On the divisibility of the rank of appearance of a Lucas sequence

ON THE DIVISIBILITY OF THE RANK OF APPEARANCE OF A LUCAS SEQUENCE

CARLO SANNA†

Abstract. Let $U = (U_n)_{n\geq 0}$ be a Lucas sequence and, for every prime number p, let $\rho_U(p)$ be the rank of appearance of p in U, that is, the smallest positive integer k such that p divides U_k, whenever it exists. Furthermore, let d be an odd positive integer. Under some mild hypotheses, we prove an asymptotic formula for the number of primes $p \leq x$ such that d divides $\rho_U(p)$, as $x \to +\infty$.

1. Introduction

Let $(U_n)_{n\geq 0}$ 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, a_2 are fixed nonzero integers. The *rank of appearance* of a prime number p, denoted by $\rho_U(p)$, is the smallest positive integer k such that $p \mid U_k$. It can be easily seen that $\rho_U(p)$ exists whenever $p \nmid a_2$. Define

$$\mathcal{R}_U(d; x) := \#\big\{p \leq x : p \nmid a_2,\, d \mid \rho_U(p)\big\},$$

for every positive integer d and for every $x > 1$.

Let $(F_n)_{n\geq 0}$ be the Lucas sequence of Fibonacci numbers, corresponding to $a_1 = a_2 = 1$. In 1985, Lagarias [5] (see [6] for a correction and [8, 10] for generalizations) showed that $\mathcal{R}_F(2; x) \sim \frac{2}{3}x$, as $x \to +\infty$. More recently, Cubre and Rouse [2], settling a conjecture of Bruckman and Anderson [1], proved that $\mathcal{R}_F(d; x) \sim \mathrm{c}(d)\, d^{-1} \prod_{p\mid d}\big(1 - p^{-2}\big)^{-1}$, as $x \to +\infty$, for every positive integer d, where $\mathrm{c}(d)$ is equal to 1, $\frac{5}{4}$, or $\frac{1}{2}$, whenever $10 \nmid d$, $d \equiv 10 \pmod{20}$, or $20 \mid d$, respectively.

Let α, β be the roots of the characteristic polynomial $f_U(X) := X^2 - a_1 X - a_2$, and assume that $\gamma := \alpha/\beta$ is not a root of unity. Let $\Delta := a_1^2 + 4a_2$ be the discriminant of $f_U(X)$, and let Δ_0 be the squarefree part of Δ. Assume that Δ is not a square, so that $K := \mathbb{Q}\big(\sqrt{\Delta}\big)$ is a quadratic number field. Let h be the greatest positive integer such that γ is a hth power in K.

Our result is the following:

Theorem 1.1. *Let d be an odd positive integer with $3 \nmid d$ whenever $\Delta_0 = -3$. Then, for every $x > \exp\big(Be^{8\omega(d)} d^8\big)$, we have*

$$\mathcal{R}_U(d; x) = \delta_U(d)\,\mathrm{Li}(x) + O_U\!\left(\frac{(\omega(d)+1)d}{\varphi(d)} \cdot \frac{x\,(\log\log x)^{\omega(d)}}{(\log x)^{9/8}}\right),$$

where $B > 0$ is an absolute constant and

$$\delta_U(d) := \frac{1}{d}\left(\frac{1}{(d^\infty, h)} + \eta_U(d)\right) \prod_{p\,\mid\, d}\left(1 - \frac{1}{p^2}\right)^{-1},$$

with $\eta_U(d) := 0$ if $\Delta > 0$ or $\Delta_0 \not\equiv 1 \pmod 4$ or $\Delta_0 \nmid d^\infty$; and

$$\eta_U(d) := \frac{(d^\infty, h)}{\big[(d^\infty, h), \Delta_0/(d, \Delta_0)\big]^2}$$

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

Key words and phrases. Lucas sequence; rank of appearance.

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

otherwise.

Cubre and Rouse's proof of the asymptotic formula for $\mathcal{R}_F(d;x)$ relies on the study of the algebraic group $G : x^2 - 5y^2 = 1$ and relates $\rho_F(p)$ with the order of $(3/2, 1/2) \in G(\mathbb{F}_p)$. Instead, our proof of Theorem 1.1 is an adaptation of the methods that Moree [9] used to prove an asymptotic formula for the number of primes $p \leq x$ such that the multiplicative order of g modulo p is divisible by d, where $g \notin \{-1, 0, +1\}$ is a fixed rational number.

2. Acknowledgements

The author thanks Laura Capuano (Politecnico di Torino) for several helpful discussions concerning Lemma 5.5.

3. Notation

We employ the Landau–Bachmann "Big Oh" notation O, as well as the associated Vinogradov symbol $\ll$. Any dependence of the implied constants is explicitly stated or indicated with subscripts. In particular, notations like O_U and $\ll_U$ are shortcuts for O_{a_1,a_2} and $\ll_{a_1,a_2}$, respectively. For $x \geq 2$ we let $\operatorname{Li}(x) := \int_2^x \frac{\mathrm{d}t}{\log t}$ denote the logarithmic integral. We reserve the letter p for prime numbers. Given an integer d, we let d^∞ denote the supernatural number $\prod_{p \mid d} p^\infty$. Given a field F and a positive integer n, we write F^n for the set of nth powers of elements of F. Given a Galois extension E/F of number fields and a prime ideal P of $\mathcal{O}_E$ lying above an unramified prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$, we write $\left[\frac{E/F}{P}\right]$ for the Frobenius automorphism corresponding to $P/\mathfrak{p}$, that is, the unique element σ of the Galois group $\operatorname{Gal}(E/F)$ that satisfies $\sigma(a) \equiv a^{N(\mathfrak{p})} \pmod{P}$ for every $a \in \mathcal{O}_E$, where $N(\mathfrak{p})$ denotes the norm of $\mathfrak{p}$. Moreover, we let $\left[\frac{E/F}{\mathfrak{p}}\right]$ be the set of all $\left[\frac{E/F}{P}\right]$ with P prime ideal of $\mathcal{O}_E$ lying over $\mathfrak{p}$. We write $\Delta_{E/F}$ for the relative discriminant of E/F, and $\Delta_E := \Delta_{E/\mathbb{Q}}$ for the absolute discriminant of E. For every integer d and for every prime number p we let $\left(\frac{d}{p}\right)$ be the Legendre symbol. For every positive integer n, we let $\zeta_n := \mathrm{e}^{2\pi\mathbf{i}/n}$ be a primitive nth root of unity. We write $\omega(n)$, $\varphi(n)$, $\mu(n)$, and $\tau(n)$, for the number of prime factors, the totient function, the Möbius function, and the number of divisors of a positive integer n, respectively.

4. General preliminaries

Lemma 4.1. *Let n be a positive integer, let p be a prime number not dividing n, and let P be a prime ideal of $\mathcal{O}_{\mathbb{Q}(\zeta_n)}$ lying over p. Then ζ_n has multiplicative order modulo P equal to n.*

Proof. Let k be the multiplicative order of ζ_n modulo P, that is, k is the least positive integer such that $\zeta_n^k \equiv 1 \pmod{P}$. On the one hand, we have that $p \mid N(P) \mid N(\zeta_n^k - 1)$. On the other hand, since $\zeta_n^n \equiv 1 \pmod{P}$, we have that $k \mid n$, and consequently ζ_n^k is a mth primitive root of unity, where $m := n/k$. If $k < n$ then $m > 1$ and $N(\zeta_n^k - 1)$ is either 1 or a prime factor of m, but both cases are impossible since $p \nmid n$. Hence, $k = n$. □

Lemma 4.2. *Let F be a field, let $a \in F$, and let n be a positive integer. Then $X^n - a$ is irreducible over F if and only if $a \notin F^p$ for each prime p dividing n and $a \notin -4F^4$ whenever $4 \mid n$.*

Proof. See [4, Chapter 8, Theorem 1.6]. □

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

Proof. See [4, Chapter 8, Theorem 3.2]. □

Lemma 4.4. *Let n be an odd positive integer and let d be a squarefree integer. Then $\sqrt{d} \in \mathbb{Q}(\zeta_n)$ if and only if $d \mid n$ and $d \equiv 1 \pmod{4}$.*

Proof. See [12, Lemma 3]. □

We need the following form of the Chebotarev Density Theorem.

Theorem 4.5. *Let E/F be a Galois extension of numbers fields with Galois group G, and let C be the union of k conjugacy classes of G. Then*

$$\#\Big\{\mathfrak{p} \text{ prime ideal of } \mathcal{O}_F \text{ non-ramifying in } E : N_{F/\mathbb{Q}}(\mathfrak{p}) \leq x,\ \left[\tfrac{E/F}{\mathfrak{p}}\right] \subseteq C\Big\}$$
$$= \frac{\#C}{\#G} \cdot \mathrm{Li}(x) + O\Big(k\, x \exp\Big(-c_1 \big(\log x / n_E\big)^{1/2}\Big)\Big)$$

for every

$$x \geq \exp\Big(c_2 \max\Big(n_E (\log |\Delta_E|)^2, |\Delta_E|^{2/n_E}/n_E\Big)\Big),$$

where $n_E := [E : \mathbb{Q}]$ and $c_1, c_2 > 0$ are absolute constants.

Proof. The result follows from the effective form of the Chebotarev Density Theorem given by Lagarias and Odlyzko [7, Theorem 1.3] and from the bounds for the exceptional zero of the Dedekind zeta function ζ_E given by Stark [13, Lemma 8 and 11]. □

5. Preliminaries to the proof of Theorem 1.1

Recalling that h is the greatest positive integer such that γ is an hth power in K, write $\gamma = \gamma_0^h$ for some $\gamma_0 \in K$. Also, let $\sigma_K \in \mathrm{Gal}(K/\mathbb{Q})$ be the nontrivial automorphism, which satisfies $\sigma_K\big(\sqrt{\Delta}\,\big) = -\sqrt{\Delta}$. Note that, since $\gamma = \alpha/\beta$ and σ_K swaps α and β, we have that $\sigma_k(\gamma) = \gamma^{-1}$. For all positive integers d, n such that $d \mid n$, let $K_{n,d} := K\big(\zeta_n, \gamma^{1/d}\big)$.

Lemma 5.1. *Let p be a prime number not dividing $a_2\Delta$ and let π be a prime ideal of $\mathcal{O}_K$ lying over p. Then $\rho_U(p)$ is equal to the multiplicative order of γ modulo π. Moreover, $\rho_U(p)$ divides $p - \big(\frac{\Delta}{p}\big)$.*

Proof. First, note that $p \nmid a_2$ ensures that β is invertible modulo π, and consequently it makes sense to consider the multiplicative order of $\gamma = \alpha/\beta$ modulo π. Also, $p \nmid \Delta$ implies that p does not ramifies in K and that $\alpha \not\equiv \beta \pmod{\pi}$.

We shall prove that $p \mid U_n$ if and only if $\gamma^n \equiv 1 \pmod{\pi}$, for every positive integer n. Then the claim on $\rho_U(p)$ follows easily. It is well known that the Binet's formula

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \tag{1}$$

holds for every positive integer n. On the one hand, if $p \mid U_n$ then, since $p\mathcal{O}_K \subseteq \pi$ and (1), we have $\alpha^n \equiv \beta^n \pmod{\pi}$, and consequently $\gamma^n \equiv 1 \pmod{\pi}$. On the other hand, if $\gamma^n \equiv 1 \pmod{\pi}$ then by (1) we get $U_n \equiv 0 \pmod{\pi}$. If p is inert in K, then $p\mathcal{O}_K = \pi$ and so $p \mid U_n$. If p splits in K, then $p\mathcal{O}_K = \pi \cap \sigma_K(\pi)$. Thus $U_n \equiv 0 \pmod{\pi}$ and $U_n \equiv \sigma_K(U_k) \equiv 0 \pmod{\sigma_K(\pi)}$ imply that $p \mid U_n$.

Let $\sigma := \left[\frac{K/\mathbb{Q}}{\pi}\right]$. On the one hand, if $\big(\frac{\Delta}{p}\big) = -1$ then $\sigma = \sigma_K$ and $\gamma^{p+1} \equiv \sigma_K(\gamma)\gamma \equiv \gamma^{-1}\gamma \equiv 1 \pmod{\pi}$, so that $\rho_U(p) \mid p+1$. On the other hand, if $\big(\frac{\Delta}{p}\big) = +1$ then $\sigma = \mathrm{id}$ and $\gamma^{p-1} \equiv \gamma\gamma^{-1} \equiv 1 \pmod{\pi}$, so that $\rho_U(p) \mid p-1$. □

For each prime number p not dividing $a_2\Delta$, let us define the *index of appearance* of p as

$$\iota_U(p) := \big(p - \big(\tfrac{\Delta}{p}\big)\big)/\rho_U(p).$$

Note that, in light of Lemma 5.1, $\iota_U(p)$ is an integer.

Lemma 5.2. *Let d, n be positive integers such that $d \mid n$, and let p be a prime number not dividing $a_2\Delta$. Moreover, let P be a prime ideal of $\mathcal{O}_{K_{n,d}}$ lying over p and let $\sigma := \left[\frac{K_{n,d}/\mathbb{Q}}{P}\right]$. Then*

$$p \equiv \big(\tfrac{\Delta}{p}\big) \pmod{n} \quad \text{and} \quad d \mid \iota_U(p) \tag{2}$$

if and only if $\sigma = \mathrm{id}$ *or*

$$\sigma(\zeta_n) = \zeta_n^{-1} \quad \textit{and} \quad \sigma\big(\gamma^{1/d}\big) = \gamma^{-1/d}. \tag{3}$$

Proof. First, suppose that $\left(\frac{\Delta}{p}\right) = -1$. Let us assume (2). On the one hand, since $p \equiv -1 \pmod n$, we have

$$\sigma(\zeta_n) \equiv \zeta_n^p \equiv \zeta_n^{-1} \pmod P. \tag{4}$$

Since $\sigma(\zeta_n) = \zeta_n^k$ for some integer k, and since p does not divide n, Lemma 4.1 and (4) yield that $\sigma(\zeta_n) = \zeta_n^{-1}$.

On the other hand, $d \mid \iota_U(p)$ implies that $\rho_U(p) \mid (p+1)/d$. Hence, letting $\pi := P \cap \mathcal{O}_K$, Lemma 5.1 yields $\gamma^{(p+1)/d} \equiv 1 \pmod \pi$. Consequently,

$$\sigma\big(\gamma^{1/d}\big) \equiv \big(\gamma^{1/d}\big)^p \equiv \gamma^{(p+1)/d} \cdot \gamma^{-1/d} \equiv \gamma^{-1/d} \pmod P. \tag{5}$$

Note that, since $\left(\frac{\Delta}{p}\right) = -1$, we have

$$\sigma(\gamma) = \sigma|_K(\gamma) = \left[\tfrac{K/\mathbb{Q}}{\pi}\right](\gamma) = \sigma_K(\gamma) = \gamma^{-1},$$

so that $\sigma\big(\gamma^{1/d}\big) = \zeta_d^k \gamma^{-1/d}$ for some integer k. Thus Lemma 4.1 and (5) yield that $\sigma\big(\gamma^{1/d}\big) = \gamma^{-1/d}$. We have proved (3).

Now let us assume (3). On the one hand, we have

$$\zeta_n^{-1} = \sigma(\zeta_n) = \sigma|_{\mathbb{Q}(\zeta_n)}(\zeta_n) = \left[\frac{\mathbb{Q}(\zeta_n)/\mathbb{Q}}{P \cap \mathcal{O}_{\mathbb{Q}(\zeta_n)}}\right](\zeta_n) = \zeta_n^p,$$

so that $p \equiv -1 \pmod n$. On the other hand,

$$\gamma^{(p+1)/d} \equiv \big(\gamma^{1/d}\big)^p \cdot \gamma^{1/d} \equiv \sigma\big(\gamma^{1/d}\big) \cdot \gamma^{1/d} \equiv \gamma^{-1/d} \cdot \gamma^{1/d} \equiv 1 \pmod P,$$

so that $\gamma^{(p+1)/d} \equiv 1 \pmod \pi$, which, by Lemma 5.1, implies $d \mid \iota_U(p)$. We have proved (2).

If $\left(\frac{\Delta}{p}\right) = +1$ then the proof proceeds similarly to the case $\left(\frac{\Delta}{p}\right) = -1$, and yields that (2) is equivalent to $\sigma(\zeta_n) = \zeta_n$ and $\sigma\big(\gamma^{1/d}\big) = \gamma^{1/d}$, that is, $\sigma = \mathrm{id}$. ☐

Lemma 5.3. *The roots of unity contained in K are: the sixth roots of unity, if $\Delta_0 = -3$; the forth roots of unity, if $\Delta_0 = -1$; or the second roots of unity, if $\Delta_0 \neq -1, -3$.*

Proof. If $\zeta_n \in K$ for some positive integer n, then $\mathbb{Q}(\zeta_n) \subseteq K$, so that $\varphi(n) \leq 2$, and $n \in \{1, 2, 3, 4, 6\}$. Then the claim follows easily since $\zeta_3 = (-1 + \sqrt{-3})/2$, $\zeta_4 = \sqrt{-1}$, and $\zeta_6 = (1 + \sqrt{-3})/2$. ☐

Lemma 5.4. *Let n be an odd positive integer with $3 \nmid n$ whenever $\Delta_0 = -3$, and let d be a positive integer dividing n. Then $a \in K \cap K(\zeta_n)^d$ if and only if $a \in K^d$.*

Proof. The "if" part if obvious. Let us prove the "only if" part. Note that, by the hypothesis on n and by Lemma 5.3, the only nth root of unity in K is 1. Suppose that $a \in K \cap K(\zeta_n)^d$. Hence, there exists $b \in K(\zeta_n)$ such that $a = b^d$. Putting $a_1 := a^{n/d}$, we get that $a_1 = b^n$. Therefore, $K\big(\zeta_n, a_1^{1/n}\big) = K(\zeta_n, b) = K(\zeta_n)$ is an abelian extension of K. Consequently, by Lemma 4.3, we have $a_1 \in K^n$, that is, $a_1 = b_1^n$ for some $b_1 \in K$. Thus $a^n = a_1^d = b_1^{dn}$, so that $a = \zeta b_1^d$, where ζ is a nth root of unity in K. We already noticed that $\zeta = 1$, hence $a \in K^d$. ☐

Lemma 5.5. *Let n be an odd positive integer with $3 \nmid n$ whenever $\Delta_0 = -3$, and let d be a positive integer dividing n. Then*

$$[K_{n,d} : \mathbb{Q}] = \frac{\varphi(n) d}{(d, h)} \cdot \begin{cases} 1 & \textit{if } \sqrt{\Delta} \in \mathbb{Q}(\zeta_n), \\ 2 & \textit{if } \sqrt{\Delta} \notin \mathbb{Q}(\zeta_n), \end{cases} \tag{6}$$

while

$$|\Delta_{K_{n,d}}|^{1/[K_{n,d}:\mathbb{Q}]} \ll_U n^3 \quad \textit{and} \quad \log |\Delta_{K_{n,d}}| \ll_U n^2 \log(n+1). \tag{7}$$

Moreover, there exists $\sigma \in \mathrm{Gal}(K_{n,d}/\mathbb{Q})$ *satisfying* (3) *if and only if* $\sqrt{\Delta} \notin \mathbb{Q}(\zeta_n)$ *or* $\Delta < 0$. *In particular, if* σ *exists then it belongs to the center of* $\mathrm{Gal}(K_{n,d}/\mathbb{Q})$.

Proof. Let $d_0 := d/(d,h)$, $h_0 := h/(d,h)$, and $f(X) = X^{d_0} - \gamma_0^{h_0}$. Suppose that $\gamma_0^{h_0} \in K(\zeta_n)^p$ for some prime number p dividing d_0. Then, by Lemma 5.4, we have $\gamma_0^{h_0} \in K^p$. In turn, by the maximality of h, it follows that $p \mid h_0$, which is impossible, since $(d_0, h_0) = 1$. Hence, $\gamma_0^{h_0} \notin K(\zeta_n)^p$ for every prime number p dividing d_0. Consequently, by Lemma 4.2, f is irreducible over $K(\zeta_n)$. Thus $K_{n,d} \cong K(\zeta_n)[X]/(f(X))$, so that $[K_{n,d} : K(\zeta_n)] = d_0$ and $\left(\gamma^{1/d}\right)^{d_0} = \gamma_0^{h_0}$. It is easy to check that $[K(\zeta_n) : \mathbb{Q}] = \varphi(n)$ if $\sqrt{\Delta} \in \mathbb{Q}(\zeta_n)$, and $[K(\zeta_n) : \mathbb{Q}] = 2\varphi(n)$ otherwise. Hence, (6) follows.

Let s be a positive integer such that $s\gamma_0 \in \mathcal{O}_K$, and put $g(X) := s^{d_0} f(X/s) = X^{d_0} - s^{d_0}\gamma_0^{h_0}$. Since f is the minimal polynomial of $\gamma^{1/d}$ over $K(\zeta_n)$, we get that g is the minimal polynomial of $s\gamma^{1/d}$ over $K(\zeta_n)$. In particular, since $g \in \mathcal{O}_K[X]$, we have that $s\gamma^{1/d} \in \mathcal{O}_{K_{n,d}}$, . Hence, from $K_{n,d} = K(\zeta_n)\left(s\gamma^{1/d}\right)$ it follows that

$$\Delta_{K_{n,d}/K(\zeta_n)} \supseteq \operatorname{disc}(g)\, \mathcal{O}_{K(\zeta_n)} = \prod_{1 \le i < j \le d_0} \left(s\gamma^{1/d}\zeta_{d_0}^i - s\gamma^{1/d}\zeta_{d_0}^j\right)^2 \mathcal{O}_{K(\zeta_n)}$$
$$= \left(s\gamma^{1/d}\right)^{d_0(d_0-1)} d_0^{d_0} \mathcal{O}_{K(\zeta_n)} = \gamma_0^{h_0(d_0-1)} \left(s^{d_0-1}d_0\right)^{d_0} \mathcal{O}_{K(\zeta_n)},$$

and

$$N_{K(\zeta_n)/\mathbb{Q}}\left(\Delta_{K_{n,d}/K(\zeta_n)}\right) = N_{K/\mathbb{Q}}\left(\gamma_0^{h_0}\right)^{(d_0-1)[K(\zeta_n):K]} \left(s^{d_0-1}d_0\right)^{d_0[K(\zeta_n):\mathbb{Q}]} \mid \left(N_{K/\mathbb{Q}}(\gamma)sn\right)^\infty.$$

Also, a quick computation shows that $\Delta_{K(\zeta_n)} \mid (4\Delta n)^\infty$. Therefore, since

$$\Delta_{K_{n,d}} = \Delta_{K(\zeta_n)}^{[K_{n,d}:K(\zeta_n)]} N_{K(\zeta_n)/\mathbb{Q}}\left(\Delta_{K_{n,d}/K(\zeta_n)}\right),$$

we get that every prime factor of $\Delta_{K_{n,d}}$ divides An, where $A := 4\Delta N_{K/\mathbb{Q}}(\gamma)s$. By Hensel's estimate (see, e.g., [11, comments after Theorem 7.3]), we have that

$$|\Delta_L|^{1/n_L} \le n_L \prod_{p \,\mid\, \Delta_L} p,$$

for every Galois extension $L/\mathbb{Q}$ of degree n_L. Consequently,

$$|\Delta_{K_{n,d}}|^{1/[K_{n,d}:\mathbb{Q}]} \le [K_{n,d} : \mathbb{Q}]An \ll_U \varphi(n)dn \le n^3,$$

and

$$\log|\Delta_{K_{n,d}}| \le [K_{n,d} : \mathbb{Q}]\left(\log(n^3) + O_U(1)\right) \ll_U \varphi(n)d\log(n+1) \ll n^2\log(n+1),$$

so that (7) is proved.

Suppose that there exists $\sigma \in \mathrm{Gal}(K_{n,d}/\mathbb{Q})$ satisfying (3). We shall prove that $\sqrt{\Delta} \notin \mathbb{Q}(\zeta_n)$ or $\Delta < 0$. Assume that $\sqrt{\Delta} \in \mathbb{Q}(\zeta_n)$. On the one hand, $\sigma(\gamma) = \sigma\left(\gamma^{1/d}\right)^d = \gamma^{-1}$, and consequently $\sigma\left(\sqrt{\Delta}\right) = -\sqrt{\Delta}$. On the other hand, since $\sqrt{\Delta} \in \mathbb{Q}(\zeta_n)$ and $\sigma(\zeta_n) = \zeta_n^{-1}$, we have that $\sigma\left(\sqrt{\Delta}\right) = \overline{\sqrt{\Delta}}$. Therefore, $\overline{\sqrt{\Delta}} = -\sqrt{\Delta}$ and so $\Delta < 0$. Now let us check that σ belongs to the center of $\mathrm{Gal}(K_{n,d}/\mathbb{Q})$. Note that $N_{K/\mathbb{Q}}(\gamma) = \gamma\,\sigma_K(\gamma) = \gamma\gamma^{-1} = 1$. Also, $N_{K/\mathbb{Q}}(\gamma_0^{h_0}) = N_{K/\mathbb{Q}}(\gamma_0^h) = N_{K/\mathbb{Q}}(\gamma) = 1$, since d is odd and so $h_0 \equiv h \pmod 2$. Therefore, for every $\tau \in \mathrm{Gal}(K_{n,q}/\mathbb{Q})$, we have $\tau(\gamma_0^{h_0}) = \gamma_0^{h_0}$, if $\tau|_K = \mathrm{id}$, or $\tau(\gamma_0^{h_0}) = N_{K/\mathbb{Q}}(\gamma_0^{h_0})\gamma_0^{-h_0} = \gamma_0^{-h_0}$ if $\tau|_K = \sigma_K$. Consequently, recalling that $\left(\gamma^{1/d}\right)^{d_0} = \gamma_0^{h_0}$, we have that $\tau(\zeta_n) = \zeta_n^s$ and $\tau\left(\gamma^{1/d}\right) = \zeta_{d_0}^t\gamma^{\pm 1/d}$ for some integers s, t. At this point, it can be easily checked that $(\sigma\tau)(\zeta_n) = (\tau\sigma)(\zeta_n)$ and $(\sigma\tau)\left(\gamma^{1/d}\right) = (\tau\sigma)\left(\gamma^{1/d}\right)$. Hence, σ belongs to the center of $\mathrm{Gal}(K_{n,d}/\mathbb{Q})$.

Suppose that $\sqrt{\Delta} \notin \mathbb{Q}(\zeta_n)$ or $\Delta < 0$. We shall prove the existence of $\sigma \in \mathrm{Gal}(K_{n,d}/\mathbb{Q})$ satisfying (3). It suffices to show that there exists $\sigma_1 \in \mathrm{Gal}(K(\zeta_n)/K)$ such that $\sigma_1(\zeta_n) = \zeta_n^{-1}$

and $\sigma_1|_K = \sigma_K$. Indeed, recalling that $K_{n,d} \cong K(\zeta_n)[X]/(f(X))$, we can extend σ_1 to an automorphism $\sigma \in \mathrm{Gal}(K_{n,d}/\mathbb{Q})$ that sends the root $\gamma^{1/d}$ of f to the root $\gamma^{-1/d}$ of

$$(\sigma_1 f)(X) = X^{d_0} - \sigma_1(\gamma_0^{h_0}) = X^{d_0} - N_{K/\mathbb{Q}}(\gamma_0^{h_0})\gamma_0^{-h_0} = X^{d_0} - \gamma_0^{-h_0},$$

and so σ satisfies (3). Pick $\sigma_0 \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ such that $\sigma_0(\zeta_n) = \zeta_n^{-1}$. If $\sqrt{\Delta} \in \mathbb{Q}(\zeta_n)$ then $K(\zeta_n) = \mathbb{Q}(\zeta_n)$, $\Delta < 0$, and $\sigma_0(\sqrt{\Delta}) = \overline{\sqrt{\Delta}} = -\sqrt{\Delta}$, so we let $\sigma_1 := \sigma_0$. If $\sqrt{\Delta} \notin \mathbb{Q}(\zeta_n)$ then $X^2 - \Delta$ is the minimal polynomial of $\sqrt{\Delta}$ over $\mathbb{Q}(\zeta_n)$ and we can extend σ_0 to $\sigma_1 \in \mathrm{Gal}(K(\zeta_n)/\mathbb{Q})$ such that $\sigma_1(\sqrt{\Delta}) = -\sqrt{\Delta}$. □

6. Proof of Theorem 1.1

The proof proceeds similarly to [9, Section 2]. For all positive integers d, n with $d \mid n$, and for all $x > 1$, let us define

$$\pi_{U,n,d}(x) := \#\left\{p \leq x : p \nmid a_2\Delta,\ p \equiv \left(\tfrac{\Delta}{p}\right) \pmod{n},\ d \mid \iota_U(p)\right\}.$$

In what follows, we will tacitly ignore the finitely many prime numbers dividing $a_2\Delta$.

Lemma 6.1. *For every positive integer d and for every $x > 1$, we have*

$$\mathcal{R}_U(d; x) = \sum_{v \mid d^\infty} \sum_{a \mid d} \mu(a)\pi_{U,dv,av}(x). \tag{8}$$

Proof. Every prime number p counted by the inner sum of (8) satisfies $p \leq x$, $p \equiv \left(\frac{\Delta}{p}\right) \pmod{dv}$, and $\iota_U(p) = vw$ for some integer w. Writing $w = w_1 w_2$, with $w_1 := (w, d)$, we get that the contribution of p to the inner sum or (8) is equal to $\sum_{a \mid w_1} \mu(a)$. Hence,

$$\sum_{a \mid d} \mu(a)\pi_{U,dv,av}(x) = \#\left\{p \leq x : p \equiv \left(\tfrac{\Delta}{p}\right) \pmod{dv},\ v \mid \iota_U(p),\ \big(\iota_U(p)/v, d\big) = 1\right\}. \tag{9}$$

Now it suffices to show that

$$\mathcal{R}_U(d; x) = \sum_{v \mid d^\infty} \#\left\{p \leq x : p \equiv \left(\tfrac{\Delta}{p}\right) \pmod{dv},\ v \mid \iota_U(p),\ \big(\iota_U(p)/v, d\big) = 1\right\}. \tag{10}$$

On the one hand, let p be a prime number counted on the right-hand side of (10). Note that this is counted only one, namely for $v = (\iota_U(p), d^\infty)$. Then, from $\rho_U(p)\iota_U(p) = p - \left(\frac{\Delta}{p}\right)$, it follows that $d \mid \rho_U(p)$. Hence, p is counted on the left-hand side of (10).

On the other hand, let p be a prime number counted by $\mathcal{R}_U(d; x)$. Then $d \mid \rho_U(p)$ and, by Lemma 5.1, $p \equiv \left(\frac{\Delta}{p}\right) \pmod{d}$. Consequently, there is an integer v such that $v \mid d^\infty$, $p \equiv \left(\frac{\Delta}{p}\right) \pmod{dv}$, and $\big(\iota_U(p)/v, d\big) = 1$. Hence, p is counted on the right-hand side of (10). □

Lemma 6.2. *Let n be an odd positive integer with $3 \nmid n$ whenever $\Delta_0 = -3$, and let d be a positive integer dividing n. There exist absolute constants $A, B > 0$ such that*

$$\pi_{U,n,d}(x) = \delta_{U,n,d} \operatorname{Li}(x) + O_U\Big(x \exp\big(-A(\log x)^{1/2}/n\big)\Big)$$

for $x \geq \exp(Bn^8)$, where

$$\delta_{U,n,d} := \frac{(d,h)}{\varphi(n)d} \cdot \begin{cases} 1 & \text{if } \Delta > 0 \text{ or } \Delta_0 \not\equiv 1 \pmod{4} \text{ or } \Delta_0 \nmid n, \\ 2 & \text{otherwise.} \end{cases} \tag{11}$$

Proof. Put $E := K_{n,d}$, $F := \mathbb{Q}$, $G := \mathrm{Gal}(E/F)$, and $C = \{\mathrm{id}, \sigma\}$ if there exists $\sigma \in \mathrm{Gal}(K_{n,d}/\mathbb{Q})$ satisfying (3), or $C = \{\mathrm{id}\}$ otherwise. By Lemma 5.5, σ belongs to the center of G, so that C is the union of conjugacy classes of G. By Lemma 5.2, we have that $\pi_{U,n,d}(x)$ is the number of primes p not exceeding x and such that $\left[\frac{E/F}{p}\right] \subseteq C$. Thus, taking into account the bounds for the degree and the discriminant of E/F given in Lemma 5.5, and considering Lemma 4.4, the asymptotic formula follows by applying Theorem 4.5. □

Lemma 6.3. *Let d be an odd positive integer with $3 \nmid d$ whenever $\Delta_0 = -3$. If $x > 1$ and $e^{\omega(d)} \leq y \leq \log x / \varphi(d)$, then*

$$\sum_{\substack{v \mid d^\infty \\ v > y}} \sum_{a \mid d} \mu(a) \pi_{U,dv,av}(x) \ll \frac{x}{\log x} \cdot \frac{\omega(d)+1}{\varphi(d)} \cdot \frac{(\log y)^{\omega(d)}}{y} \tag{12}$$

and

$$\sum_{\substack{v \mid d^\infty \\ v > y}} \sum_{a \mid d} \mu(a) \delta_{U,dv,av} \ll_U \frac{\omega(d)+1}{\varphi(d)} \cdot \frac{(\log y)^{\omega(d)}}{y}.$$

Proof. Let $\pi(m, r; x) := \#\{p \leq x : p \equiv r \pmod m\}$. From (9) it follows that

$$\left| \sum_{a \mid d} \mu(a) \pi_{U,dv,av}(x) \right| \leq \pi_{U,dv,v}(x) \leq \pi(x; dv, \pm 1). \tag{13}$$

Moreover, letting $x \to +\infty$, Lemma 6.2 and the first inequality of (13) yield

$$\left| \sum_{a \mid d} \mu(a) \delta_{U,dv,av} \right| \leq \delta_{U,dv,v}. \tag{14}$$

Now we have $M_d(x) := \#\{v \leq x : v \mid d^\infty\} \ll (\log x)^{\omega(d)}$, for every $x \geq 2$. Hence, by partial summation and since $y \geq e^{\omega(d)}$, we obtain that

$$\sum_{\substack{v \mid d^\infty \\ v > y}} \frac{1}{v} = \frac{M_d(t)}{t} \bigg|_{t=y}^{+\infty} + \int_y^{+\infty} \frac{M_d(t)}{t^2}\, \mathrm{d}t \ll \int_y^{+\infty} \frac{(\log t)^{\omega(d)}}{t^2}\, \mathrm{d}t \leq \frac{(\omega(d)+1)(\log y)^{\omega(d)}}{y}. \tag{15}$$

On the one hand, using the Brun–Titchmarsh inequality [3, Theorem 12.7]

$$\pi(m, r; x) \ll \frac{x}{\varphi(m) \log(x/m)},$$

holding for $x > m$, and (15) we get that

$$\sum_{\substack{v \mid d^\infty \\ v > y,\, dv \leq x^{2/3}}} \pi(dv, \pm 1; x) \ll \frac{x}{\varphi(d) \log x} \sum_{\substack{v \mid d^\infty \\ v > y}} \frac{1}{v} \ll \frac{x}{\log x} \cdot \frac{\omega(d)+1}{\varphi(d)} \cdot \frac{(\log y)^{\omega(d)}}{y}. \tag{16}$$

On the other hand, using the trivial bound $\pi(m, \pm 1; x) \ll x/m$, holding for $x \geq 1$, and (15) again, we find that

$$\sum_{\substack{v \mid d^\infty \\ dv > x^{2/3}}} \pi(dv, \pm 1; x) \ll \sum_{\substack{v \mid d^\infty \\ dv > x^{2/3}}} \frac{x}{dv} \leq \sum_{\substack{w \mid d^\infty \\ w > x^{2/3}}} \frac{x}{w} \ll x^{1/3} (\omega(d)+1)(\log x)^{\omega(d)}. \tag{17}$$

Putting together (16), (17), and (13), taking into account that $\omega(d) \leq \log y$ and $\varphi(d) y \leq \log x$, we obtain (12). Finally, from (14), (11), and (15), we get

$$\sum_{\substack{v \mid d^\infty \\ v > y}} \sum_{a \mid d} \mu(a) \delta_{U,dv,av} \leq \sum_{\substack{v \mid d^\infty \\ v > y}} \delta_{U,dv,v} \ll_U \frac{1}{\varphi(d)} \sum_{\substack{v \mid d^\infty \\ v > y}} \frac{1}{v^2} \ll \frac{\omega(d)+1}{\varphi(d)} \cdot \frac{(\log y)^{\omega(d)}}{y},$$

as desired. □

Lemma 6.4. *Let d be an odd positive integer with $3 \nmid d$ whenever $\Delta_0 = -3$. Then*

$$\sum_{v \mid d^\infty} \sum_{a \mid d} \mu(a) \delta_{U,dv,av} = \delta_U(d).$$

Proof. For every integer e dividing d^∞, define

$$S_{d,e,h} := \sum_{\substack{v \,|\, d^\infty \\ e \,|\, v}} \sum_{a \,|\, d} \frac{\mu(a)(av,h)}{\varphi(dv)av}.$$

The value of $S_{d,1,h}$ was computed in [9, Lemma 4] and a slight modification of the proof (precisely, replacing (h, d^∞) with $[e, (h, d^\infty)]$ in the last equation) yields

$$S_{d,e,h} = \frac{(d^\infty, h)}{d\big[(d^\infty, h), e\big]^2} \prod_{p \,|\, d} \left(1 - \frac{1}{p^2}\right)^{-1}.$$

At this point, by (11) and considering that $\Delta_0 \mid dv$ if and only if $e \mid v$, where $e := \Delta_0/(d, \Delta_0)$, we have

$$\sum_{v \,|\, d^\infty} \sum_{a \,|\, d} \mu(a)\delta_{U,dv,av} = \begin{cases} S_{d,1,h} & \text{if } \Delta > 0 \text{ or } \Delta_0 \not\equiv 1 \pmod 4 \text{ or } \Delta_0 \nmid d^\infty \\ S_{d,1,h} + S_{d,e,h} & \text{otherwise} \end{cases} = \delta_U(d),$$

as claimed. □

Proof of Theorem 1.1. Let $A, B > 0$ be the constants of Lemma 6.2. Assume that $x \geq \exp\big(Be^{8\omega(d)}d^8\big)$ and put $y := (\log x/B)^{1/8}/d$. Note that $e^{\omega(d)} \leq y \leq \log x/\varphi(d)$ and $\log y \leq \log\log x$, for every $x \gg_B 1$. By Lemma 6.1, Lemma 6.2, and Lemma 6.4, we obtain that

$$\begin{aligned} \mathcal{R}_U(d; x) &= \sum_{\substack{v \,|\, d^\infty \\ v \leq y}} \sum_{a \,|\, d} \mu(a)\pi_{U,dv,av}(x) + O(E_1) \\ &= \sum_{\substack{v \,|\, d^\infty \\ v \leq y}} \sum_{a \,|\, d} \mu(a)\delta_{U,dv,av}\operatorname{Li}(x) + O(E_1) + O_U(E_2) \\ &= \delta_U(d)\operatorname{Li}(x) + O(E_1) + O_U(E_2) + O(E_3), \end{aligned}$$

where, by Lemma 6.3, we have

$$E_1 := \sum_{\substack{v \,|\, d^\infty \\ v > y}} \sum_{a \,|\, d} \mu(a)\pi_{U,dv,av}(x) \ll \frac{x}{\log x} \cdot \frac{\omega(d)+1}{\varphi(d)} \cdot \frac{(\log y)^{\omega(d)}}{y} \ll \frac{(\omega(d)+1)d}{\varphi(d)} \cdot \frac{x\,(\log\log x)^{\omega(d)}}{(\log x)^{9/8}}$$

and

$$E_3 := \sum_{\substack{v \,|\, d^\infty \\ v > y}} \sum_{a \,|\, d} \mu(a)\delta_{U,dv,av}\operatorname{Li}(x) \ll_U \frac{\omega(d)+1}{\varphi(d)} \cdot \frac{(\log y)^{\omega(d)}}{y} \cdot \operatorname{Li}(x) \ll \frac{(\omega(d)+1)d}{\varphi(d)} \cdot \frac{x\,(\log\log x)^{\omega(d)}}{(\log x)^{9/8}},$$

while, also using the inequality $\tau(d)/d \leq d/\varphi(d)$, we have

$$\begin{aligned} E_2 &:= \sum_{\substack{v \,|\, d^\infty \\ v \leq y}} \sum_{a \,|\, d} x\exp\big(-A(\log x)^{1/2}/(dv)\big) \ll x\exp\big(-AB^{1/8}(\log x)^{3/8}\big)\tau(d)y \\ &\ll x\exp\big(-AB^{1/8}(\log x)^{3/8}\big)(\log x)^{1/8} \cdot \frac{\tau(d)}{d} \ll \frac{d}{\varphi(d)} \cdot \frac{x}{(\log x)^{9/8}}. \end{aligned}$$

The result follows. □

References

1. P. S. Bruckman and P. G. Anderson, *Conjectures on the Z-densities of the Fibonacci sequence*, Fibonacci Quart. **36** (1998), no. 3, 263–271.
2. P. Cubre and J. Rouse, *Divisibility properties of the Fibonacci entry point*, Proc. Amer. Math. Soc. **142** (2014), no. 11, 3771–3785.
3. 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.

4. G. Karpilovsky, *Topics in field theory*, North-Holland Mathematics Studies, vol. 155, North-Holland Publishing Co., Amsterdam, 1989, Notas de Matemática [Mathematical Notes], 124.
5. J. C. Lagarias, *The set of primes dividing the Lucas numbers has density* 2/3, Pacific J. Math. **118** (1985), no. 2, 449–461.
6. J. C. Lagarias, *Errata to: "The set of primes dividing the Lucas numbers has density* 2/3*" [Pacific J. Math.* **118** *(1985), no. 2, 449–461; MR0789184 (86i:11007)]*, Pacific J. Math. **162** (1994), no. 2, 393–396.
7. J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem*, Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), pp. 409–464.
8. P. Moree, *On the prime density of Lucas sequences*, J. Théor. Nombres Bordeaux **8** (1996), no. 2, 449–459.
9. P. Moree, *On primes p for which d divides* $\operatorname{ord}_p(g)$, Funct. Approx. Comment. Math. **33** (2005), 85–95.
10. P. Moree and P. Stevenhagen, *Prime divisors of Lucas sequences*, Acta Arith. **82** (1997), no. 4, 403–410.
11. M. R. Murty and V. K. Murty, *Non-vanishing of L-functions and applications*, Progress in Mathematics, vol. 157, Birkhäuser Verlag, Basel, 1997.
12. A. Schinzel, *A refinement of a theorem of Gerst on power residues*, Acta Arith. **17** (1970), 161–168.
13. H. M. Stark, *Some effective cases of the Brauer-Siegel theorem*, Invent. Math. **23** (1974), 135–152.

Politecnico di Torino, Department of Mathematical Sciences
Corso Duca degli Abruzzi 24, 10129 Torino, Italy
E-mail address: carlo.sanna.dev@gmail.com