result follows from Proposition 3.2.

If $p = 2$ and $4 \parallel D$, then $\chi_2 = \psi_{K,2}\chi_{D,2}$, where $\chi_{D,2}$ is the Dirichlet character mod 8 of conductor 4. We are looking for a positive integer k such that $\psi_{K,2}(\alpha) \neq \chi_{D,2}(\alpha)$ for an element $\alpha \in \ker \varphi_{2^{k-1}}$, and $\psi_{K,2}(\alpha) = \chi_{D,2}(\alpha)$ for all $\alpha \in \ker \varphi_{2^k}$. Note that 2 is the smallest values of k for which $\chi_{D,2}$ factors via $A(2^k)$, and, by Proposition 3.2, s is the smallest value of k for which $\psi_{K,2}$ factors via $A(2^k)$. Thus, $\chi_{D,2}$ is trivial on $\ker \varphi_{2^k}$ for $k \geq 2$ and is nontrivial on $\ker \varphi_{2^k}$ for $0 \leq k \leq 1$. Also, $\psi_{K,2}$ is trivial on $\ker \varphi_{2^k}$ for $k \geq s$ and is nontrivial on $\ker \varphi_{2^k}$ for $0 \leq k \leq s$. Using these facts and a case-by-case analysis in terms of the values of $\nu_2(e)$, and for the untwisted and twisted cases, we can see that the claimed assertion, in this case, holds. More precisely, if $\nu_2(e) = 0$, then χ_2 factors via $A(2^2)$. Otherwise, χ_2 factors via $A(2^s)$. The only case that needs special attention is when a is an exact perfect square (i.e., $a > 0$ and $\nu_2(e) = 1$). In this case, $\max\{2, s\} = 2$ and both $\psi_{K,2}$ and $\chi_{D,2}$ are trivial on $\ker \varphi_{2^2}$, hence χ_2 is trivial on $\ker \varphi_{2^2}$. Let $\alpha \in \ker \varphi_2$ be such that $\varphi_{2^2}(\alpha) = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix} \in A(2^2)$. Note that $0 + 1 \equiv 3 \pmod{2}$, so by Proposition 3.1(iii) such α exists. We have $\chi_2(\alpha) = \psi_{K,2}(\alpha)\chi_{D,2}(\alpha) = (1)(-1) = -1$. Thus, χ_2 is non-trivial on $\ker \varphi_2$. Hence, χ_2 factors via $A(2^2) = A(2^s) = A(2^{\max\{2,s\}})$.

If $p = 2$ and $8 \parallel D$, similar to part (iv), a case-by-case analysis in terms of the values of $\nu_2(e)$, and for the untwisted and twisted cases, verifies the result. (Note that in this case 3 is the smallest values of k for which $\chi_{D,2}$ factors via $A(2^k)$.) More precisely, if $\nu_2(e) = 0$ or 1, and a is not negative of a perfect square, then χ_2 factors via $A(2^3)$. Also, if $\nu_2(e) = 1$ and $a < 0$, then χ_2 factors via $A(2^2)$. Otherwise, χ_2 factors via $A(2^s)$. Two cases need special attention.

Case 1: The number a is negative of an exact perfect square (i.e., $a < 0$ and $\nu_2(e) = 1$). In this case, $\max\{3, s\} = 3$ and both $\psi_{K,2}$ and $\chi_{D,2}$ are trivial on $\ker \varphi_{2^3}$, hence χ_2 is trivial on $\ker \varphi_{2^3}$. Thus, χ_2 acts through $A(2^3)$. Let $\alpha \in \ker \varphi_{2^2}$. Then $\varphi_{2^3}(\alpha) = \begin{pmatrix} 1 & 0 \\ b & d \end{pmatrix} \in A(2^3)$ such that $\begin{pmatrix} 1 & 0 \\ b & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{2^2}$. Hence,

$$\begin{pmatrix} 1 & 0 \\ b & d \end{pmatrix} \in \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 4 & 5 \end{pmatrix} \right\} \subset A(2^3).$$

Since for each α corresponding to the above matrices we have $\chi_2(\alpha) = \psi_{K,2}(\alpha)\chi_{D,2}(\alpha) = 1$, we conclude that χ_2 is trivial on $\ker \varphi_{2^2}$. Now let $\alpha \in \ker \varphi_2$ be such that $\varphi_{2^2}(\alpha) = \begin{pmatrix} 1 & 0 \\ 6 & 1 \end{pmatrix} \in A(2^2)$. Note that $(2)(6) + 1 \equiv 1 \pmod{2^2}$, so by Proposition 3.1(ii) such α exists. We have $\chi_2(\alpha) = \psi_{K,2}(\alpha)\chi_{D,2}(\alpha) = (-1)(1) = -1$. Thus, χ_2 is non-trivial on $\ker \varphi_2$. Hence, χ_2 factors via $A(2^2)$ as claimed.

Case 2: The number a is an exact perfect fourth power (i.e., $a > 0$ and $\nu_2(e) = 2$). In this case, $\max\{3, s\} = 3$ and both $\psi_{K,2}$ and $\chi_{D,2}$ are trivial on $\ker \varphi_{2^3}$, hence χ_D is trivial on $\ker \varphi_{2^3}$. Let $\alpha \in \ker \varphi_{2^2}$ be such that $\varphi_{2^3}(\alpha) = \begin{pmatrix} 1 & 0 \\ 0 & 9 \end{pmatrix} \in A(2^3)$. Note that $0 + 1 \equiv 9 \pmod{2^2}$, so by Proposition 3.1(iii) such α exists. We have $\chi_2(\alpha) = \psi_{K,2}(\alpha)\chi_{D,2}(\alpha) = (1)(-1) = -1$. Thus, χ_2 is non-trivial on $\ker \varphi_{2^2}$. Hence, χ_2 factors via $A(2^3) = A(2^s) = A(2^{\max\{3,s\}})$. \square

4. PROOF OF THEOREM 1.6

Proof of Theorem 1.6. Let ν_G be the normalized Haar measure on the profinite group G , and ν_A be the normalized Haar measure on the profinite group A . We start by writing the summation

$$\sum_{n \geq 1} \frac{g(n)}{\#G(n)}$$

in terms of measures of certain measurable subgroups of G . For this purpose, let $\pi_{G,n} : G \rightarrow G(n)$ be the projection map for each $n \geq 1$. Then, $G/\ker \pi_{G,n} \cong G(n)$ and $[G : \ker \pi_{G,n}] = \#G(n)$. Hence, since $\ker \pi_{G,n}$ is a closed subgroup of G , we have $\nu_G(\ker \pi_{G,n}) = 1/\#G(n)$. Thus,

$$(4.1) \quad \sum_{n \geq 1} \frac{g(n)}{\#G(n)} = \sum_{n \geq 1} g(n) \nu_G(\ker \pi_{G,n}).$$

Observe that the number of cosets of the set $A/r(\ker \pi_{G,n})$ divided by the number of cosets of the group $G/\ker \pi_{G,n} \cong r(G)/r(\ker \pi_{G,n})$ is equal to $\#(A/r(G))$. Hence, we have

$$(4.2) \quad \nu_G(\ker \pi_{G,n}) = \frac{\nu_A(r(\ker \pi_{G,n}))}{\nu_A(r(G))}.$$

Now, since

$$(4.3) \quad 1 \rightarrow G \xrightarrow{r} A \xrightarrow{\chi} \mu_m \rightarrow 1$$

is an exact sequence, by (4.2), we have

$$(4.4) \quad \begin{aligned} \sum_{n \geq 1} g(n) \nu_G(\ker \pi_{G,n}) &= \sum_{n \geq 1} g(n) \frac{\nu_A(r(\ker \pi_{G,n}))}{\nu_A(\ker \chi)} \\ &= \frac{1}{\nu_A(\ker \chi)} \sum_{n \geq 1} g(n) \nu_A(r(\ker \pi_{G,n})). \end{aligned}$$

Next, we show that $r(\ker \pi_{G,n}) = \ker(\pi_{A,n}) \cap \ker \chi$, where $\pi_{A,n} : A \rightarrow A(n)$ is the projection map for each $n \geq 1$. To prove this claim, we note that the diagram

$$(4.5) \quad \begin{array}{ccc} G & \xrightarrow{\pi_{G,n}} & G(n) \\ \downarrow r & & \downarrow r_n \\ A & \xrightarrow{\pi_{A,n}} & A(n) \end{array}$$

commutes. For a group H , let e_H denote its identity element. Note that if $\sigma \in \ker \pi_{G,n}$, then $r_n(\pi_{G,n}(\sigma)) = r_n(e_{G(n)}) = e_{A(n)}$. Hence, by the commutative diagram (4.5), we have $r(\sigma) \in \ker(\pi_{A,n})$. Moreover, by the exact sequence (4.3), we have $r(\sigma) \in r(G) = \ker \chi$. Therefore,

$$(4.6) \quad r(\ker \pi_{G,n}) \subset \ker(\pi_{A,n}) \cap \ker \chi.$$

On the other hand, if $\alpha \in \ker(\pi_{A,n}) \cap \ker \chi \subset \ker \chi = r(G)$, then there exists a $\sigma \in G$ such that $r(\sigma) = \alpha$. Moreover, $r(\sigma) \in \ker(\pi_{A,n})$ means $\pi_{A,n}(r(\sigma)) = e_{A(n)}$. Hence, $r_n(\pi_{G,n}(\sigma)) = e_{A(n)}$ as (4.5) is commutative. Thus, $\sigma \in \ker \pi_{G,n}$, since r_n is injective. This shows that

$$(4.7) \quad \ker(\pi_{A,n}) \cap \ker \chi \subset r(\ker \pi_{G,n}).$$

Therefore, from (4.6) and (4.7), we have

$$(4.8) \quad r(\ker \pi_{G,n}) = \ker(\pi_{A,n}) \cap \ker \chi.$$

From (4.8), we have

$$(4.9) \quad \begin{aligned} \sum_{n \geq 1} g(n) \nu_A(r(\ker \pi_{G,n})) &= \sum_{n \geq 1} g(n) \nu_A(\ker \pi_{A,n} \cap \ker \chi) \\ &= \sum_{n \geq 1} g(n) \int_A 1_{\ker \pi_{A,n} \cap \ker \chi} d\nu_A \\ &= \int_A \left(\sum_{n \geq 1} g(n) 1_{\ker \pi_{A,n}} \right) 1_{\ker \chi} d\nu_A. \end{aligned}$$

To justify the interchange of the summation and the integral in the last equality, observe that

$$\left| \sum_{n=1}^m g(n) 1_{\ker \pi_{A,n} \cap \ker \chi} \right| \leq \sum_{n \geq 1} |g(n)| 1_{\ker \pi_{A,n} \cap \ker \chi}.$$

Since by the assumption, $\sum_{n \geq 1} |g(n)| / \#G(n)$ converges, then, by [17, Theorem 1.27], $\sum_{n \geq 1} |g(n)| 1_{\ker \pi_{A,n} \cap \ker \chi}$ is integrable. Thus, by Lebesgue's dominated convergence theorem (see [17, Theorem 1.34]), the interchange of the summation and the integral in (4.9) is justified. Also, since $\#A(n) \geq \#G(n)$, then $\sum_{n \geq 1} |g(n)| / \#A(n) < \infty$. Hence, by [17, Theorem 1.38],

$$\tilde{g} = \sum_{n \geq 1} g(n) 1_{\ker \pi_{A,n}} \in L^1(\nu_A).$$

Now from (4.1), (4.4), and (4.9), we have

$$(4.10) \quad \sum_{n \geq 1} \frac{g(n)}{\#G(n)} = \frac{\int_A \tilde{g} 1_{\ker \chi} d\nu_A}{\int_A 1_{\ker \chi} d\nu_A}.$$

Note that the character $\chi : A \rightarrow \mu_m$ in (4.3) induces the character $\chi' : A/r(G) \xrightarrow{\sim} \mu_m$ by $\chi'(\bar{\alpha}) = \chi(\alpha)$, where $\alpha \in A$ and $\bar{\alpha}$ is the coset associated to α in $A/r(G)$. More precisely, χ is the lift of χ' to A . Since χ' sends a generator of $A/r(G)$ to a generator of μ_m , then χ' is a generator of the group of characters of $A/r(G)$ denoted by $\widehat{A/r(G)}$. Thus, for $\bar{\alpha} \in A/r(G)$, by [18, Chapter VI, Proposition 4], we have

$$\sum_{\bar{\alpha} \in \widehat{A/r(G)}} \epsilon(\bar{\alpha}) = \sum_{i=0}^{m-1} (\chi')^i(\bar{\alpha}) = \begin{cases} m & \text{if } \bar{\alpha} = 1, \\ 0 & \text{if } \bar{\alpha} \neq 1. \end{cases}$$

Therefore, since $\bar{\alpha} = 1$ means $\alpha \in \ker \chi$, we have

$$\sum_{i=0}^{m-1} \chi^i(\alpha) = \begin{cases} m & \text{if } \alpha \in \ker \chi, \\ 0 & \text{if } \alpha \notin \ker \chi. \end{cases}$$

This implies $\sum_{i=0}^{m-1} \chi^i(\alpha) = m \cdot 1_{\ker \chi}(\alpha)$. Thus,

$$(4.11) \quad \frac{\int_A \tilde{g} 1_{\ker \chi} d\nu_A}{\int_A 1_{\ker \chi} d\nu_A} = \frac{\int_A \tilde{g} \sum_{i=0}^{m-1} \chi^i d\nu_A}{m \int_A 1_{\ker \chi} d\nu_A}.$$

Furthermore, by (4.3), we have $[A : \ker \chi] = [A : r(G)] = m$. Hence, $\nu_A(\ker \chi) = 1/m$. Thus, the desired result follows from (4.10) and (4.11). \square

The following corollary considers a special case of Theorem 1.6.

Corollary 4.1. *In Theorem 1.6, suppose that g is a multiplicative arithmetic function. In addition, assume that $A \cong \prod_p A_p$, where $A_p = \varprojlim A(p^i)$, and $\chi = \prod_p \chi_p$, where $\chi_p : A_p \rightarrow \mu_m$ is a character of A_p . Then*

$$(4.12) \quad \tilde{g}_p = \sum_{k \geq 0} g(p^k) 1_{\ker \varphi_{p^k}} \in L^1(\nu_{A_p}).$$

Moreover,

$$(4.13) \quad \sum_{n \geq 1} \frac{g(n)}{\#G(n)} = \sum_{i=0}^{m-1} \prod_p \int_{A_p} \tilde{g}_p \chi_p^i d\nu_{A_p},$$

where ν_{A_p} is the normalized Haar measure on A_p .

Proof. By Theorem 1.6, we have

$$(4.14) \quad \sum_{n \geq 1} \frac{g(n)}{\#G(n)} = \sum_{i=0}^{m-1} \int_A \tilde{g} \chi^i d\nu_A.$$

Since $g(n)$ is multiplicative, $A \cong \prod_p A_p$, $\nu_A = \prod_p \nu_{A_p}$, $\chi = \prod_p \chi_p$, and $\tilde{g} = \prod_p \tilde{g}_p$, then (4.14) yields (4.13). Note that, since $\#A(p^k) \geq \#G(p^k)$, then $\sum_{k \geq 0} |g(n)| / \#A(p^k) < \infty$. Hence, by [17, Theorem 1.38], $\tilde{g}_p \in L^1(\nu_{A_p})$. Thus, the integrals in (4.13) are finite. \square

5. PROOF OF THEOREM 1.2

Proof of Theorem 1.2. We employ Corollary 4.1 and compute $\int_{A_p} \tilde{g}_p d\nu_{A_p}$ and $\int_{A_p} \tilde{g}_p \chi_p d\nu_{A_p}$ for primes p . Since $\ker \varphi_{p^k}$ is a closed subgroup of A_p , we have $\nu_{A_p}(\ker \varphi_{p^k}) = 1/[A_p : \ker \varphi_{p^k}] = 1/\#A(p^k)$. Observe that

$$(5.1) \quad \begin{aligned} \int_{A_p} \tilde{g}_p d\nu_{A_p} &= \int_{A_p} \sum_{k \geq 0} g(p^k) 1_{\ker \varphi_{p^k}} d\nu_{A_p} \\ &= \sum_{k \geq 0} g(p^k) \nu_{A_p}(\ker \varphi_{p^k}) \\ &= \sum_{k \geq 0} \frac{g(p^k)}{\#A(p^k)}. \end{aligned}$$

In addition, by Proposition 3.3,

$$(5.2) \quad \begin{aligned} \int_{A_p} \tilde{g}_p \chi_p d\nu_{A_p} &= \int_{A_p} \left(1_{A_p} \chi_p + g(p) 1_{\ker \varphi_p} \chi_p + \cdots + g(p^k) 1_{\ker \varphi_{p^k}} \chi_p + \cdots \right) d\nu_{A_p} \\ &= 0 + \sum_{k \geq \ell(p)} g(p^k) \nu_{A_p}(\ker \varphi_{p^k}) \\ &= \sum_{k \geq \ell(p)} \frac{g(p^k)}{\#A(p^k)}. \end{aligned}$$

Thus, by Corollary 4.1 with $m = 2$, (5.1), and (5.2), we get (1.8). \square

6. PROOF OF PROPOSITION 1.4

Proof of Proposition 1.4. For integer $k \geq 1$ and odd prime p , let

$$(6.1) \quad k' = \begin{cases} 0 & \text{if } k \leq \nu_p(e), \\ k - \nu_p(e) & \text{if } k > \nu_p(e), \end{cases}$$

and for $k \geq 1$ and $p = 2$, let

$$(6.2) \quad k' = \begin{cases} 0 & \text{if } k \leq \nu_2(e) \text{ and } (a > 0 \text{ or } e \text{ is odd}), \\ 1 & \text{if } k \leq \nu_2(e) \text{ and } (a < 0 \text{ and } e \text{ is even}), \\ k - \nu_2(e) & \text{if } k > \nu_2(e). \end{cases}$$

Then, from Proposition 3.1 (i), we have

$$(6.3) \quad \#A(p^k) = \begin{cases} p^{k+k'-1}(p-1) & \text{if } k \geq 1, \\ 1 & \text{if } k = 0. \end{cases}$$

Now by employing (6.3) in (1.8) we get

$$(6.4) \quad \sum_{n=1}^{\infty} \frac{g(n)}{\#G(n)} = \prod_p \sum_{k \geq 0} \frac{g(p^k)}{p^{k+k'-1}(p-1)} + \prod_p \sum_{k \geq \ell(p)} \frac{g(p^k)}{p^{k+k'-1}(p-1)}.$$

We set $g = 1$ in (6.4) to get the product expression for the constant in the conjectured asymptotic formula in the Titchmarsh Divisor Problem for a given Kummer family. Therefore, by (6.4),

$$(6.5) \quad \sum_{n \geq 1} \frac{1}{[K_n : \mathbb{Q}]} = \left(1 + \prod_{p|2D} \frac{C_p}{1 + B_p} \right) \prod_p (1 + B_p),$$

for the following values for B_p and C_p .

If p is odd, we have

$$(6.6) \quad B_p = \sum_{k \geq 1} \frac{1}{p^{k+k'-1}(p-1)} = \frac{p^{\nu_p(e)+2} + p^{\nu_p(e)+1} - p^2}{p^{\nu_p(e)}(p-1)(p^2-1)},$$

and $C_p = B_p$, where k' is given by (6.1).

For $p = 2$, we have the following cases for B_2 and C_2 with k' as given by (6.2).

Case (i). Let e be odd or $a > 0$. Hence, $s = \nu_2(e) + 1$. Then B_2 is the same as (6.6) with $p = 2$. Now, if D is odd; or $4 \parallel D$ and $s \geq 2$; or $8 \parallel D$ and $s \geq 3$, then

$$C_2 = \sum_{k \geq \ell(2)} \frac{1}{2^{k+k'-1}} = \frac{2}{2^{\nu_2(e)}(2^2-1)}.$$

Otherwise,

$$C_2 = \sum_{k \geq \ell(2)} \frac{1}{2^{k+k'-1}} = \frac{2^{\nu_2(e)+1}}{2^\beta(2^2-1)},$$

where $\beta = 2$ if $4 \parallel D$ and $s = 1$; and $\beta = 4$ if $8 \parallel D$ and $s \in \{1, 2\}$.

Case (ii). Let e be even and $a < 0$. Then

$$B_2 = \sum_{k \geq 1} \frac{1}{2^{k+k'-1}} = \frac{2^{\nu_2(e)+2} - 2^{\nu_2(e)} - 1}{2^{\nu_2(e)}(2^2-1)}.$$

If $8 \parallel D$ and $\nu_2(e) = 1$, we have $\ell(2) = 2$. Hence,

$$C_2 = \sum_{k \geq \ell(2)} \frac{1}{2^{k+k'-1}} = \frac{1}{2^2-1}.$$

Otherwise, we have $\ell(2) = s = \nu_2(e) + 2$ and thus

$$C_2 = \sum_{k \geq \ell(2)} \frac{1}{2^{k+k'-1}} = \frac{1}{2^{\nu_2(e)+1}(2^2-1)}.$$

By applying the above expressions in (6.5) and by case-by-case simplifying, we get (1.11). \square

7. SERRE CURVES

Let E be an elliptic curve defined over \mathbb{Q} given by a Weierstrass equation

$$y^2 = x^3 + ax + b,$$

where $a, b \in \mathbb{Q}$. Let $\mathbb{Q}(E[n])$ be the n -division field of E . By taking the inverse limit of the natural injective maps

$$r_n : \text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \rightarrow \text{Aut}(E[n]) \cong \text{GL}_2(\mathbb{Z}/n\mathbb{Z}),$$

over all $n \geq 1$, we have an injective profinite homomorphism

$$r : \text{Gal}(\mathbb{Q}(E[\infty])/\mathbb{Q}) \rightarrow \text{Aut}(E[\infty]) \cong \text{GL}_2(\widehat{\mathbb{Z}}).$$

Let Δ be the discriminant of the cubic equation $x^3 + ax + b = 0$. Set $K = \mathbb{Q}(\Delta^{1/2})$ and let D be the discriminant of K . In anticipation of applying Theorem 1.6, let \det be the determinant map $\det : \text{GL}_2(\widehat{\mathbb{Z}}) \rightarrow \widehat{\mathbb{Z}}^\times$ and

$$\chi_D : \text{GL}_2(\widehat{\mathbb{Z}}) \xrightarrow{\det} \widehat{\mathbb{Z}}^\times \xrightarrow{\left(\frac{D}{\cdot}\right)} \mu_2$$

be the composition of \det with the lift to $\widehat{\mathbb{Z}}^\times$ of the Kronecker symbol attached to D . We note that $\text{GL}_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3$, where S_3 is the symmetric group on three letters. Let

$$\psi : \text{GL}_2(\widehat{\mathbb{Z}}) \rightarrow \text{GL}_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3 \xrightarrow{\text{sign}} \mu_2$$

be the composition of the projection map from $\text{GL}_2(\widehat{\mathbb{Z}})$ to $\text{GL}_2(\mathbb{Z}/2\mathbb{Z})$ with the signature character on S_3 . Let $G = \text{Gal}(\mathbb{Q}(E[\infty])/\mathbb{Q})$. For $\eta \in G$ we can show that the image of $r(\eta)$ under ψ is the same as $\chi_D(r(\eta)) = \eta(\Delta^{1/2})/\Delta^{1/2}$. We now set $\chi = \chi_D \cdot \psi$.

The above construction of character χ is described by J.-P. Serre in [19]. In addition, in [19], Serre shows that always $[\text{GL}_2(\widehat{\mathbb{Z}}) : r(G)] \geq 2$. We name E a *Serre curve* if $[\text{GL}_2(\widehat{\mathbb{Z}}) : r(G)] = 2$. This is equivalent to saying that $r(G) = \ker \chi$. Thus, letting $A = \text{GL}_2(\widehat{\mathbb{Z}})$, for Serre curve E , the sequence

$$(7.1) \quad 1 \longrightarrow G \xrightarrow{r} A \xrightarrow{\chi} \mu_2 \longrightarrow 1$$

is an exact sequence. In addition for a Serre curve $K = \mathbb{Q}(\Delta^{1/2})$ is a quadratic field.

The quadratic character $\chi : \text{GL}_2(\widehat{\mathbb{Z}}) (\cong \prod_p \text{GL}_2(\mathbb{Z}_p)) \rightarrow \mu_2$ can be written as a product of local characters $\chi_p : \text{GL}_2(\mathbb{Z}_p) \rightarrow \mu_2$. Observe that since ψ factors via $\text{GL}_2(\mathbb{Z}/2\mathbb{Z})$, then it factors via $\text{GL}_2(\mathbb{Z}_2)$. Let $\psi_2 : \text{GL}_2(\mathbb{Z}_2) \rightarrow \mu_2$ be the corresponding homomorphism obtained from factorization of ψ via $\text{GL}_2(\mathbb{Z}_2)$. For prime $p \nmid 2D$, let χ_p be constantly equal to 1. For odd prime $p \mid D$, let $\chi_p = \chi_{D,p}$ be the lift of the Legendre symbol mod p to \mathbb{Z}_p^\times , i.e.,

$$\chi_p : \text{GL}_2(\mathbb{Z}_p^\times) \xrightarrow{\det} \mathbb{Z}_p^\times \longrightarrow \mu_2$$

where the last map is the composition of projection map to $\mathbb{Z}/p\mathbb{Z}$ and the Legendre symbol mod p . For prime 2, let $\chi_2 = \chi_{D,2} \cdot \psi_2$, where $\chi_{D,2}$, similar to the Kummer case, is the lift of one of the Dirichlet characters mod 8 to \mathbb{Z}_2^\times (if D is odd, then $\chi_{D,2}$ is trivial). Therefore, by the above construction of χ , we have the decomposition $\chi = \prod_p \chi_p$.

Let $A_p = \text{GL}_2(\mathbb{Z}_p)$ and $A(p^k) = \text{GL}_2(\mathbb{Z}/p^k\mathbb{Z})$. The following is an analogous of Proposition 3.3 for Serre curves.

Proposition 7.1. *For a Serre curve E , assume the above notations. Let $\ell(p)$ be the smallest integer k for which χ_p factors via $A(p^k)$. Then*

$$\ell(p) = \begin{cases} 0 & \text{if } p \text{ is odd and } p \nmid D, \\ 1 & \text{if } p \text{ is odd and } p \mid D, \\ 1 & \text{if } p = 2 \text{ and } D \text{ is odd,} \\ 2 & \text{if } p = 2 \text{ and } 4 \parallel D, \\ 3 & \text{if } p = 2 \text{ and } 8 \parallel D. \end{cases}$$

Proof. If $p \nmid 2D$, then χ_p is constantly equal to 1. Hence, it factors via $A(1)$. If p is odd and $p \mid D$, then χ_p is the Legendre symbol mod p , and so it factors via $A(p)$, and since it is non-trivial, it does not factor via $A(1)$. The result for $p = 2$ follows from the construction of χ_2 described above, noting that the smallest integer k for which ψ_2 factors via $A(p^k)$ is $k = 1$, for $4 \parallel D$ the smallest such k is $k = 2$, and for $8 \parallel D$ the smallest such k is $k = 3$. \square

We are now ready to prove our last remaining assertion.

Proof of Proposition 1.7. Following steps similar to the proof of Theorem 1.2 and by employing Corollary 4.1 with $m = 2$, Proposition 7.1, and

$$|\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})| = \prod_{p^e \parallel n} p^{4e-3}(p^2 - 1)(p - 1)$$

(see [10, page 231]) we have the stated product expression. \square

Acknowledgements. The authors thank the reviewers for their valuable comments and suggestions. The authors thank David Basil and Solaleh Bolvardizadeh for help computing the explicit constants c_a given in the table after Proposition 1.4.

REFERENCES

- [1] Amir Akbary and Dragos Ghioca, *A geometric variant of Titchmarsh divisor problem*, Int. J. Number Theory **8** (2012), no. 1, 53–69, DOI 10.1142/S1793042112500030. MR2887882
- [2] Amir Akbary and Adam Tyler Felix, *On the average value of a function of the residual index*, Springer Proc. Math. Stat. **251** (2018), 19–37. MR3880381
- [3] Emil Artin, *The collected papers of Emil Artin*, Addison-Wesley Publishing Co., Inc., Reading, Mass.-London, 1965. Edited by Serge Lang and John T. Tate. MR0176888
- [4] Eric Bach, Richard Lukes, Jeffrey Shallit, and H. C. Williams, *Results and estimates on pseudopowers*, Math. Comp. **65** (1996), no. 216, 1737–1747. MR1355005
- [5] Renee Bell, Clifford Blakestad, Alina Carmen Cojocaru, Alexander Cowan, Nathan Jones, Vlad Matei, Geoffrey Smith, and Isabel Vogt, *Constants in Titchmarsh divisor problems for elliptic curves*, Res. Number Theory **6** (2020), no. 1, Paper No. 1, 24, DOI 10.1007/s40993-019-0175-9. MR4041152
- [6] David A. Cox, *Primes of the form $x^2 + ny^2$* , 2nd ed., Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc., Hoboken, NJ, 2013. Fermat, class field theory, and complex multiplication. MR3236783
- [7] Harold Davenport, *Multiplicative number theory*, 3rd ed., Graduate Texts in Mathematics, vol. 74, Springer-Verlag, New York, 2000. Revised and with a preface by Hugh L. Montgomery. MR1790423
- [8] Adam Tyler Felix and M. Ram Murty, *A problem of Fomenko’s related to Artin’s conjecture*, Int. J. Number Theory **8** (2012), no. 7, 1687–1723, DOI 10.1142/S1793042112500984. MR2968946
- [9] Christopher Hooley, *On Artin’s conjecture*, J. Reine Angew. Math. **225** (1967), 209–220, DOI 10.1515/crll.1967.225.209. MR207630
- [10] Neal Koblitz, *Introduction to elliptic curves and modular forms*, 2nd ed., Graduate Texts in Mathematics, vol. 97, Springer-Verlag, New York, 1993. MR1216136
- [11] E. Kowalski, *Analytic problems for elliptic curves*, J. Ramanujan Math. Soc. **21** (2006), no. 1, 19–114. MR2226355
- [12] Serge Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. MR1878556
- [13] R. R. Laxton, *On groups of linear recurrences. I*, Duke Math. J. **36** (1969), 721–736. MR0258781
- [14] H. W. Lenstra Jr., P. Moree, and P. Stevenhagen, *Character sums for primitive root densities*, Math. Proc. Cambridge Philos. Soc. **157** (2014), no. 3, 489–511, DOI 10.1017/S0305004114000450. MR3286520
- [15] P. Moree and P. Stevenhagen, *Computing higher rank primitive root densities*, Acta Arith. **163** (2014), no. 1, 15–32, DOI 10.4064/aa163-1-2. MR3194054
- [16] F. Pappalardi, *On Hooley’s theorem with weights*, Rend. Sem. Mat. Univ. Politec. Torino **53** (1995), no. 4, 375–388. Number theory, II (Rome, 1995). MR1452393
- [17] Walter Rudin, *Real and complex analysis*, 3rd ed., McGraw-Hill Book Co., New York, 1987. MR924157
- [18] J.-P. Serre, *A course in arithmetic*, Graduate Texts in Mathematics, No. 7, Springer-Verlag, New York-Heidelberg, 1973. Translated from the French. MR0344216
- [19] Jean-Pierre Serre, *Propriétés galoisiennes des points d’ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331, DOI 10.1007/BF01405086 (French). MR387283
- [20] Samuel S. Wagstaff Jr., *Pseudoprimes and a generalization of Artin’s conjecture*, Acta Arith. **41** (1982), no. 2, 141–150, DOI 10.4064/aa-41-2-141-150. MR674829

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, UNIVERSITY OF LETHBRIDGE, LETHBRIDGE,
ALBERTA T1K 3M4, CANADA

Email address: amir.akbary@uleth.ca

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, UNIVERSITY OF LETHBRIDGE, LETHBRIDGE,
ALBERTA T1K 3M4, CANADA

Email address: milad.fakhari@uleth.ca