On the index of appearance of a Lucas sequence

ON THE INDEX OF APPEARANCE OF A LUCAS SEQUENCE

CARLO SANNA†

Abstract. Let $\boldsymbol{u} = (u_n)_{n\geq 0}$ be a Lucas sequence, that is, a sequence of integers satisfying $u_0 = 0$, $u_1 = 1$, and $u_n = a_1 u_{n-1} + a_2 u_{n-2}$ for every integer $n \geq 2$, where a_1 and a_2 are fixed nonzero integers. For each prime number p with $p \nmid 2a_2 D_{\boldsymbol{u}}$, where $D_{\boldsymbol{u}} := a_1^2 + 4a_2$, let $\rho_{\boldsymbol{u}}(p)$ be the *rank of appearance* of p in $\boldsymbol{u}$, that is, the smallest positive integer k such that $p \mid u_k$. It is well known that $\rho_{\boldsymbol{u}}(p)$ exists and that $p \equiv \left(D_{\boldsymbol{u}} \mid p\right) \pmod{\rho_{\boldsymbol{u}}(p)}$, where $\left(D_{\boldsymbol{u}} \mid p\right)$ is the Legendre symbol. Define the *index of appearance* of p in $\boldsymbol{u}$ as $\iota_{\boldsymbol{u}}(p) := \left(p - \left(D_{\boldsymbol{u}} \mid p\right)\right)/\rho_{\boldsymbol{u}}(p)$. For each positive integer t and for every $x > 0$, let $\mathcal{P}_{\boldsymbol{u}}(t, x)$ be the set of prime numbers p such that $p \leq x$, $p \nmid 2a_2 D_{\boldsymbol{u}}$, and $\iota_{\boldsymbol{u}}(p) = t$.

Under the Generalized Riemann Hypothesis, and under some mild assumptions on $\boldsymbol{u}$, we prove that

$$\#\mathcal{P}_{\boldsymbol{u}}(t, x) = A\, F_{\boldsymbol{u}}(t)\, G_{\boldsymbol{u}}(t)\, \frac{x}{\log x} + O_{\boldsymbol{u}}\left(\frac{x}{(\log x)^2} + \frac{x \log\log(3x)}{\varphi(t)(\log x)^2}\right),$$

for all positive integers t and for all $x > t^3$, where A is the Artin constant, $F_{\boldsymbol{u}}(\cdot)$ is a multiplicative function, and $G_{\boldsymbol{u}}(\cdot)$ is a periodic function (both these functions are effectively computable in terms of $\boldsymbol{u}$). Furthermore, we provide some explicit examples and numerical data.

1. Introduction

Let $\boldsymbol{u} = (u_n)_{n\geq 0}$ be a Lucas sequence, that is, a sequence of integers satisfying $u_0 = 0$, $u_1 = 1$, and $u_n = a_1 u_{n-1} + a_2 u_{n-2}$ for every integer $n \geq 2$, where a_1 and a_2 are fixed nonzero integers. For each prime number p with $p \nmid a_2$, let $\rho_{\boldsymbol{u}}(p)$ be the *rank of appearance* of p in $\boldsymbol{u}$, that is, the smallest positive integer k such that $p \mid u_k$. It is well known that $\rho_{\boldsymbol{u}}(p)$ exists (for this and other elementary facts on $\rho_{\boldsymbol{u}}(p)$ mentioned in the introduction, see [14, Chapter 1]). Furthermore, we have that $p \equiv \left(D_{\boldsymbol{u}} \mid p\right) \pmod{\rho_{\boldsymbol{u}}(p)}$ for every prime number p with $p \nmid 2a_2 D_{\boldsymbol{u}}$, where $D_{\boldsymbol{u}} := a_1^2 + 4a_2$ and $\left(D_{\boldsymbol{u}} \mid p\right)$ is the Legendre symbol. We define the *index of appearance* of p in $\boldsymbol{u}$ as $\iota_{\boldsymbol{u}}(p) := \left(p - \left(D_{\boldsymbol{u}} \mid p\right)\right)/\rho_{\boldsymbol{u}}(p)$, which, by the previous consideration, is a positive integer. Moreover, for each positive integer t and for every $x > 0$, we define

$$\mathcal{P}_{\boldsymbol{u}}(t, x) := \left\{p \leq x : p \nmid 2a_2 D_{\boldsymbol{u}},\, \iota_{\boldsymbol{u}}(p) = t\right\}.$$

Note that $\rho_{\boldsymbol{u}}(p)$, respectively $\iota_{\boldsymbol{u}}(p)$, is somehow analogous to the multiplicative order $r_g(p)$ modulo p, respectively the residual index $i_g(p) := (p-1)/r_g(p)$ modulo p, of a rational number g, assuming that p does not divide the numerator and the denominator of g. (By Lemma 3.4, $\rho_{\boldsymbol{u}}(p)$ is indeed a multiplicative order. However, $\iota_{\boldsymbol{u}}(p)$ is not always a residual index.) In particular, the set $\mathcal{P}_{\boldsymbol{u}}(t, x)$ is analogous to the set of prime numbers p for which g is a *near-primitive root* modulo p, that is, $i_p(g) = t$ for a fixed t. This latter set has been studied by several authors [8, 9, 10, 11] (see also [17, 19] for generalizations to number fields). We also mention that the set of prime numbers p such that $d \mid \rho_{\boldsymbol{u}}(p)$, for some fixed positive integer d, has been studied by many authors [2, 3, 15].

As a first result, we provide a (conditional) asymptotic formula for $\#\mathcal{P}_{\boldsymbol{u}}(t, x)$. We remark that the proof is a close adaptation of Hooley's proof of the Artin's conjecture under the

2010 *Mathematics Subject Classification.* Primary: 11B39, Secondary: 11N05, 11N37.

Key words and phrases. asymptotic formula; Fibonacci numbers; index of appearance; Lucas sequence; prime numbers; rank of appearance.

† C. Sanna is a member of the INdAM group GNSAGA and of CrypTO, the group of Cryptography and Number Theory of the Politecnico di Torino.

Generalized Riemann Hypothesis (GRH) [5]. Recall that the Lucas sequence $\boldsymbol{u}$ is said to be *nondegenerate* if the ratio of the roots of the polynomial $X^2 - a_1X - a_2$ is not a root of unity.

Theorem 1.1. *Assume the GRH. Let $\boldsymbol{u} = (u_n)_{n\geq 0}$ be a nondegenerate Lucas sequence with nonsquare $D_{\boldsymbol{u}}$. Then, for every positive integer t, there exists $\delta_{\boldsymbol{u}}(t) \geq 0$ such that*

$$\#\mathcal{P}_{\boldsymbol{u}}(t,x) = \delta_{\boldsymbol{u}}(t)\,\frac{x}{\log x} + O_{\boldsymbol{u}}\left(\frac{x}{(\log x)^2} + \frac{x\log\log(3x)}{\varphi(t)(\log x)^2}\right),$$

for all $x > t^3$, where φ is the Euler totient function.

The proof of Theorem 1.1 yields an expression for $\delta_{\boldsymbol{u}}(t)$ in terms of an infinite series, which however is not very enlightening. Let

$$A := \prod_{p}\left(1 - \frac{1}{p(p-1)}\right) = 0.3739558136\ldots$$

be the *Artin constant*, and let

$$F_h(t) := \frac{(t,h)}{\varphi(t)t}\prod_{\substack{p>2\\ p\,|\,t}}\left(1 - \frac{(pt,h)}{p^2(t,h)}\right)\left(1 - \frac{(p,h)}{p(p-1)}\right)^{-1},$$

for all positive integers h and t. Note that $F_h(\cdot)$ is a multiplicative function. Our second result is a more explicit description of $\delta_{\boldsymbol{u}}(t)$.

Theorem 1.2. *Let $\boldsymbol{u} = (u_n)_{n\geq 0}$ be a nondegenerate Lucas sequence such that $D_{\boldsymbol{u}}$ is not a square and the discriminant of $\mathbb{Q}(\sqrt{D_{\boldsymbol{u}}})$ is not equal to -3 or to -4. Then there exist a positive integer h and a periodic function with rational values $G_{\boldsymbol{u}}(\cdot)$ such that $\delta_{\boldsymbol{u}}(t) = A\,F_{2h}(t)\,G_{\boldsymbol{u}}(t)$ for every positive integer t.*

The function $G_{\boldsymbol{u}}(\cdot)$ can be effectively computed in terms of $\boldsymbol{u}$. We provide the following examples (see Section 5 for more details).

Example 1.1. If $a_1 = a_2 = 1$, that is, if $\boldsymbol{u}$ is the sequence of Fibonacci numbers, then we have

$$G_{\boldsymbol{u}}(t) = \begin{cases} 3/4 & \text{if } t \equiv 0 \pmod{20};\\ 1 & \text{if } t \equiv 1 \pmod{2};\\ 29/38 & \text{if } t \equiv 2,6,14,18 \pmod{20};\\ 27/76 & \text{if } t \equiv 4,8,12,16 \pmod{20};\\ 1/2 & \text{if } t \equiv 10 \pmod{20}; \end{cases}$$

for all positive integers t.

Example 1.2. If $a_1 = 4$ and $a_2 = -1$, then we have

$$G_{\boldsymbol{u}}(t) = \begin{cases} 3/2 & \text{if } t \equiv 0,2,6,10,14,18,22 \pmod{24};\\ 0 & \text{if } t \equiv 1 \pmod{2};\\ 4/5 & \text{if } t \equiv 4,20 \pmod{24};\\ 3/5 & \text{if } t \equiv 8,16 \pmod{24};\\ 1/2 & \text{if } t \equiv 12 \pmod{24}; \end{cases}$$

for all positive integers t.

Example 1.3. If $a_1 = 10$ and $a_2 = 2$, then we have

$$G_{\boldsymbol{u}}(t) = \begin{cases} 9/10 & \text{if } t \equiv 0 \pmod{24};\\ 3/5 & \text{if } t \equiv 1,3,4,5,7,9,11,13,15,17,19,20,21,23 \pmod{24};\\ 9/20 & \text{if } t \equiv 2,6,10,14,18,22 \pmod{24};\\ 0 & \text{if } t \equiv 8,16 \pmod{24};\\ 3/10 & \text{if } t \equiv 12 \pmod{24}; \end{cases}$$

for all positive integers t.

For Examples 1.1, 1.2, and 1.3, we compared the value of $\delta_{\boldsymbol{u}}(t)$ given by Theorem 1.2 with the empirical value $\widetilde{\delta}_{\boldsymbol{u}}(t) := \mathcal{P}_{\boldsymbol{u}}(t, p_{10^6})/10^6$, where p_n denotes the nth prime number. The results are in agreement, see Tables 1, 2, and 3.

2. Notation

We reserve the letters p and q for prime numbers. We employ the Landau–Bachmann "Big Oh" notation O, as well as the associated Vinogradov symbols $\ll$ and $\gg$, with their usual meanings. Any dependence of the implied constants is explicitly stated or indicated with subscripts. In particular, notations like $O_{\boldsymbol{u}}$ and $\ll_{\boldsymbol{u}}$ are shortcuts for O_{a_1,a_2} and $\ll_{a_1,a_2}$, respectively. We let $\mathbf{i}$ denote the imaginary unity, and we put $\zeta_n := \mathrm{e}^{2\pi\mathbf{i}/n}$ for every positive integer n. For every field F, we let $F^n := \{a^n : a \in F\}$. If F is a number field, we write Δ_F for the discriminant of F over $\mathbb{Q}$, we let $\mathrm{N}_F(a)$ be the norm of $a \in K$ over $\mathbb{Q}$, and we write $a^{1/n}$ for an arbitrary, but fixed, nth root of a (in some extension of F). Moreover, $\varphi(n)$, $\mu(n)$, and $\nu_p(n)$ denote the Euler totient function, the Möbius function, and the p-adic valuation, of a positive integer n. Given a Galois extension E/F of number fields, a prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$ that does not ramify in E, and a prime ideal $\mathfrak{P}$ of $\mathcal{O}_E$ lying over $\mathfrak{p}$, we write $\left[E/F \mid \mathfrak{P}\right]$ for the Frobenius automorphism corresponding to $\mathfrak{P}/\mathfrak{p}$, that is, the unique $\sigma \in \mathrm{Gal}(E/F)$ such that $\sigma(a) \equiv a^{\mathrm{N}_F(\mathfrak{p})} \pmod{\mathfrak{P}}$ for every $a \in \mathcal{O}_E$, where $\mathrm{N}_F(\mathfrak{p})$ denotes the norm of $\mathfrak{p}$ in F. Moreover, we let $\left[E/F \mid \mathfrak{p}\right]$ be the conjugacy class of $\mathrm{Gal}(E/F)$ whose elements are $\left[E/F \mid \mathfrak{P}\right]$, where $\mathfrak{P}$ runs over the prime ideals of $\mathcal{O}_E$ lying over $\mathfrak{p}$.

3. Proof of Theorem 1.1

3.1. **Preliminaries.** We need the following conditional version of the Chebotarev density theorem.

Theorem 3.1. *Assume the GRH. Let $F/\mathbb{Q}$ be a finite Galois extension with Galois group G, and let C be a union of conjugacy classes of G. Then we have that*

$$\begin{aligned}\pi_{F,C}(x) &:= \#\left\{p \le x : p \text{ does not ramify in } F \text{ and } \left[F/\mathbb{Q} \mid p\right] \subseteq C\right\} \\ &= \frac{\#C}{\#G}\,\mathrm{Li}(x) + O\left(\#C\, x^{1/2}\left(\frac{\log|\Delta_F|}{\#G} + \log x\right)\right),\end{aligned}$$

for all $x \ge 2$, where $\mathrm{Li}(x) := \int_2^x \mathrm{d}s/\log s$ is the logarithmic integral.

Proof. See, e.g., [12, Chapter 2, Section 7]. □

We also need some results on the degree and the discriminant of certain number fields.

Lemma 3.2. *Let F be a number field, let $a \in F^*$ with a not a root of unity, and let n be a positive integer. Then:*

(i) $[F(\zeta_n, a^{1/n}) : \mathbb{Q}] \gg_{F,a} \varphi(n)n$;

(ii) $\log|\Delta_{F(\zeta_n,a^{1/n})}| \ll_{F,a} \varphi(n)n\log(2n)$;

(iii) Each prime factor of $\Delta_{F(\zeta_n,a^{1/n})}$ divides $\mathrm{N}_F(a)\Delta_F n$.

Proof. See, e.g., [19, Lemma 3 and Lemma 5]. (Claim (iii) is implicit in the proof of [19, Lemma 5].) □

Finally, we need an upper bound for a series involving the Euler totient function.

Lemma 3.3. *We have that*

$$\sum_{n>x} \frac{1}{\varphi(n)n} \ll \frac{1}{x},$$

for all $x > 0$.

Proof. See, e.g., [17, Theorem 5]. □

3.2. **Proof of Theorem 1.1.** Throughout this section, let $\boldsymbol{u} = (u_n)_{n\geq 0}$ be the Lucas sequence defined recursively by $u_0 = 0$, $u_1 = 1$, and $u_n = a_1u_{n-1} + a_2u_{n-2}$, for every integer $n \geq 2$, where a_1 and a_2 are fixed nonzero integers. Let $f_{\boldsymbol{u}} := X^2 - a_1X - a_2$ be the characteristic polynomial of $\boldsymbol{u}$ and let $D_{\boldsymbol{u}} := a_1^2 + 4a_2$ be the discriminant of $f_{\boldsymbol{u}}$. Assume that $D_{\boldsymbol{u}}$ is not a square in $\mathbb{Z}$, so that $K := \mathbb{Q}(\sqrt{D_{\boldsymbol{u}}})$ is a quadratic number field. Let $\alpha, \beta \in K$ be the two roots of $f_{\boldsymbol{u}}$, and put $\gamma := \alpha/\beta$. Note that $\mathrm{N}_K(\gamma) = 1$. Finally, assume that $\boldsymbol{u}$ is *nondegenerate*, that is, γ is not a root of unity.

For every positive integer n, let $K_n := K(\zeta_n, \gamma^{1/n})$. Note that $K_n/\mathbb{Q}$ is a Galois extension. Indeed, writing $\gamma = a + b\sqrt{\Delta_K}$ with $a, b \in \mathbb{Q}$, we have that K_n is the splitting field of $X^{2n} - 2aX^n + 1$. Furthermore, let $C_n \subseteq \mathrm{Gal}(K_n/\mathbb{Q})$ be defined as $C_n := \{\mathrm{id}, \sigma\}$, if there exists $\sigma \in \mathrm{Gal}(K_n/\mathbb{Q})$ such that $\sigma(\zeta_n) = \zeta_n^{-1}$ and $\sigma(\gamma^{1/n}) = \gamma^{-1/n}$, and as $C_n := \{\mathrm{id}\}$, if such σ does not exist. Note that C_n is a union of conjugacy classes, since σ belongs to the center of $\mathrm{Gal}(K_n/\mathbb{Q})$.

Lemma 3.4. *Let p be a prime number with $p \nmid a_2\Delta_K$ and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ lying over p. Then $\rho_{\boldsymbol{u}}(p)$ is equal to the multiplicative order of γ modulo $\mathfrak{p}$.*

Proof. See [15, Lemma 5.1]. We remark that [15, Lemma 5.1] is stated, incorrectly, with $D_{\boldsymbol{u}}$ in place of Δ_K, which makes a difference only for $p = 2$. □

The next lemma is the key tool to the proof of Theorem 1.1.

Lemma 3.5. *Let n be a positive integer and let p be a prime number such that $p \nmid a_2\Delta_K$. Then $n \mid \iota_{\boldsymbol{u}}(p)$ if and only if p does not ramify in K_n and $[K_n/\mathbb{Q} \mid p] \subseteq C_n$.*

Proof. Note that $(D_{\boldsymbol{u}} \mid p) = (\Delta_K \mid p)$. Suppose that $n \mid \iota_{\boldsymbol{u}}(p)$. Hence, we have that $p \equiv s \pmod n$, where $s := \big(\Delta_K \mid p\big)$. Note that $s \in \{-1, +1\}$, since $p \nmid \Delta_K$. In particular, it follows that $p \nmid n$ and so, by Lemma 3.2(iii), we have that p does not ramify in K_n. Let $\mathfrak{P}$ be a prime ideal of K_n lying over p, and put $\sigma := [K_n/\mathbb{Q} \mid \mathfrak{P}]$. Then

$$\sigma(\zeta_n) \equiv \zeta_n^p \equiv \zeta_n^s \pmod{\mathfrak{P}}$$

and

$$\sigma(\gamma^{1/n}) \equiv (\gamma^{1/n})^p \equiv \gamma^{(p-s)/n} \cdot \gamma^{s/n} \equiv \gamma^{s/n} \pmod{\mathfrak{P}},$$

where we used Lemma 3.4 and the fact that $\rho_{\boldsymbol{u}}(p) \mid (p-s)/n$. Moreover, we have that

$$\sigma(\gamma) = \sigma|_K(\gamma) = \left[\frac{K/\mathbb{Q}}{\mathfrak{P} \cap \mathcal{O}_K}\right](\gamma) = \gamma^s,$$

since $\mathrm{N}_K(\gamma) = 1$ (and so γ^{-1} is the algebraic conjugate of γ). Consequently, we get that $\sigma(\gamma^{1/n}) = \eta\gamma^{s/n}$, for some nth root of unity η. Since p does not divide n, the polynomial $X^n - 1$ has no multiple roots modulo $\mathfrak{P}$. Hence, reduction modulo $\mathfrak{P}$ is injective on the set of nth roots of unity. Therefore, we get that $\sigma(\zeta_n) = \zeta_n^s$ and $\sigma(\gamma^{1/n}) = \gamma^{s/n}$, which in turn means that $\sigma \in C_n$. Thus $[K_n/\mathbb{Q} \mid p] \subseteq C_n$, as desired.

Suppose that p does not ramify in K_n and that $[K_n/\mathbb{Q} \mid p] \subseteq C_n$. Let $\mathfrak{P}$ be a prime ideal of K_n lying over p, and put $\sigma := [K_n/\mathbb{Q} \mid \mathfrak{P}]$. Thus $\sigma(\zeta_n) = \zeta_n^t$ and $\sigma(\gamma^{1/n}) = \gamma^{t/n}$ for some $t \in \{-1, +1\}$. Then

$$\zeta_n^t = \sigma(\zeta_n) = \sigma|_{\mathbb{Q}(\zeta_n)}(\zeta_n) = \left[\frac{\mathbb{Q}(\zeta_n)/\mathbb{Q}}{\mathfrak{P} \cap \mathcal{O}_{\mathbb{Q}(\zeta_n)}}\right](\zeta_n) = \zeta_n^p,$$

which implies that $p \equiv t \pmod n$. Furthermore, we have that

$$\gamma^{(p-t)/n} \equiv (\gamma^{1/n})^p \cdot \gamma^{-t/n} \equiv \sigma(\gamma^{1/n}) \cdot \gamma^{-t/n} \equiv \gamma^{t/n} \cdot \gamma^{-t/n} \equiv 1 \pmod{\mathfrak{P}},$$

which, by Lemma 3.4, implies that $\rho_{\boldsymbol{u}}(p) \mid (p-t)/n$. Hence, we have that $t = \big(\Delta_K \mid p\big)$ and $n \mid \iota_{\boldsymbol{u}}(p)$, as desired. □

The rest of the proof follows closely Hooley's proof of Artin's conjecture under the GRH [5], with some minor adaptations. The main differences are the following. First, while Hooley's proof relies on the equivalence "$n \mid i_g(p)$ if and only if p splits completely in $\mathbb{Q}(\zeta_n, g^{1/n})$" (where $i_g(p)$ is the residual index of the rational number g modulo p), we rely on the equivalence for $n \mid \iota_{\boldsymbol{u}}(p)$ provided by Lemma 3.5. Second, for some bounds (proofs of Lemma 3.8 and Lemma 3.9), we have to employ properties of the rank of appearance.

For each positive integer t, let us define

$$\delta_{\boldsymbol{u}}(t) := \sum_{n=1}^{\infty} \frac{\mu(n)\,\#C_{nt}}{[K_{nt}:\mathbb{Q}]}. \tag{1}$$

Note that the series in (1) converges absolutely, thanks to Lemma 3.2(i) and Lemma 3.3.

For the rest of this section, we shall tacitly ignore the finitely many prime numbers that divide $a_2\Delta_K$. For all $x, y, z > 0$, define the sets

$$\mathcal{P}_{\boldsymbol{u}}(t,x,y) := \big\{p \le x : t \mid \iota_{\boldsymbol{u}}(p) \text{ and } qt \nmid \iota_{\boldsymbol{u}}(p) \text{ for every } q \le y\big\}$$

and

$$\mathcal{Q}_{\boldsymbol{u}}(t,x,y,z) := \big\{p \le x : qt \mid \iota_{\boldsymbol{u}}(p) \text{ for some } q \in [y,z]\big\}.$$

Moreover, for every $x > 0$, put $y_1 := (\log x)/6$, $y_2 := x^{1/2}/(\log x)^2$, and $y_3 := x^{1/2}\log x$. Then, it follows easily that

$$\#\mathcal{P}_{\boldsymbol{u}}(t,x) = \#\mathcal{P}_{\boldsymbol{u}}(t,x,y_1) + O\big(\#\mathcal{Q}_{\boldsymbol{u}}(t,x,y_1,y_2) + \#\mathcal{Q}_{\boldsymbol{u}}(t,x,y_2,y_3) + \#\mathcal{Q}_{\boldsymbol{u}}(t,x,y_3,x)\big), \tag{2}$$

for all sufficiently large x. The rest of the proof consists of four lemmas estimating the terms of (2).

Lemma 3.6. *Assume the GRH. Then*

$$\#\mathcal{P}_{\boldsymbol{u}}(t,x,y_1) = \delta_{\boldsymbol{u}}(t)\,\frac{x}{\log x} + O_{\boldsymbol{u}}\left(\frac{x}{(\log x)^2}\right),$$

for all positive integers t and for all $x > t^3$.

Proof. Let $\mathcal{S}(y_1)$ be the set of all positive squarefree integers whose prime factors are not exceeding y_1. By the inclusion-exclusion principle and by Lemma 3.5, we get that

$$\#\mathcal{P}_{\boldsymbol{u}}(t,x,y_1) = \sum_{n\in\mathcal{S}(y_1)} \mu(n)\,\#\big\{p \le x : nt \mid \iota_u(p)\big\} = \sum_{n\in\mathcal{S}(y_1)} \mu(n)\,\pi_{K_{nt},C_{nt}}(x). \tag{3}$$

Moreover, by Theorem 3.1 and Lemma 3.2(i) and (ii), we have that

$$\sum_{n\in\mathcal{S}(y_1)} \mu(n)\,\pi_{K_{nt},C_{nt}}(x) = \sum_{n\in\mathcal{S}(y_1)} \frac{\mu(n)\,\#C_{nt}}{[K_{nt}:\mathbb{Q}]}\,\mathrm{Li}(x) + O\left(x^{1/2}\sum_{n\in\mathcal{S}(y_1)}\log(2ntx)\right). \tag{4}$$

If $n \in \mathcal{S}(y_1)$ then $n \le \prod_{p\le y_1} p \le 4^{y_1} \le x^{1/3}$ (see [4, Lemma 2.8]). Consequently, a fortiori, $\#\mathcal{S}(y_1) \le x^{1/3}$. Therefore, also recalling that $t < x^{1/3}$, we get that

$$\sum_{n\in\mathcal{S}(y_1)} \log(2ntx) \ll x^{1/3}\log x. \tag{5}$$

Furthermore, by (1), Lemma 3.2(i), and Lemma 3.3, we have that

$$\delta_{\boldsymbol{u}}(t) - \sum_{n\in\mathcal{S}(y_1)} \frac{\mu(n)\,\#C_{nt}}{[K_{nt}:\mathbb{Q}]} \ll \sum_{n>y_1} \frac{1}{[K_{nt}:\mathbb{Q}]} \ll \sum_{n>y_1} \frac{1}{\varphi(n)n} \ll \frac{1}{y_1} \ll \frac{1}{\log x}. \tag{6}$$

Putting together (3), (4), (5), and (6), and also employing the fact that

$$\mathrm{Li}(x) = \frac{x}{\log x} + O\left(\frac{x}{(\log x)^2}\right),$$

the claim follows. □

Lemma 3.7. *Assume the GRH. Then*

$$\#\mathcal{Q}_{\boldsymbol{u}}(t,x,y_1,y_2) \ll \frac{x}{(\log x)^2},$$

for all positive integers t and for all $x > t^3$.

Proof. If $p \in \mathcal{Q}_{\boldsymbol{u}}(t,x,y_1,y_2)$ then $qt \mid \iota_{\boldsymbol{u}}(p)$ for some $q \in [y_1,y_2]$. Consequently, by Lemma 3.5, we have that

$$\#\mathcal{Q}_{\boldsymbol{u}}(t,x,y_1,y_2) \le \sum_{q\in[y_1,y_2]} \pi_{K_{qt},C_{qt}}(x).$$

Furthermore, by Theorem 3.1 and Lemma 3.2(i) and (ii), we get that

$$\begin{aligned}\sum_{q\in[y_1,y_2]} \pi_{K_{qt},C_{qt}}(x) &= \sum_{q\in[y_1,y_2]} \frac{\#C_{qt}}{[K_{qt}:\mathbb{Q}]}\operatorname{Li}(x) + O\left(x^{1/2}\sum_{q\in[y_1,y_2]}\left(\frac{\log|\Delta_{K_{qt}}|}{[K_{qt}:\mathbb{Q}]}+\log x\right)\right)\\ &\ll \sum_{q\in[y_1,y_2]}\frac{1}{\varphi(qt)qt}\frac{x}{\log x} + x^{1/2}\sum_{q\in[y_1,y_2]}\log(2qtx)\\ &\ll \sum_{q\ge y_1}\frac{1}{q^2}\frac{x}{\log x} + x^{1/2}\log x\sum_{q\le y_2}1\\ &\ll \frac{1}{y_1}\frac{x}{\log x} + x^{1/2}\log x\,\frac{y_2}{\log y_2}\\ &\ll \frac{x}{(\log x)^2},\end{aligned}$$

where we used the upper bound $\sum_{q\ge z}1/q^2 \ll 1/z$ and Chebyshev's estimate $\sum_{q\le z}1 \ll z/\log z$, which holds for every $z>1$. □

Lemma 3.8. *We have that*

$$\#\mathcal{Q}_{\boldsymbol{u}}(t,x,y_2,y_3) \ll \frac{x\log\log(3x)}{\varphi(t)(\log x)^2},$$

for all positive integers t and for all $x > t^3$.

Proof. If $p \in \mathcal{Q}_{\boldsymbol{u}}(t,x,y_2,y_3)$ then $qt \mid \iota_{\boldsymbol{u}}(p)$ for some prime number $q \in [y_2,y_3]$. In particular, we have that $p \equiv \pm 1 \pmod{qt}$. Consequently, assuming that x is sufficiently large so that $qt \le y_3 x^{1/3} < x$, by the Brun–Titchmarsh inequality (see, e.g., [4, Theorem 12.7]), we get that

$$\begin{aligned}\#\mathcal{Q}_{\boldsymbol{u}}(t,x,y_2,y_3) &\le \sum_{q\in[y_2,y_3]} \#\{p\le x : p\equiv\pm1 \pmod{qt}\} \ll \sum_{q\in[y_2,y_3]}\frac{x}{\varphi(qt)\log\big(x/(qt)\big)}\\ &\ll \frac{x}{\varphi(t)\log x}\sum_{q\in[y_2,y_3]}\frac{1}{q} \ll \frac{x\log\log(3x)}{\varphi(t)(\log x)^2},\end{aligned}$$

where the last estimate follows from the Mertens theorem. □

Lemma 3.9. *We have that*

$$\#\mathcal{Q}_{\boldsymbol{u}}(t,x,y_3,x) \ll_{\boldsymbol{u}} \frac{x}{(\log x)^2},$$

for all positive integers t and for all $x > 1$.

Proof. If $p \in \mathcal{Q}_{\boldsymbol{u}}(t,x,y_3,x)$ then $p \le x$ and $qt \mid \iota_u(p)$ for some prime number $q \ge y_3$. Hence, we have that $\rho_{\boldsymbol{u}}(p)$ divides

$$m := \frac{p-(D_{\boldsymbol{u}}\,|\,p)}{q} \le \frac{2x}{y_3} = \frac{2x^{1/2}}{\log x},$$

and consequently $p \mid u_m$ (since, in general, $p \mid u_n$ if and only if $p \nmid a_2$ and $\rho_{\boldsymbol{u}}(p) \mid n$, see, e.g., [14, Chapter 1, Section 3]). Therefore, we get that

$$\prod_{p \in \mathcal{Q}_{\boldsymbol{u}}(t,x,y_3,x)} p \quad \text{divides} \quad \prod_{m \le 2x^{1/2}/\log x} u_m,$$

where the second product is nonzero, since $\boldsymbol{u}$ is nondegenerate. Consequently, we have that

$$2^{\#\mathcal{Q}_{\boldsymbol{u}}(t,x,y_3,x)} \le \prod_{p \in \mathcal{Q}_{\boldsymbol{u}}(t,x,y_3,x)} p \le \prod_{m \le 2x^{1/2}/\log x} |u_m| \le A^{2\sum_{m \le 2x^{1/2}/\log x} m} = A^{O(x/(\log x)^2)},$$

where $A := \max\{|\alpha|, |\beta|, 2\}$ and where we used the upper bound $|u_m| \le A^{2m}$, which follows easily from the Binet formula. The claim follows. □

At this point, Theorem 1.1 follows by putting together (2) and Lemmas 3.6, 3.7, 3.8, and 3.9. The proof is complete.

4. Proof of Theorem 1.2

4.1. General preliminaries.

This section collects some general results needed later.

Lemma 4.1. *Let $n > 0$ and m be integers. Then we have that:*

(i) $\sqrt{m} \in \mathbb{Q}(\zeta_n)$ if and only if $\Delta_{\mathbb{Q}(\sqrt{m})} \mid n$;

(ii) if $\sqrt{m} \notin \mathbb{Q}(\zeta_n)$ and $\sqrt{m} \in \mathbb{Q}(\zeta_{2n})$, then $\nu_2(n) \in \{1, 2\}$;

(iii) if $\nu_2(n) = 1$ then $-\zeta_n \in \mathbb{Q}(\zeta_n)^2$;

(iv) if $\nu_2(n) = 2$ then $2\zeta_n \in \mathbb{Q}(\zeta_n)^2$.

Proof. Fact (i) is well known (cf. [16, Lemma 3]). Let us prove (ii). If $\sqrt{m} \notin \mathbb{Q}(\zeta_n)$ and $\sqrt{m} \in \mathbb{Q}(\zeta_{2n})$ then, by (i), we get that $D \nmid n$ and $D \mid 2n$, where $D := \Delta_{\mathbb{Q}(\sqrt{m})}$. Let d be the squarefree integer such that $\mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\sqrt{d})$. If $d \equiv 1 \pmod 4$ then $D = d$. Hence, $d \nmid n$ and $d \mid 2n$, which is impossible, since d is odd. If $d \equiv 2, 3 \pmod 4$ then $D = 4d$. Hence, $4d \nmid n$ and $2d \mid n$, which implies that $\nu_2(n) = \nu_2(d) + 1 \in \{1, 2\}$, as claimed. Finally, (iii) and (iv) follow by a quick verification of the identities $-\zeta_n = \left(\zeta_n^{(n+2)/4}\right)^2$ and $2\zeta_n = \left((1 - \mathbf{i})\zeta_n^{(n+4)/8}\right)^2$, respectively. □

Lemma 4.2. *Let F be a field of characteristic zero, and let $X^4 + aX^2 + b \in F[X]$ be an irreducible polynomial with Galois group G. Then:*

(i) if $b \in F^2$, then $G \cong C_2 \times C_2$;

(ii) if $b \notin F^2$ and $b(a^2 - 4b) \in F^2$, then $G \cong C_4$;

(iii) if $b \notin F^2$ and $b(a^2 - 4b) \notin F^2$, then $G \cong D_8$;

where C_n and D_n denote the cyclic group and the dihedral groups of n elements, respectively.

Proof. See [6, Chapter V, Section 4, Exercise 9]. □

Lemma 4.3. *Let F be a field, let n be a positive integer not divisible by the characteristic of F, let m be the number of nth roots of unity contained in F, and let $a \in F$. Then $F(\zeta_n, a^{1/n})/F$ is abelian if and only if $a^m \in F^n$.*

Proof. See [7, Chapter 8, Theorem 3.2]. □

Lemma 4.4. *Let F be a number field, let $a \in F^*$, and let n be a positive integer. Then $[F(\zeta_n, a^{1/n}) : F(\zeta_n)]$ is equal to the minimum positive integer ℓ such that $a^\ell \in F(\zeta_n)^n$. Moreover, we have that $f := X^\ell - (a^{1/n})^\ell$ is an irreducible polynomial over $F(\zeta_n)[X]$ and it holds $F(\zeta_n, a^{1/n}) \cong F(\zeta_n)[X]/(f)$.*

Proof. This fact follows from Kummer theory [1]. □

4.2. **Preliminaries on a Kummer extension.** Throughout this section, let K be a quadratic extension of $\mathbb{Q}$ with $\Delta_K \notin \{-3,-4\}$. Note that the condition on Δ_K implies that K contains only two roots of unity (namely, -1 and $+1$).

This section is devoted to the study of the extension $K(\zeta_n,\gamma^{1/n})/K(\zeta_n)$, where n is a positive integer and $\gamma \in K$. (In fact, for our purpose, we can assume $|\mathrm{N}_K(\gamma)|=1$, as we will do later.) The main goals are obtaining a formula for $[K(\zeta_n,\gamma^{1/n}) : K(\zeta_n)]$ and finding necessary and sufficient conditions for the nontriviality of the conjugacy class C_n. These tasks require first to study when $\sqrt{\gamma} \in K(\zeta_n)$ (Lemmas 4.6, 4.5, and 4.7), and then when $\gamma \in K(\zeta_n)^n$ (Lemma 4.8). The goals are achieved by Lemma 4.10 and Lemma 4.11, with the latter needed to check which of the conditions (D1)–(D5) of the former hold.

Lemma 4.5. *Let $a \in \mathbb{Q}\setminus\mathbb{Q}^2$. Then $\sqrt{a} \in K(\zeta_n)$ if and only if $\sqrt{a} \in \mathbb{Q}(\zeta_n)$ or $\sqrt{a/\Delta_K} \in \mathbb{Q}(\zeta_n)$.*

Proof. Suppose that $\sqrt{a} \in K(\zeta_n)$. Then $\sqrt{a} = x + y\sqrt{\Delta_K}$ for some $x,y \in \mathbb{Q}(\zeta_n)$. If $y=0$ then $\sqrt{a} = x \in \mathbb{Q}(\zeta_n)$. If $x=0$ and $y \neq 0$, then $\sqrt{a/\Delta_K} = \pm y \in \mathbb{Q}(\zeta_n)$. If $x \neq 0$ and $y \neq 0$, then $\sqrt{\Delta_K} = (2xy)^{-1}(a - x^2 - y^2\Delta_K) \in \mathbb{Q}(\zeta_n)$, and so $\sqrt{a} = x + y\sqrt{\Delta_K} \in \mathbb{Q}(\zeta_n)$.

Suppose that $\sqrt{a} \in \mathbb{Q}(\zeta_n)$ or $\sqrt{a/\Delta_K} \in \mathbb{Q}(\zeta_n)$. Then it follows easily that $\sqrt{a} \in K(\zeta_n)$, since $K(\zeta_n) = \mathbb{Q}(\sqrt{\Delta_K},\zeta_n)$. □

Lemma 4.6. *Let $\gamma \in K\setminus(\mathbb{Q}\cup K^2)$ with $\mathrm{N}_K(\gamma)\Delta_K \notin \mathbb{Q}^2$, and let n be a positive integer. Write $\gamma = a + b\sqrt{\Delta_K}$, with $a,b \in \mathbb{Q}$. Then $\sqrt{\gamma} \in K(\zeta_n)$ if and only if $N \in \mathbb{Q}^2$, and $\sqrt{c} \in \mathbb{Q}(\zeta_n)$ or $\sqrt{d} \in \mathbb{Q}(\zeta_n)$, where $N := \mathrm{N}_K(\gamma)$, $c := (a - \sqrt{N})/2$, and $d := c/\Delta_K$.*

Proof. First, note that $f = X^4 - 2aX^2 + N$ is the minimal polynomial of $\sqrt{\gamma}$ over $\mathbb{Q}$. Indeed, on the one hand, an easy computation shows that $f(\sqrt{\gamma}) = 0$; while, on the other hand, $\gamma \notin K^2$ implies that $[\mathbb{Q}(\sqrt{\gamma}) : \mathbb{Q}] = 4$, and so the claim follows. Let L be the splitting field of f over $\mathbb{Q}$ and put $G := \mathrm{Gal}(L/\mathbb{Q})$. Note that $K(\zeta_n)$ is an abelian extension over $\mathbb{Q}$, since it is the compositum of $\mathbb{Q}(\sqrt{\Delta_K})$ and $\mathbb{Q}(\zeta_n)$, which are abelian over $\mathbb{Q}$.

Suppose that $N \notin \mathbb{Q}^2$. We have to prove that $\sqrt{\gamma} \notin K(\zeta_n)$. Note that $N((-2a)^2 - 4N) = N\Delta_K(2b)^2 \notin \mathbb{Q}^2$, by hypothesis. Then, by Lemma 4.2, we have that $G \cong D_8$ and, in particular, $L/\mathbb{Q}$ is a nonabelian extension. If $\sqrt{\gamma} \in K(\zeta_n)$ then, since $K(\zeta_n)/\mathbb{Q}$ is Galois, we get that $L \subseteq K(\zeta_n)$, which in turn implies that $L/\mathbb{Q}$ is an abelian extension, but this is absurd. Therefore, we have that $\sqrt{\gamma} \notin K(\zeta_n)$, as desired.

For the rest of the proof, suppose that $N \in \mathbb{Q}^2$. We have to prove that, under this last hypothesis, $\sqrt{\gamma} \in K(\zeta_n)$ if and only if $\sqrt{c} \in \mathbb{Q}(\zeta_n)$ or $\sqrt{d} \in \mathbb{Q}(\zeta_n)$. Before doing that, let us prove that $L = \mathbb{Q}(\sqrt{c},\sqrt{d})$. Since $N \in \mathbb{Q}^2$, Lemma 4.2 yields that $G \cong C_2 \times C_2$ and, in particular, $[L : \mathbb{Q}] = |G| = 4$. Consequently, we have that $L = \mathbb{Q}(\sqrt{\gamma})$. Put $e := (a + \sqrt{N})/2$. It can be easily checked that $\sqrt{\gamma} = s\sqrt{c} + t\sqrt{e}$ for the right choice of signs $s,t \in \{-1,+1\}$. Hence, we have that $L \subseteq \mathbb{Q}(\sqrt{c},\sqrt{e}) = \mathbb{Q}(\sqrt{c},\sqrt{d})$, where the last equality follows from the identity $e = d^{-1}(b/2)^2$ (note that $d \neq 0$ since $\gamma \notin \mathbb{Q}$). Furthermore, since $[\mathbb{Q}(\sqrt{c},\sqrt{d}) : \mathbb{Q}] \leq 4$, we get that $L = \mathbb{Q}(\sqrt{c},\sqrt{d})$, as desired.

Suppose that $\sqrt{\gamma} \in K(\zeta_n)$. Then, since $K(\zeta_n)/\mathbb{Q}$ is Galois, we have that $L \subseteq K(\zeta_n)$ and so $\sqrt{c} \in K(\zeta_n)$. Note that $c \in \mathbb{Q}$, since $N \in \mathbb{Q}^2$, and $c \notin \mathbb{Q}^2$, since $[L : \mathbb{Q}] = 4$. Hence, by Lemma 4.5, we get that $\sqrt{c} \in \mathbb{Q}(\zeta_n)$ or $\sqrt{d} \in \mathbb{Q}(\zeta_n)$, as desired.

Suppose that $\sqrt{c} \in \mathbb{Q}(\zeta_n)$ or $\sqrt{d} \in \mathbb{Q}(\zeta_n)$. If $\sqrt{c} \in \mathbb{Q}(\zeta_n)$ then, recalling that $d = c/\Delta_K$ and $K = \mathbb{Q}(\sqrt{\Delta_K})$, we get that $\sqrt{c},\sqrt{d} \in K(\zeta_n)$. Therefore, $\sqrt{\gamma} \in L = \mathbb{Q}(\sqrt{c},\sqrt{d}) \subseteq K(\zeta_n)$, so that $\sqrt{\gamma} \in K(\zeta_n)$. If $\sqrt{d} \in \mathbb{Q}(\zeta_n)$ then a similar reasoning yields again that $\sqrt{\gamma} \in K(\zeta_n)$. □

Lemma 4.7. *Let $\gamma \in K$ with $|\mathrm{N}_K(\gamma)| = 1$, and let n be a positive integer. If $\sqrt{\gamma} \notin K(\zeta_n)$ and $\sqrt{\gamma} \in K(\zeta_{2n})$, then $\nu_2(n) \in \{1,2\}$.*

Proof. Suppose that $\sqrt{\gamma} \notin K(\zeta_n)$ and $\sqrt{\gamma} \in K(\zeta_{2n})$.

First, assume that $\gamma \in \mathbb{Q}$. Since $|\mathrm{N}_K(\gamma)| = 1$, we get that either $\gamma = 1$ or $\gamma = -1$. The case $\gamma = 1$ is impossible, since $\sqrt{\gamma} \notin K(\zeta_n)$ by hypothesis. If $\gamma = -1$, then $\gamma \in \mathbb{Q}\setminus\mathbb{Q}^2$. Hence, Lemma 4.5 and the hypotheses $\sqrt{\gamma} \notin K(\zeta_n)$ and $\sqrt{\gamma} \in K(\zeta_{2n})$, yield that $\sqrt{-1} \notin \mathbb{Q}(\zeta_n)$,

$\sqrt{-\Delta_K} \notin \mathbb{Q}(\zeta_n)$; and $\sqrt{-1} \in \mathbb{Q}(\zeta_{2n})$ or $\sqrt{-\Delta_K} \in \mathbb{Q}(\zeta_{2n})$. Therefore, from Lemma 4.1(ii) we get that $\nu_2(n) \in \{1, 2\}$, as desired.

Now assume that $\gamma \notin \mathbb{Q}$. From $\sqrt{\gamma} \notin K(\zeta_n)$ it follows that $\gamma \notin K^2$. Moreover, we have that $\mathrm{N}_K(\gamma)\Delta_K \notin \mathbb{Q}^2$, since $\mathrm{N}_K(\gamma) = \pm 1$ and $\Delta_K \neq -4$ by the hypothesis on K. Hence, we can apply Lemma 4.6 and, with the same notation of Lemma 4.6, we get that $\mathrm{N}_K(\gamma) = 1$, $\sqrt{c} \notin \mathbb{Q}(\zeta_n)$, $\sqrt{d} \notin \mathbb{Q}(\zeta_n)$; and $\sqrt{c} \in \mathbb{Q}(\zeta_{2n})$ or $\sqrt{d} \in \mathbb{Q}(\zeta_{2n})$. Then from Lemma 4.1(ii) we get that $\nu_2(n) \in \{1, 2\}$, as desired. □

The proof of the next lemma is similar to that of [16, Lemma 4], which characterizes rational numbers in $\mathbb{Q}(\zeta_n)^n$.

Lemma 4.8. *Let $\gamma \in K$ with $|\mathrm{N}_K(\gamma)| = 1$, and let n be a positive integer. Then $\gamma \in K(\zeta_n)^n$ if and only if:*

(i) n is odd and $\gamma = \delta^n$ for some $\delta \in K$; or

(ii) n is even and $\gamma = \delta^{n/2}$ for some $\delta \in K \cap K(\zeta_n)^2$; or

(iii) $\nu_2(n) = 2$ and $\gamma = -(2\delta)^{n/2}$ for some $\delta \in K \cap K(\zeta_n)^2$.

Proof. First, suppose that $\gamma \in K(\zeta_n)^n$. Let us prove that one of (i)–(iii) holds. We have that $\gamma = \varepsilon^n$ for some $\varepsilon \in K(\zeta_n)$. Consequently, we get that $K(\zeta_n, \gamma^{1/n}) = K(\zeta_n, \varepsilon) = K(\zeta_n)$, which is an abelian extension of K. Hence, by Lemma 4.3, we have that $\gamma^m \in K^n$, where m is the number of nth roots of unity in K. Therefore, there exists $\delta \in K$ such that $\gamma^m = \delta^n$. Note that $m = (n, 2)$, since, by hypothesis, K contains only two roots of unity. Furthermore, note that $|\mathrm{N}_K(\delta)| = 1$, since $|\mathrm{N}_K(\gamma)| = 1$. We have to consider several cases.

If n is odd, then $m = 1$ and we have (i). Suppose that n is even, so that $\gamma^2 = \delta^n$. Therefore, $\gamma = s\delta^{n/2}$ for some $s \in \{-1, +1\}$. In particular, if $\nu_2(n) = 1$ then, after eventually changing the sign of δ, we pick $s = 1$. Moreover, we have that $(\sqrt{\delta})^n = \delta^{n/2} = s\gamma = s\varepsilon^n$.

If we may take $s = 1$, then $(\sqrt{\delta})^n = \varepsilon^n$ and so $\sqrt{\delta} = \eta\varepsilon$, where η is a nth root of unity. Hence, $\sqrt{\delta} \in K(\zeta_n)$ and we have (ii). Suppose that s must be -1, implying that $\nu_2(n) \geq 2$ and $(\sqrt{\delta})^n = -\varepsilon^n$. Hence, $\sqrt{\delta} = \zeta_{2n}\eta\varepsilon$ where η is a nth root of unity. Consequently, we have that $\zeta_{2n}\sqrt{\delta} \in K(\zeta_n)$ and so $\sqrt{\delta} \in K(\zeta_{2n})$.

Let us prove that $\nu_2(n) = 2$. If $\zeta_{2n} \notin K(\zeta_n)$, then $\sqrt{\delta} \notin K(\zeta_n)$ (otherwise from $\zeta_{2n}\sqrt{\delta} \in K(\zeta_n)$ we would get that $\zeta_{2n} \in K(\zeta_n)$). Hence, we have that $\sqrt{\delta} \notin K(\zeta_n)$ and $\sqrt{\delta} \in K(\zeta_{2n})$. Therefore, Lemma 4.7 yields that $\nu_2(n) = 2$. If $\zeta_{2n} \in K(\zeta_n)$ then $K(\zeta_{2n}) = K(\zeta_n)$. Thus $[K(\zeta_{2n}) : \mathbb{Q}] = [K(\zeta_n) : \mathbb{Q}]$, which implies that $\sqrt{\Delta_K} \notin \mathbb{Q}(\zeta_n)$ and $\sqrt{\Delta_K} \in \mathbb{Q}(\zeta_{2n})$. Therefore, Lemma 4.1(ii) yields that $\nu_2(n) = 2$. The claim is proved.

Recall that $\zeta_{2n}\sqrt{\delta} \in K(\zeta_n)$ and thus $\zeta_n\delta \in K(\zeta_n)^2$. Since $\nu_2(n) = 2$, from Lemma 4.1(iv) we have that $2\zeta_n \in \mathbb{Q}(\zeta_n)^2$, and it follows that $\delta' := \delta/2 \in K(\zeta_n)^2$. Hence, we get that $\gamma = -\delta^{n/2} = -(2\delta')^{n/2}$, and we have (iii).

It remains only to prove that each of (i)-(iii) implies that $\gamma \in K(\zeta_n)^n$, that is, $\gamma = \varepsilon^n$ for some $\varepsilon \in K(\zeta_n)$. In order to do so, it suffices to pick ε equal to δ, $\sqrt{\delta}$, and $(1 + \mathbf{i})\sqrt{\delta}$, for (i), (ii), and (iii), respectively. □

Lemma 4.9. *Every nonzero $\gamma \in K$ can be written as $\gamma = s\gamma_0^h$, where $s \in \{-1, +1\}$, h is a positive integer, and $\gamma_0 \in K$ is not a power in K. Moreover, this representation is unique except peharps for the sign of γ_0. Furthermore, we have that $\gamma^\ell = z\delta^m$, for some $\delta \in K$ and some integers $\ell, m > 0$ and $z \in \{-1, +1\}$, if and only if $m \mid \ell h$ and*

(i) m is even, $s^\ell = z$, and $\delta = \pm\gamma_0^{\ell h/m}$; or

(ii) m is odd and $\delta = s^\ell z\gamma_0^{\ell h/m}$.

Proof. Let S be a finite set of nonequivalent normalized valuations of K containing all the Archimedean valuations and all the valuations $|\cdot|_v$ such that $|\gamma|_v \neq 1$. Hence, by construction, γ is an S-unit of K. Let $\varepsilon_1, \ldots, \varepsilon_w$ be a fundamental system of S-units of K, where $w := |S| - 1$.

By the Dirichlet–Chevalley–Hasse Theorem [13, Theorem 3.12], every S-unit of K can be uniquely written as $s\varepsilon_1^{a_1}\cdots\varepsilon_w^{a_w}$, where $s\in\{-1,+1\}$ and $a_1,\dots,a_w\in\mathbb{Z}$. If $\gamma=s\varepsilon_1^{a_1}\cdots\varepsilon_w^{a_w}$, then $\gamma=s\gamma_0^h$, where $h:=\gcd(a_1,\dots,a_w)$, $b_i:=a_i/h$ for $i=1,\dots,w$, and $\gamma_0:=\varepsilon_1^{b_1}\cdots\varepsilon_w^{b_w}$ is not a power in K. Then the claim on the uniqueness of this representation follows easily.

Suppose that $\gamma^\ell=z\delta^m$, for some $\delta\in K$ and some integers $\ell,m>0$ and $z\in\{-1,+1\}$. Write $\delta=t\varepsilon_1^{c_1}\cdots\varepsilon_w^{c_w}$ for some $t\in\{-1,+1\}$ and $c_1,\dots,c_w\in\mathbb{Z}$. Then $\gamma^\ell=z\delta^m$ if and only if $s^\ell=zt^m$ and $b_i\ell h=c_i m$ for $i=1,\dots,w$. In particular, we have that $m\mid\gcd(b_1\ell h,\dots,b_w\ell h)$ and so $m\mid\ell h$. If m is even and $s^\ell=z$, then the equality $s^\ell=zt^m$ is satisfied for every $t\in\{-1,+1\}$, and so $\delta=\pm\gamma_0^{\ell h/m}$, which is (i). If m is even and $s^\ell\neq z$, then the equality $s^\ell=zt^m$ is impossible. If m is odd then $s^\ell=zt^m$ implies that $t=s^\ell z$ and so $\delta=s^\ell z\gamma_0^{\ell h/m}$, which is (ii).

Vice versa, if $\delta\in K$ and $\ell,m>0$ and $z\in\{-1,+1\}$ are integers such that $m\mid\ell h$ and either (i) or (ii) holds, then it follows easily that $\gamma^\ell=z\delta^m$. □

The first part of the proof of the next lemma follows a strategy similar to the proof of [16, Lemma 5].

Lemma 4.10. *Let $\gamma\in K$ with $|\mathrm{N}_K(\gamma)|=1$. Write $\gamma=s\gamma_0^h$, where $s\in\{-1,+1\}$, h is a positive integer, and $\gamma_0\in K$ is not a power in K (see Lemma 4.9). Let n be a positive integer and put $n':=n/(n,2h)$ and $h':=2h/(n,2h)$. Then we have that*

$$\big[K(\zeta_n,\gamma^{1/n}):K(\zeta_n)\big]=n'\cdot\begin{cases}1 & \text{if one of (C1)–(C4) holds;}\\ 2 & \text{otherwise;}\end{cases}\tag{7}$$

where the conditions in (7) are the following

- *(C1) n is odd;*
- *(C2) $s^{n'}=1$, n is even, and $\gamma_0^{h'}\in K(\zeta_n)^2$;*
- *(C3) $s=-1$, $\nu_2(n)=1$, and $-\gamma_0^{h'}\in K(\zeta_n)^2$;*
- *(C4) $s^{n'}=-1$, $\nu_2(n)=2$, and $2\gamma_0^{h'}\in K(\zeta_n)^2$.*

Furthermore, let $\sigma_1\in\mathrm{Gal}(K(\zeta_n)/\mathbb{Q})$ be the complex conjugation and, if $\sqrt{\Delta_K}\notin\mathbb{Q}(\zeta_n)$, let $\sigma_2\in\mathrm{Gal}(K(\zeta_n)/\mathbb{Q})$ be the unique automorphism satisfying $\sigma_2(\zeta_n)=\zeta_n^{-1}$ and $\sigma_2(\sqrt{\Delta_K})=-\sqrt{\Delta_K}$, otherwise let $\sigma_2:=\sigma_1$. Then there exists $\sigma\in\mathrm{Gal}(K(\zeta_n,\gamma^{1/n})/\mathbb{Q})$ such that $\sigma(\zeta_n)=\zeta_n^{-1}$ and $\sigma(\gamma^{1/n})=\gamma^{-1/n}$ if and only if one of the following holds

- *(D1) it holds (C1) and $\sigma_i\big(\gamma_0^{h'/2}\big)=\gamma_0^{-h'/2}$ for some $i\in\{1,2\}$;*
- *(D2) it holds (C2) and $\sigma_i\Big(\sqrt{\gamma_0^{h'}}\Big)=\sqrt{\gamma_0^{h'}}^{-1}$ for some $i\in\{1,2\}$;*
- *(D3) it holds (C3) and $\sigma_i\Big(\sqrt{-\gamma_0^{h'}}\Big)=\sqrt{-\gamma_0^{h'}}^{-1}$ for some $i\in\{1,2\}$;*
- *(D4) it holds (C4) and $\sigma_i\Big(\sqrt{2\gamma_0^{h'}}\Big)=2\sqrt{2\gamma_0^{h'}}^{-1}$ for some $i\in\{1,2\}$;*
- *(D5) neither of (C1)–(C4) holds and $\sigma_i\big(\gamma_0^{h'}\big)=\gamma_0^{-h'}$ for some $i\in\{1,2\}$.*

Proof. By Lemma 4.4, we have that $\big[K(\zeta_n,\gamma^{1/n}):K(\zeta_n)\big]$ is equal to the least positive integer ℓ such that $\gamma^\ell\in K(\zeta_n)^n$.

First, let us prove that $\ell\in\{n',2n'\}$. On the one hand, by Lemma 4.8, $\gamma^\ell\in K(\zeta_n)^n$ implies that $\gamma^{2\ell}\in K^n$, which in turn, by Lemma 4.9, yields that $n\mid 2h\ell$, and so $n'\mid\ell$. On the other hand, we have that $\gamma^{2n'}=(\gamma_0^{h'})^n\in K^n\subseteq K(\zeta_n)^n$, so that $\ell\le 2n'$. The claim is proved.

At this point, by Lemma 4.8, we have that $\gamma^{n'}\in K(\zeta_n)^n$ if and only if one of the following cases holds

(A1) n is odd and $\gamma^{n'} = \delta^n$ for some $\delta \in K$;

(A2) n is even and $\gamma^{n'} = \delta^{n/2}$ for some $\delta \in K \cap K(\zeta_n)^2$;

(A3) $\nu_2(n) = 2$ and $\gamma^{n'} = -(2\delta)^{n/2}$ for some $\delta \in K \cap K(\zeta_n)^2$.

By studying each of the cases (A1), (A2), and (A3) with the aid of Lemma 4.9 (with (ℓ, m, z) equal to $(n', n, 1)$, $(n', n/2, 1)$, and $(n', n/2, -1)$, respectively), and also employing the fact that $-1 \in K(\zeta_n)^2$ when $4 \mid n$, we get that "(A1) or (A2) or (A3)" is equivalent to the logical disjunction of the following cases

(B1) n is odd;

(B2) $4 \mid n$, $s^{n'} = 1$, and $\gamma_0^{h'} \in K(\zeta_n)^2$;

(B3) $\nu_2(n) = 1$ and $s^{n'}\gamma_0^{h'} \in K(\zeta_n)^2$;

(B4) $\nu_2(n) = 2$, $s^{n'} = -1$, and $2\gamma_0^{h'} \in K(\zeta_n)^2$.

Finally, one can easily check that "(B1) or (B2) or (B3) or (B4)" is equivalent to "(C1) or (C2) or (C3) or (C4)". (Note that (B1)≡(C1) and (B4)≡(C4), so that one has only to check that "(B2) or (B3)" is equivalent to "(C2) or (C3)".) Therefore, we have proved (7).

It remains to prove the statement on the existence of σ. Thanks to Lemma 4.4, we have that $K(\zeta_n, \gamma^{1/n}) \cong K(\zeta_n)[X]/(f)$ where $f \in K(\zeta_n)[X]$ is equal to $X^{n'} - \eta s\gamma_0^{h'/2}$, $X^{n'} - \eta\sqrt{\gamma_0^{h'}}$, $X^{n'} - \eta\sqrt{-\gamma_0^{h'}}$, $X^{n'} - \eta 2^{-1}(1+\mathbf{i})\sqrt{2\gamma_0^{h'}}$, or $X^{2n'} - \eta\gamma_0^{h'}$, for some nth root of unity η, if it holds (C1), (C2), (C3), (C4), or none of them, respectively. We consider only the case in which (C3) holds, since the proofs of the other cases are very similar. Suppose that (C3) holds. We have to prove that σ exists if and only if there exists $\sigma_0 \in \mathrm{Gal}(K(\zeta_n)/\mathbb{Q})$ such that $\sigma_0(\zeta_n) = \zeta_n^{-1}$ and $\sigma_0\big(\sqrt{-\gamma_0^{h'}}\big)\sqrt{-\gamma_0^{h'}} = 1$ (note that $\sigma_0 \in \{\sigma_1, \sigma_2\}$).

Suppose that σ exists. Note that $\sqrt{-\gamma_0^{h'}} = \rho(\gamma^{1/n})^{n'}$ for some nth root of unity ρ. Then, letting $\sigma_0 := \sigma|_{K(\zeta_n)}$, we have that $\sigma_0(\zeta_n) = \zeta_n^{-1}$ and

$$\sigma_0\Big(\sqrt{-\gamma_0^{h'}}\Big) = \sigma\big(\rho(\gamma^{1/n})^{n'}\big) = \sigma(\rho)\,\sigma(\gamma^{1/n})^{n'} = \rho^{-1}(\gamma^{1/n})^{-n'} = \sqrt{-\gamma_0^{h'}}^{-1},$$

as desired.

Vice versa, suppose that σ_0 exists. Then σ_0 can be extended to an automorphism $\widetilde{\sigma} \in \mathrm{Gal}(K(\zeta_n, \gamma^{1/n})/\mathbb{Q})$ that sends the root $\gamma^{1/n}$ of f to the root $\gamma^{-1/n}$ of

$$\sigma_0 f = X^{n'} - \sigma_0\Big(\eta\sqrt{-\gamma_0^{h'}}\Big) = X^{n'} - \eta^{-1}\sqrt{-\gamma_0^{h'}}^{-1},$$

and we can take $\sigma := \widetilde{\sigma}$. The proof is complete. □

Lemma 4.11. *Let $\gamma \in K\setminus(\mathbb{Q}\cup K^2)$ with $\mathrm{N}_K(\gamma)\Delta_K \notin \mathbb{Q}^2$, and let n be a positive integer. Write $\gamma = a+b\sqrt{\Delta_K}$, with $a, b \in \mathbb{Q}$. Suppose that $\sqrt{\gamma} \in K(\zeta_n)$ and let $N := \mathrm{N}_K(\gamma)$, $c := (a-\sqrt{N})/2$, and $d := c/\Delta_K$ (Note that $N \in \mathbb{Q}^2$ by Lemma 4.6). Suppose that $\sqrt{\Delta_K} \notin \mathbb{Q}(\zeta_n)$ and let $\sigma \in \mathrm{Gal}(K(\zeta_n)/\mathbb{Q})$ be the unique automorphism such that $\sigma(\zeta_n) = \zeta_n^{-1}$ and $\sigma(\sqrt{\Delta_K}) = -\sqrt{\Delta_K}$. Then*

$$\sigma(\sqrt{\gamma})\sqrt{\gamma} = \begin{cases} \sqrt{N} & \text{if } \Delta_K > 0 \text{ and } \big(\big(\sqrt{c} \in \mathbb{Q}(\zeta_n), c < 0\big) \text{ or } \big(\sqrt{d} \in \mathbb{Q}(\zeta_n), d > 0\big)\big); \\ -\sqrt{N} & \text{if } \Delta_K > 0 \text{ and } \big(\big(\sqrt{c} \in \mathbb{Q}(\zeta_n), c > 0\big) \text{ or } \big(\sqrt{d} \in \mathbb{Q}(\zeta_n), d < 0\big)\big); \\ \gamma & \text{if } \Delta_K < 0 \text{ and } \big(\big(\sqrt{c} \in \mathbb{Q}(\zeta_n), c > 0\big) \text{ or } \big(\sqrt{d} \in \mathbb{Q}(\zeta_n), d > 0\big)\big); \\ -\gamma & \text{if } \Delta_K < 0 \text{ and } \big(\big(\sqrt{c} \in \mathbb{Q}(\zeta_n), c < 0\big) \text{ or } \big(\sqrt{d} \in \mathbb{Q}(\zeta_n), d < 0\big)\big). \end{cases}$$

Proof. Since $\sqrt{\gamma} \in K(\zeta_n)$, by Lemma 4.6 we get that $\sqrt{c} \in \mathbb{Q}(\zeta_n)$ or $\sqrt{d} \in \mathbb{Q}(\zeta_n)$. Suppose that $\sqrt{c} \in \mathbb{Q}(\zeta_n)$. Note that, since $N = a^2 - b^2\Delta_K$, we have that

$$\left(\sqrt{c} + \frac{b\sqrt{\Delta_K}}{2\sqrt{c}}\right)^2 = c + \frac{b^2\Delta_K}{4c} + b\sqrt{\Delta_K} = c + \frac{a^2 - N}{4c} + b\sqrt{\Delta_K} \\ = \frac{a - \sqrt{N}}{2} + \frac{a + \sqrt{N}}{2} + b\sqrt{\Delta_K} = a + b\sqrt{\Delta_K} = \gamma. \tag{8}$$

Consequently, we obtain that $\sqrt{\gamma} = s\big(\sqrt{c} + b\sqrt{\Delta_K}/(2\sqrt{c})\big)$, where $s \in \{-1, +1\}$. Hence, we get that

$$\sigma(\sqrt{\gamma})\sqrt{\gamma} = \left(\overline{\sqrt{c}} - \frac{b\,\overline{\sqrt{\Delta_K}}}{2\overline{\sqrt{c}}}\right)\left(\sqrt{c} + \frac{b\sqrt{\Delta_K}}{2\sqrt{c}}\right) = |c| - \frac{b^2|\Delta_K|}{4|c|} + \frac{b}{2}\left(\frac{\overline{\sqrt{c}}}{\sqrt{c}}\sqrt{\Delta_K} - \frac{\sqrt{c}}{\overline{\sqrt{c}}}\overline{\sqrt{\Delta_K}}\right).$$

The claim follows by considering the possible signs of c and Δ_K. For instance, if $c > 0$ and $\Delta_K < 0$, then

$$\sigma(\sqrt{\gamma})\sqrt{\gamma} = c + \frac{b^2\Delta_K}{4c} + \frac{b}{2}\left(\sqrt{\Delta_K} - \overline{\sqrt{\Delta_K}}\right) = c + \frac{b^2\Delta_K}{4c} + b\sqrt{\Delta_K} = \gamma,$$

where we also used (8). The case $\sqrt{d} \in \mathbb{Q}(\zeta_n)$ is handled similarly, using the identity $\sqrt{\gamma} = s\big(b/(2\sqrt{d}) + \sqrt{d}\sqrt{\Delta_K}\big)$, where $s \in \{-1, +1\}$. □

4.3. **Wagstaff sums.** Let h, m, t be positive integers. Define the *Wagstaff sum* [18]

$$S_{h,m}(t) := \sum_{\substack{n=1 \\ m \mid nt}}^{\infty} \frac{\mu(n)(nt, h)}{\varphi(nt)nt}.$$

(We adopt a notation different from [18] since we are mostly interested in considering the Wagstaff sum as a function of t, for fixed h and m.) In this section, we provide an explicit formula for $S_{h,m}(t)$ as a product involving the Artin constant, a multiplicative function, and a periodic function, with both these functions having rational values. Formulas for $S_{h,m}(t)$ as a rational multiple of the Artin constant were already proved by Wagstaff [18] (see also [11, Section 3]), and our result can be deduced from them. However, we believe it is easier to give an independent proof. Let

$$B_h := 2\prod_{\substack{p>2 \\ p \mid h}}\left(1 - \frac{p-1}{p^2 - p - 1}\right) \quad \text{and} \quad f_h(t, n) := \frac{(nt, h)\varphi(t)}{(t, h)\varphi(nt)n},$$

for every positive integer n. Note that $f_h(t, \cdot)$ is a multiplicative function and

$$f_h(t, p) = \begin{cases} p^{-1} & \text{if } p \mid t \text{ and } \nu_p(t) < \nu_p(h); \\ p^{-2} & \text{if } p \mid t \text{ and } \nu_p(t) \geq \nu_p(h); \\ (p-1)^{-1} & \text{if } p \nmid t \text{ and } p \mid h; \\ (p(p-1))^{-1} & \text{if } p \nmid t \text{ and } p \nmid h; \end{cases}$$

for each prime number p. Furthermore, put

$$F_h(t) := \frac{(t, h)}{\varphi(t)t}\widetilde{F}_h(t) \quad \text{and} \quad \widetilde{F}_h(t) := \prod_{\substack{p>2 \\ p \mid t}}\left(1 - \frac{(pt, h)}{p^2(t, h)}\right)\left(1 - \frac{(p, h)}{p(p-1)}\right)^{-1}.$$

Note that $F_h(\cdot)$ is a multiplicative function. Finally, let $G_{h,m}(t) := \widetilde{G}_{h,m/(m,t)}(t)$ and

$$\widetilde{G}_{h,m}(t) := |\mu(m)| \prod_{\substack{p>2 \\ p \mid m}}\left(1 - \frac{1}{f_h(t, p)}\right)^{-1} \cdot \begin{cases} 1 - f_h(t, 2) & \text{if } 2 \nmid m; \\ -f_h(t, 2) & \text{if } 2 \mid m. \end{cases}$$

Note that $G_{h,m}(\cdot)$ is a periodic function. Indeed, on the one hand, $m' := m/(m,t)$ depends only on the residue class of t modulo m. On the other hand, for every t in a fixed residue class modulo m (so that m' is constant), we have that $G_{h,m}(t) = \widetilde{G}_{h,m'}(t)$ depends only on the values $f_h(t,p)$, where $p \mid 2m'$, and each of these values depends only on the residue class of t modulo $p^{\nu_p(h)}$. In particular, the length of the period of $G_{h,m}(\cdot)$ is not exceeding the least common multiple of $2m$ and h.

Lemma 4.12. *We have that*

$$S_{h,m}(t) = A\, B_h\, F_h(t)\, G_{h,m}(t),$$

for all positive integers h, m, t.

Proof. For each prime number $p > 2$, put

$$g_h(p) := \begin{cases} \big(1 - (p-1)^{-1}\big)^{-1} & \text{if } p \mid h; \\ \big(1 - (p(p-1))^{-1}\big)^{-1} & \text{if } p \nmid h. \end{cases}$$

Since $f_h(t,\cdot)$ is multiplicative, we have that

$$\begin{aligned} T_h(t) &:= \sum_{\substack{n=1 \\ 2\nmid n}}^{\infty} \mu(n) f_h(t,n) = \prod_{p>2} \big(1 - f_h(t,p)\big) \\ &= \prod_{\substack{p>2 \\ p\nmid t,\, p\nmid h}} \left(1 - \frac{1}{p(p-1)}\right) \prod_{\substack{p>2 \\ p\nmid t,\, p\mid h}} \left(1 - \frac{1}{p-1}\right) \prod_{\substack{p>2 \\ p\mid t}} \big(1 - f_h(t,p)\big) \\ &= \prod_{\substack{p>2 \\ p\nmid h}} \left(1 - \frac{1}{p(p-1)}\right) \prod_{\substack{p>2 \\ p\mid h}} \left(1 - \frac{1}{p-1}\right) \prod_{\substack{p>2 \\ p\mid t}} \big(1 - f_h(t,p)\big) g_h(p) \\ &= \prod_{p>2} \left(1 - \frac{1}{p(p-1)}\right) \prod_{\substack{p>2 \\ p\mid h}} \left(1 - \frac{1}{p-1}\right) \left(1 - \frac{1}{p(p-1)}\right)^{-1} \widetilde{F}_h(t) \\ &= A\, B_h\, \widetilde{F}_h(t). \end{aligned}$$

Consequently, letting

$$\widetilde{S}_{h,m}(t) := \sum_{\substack{n=1 \\ m\mid n}}^{\infty} \mu(n) f_h(t,n),$$

we get that

$$\widetilde{S}_{h,1}(t) = T_h(t)\big(1 - f_h(t,2)\big) = A\, B_h\, \widetilde{F}_h(t)\big(1 - f_h(t,2)\big) \tag{9}$$

and

$$\widetilde{S}_{h,2}(t) = \widetilde{S}_{h,1}(t) - T_h(t) = A\, B_h\, \widetilde{F}_h(t) \cdot \big(-f_h(t,2)\big). \tag{10}$$

If m is not squarefree, then it is clear that $\widetilde{S}_{h,m}(t) = 0$. Suppose that m is squarefree and that p is an odd prime factor of m. Then

$$\begin{aligned} \widetilde{S}_{h,m}(t) &= \sum_{\substack{n'=1 \\ m/p\mid n',\, p\nmid n'}}^{\infty} \mu(pn') f_h(t,pn') = -f_h(t,p) \sum_{\substack{n'=1 \\ m/p\mid n',\, p\nmid n'}}^{\infty} \mu(n') f_h(t,n') \\ &= -f_h(t,p) \sum_{\substack{n'=1 \\ m/p\mid n',\, m\nmid n'}}^{\infty} \mu(n') f_h(t,n') = -f_h(t,p)\big(\widetilde{S}_{h,m/p}(t) - \widetilde{S}_{h,m}(t)\big), \end{aligned}$$

from which it follows that

$$\widetilde{S}_{h,m}(t) = \widetilde{S}_{h,m/p}(t)\left(1 - \frac{1}{f_h(t,p)}\right)^{-1}. \tag{11}$$

Therefore, from (9), (10), and (11), we get that

$$\widetilde{S}_{h,m}(t) = A\, B_h\, \widetilde{F}_h(t)\, \widetilde{G}_{h,m}(t).$$

In conclusion, by noticing that

$$S_{h,m}(t) = \frac{(t,h)}{\varphi(t)t}\widetilde{S}_{h,m/(m,t)}(t),$$

the claim follows. □

4.4. **Proof of Theorem 1.2.** The main ideas of the proof are the following. First, by employing the expressions provided by Lemma 4.10 for the degree of the extension $K_n/K(\zeta_n)$ and for the cardinality of the conjugacy class C_n, each term of the infinite series (1) that defines $\delta_{\boldsymbol{u}}(t)$ is written as a $\mathbb{Q}$-linear combination of characteristic functions of $m_i\mathbb{Z}$, for certain integers $m_1, \dots, m_k$. In particular, by Lemma 4.1(i), Lemma 4.6, and Lemma 4.5, the integers $m_1, \dots, m_k$ and the coefficients of the linear combination are completely determined by a_1 and a_2. Then, this linear combination is plugged into the series (1) and, after a few manipulations, the series is written as a linear combination of Wagstaff sums, which are finally computed with the tools developed in Section 4.3, thus obtaining the desired result.

We employ the same notation of Section 3.2. Furthermore, we assume that $\Delta_K \notin \{-3, -4\}$, in order to apply to K the results of Section 4.2. By Lemma 4.9, there exists $s \in \{-1, +1\}$, a positive integer h, and $\gamma_0 \in K$ which is not a power in K, such that $\gamma = s\gamma_0^h$. For every positive integer n, we have that

$$[K_n : \mathbb{Q}] = [K_n : K(\zeta_n)][K(\zeta_n) : \mathbb{Q}] = [K_n : K(\zeta_n)]\,\varphi(n)\begin{cases} 2 & \text{if } \sqrt{\Delta_K} \notin \mathbb{Q}(\zeta_n); \\ 1 & \text{otherwise.} \end{cases}$$

Note that Lemmas 4.1(i), 4.6, and 4.5, make possible to rewrite the conditions (C1)–(C4) of Lemma 4.10 in terms of n being, or not being, divisible by certain integers, which are determined by s, h, γ_0, and Δ_K, which in turn are determined by a_1 and a_2. For example, suppose that $s = -1$, $h = 3$, and $\gamma_0 = a + b\sqrt{\Delta_K}$ for some given $a, b \in \mathbb{Q}$. Then, with the notation of Lemma 4.10, we have that $s^{n'} = 1$ if and only if $4 \mid n$, while $\gamma_0^{h'} \in K(\zeta_n)^2$ if and only if either $2 \mid h'$, or $2 \nmid h'$ and $\gamma_0 \in K(\zeta_n)^2$. In turn, $2 \nmid h'$ is equivalent to $2 \mid n$; while, by using Lemmas 4.1(i), 4.6, and 4.5, the condition $\gamma_0 \in K(\zeta_n)^2$ is equivalent to n being divisible by integers depending on a, b, and Δ_K. Similarly, using Lemma 4.11, the conditions (D1)–(D5) of Lemma 4.10 can be rewritten in terms of n being, or not being, divisible by certain integers, which are determined by a_1 and a_2. (See Section 5 for more details on how to practically obtain these conditions of divisibility).

Consequently, there exist $c_1, \dots, c_k \in \mathbb{Q}$ and $m_1, \dots, m_k \in \mathbb{Z}^+$, depending only on a_1 and a_2, such that

$$\frac{\#C_n}{[K_n : \mathbb{Q}]} = \frac{(n, 2h)}{\varphi(n)n}\sum_{i=1}^{k} c_i \chi_{m_i}(n), \tag{12}$$

for every positive integer n, where $\chi_m(\cdot)$ is the characteristic function of $m\mathbb{Z}$. For every positive integer t, let

$$G_{\boldsymbol{u}}(t) := B_{2h}\sum_{i=1}^{k} c_i G_{2h,m_i}(t). \tag{13}$$

Note that $G_{\boldsymbol{u}}(\cdot)$ is a periodic function, since it is a linear combination of the periodic functions $G_{2h,m_i}(\cdot)$. Furthermore, given $\boldsymbol{u}$ (that is, given a_1 and a_2), we have that B_{2h}, $c_1, \dots, c_k$,

$m_1, \dots, m_k$, and the periods of the functions $G_{2h,m_i}(\cdot)$, can be all computed explicitly, so that $G_{\boldsymbol{u}}(\cdot)$ is effectively computable. Then, by (1), (12), and Lemma 4.12, we get that

$$\delta_{\boldsymbol{u}}(t) := \sum_{n=1}^{\infty} \frac{\mu(n)\,\#C_{nt}}{[K_{nt}:\mathbb{Q}]} = \sum_{n=1}^{\infty} \frac{\mu(n)(nt,2h)}{\varphi(nt)nt} \sum_{i=1}^{k} c_i \chi_{m_i}(nt) = \sum_{i=1}^{k} c_i \sum_{\substack{n=1 \\ m_i \mid nt}}^{\infty} \frac{\mu(n)(nt,2h)}{\varphi(nt)nt}$$

$$= \sum_{i=1}^{k} c_i S_{2h,m_i}(t) = AB_{2h}\, F_{2h}(t) \sum_{i=1}^{k} c_i G_{2h,m_i}(t) = A\, F_{2h}(t)\, G_{\boldsymbol{u}}(t),$$

for every positive integer t. The proof is complete.

5. Examples

We employ the same notation of Section 3.2. We provide only the main details and leave the rest of the computations to the reader.

5.1. **Fibonacci numbers (Example 1.1).** Let $a_1 = a_2 = 1$, so that $\boldsymbol{u}$ is the sequence of Fibonacci numbers. Then $K = \mathbb{Q}(\sqrt{5})$, $s = -1$, $h = 2$, and $\gamma_0 = \frac{1}{2} + \frac{1}{2}\sqrt{5}$. Since $\mathrm{N}_K(\gamma_0) = -1$, it follows from Lemma 4.6 that, for every positive integer n, neither $\sqrt{\gamma_0}$ nor $\sqrt{2\gamma_0}$ belongs to $K(\zeta_n)$. This implies that (C2) and (C4) cannot occur. Moreover, with the aid of Lemma 4.5 and Lemma 4.1(i), we get that (C3) cannot occur. Furthermore, with the notation of Lemma 4.10, we have that $\sigma_1(\gamma_0)\gamma_0 = |\gamma_0|^2$ is not a root of unity and, if $\sqrt{5} \notin \mathbb{Q}(\zeta_n)$, then $\sigma_2(\gamma_0) = -\gamma_0^{-1}$. Therefore, Lemma 4.10 yields that

$$[K_n:\mathbb{Q}] = \frac{\varphi(n)n}{(n,4)} \cdot \begin{cases} 2 & \text{if } 2 \mid n \\ 1 & \text{if } 2 \nmid n \end{cases} \cdot \begin{cases} 1 & \text{if } 5 \mid n \\ 2 & \text{if } 5 \nmid n \end{cases}$$

and

$$\#C_n = \begin{cases} 2 & \text{if } 4 \nmid n \text{ and } 5 \nmid n; \\ 1 & \text{otherwise.} \end{cases}$$

Consequently, we have that

$$\frac{\#C_n}{[K_n:\mathbb{Q}]} = \frac{(n,4)}{\varphi(n)n} \left(\chi_1(n) - \tfrac{1}{2}\chi_2(n) - \tfrac{1}{4}\chi_4(n) + \tfrac{1}{4}\chi_{20}(n)\right)$$

At this point, the claim follows from (12) and (13).

5.2. **Example 1.2.** Let $a_1 = 4$ and $a_2 = -1$. Then $K = \mathbb{Q}(\sqrt{3})$, $s = 1$, $h = 2$, and $\gamma_0 = 2+\sqrt{3}$. Since $\mathrm{N}_K(\gamma_0) = 1$, by Lemma 4.6 and Lemma 4.1(i), we have that $\sqrt{\gamma_0} \in K(\zeta_n)$ if and only if $8 \mid n$, for every positive integer n. With some patience, one can work out that the conditions of Lemma 4.10 are equivalent to the following:

(C1′) $2 \nmid n$;

(C2′) $\nu_2(n) = 1$ or $8 \mid n$;

(C3′) $\perp$;

(C4′) $\perp$;

(D1′) $2 \nmid n$;

(D2′) $\nu_2(n) = 1$;

(D3′) $\perp$;

(D4′) $\perp$;

(D5′) $\nu_2(n) = 2$ and $3 \nmid n$;

where $\perp$ denotes a condition that is never satisfied. Consequently, one gets that

$$\frac{\#C_n}{[K_n:\mathbb{Q}]} = \frac{(n,4)}{\varphi(n)n}\left(\chi_1(n) - \tfrac{1}{2}\chi_4(n) + \tfrac{1}{2}\chi_{24}(n)\right).$$

Then the claim follows from (12) and (13).

5.3. **Example 1.3.** Let $a_1 = 10$ and $a_2 = 2$. Then $K = \mathbb{Q}(\sqrt{3})$, $s = -1$, $h = 3$, and $\gamma_0 = 2+\sqrt{3}$. With some effort, one finds that the conditions of Lemma 4.10 are equivalent to the following:

(C1″) $2 \nmid n$;

(C2″) $8 \mid n$;

(C3″) $\perp$;

(C4″) $\perp$;

(D1″) $2 \nmid n$;

(D2″) $\perp$;

(D3″) $\perp$;

(D4″) $\perp$;

(D5″) $\nu_2(n) = 1$, or $\nu_2(n) = 2$ and $3 \nmid n$.

Consequently, one gets that

$$\frac{\#C_n}{[K_n:\mathbb{Q}]} = \frac{(n,6)}{\varphi(n)n}\left(\chi_1(n) - \tfrac{1}{2}\chi_2(n) + \tfrac{1}{2}\chi_{24}(n)\right).$$

Then the claim follows from (12) and (13).

6. Tables

In Tables 1, 2, and 3, we provide a comparison of the value of $\delta_{\boldsymbol{u}}(t)$ given by Theorem 1.2 with the empirical value $\widetilde{\delta}_{\boldsymbol{u}}(t) := \mathcal{P}_{\boldsymbol{u}}(t, p_{10^6})/10^6$, where p_n denotes the nth prime number, for each of the Lucas sequences $\boldsymbol{u}$ of the Examples 1.1, 1.2, and 1.3, respectively. As it can be seen, the theorical and empirical values are in agreement.

Acknowledgments

The author is very grateful to the anonymous referee for providing many useful suggestions that greatly improved the quality of the paper.

Statements and declarations

Competing interests. The author has no conflicts of interest to declare that are relevant to the content of this article.

Financial interests. The author has no relevant financial or non-financial interests to disclose.

References

[1] B. J. Birch, *Cyclotomic fields and Kummer extensions*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 85–93.

[2] P. S. Bruckman and P. G. Anderson, *Conjectures on the Z-densities of the Fibonacci sequence*, Fibonacci Quart. **36** (1998), no. 3, 263–271.

[3] P. Cubre and J. Rouse, *Divisibility properties of the Fibonacci entry point*, Proc. Amer. Math. Soc. **142** (2014), no. 11, 3771–3785.

[4] J.-M. De Koninck and F. Luca, *Analytic number theory*, Graduate Studies in Mathematics, vol. 134, American Mathematical Society, Providence, RI, 2012, Exploring the anatomy of integers.

[5] C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math. **225** (1967), 209–220.

[6] T. W. Hungerford, *Algebra*, Graduate Texts in Mathematics, vol. 73, Springer-Verlag, New York-Berlin, 1980, Reprint of the 1974 original. MR 600654
[7] G. Karpilovsky, *Topics in field theory*, North-Holland Mathematics Studies, vol. 155, North-Holland Publishing Co., Amsterdam, 1989, Notas de Matemática [Mathematical Notes], 124.
[8] H. W. Lenstra, Jr., P. Stevenhagen, and P. Moree, *Character sums for primitive root densities*, Math. Proc. Cambridge Philos. Soc. **157** (2014), no. 3, 489–511.
[9] P. Moree, *Asymptotically exact heuristics for (near) primitive roots*, J. Number Theory **83** (2000), no. 1, 155–181.
[10] P. Moree, *Asymptotically exact heuristics for (near) primitive roots. II*, Japan. J. Math. (N.S.) **29** (2003), no. 2, 143–157.
[11] P. Moree, *Near-primitive roots*, Funct. Approx. Comment. Math. **48** (2013), no. part 1, 133–145.
[12] M. R. Murty and V. K. Murty, *Non-vanishing of L-functions and applications*, Modern Birkhäuser Classics, Birkhäuser/Springer Basel AG, Basel, 1997, [2011 reprint of the 1997 original].
[13] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, third ed., Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2004.
[14] P. Ribenboim, *My numbers, my friends*, Springer-Verlag, New York, 2000, Popular lectures on number theory.
[15] C. Sanna, *On the divisibility of the rank of appearance of a Lucas sequence*, Int. J. Number Theory **18** (2022), no. 10, 2145–2156.
[16] A. Schinzel, *A refinement of a theorem of Gerst on power residues*, Acta Arith. **17** (1970), 161–168.
[17] P. Sgobba, *On the distribution of the order and index for the reductions of algebraic numbers*, J. Number Theory **223** (2021), 132–152.
[18] S. S. Wagstaff, Jr., *Pseudoprimes and a generalization of Artin's conjecture*, Acta Arith. **41** (1982), no. 2, 141–150.
[19] V. Ziegler, *On the distribution of the order of number field elements modulo prime ideals*, Unif. Distrib. Theory **1** (2006), no. 1, 65–85.

t	$\delta_{\boldsymbol{u}}(t)$	$\widetilde{\delta}_{\boldsymbol{u}}(t)$	error	t	$\delta_{\boldsymbol{u}}(t)$	$\widetilde{\delta}_{\boldsymbol{u}}(t)$	error
1	0.373956	0.374149	0.052%	21	0.001588	0.001621	2.053%
2	0.285387	0.285535	0.052%	22	0.002597	0.002563	1.294%
3	0.066481	0.066427	0.081%	23	0.000739	0.000742	0.391%
4	0.066426	0.066530	0.156%	24	0.002952	0.002955	0.092%
5	0.018895	0.018834	0.321%	25	0.000756	0.000752	0.501%
6	0.050736	0.050770	0.068%	26	0.001830	0.001795	1.929%
7	0.008935	0.008883	0.579%	27	0.000821	0.000879	7.097%
8	0.016607	0.016649	0.255%	28	0.001587	0.001497	5.676%
9	0.007387	0.007456	0.937%	29	0.000461	0.000461	0.096%
10	0.009447	0.009511	0.674%	30	0.001680	0.001678	0.091%
11	0.003402	0.003362	1.188%	31	0.000402	0.000412	2.458%
12	0.011809	0.011720	0.755%	32	0.001038	0.001012	2.497%
13	0.002398	0.002453	2.279%	33	0.000605	0.000597	1.302%
14	0.006819	0.006839	0.299%	34	0.001049	0.001028	2.044%
15	0.003359	0.003316	1.281%	35	0.000451	0.000486	7.656%
16	0.004152	0.004080	1.726%	36	0.001312	0.001310	0.162%
17	0.001375	0.001390	1.081%	37	0.000281	0.000260	7.392%
18	0.005637	0.005641	0.066%	38	0.000835	0.000876	4.961%
19	0.001094	0.001096	0.219%	39	0.000426	0.000458	7.418%
20	0.007085	0.007095	0.134%	40	0.001771	0.001766	0.303%

TABLE 1. Comparison of $\delta_{\boldsymbol{u}}(t)$ and $\widetilde{\delta}_{\boldsymbol{u}}(t)$ for $a_1 = 1$ and $a_2 = 1$.

t	$\delta_{\boldsymbol{u}}(t)$	$\widetilde{\delta}_{\boldsymbol{u}}(t)$	error	t	$\delta_{\boldsymbol{u}}(t)$	$\widetilde{\delta}_{\boldsymbol{u}}(t)$	error
1	0.000000	0.000000	0.000%	21	0.000000	0.000000	0.000%
2	0.560934	0.561025	0.016%	22	0.005104	0.005157	1.045%
3	0.000000	0.000000	0.000%	23	0.000000	0.000000	0.000%
4	0.149582	0.149481	0.068%	24	0.012465	0.012304	1.293%
5	0.000000	0.000000	0.000%	25	0.000000	0.000000	0.000%
6	0.099722	0.099698	0.024%	26	0.003598	0.003597	0.014%
7	0.000000	0.000000	0.000%	27	0.000000	0.000000	0.000%
8	0.028047	0.028217	0.607%	28	0.003574	0.003516	1.620%
9	0.000000	0.000000	0.000%	29	0.000000	0.000000	0.000%
10	0.028342	0.028577	0.829%	30	0.005039	0.005052	0.267%
11	0.000000	0.000000	0.000%	31	0.000000	0.000000	0.000%
12	0.016620	0.016633	0.077%	32	0.001753	0.001770	0.974%
13	0.000000	0.000000	0.000%	33	0.000000	0.000000	0.000%
14	0.013402	0.013374	0.210%	34	0.002063	0.002128	3.166%
15	0.000000	0.000000	0.000%	35	0.000000	0.000000	0.000%
16	0.007012	0.007062	0.718%	36	0.001847	0.001930	4.511%
17	0.000000	0.000000	0.000%	37	0.000000	0.000000	0.000%
18	0.011080	0.011106	0.233%	38	0.001640	0.001595	2.768%
19	0.000000	0.000000	0.000%	39	0.000000	0.000000	0.000%
20	0.007558	0.007560	0.029%	40	0.001417	0.001418	0.064%

TABLE 2. Comparison of $\delta_{\boldsymbol{u}}(t)$ and $\widetilde{\delta}_{\boldsymbol{u}}(t)$ for $a_1 = 4$ and $a_2 = -1$.

t	$\delta_{\boldsymbol{u}}(t)$	$\widetilde{\delta}_{\boldsymbol{u}}(t)$	error	t	$\delta_{\boldsymbol{u}}(t)$	$\widetilde{\delta}_{\boldsymbol{u}}(t)$	error
1	0.224373	0.224381	0.003%	21	0.004765	0.004761	0.088%
2	0.168280	0.168315	0.021%	22	0.001531	0.001548	1.104%
3	0.199443	0.199323	0.060%	23	0.000443	0.000446	0.572%
4	0.056093	0.056196	0.183%	24	0.018698	0.018774	0.408%
5	0.011337	0.011407	0.620%	25	0.000453	0.000455	0.337%
6	0.149582	0.149463	0.080%	26	0.001079	0.001082	0.254%
7	0.005361	0.005354	0.128%	27	0.002462	0.002485	0.924%
8	0.000000	0.000000	0.000%	28	0.001340	0.001352	0.880%
9	0.022160	0.022184	0.107%	29	0.000276	0.000290	4.946%
10	0.008503	0.008521	0.217%	30	0.007558	0.007623	0.862%
11	0.002041	0.002023	0.904%	31	0.000241	0.000230	4.671%
12	0.024930	0.024918	0.050%	32	0.000000	0.000000	0.000%
13	0.001439	0.001428	0.765%	33	0.001815	0.001792	1.247%
14	0.004021	0.003973	1.185%	34	0.000619	0.000663	7.141%
15	0.010077	0.010214	1.358%	35	0.000271	0.000285	5.219%
16	0.000000	0.000000	0.000%	36	0.002770	0.002769	0.038%
17	0.000825	0.000860	4.232%	37	0.000168	0.000180	6.855%
18	0.016620	0.016679	0.353%	38	0.000492	0.000478	2.870%
19	0.000656	0.000627	4.445%	39	0.001279	0.001292	1.007%
20	0.002834	0.002852	0.628%	40	0.000000	0.000000	0.000%

TABLE 3. Comparison of $\delta_{\boldsymbol{u}}(t)$ and $\widetilde{\delta}_{\boldsymbol{u}}(t)$ for $a_1 = 10$ and $a_2 = 2$.

Department of Mathematical Sciences, Politecnico di Torino
Corso Duca degli Abruzzi 24, 10129 Torino, Italy
Email address: carlo.sanna@polito.it