#A85 INTEGERS 23 (2023)

PRIME DENSITY OF LEHMER SEQUENCES

Christian Ballot
Département de Mathématiques et Informatique, Université de Caen-Normandie, Caen, France
christian.ballot@unicaen.fr

Received: 7/22/23, Accepted: 10/29/23, Published: 11/20/23

Abstract

The prime density of companion Lucas sequences is known to be computable using a method due to Hasse and Lagarias. This paper demonstrates that companion Lehmer sequences have a prime density amenable to the same method. We compute these densities for two particular sequences. A connection between Lehmer sequences and some recurrences studied by Laxton is revealed.

– Dedicated to Hugh Williams on the occasion of his 80th birthday

1. Introduction

If $X = (X_n)_{n\geq 0}$ is a sequence of integers, we say that a prime p divides X, and write $p \mid X$, if some term X_k of X is divisible by p. The *prime density* of X, if it exists, is defined as

$$\lim_{x\to\infty} \frac{\#\{p \leq x;\ p \mid X\}}{\pi(x)},$$

where $\pi(x)$ is the usual counting function for primes not exceeding x. If S is a set of primes, we say some property holds for *essentially all primes* in S if it holds for all primes in S with possibly a finite number of exceptions.

Lucas sequences $U = (U_n(P,Q))$, $V = (V_n(P,Q))$ are defined by the initial conditions $U_0 = 0$, $U_1 = 1$, $V_0 = 2$ and $V_1 = P$ and the common second-order recursion

$$X_{n+2} = PX_{n+1} - QX_n, \quad \text{for all } n \geq 0,$$

where $X = U$ or V, and P and Q are nonzero integers. The sequence U is called the *fundamental sequence*, whereas the V sequence is called the *companion* or the

DOI: 10.5281/zenodo.10160448

associated Lucas sequence. In particular if the zeros, α and β, of $x^2 - Px + Q$ are distinct, then

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad V_n = \alpha^n + \beta^n.$$

The discriminant $P^2 - 4Q$ of the characteristic polynomial $x^2 - Px + Q$ of the two linear recurrences U and V can only be congruent to 0 or 1 modulo 4.

D. H. Lehmer replaced the parameter P by $\sqrt{R}$ for some nonzero integer R so that the discriminant $D = R - 4Q$ could take any value modulo 4. In order for $U(\sqrt{R}, Q)$ and $V(\sqrt{R}, Q)$ to have integer terms, Lehmer [8] defined a pair of sequences, now called *Lehmer sequences*, $\bar{U} = (\bar{U}_n(R, Q))$ and $\bar{V} = (\bar{V}_n(R, Q))$ as follows:

$$\begin{aligned}\bar{U}_n(R,Q) &= U_n(\sqrt{R},Q), \quad (n \text{ odd}),\\ \bar{U}_n(R,Q) &= U_n(\sqrt{R},Q)/\sqrt{R}, \quad (n \text{ even});\end{aligned}$$

and

$$\begin{aligned}\bar{V}_n(R,Q) &= V_n(\sqrt{R},Q)/\sqrt{R}, \quad (n \text{ odd}),\\ \bar{V}_n(R,Q) &= V_n(\sqrt{R},Q), \quad (n \text{ even}).\end{aligned}$$

The Lehmer sequences $\bar{U}$ and $\bar{V}$ are fourth order linear recurrences that satisfy

$$X_{n+4} = (R - 2Q)X_{n+2} - Q^2 X_n, \tag{1}$$

for all $n \geq 0$ and X either $\bar{U}$ or $\bar{V}$. Their initial values are

$$\bar{U}_0 = 0,\ \bar{U}_1 = \bar{U}_2 = 1,\ \bar{U}_3 = R - Q, \tag{2}$$

and

$$\bar{V}_0 = 2,\ \bar{V}_1 = 1,\ \bar{V}_2 = R - 2Q,\ \bar{V}_3 = R - 3Q. \tag{3}$$

If R and Q are coprime, then the fundamental Lehmer sequence $\bar{U}$ is a strong divisibility sequence, i.e., $|\bar{U}_{\gcd(m,n)}| = \gcd(\bar{U}_m, \bar{U}_n)$, for all m, n nonnegative integers.

Because the initial value of a fundamental Lucas or Lehmer sequence (U or $\bar{U}$) is 0, all primes divide such a sequence. Thus, their prime density is trivially equal to 1. More precisely, if ρ is the rank of appearance of a prime p, ($p \nmid Q$), i.e., the least positive integer t such that $p \mid U_t$ (resp. $\bar{U}_t$), then

$$p \mid U_n \text{ (resp. } \bar{U}_n) \text{ if and only if } \rho \mid n. \tag{4}$$

Prime divisors of a companion Lucas or Lehmer sequence (i.e., a V or a $\bar{V}$ sequence) are essentially all primes of even rank. Companion Lucas sequences have a prime density and there exists a well-known method, the Hasse-Lagarias method, to compute this density. Hasse [5] first discovered an unconditional method that shows companion Lucas sequences of the type $(a^n+1)_{n\geq 0}$, a a square-free integer, possess a computable prime density. The method extends easily to all companion Lucas sequences with reducible characteristic polynomial, i.e., sequences $(a^n+b^n)_{n\geq 0}$, where a and b are nonzero integers. (One may consult, for instance, [1, Thm. 3.1.3] for a complete description of the prime densities of the sequences $(a^n+b^n)_{n\geq 0}$.) The method of Hasse computes the prime density of divisors within the set of primes p such that $p-1$ is exactly divisible by 2^j, where $j\geq 1$ is a fixed integer. Such primes are described by how they split in some Galois number field, say K_j. The Cebotarev density theorem is then used to evaluate their density; this is done for all $j\geq 1$. Lagarias [6] chose a couple of second-order linear recurrences, with irreducible characteristic polynomials, one of which was the sequence of Lucas numbers $L=(L_n)$, where $L_n=\alpha^n+\beta^n$, α and β are the real zeros of x^2-x-1, and showed the method of Hasse could be successfully extended to computing the prime densities of these two sequences, as well as the prime density of other second-order linear recurrences of a certain type. In the irreducible case, one computes separately the prime density among primes for which D is a square modulo p, and the prime density of divisors for which D is a quadratic nonresidue. In the former subset, sub-densities are computed, as Hasse did, within primes with a fixed power of 2 in $p-1$, whereas in the latter subset, the same method applies for subsets of primes with a fixed power of 2 in $p+1$. Lagarias [6, pp. 450-451] gave a set of sufficient conditions on linear irreducible second-order recurrences for the Hasse-Lagarias method to apply. Suppose α and $\bar{\alpha}=\beta$ are the irrational zeros of x^2-Px+Q. Assume X is a linear recurrence with characteristic polynomial x^2-Px+Q. Write $X_n=c\alpha^n+\bar{c}\bar{\alpha}^n$, for all nonnegative integers n and some constants c and $\bar{c}$. If there is an element φ and a root of unity ζ in the root field $\mathbb{Q}(\alpha)$ such that

$$\alpha/\bar{\alpha}=\epsilon\varphi^k,\ (\epsilon=\pm 1,\ k=1 \text{ or } 2),\qquad \text{and}\qquad \bar{c}/c=\zeta\varphi^j,\ (j\in\mathbb{Z}), \tag{5}$$

then we can wrestle out the prime density of X by the Hasse-Lagarias method. Actually, all companion Lucas sequences $V(P,Q)$ satisfy the Lagarias conditions (5); take $\varphi=\alpha/\bar{\alpha}, j=0, \zeta=1, \epsilon=k=1$. Thus, with enough care, given $V(P,Q)$ we can compute its prime density. Finding out general theorems on the densities of companion Lucas sequences is not an easy task. However, we cite, as an example, the work of Moree and Stevenhagen [11] who gave the prime densities of companion Lucas sequences $(\varepsilon^n+\bar{\varepsilon}^n)$, when ε is any fundamental unit of a real quadratic number field. The other sequence, W, for which Lagarias worked out the prime density is not a companion Lucas sequence, but it shares a common feature with companion Lucas sequences: It is a torsion sequence in the Laxton group. Laxton [7] constructed a group $G(f)$ based on classes of integral second-order linear recurrences that satisfy the same characteristic polynomial $f(x)=x^2-Px+Q$. Two recurrences live in the same class if they differ by rational scalars and a possible shift in their indices. The group $G(f)$ is infinite. The subgroup of finite-order elements, $T(f)$, is always finite, and often contains only two elements, the class of $U(P,Q)$ which is the identity element of $G(f)$, and the class of the companion Lucas sequence $V(P,Q)$ of order 2 in $G(f)$. The group operation has the interesting feature of preserving prime division: if two recurrences are divisible by the same prime, then the group product of the two recurrences is also divisible by that prime. The sequence W has order 3. Its prime divisors are essentially the primes with a rank of appearance divisible by 3. It was shown in [1, p. 20] that all sequences satisfying the Lagarias conditions (5) must belong to $T(f)$, where f has zeros α and $\bar{\alpha}$. In fact, their order in $G(f)$ must divide 12, and the set $L(f)$ of all (classes of) recurrences satisfying (5) forms a subgroup of $T(f)$. The question of whether the Hasse-Lagarias method works out on X if and only if X is a torsion sequence remains open. There are polynomials f such that $T(f)$ is strictly larger than $L(f)$; see [1, Prop. 2.4.5]. Also, the narrower question of whether belonging to $T(f)$ garanties a potential successful application of the Hasse-Lagarias method is open.

In 1994, the author was invited to Cambridge, England, to give a couple of lectures on the material developed in the memoir [1]. Alan Baker was in the audience and asked the pertinent question of whether the prime density of Lehmer sequences could also be worked out. This short paper is a belated answer to Baker's question. This question, among others related to Lehmer sequences, appears in the recent book [4, Chap. 10, Item **9**].

We wish to find out whether companion Lehmer sequences $\bar{V}(R,Q)$ have a computable prime density. The set of primes dividing terms of $\bar{V}$ is essentially the set of primes which have even rank in $\bar{U}$. Thus, its complementary set within the set of all primes is made of the primes which divide terms of the second-order linear recurrence $(\bar{U}_{2n+1})$. We begin with two sets of parameter values that stand out, namely $(R,Q)=(5,1)$ and $(R,Q)=(2,-1)$. The case $(R,Q)=(5,1)$ relates to Fibonacci and Lucas numbers, while the case $(R,Q)=(2,-1)$ was used by D. H. Lehmer to produce the famous Lucas-Lehmer test for primality of Mersenne numbers [8, Thm. 5.4, p. 443]. We note in passing that Lehmer [9] later found a simple proof of the Lucas-Lehmer test for primality of Mersenne numbers that used only the Lucas sequences associated with the polynomial x^2-2x-2 whose zeros are $1\pm\sqrt{3}$.

There is a law of appearance and an Euler criterion for Lehmer sequences similar to those for Lucas sequences. Here, the symbol $(*\,|\,*)$ stands for the Legendre symbol and $D=R-4Q$. They appear respectively as Theorems 1.7 and 4.9 in D. H. Lehmer's thesis [8].

Proposition 1. (Law of appearance) *If p is an odd prime and $p \nmid QR$, then*

$$p \mid \bar{U}_{p-\varepsilon\eta},$$

where $\varepsilon=(D\,|\,p)$ and $\eta=(R\,|\,p)$.

Proposition 2. (Euler's criterion) *If $p \nmid 2QRD$, then*

$$p \mid \bar{U}_{(p-\varepsilon\eta)/2} \text{ if and only if } \eta = (Q \,|\, p),$$

where $\varepsilon = (D \,|\, p)$ and $\eta = (R \,|\, p)$.

In Section 2 density calculations use the Kummer-Dedekind and the Cebotarev density theorems. The Kronecker-Fröbenius density theorem is a particular case of the Cebotarev theorem for primes that split completely in a Galois number field extension. The Kummer-Dedekind theorem relates the factorization of the minimal polynomial of an algebraic integer α modulo a prime ideal, to the factorization of this prime ideal in the field extension defined by α — see for instance [10, p. 79] or [12, p. 15]. The prime density of $\bar{V}(2,-1)$ is computed for each class of primes modulo 12; for some classes we provide two distinct density proofs. Section 3 proves that the Lehmer $\bar{V}$ sequences are always amenable to the Hasse-Lagarias method. Section 4 identifies sub-sequences of $\bar{U}(R,Q)$ and $\bar{V}(R,Q)$ to recurrences that form a copy of the Klein group within the Laxton group $G(f)$, where $f(x) = x^2 - (R-2Q)x + Q^2$.

We denote $e^{2i\pi/n}$ by ζ_n, where n is an integer. If p is a prime and n an integer, we write $p^e \,||\, n$ if $p^e \mid n$, but $p^{e+1} \nmid n$.

2. Density Computations

Theorem 1. *The companion Lehmer sequence $\bar{V}(5,1)$ admits a prime density equal to $2/3$.*

Proof. Here, we find that $\bar{V}_{2n} = L_{2n}$ and $\bar{V}_{2n+1} = F_{2n+1}$. Prime divisors of (F_{2n+1}) are the primes of odd rank in the Fibonacci sequence; their density was calculated in the Lagarias paper [6] and is equal to $1/3$. The prime divisors of (L_{2n}) are the primes with Fibonacci rank divisible by 4. Their density is also known to be $1/3$; see [3]. Thus, we find out that $\delta(\bar{V}(5,1)) = 2/3$. □

Theorem 2. *The companion Lehmer sequence $\bar{V}(2,-1)$ admits a prime density equal to $2/3$. This two-third density decomposes into four sub-densities according to whether primes are congruent to 1, -1, 5 or -5 modulo 12, respectively, as follows:*

$$\frac{11}{48} + \frac{1}{8} + \frac{1}{8} + \frac{3}{16}.$$

We will prove Theorem 2 by actually proving the existence of a prime density for the complementary set, i.e., for the prime divisors of $(\bar{U}_{2n+1}(2,-1))$. By (1), we find that $(\bar{U}_{2n+1})$ is a second-order linear recurrence with characteristic polynomial $x^2 - 4x + 1$. Since the zeros of $x^2 - 4x + 1$ are $2 \pm \sqrt{3}$, $\bar{U}_1 = 1$ and $\bar{U}_3 = 3$, we get the closed-form expression[1]

$$\bar{U}_{2n+1} = \frac{3+\sqrt{3}}{6}(2+\sqrt{3})^n + \frac{3-\sqrt{3}}{6}(2-\sqrt{3})^n. \tag{6}$$

Put $\alpha = 2+\sqrt{3}$ and $\bar{\alpha} = 2-\sqrt{3}$. Given a prime number p, we denote by (p) the prime ideal generated by p in $\mathbb{Z}[\sqrt{3}]$ and by h the order of α in the group $(\mathbb{Z}[\sqrt{3}]/(p))^*$. We remark that if π is a prime ideal above p in $\mathbb{Z}[\sqrt{3}]$, then h is also the order of α in the cyclic group $(\mathbb{Z}[\sqrt{3}]/\pi)^*$. Indeed, the following equivalence holds for all n:

$$\alpha^n \equiv 1 \pmod{(p)} \text{ if and only if } \alpha^n \equiv 1 \pmod{\pi}. \tag{7}$$

If p is inert in $\mathbb{Z}[\sqrt{3}]$, then $\pi = (p)$ and (7) clearly holds. If p splits into two prime ideals $\pi\bar{\pi}$ in $\mathbb{Z}[\sqrt{3}]$, then the forward implication in (7) is true since $(p) \subset \pi$. To see the converse direction, note that $\alpha\bar{\alpha} = 1$ so that $\alpha^n \equiv 1 \pmod{\pi}$ implies $1 = (\alpha\bar{\alpha})^n \equiv \bar{\alpha}^n \pmod{\pi}$, which, by algebraic conjugation, gives $\alpha^n \equiv 1 \pmod{\bar{\pi}}$. The conclusion holds since $\pi \cap \bar{\pi} = (p)$.

Divisors of $(\bar{U}_{2n+1})$ obey a simple characterization given in the next lemma.

Lemma 1. *The equivalence*

$$p \mid (\bar{U}_{2n+1}) \textit{ if and only if } 2 \,||\, h,$$

holds for all primes $p \geq 5$.

Proof. By Equation (6), $p \mid \bar{U}_{2n+1}$ for some n if and only if

$$\left(\frac{2+\sqrt{3}}{2-\sqrt{3}}\right)^n \equiv -\frac{3-\sqrt{3}}{3+\sqrt{3}} \pmod{(p)}.$$

This yields $\alpha^{2n} \equiv -\frac{3-\sqrt{3}}{3+\sqrt{3}} \pmod{(p)}$. Noticing that

$$\frac{3+\sqrt{3}}{3-\sqrt{3}} = \frac{\sqrt{3}+1}{\sqrt{3}-1} = 2+\sqrt{3} = \alpha, \tag{8}$$

we conclude that

$$p \mid \bar{U}_{2n+1} \text{ if and only if } \alpha^{2n+1} \equiv -1 \pmod{(p)}, \tag{9}$$

which, using (7), shows that $2 \,||\, h$ if, and only if, $p \mid (\bar{U}_{2n+1})$. □

[1] The referee made the observation that

$$\bar{U}_{2n+1} = \left[(3+\sqrt{3})^{2n+1} + (3-\sqrt{3})^{2n+1}\right]/6^{n+1} = \sum_{k=0}^{n} 2^k \binom{n+k}{2k}.$$

Since, by (4), $p \mid (\bar{U}_{2n+1})$ if and only if ρ is odd, a necessary condition for an odd prime $p \nmid RD$ to divide $(\bar{U}_{2n+1})$ is that $\rho \mid (p - \varepsilon\eta)/2$. Thus, by Proposition 2, a necessary condition for an odd prime $p \geq 5$, $p \nmid QRD$, to divide $(\bar{U}_{2n+1})$ is that

$$(2 \,|\, p) = (-1 \,|\, p). \tag{10}$$

Proof of Theorem 2. We prove that $(\bar{U}_{2n+1})$ has the prime density

$$d_1 + d_{-1} + d_5 + d_{-5},$$

where d_i is the natural density of primes that divide $(\bar{U}_{2n+1})$ and are congruent to $i \pmod{12}$. Thus, we compute four sub-densities and consider the four cases separately. Primes that are congruent to $\pm 1 \pmod{12}$ satisfy $(3 \,|\, p) = 1$, i.e., they split in $\mathbb{Q}(\sqrt{3})$. We start with primes congruent to $1 \pmod{12}$. As before, π represents a fixed prime ideal above p in $\mathbb{Z}[\sqrt{3}]$.

Case 1. Density of divisors among primes congruent to $1 \pmod{12}$.

Let $j \geq 2$. Define the set of primes $\mathcal{P}_j^+$ as $\{p;\ 2^j \,||\, p-1 \text{ and } 3 \mid p-1\}$, and F_j as the number field $\mathbb{Q}(\sqrt{3}, \zeta_{2^j})$. Furthermore, we denote $F_j(\sqrt[2^{j-1}]{\alpha})$ by K_j.

Suppose $j = 2$. Then $p \equiv 5 \pmod{8}$. Thus, 2 is a nonresidue of p. But

$$\alpha = 2 + \sqrt{3} = \frac{(1+\sqrt{3})^2}{2}. \tag{11}$$

Therefore, α is a nonresidue of π. Thus, $4 \mid h$ and no prime in $\mathcal{P}_2^+$ divides $(\bar{U}_{2n+1})$.

Alternatively, primes $p \equiv 5 \pmod{8}$ do not meet the necessary condition (10), because $(2 \,|\, p) = -1$ and $(-1 \,|\, p) = 1$. Thus, none divides $(\bar{U}_{2n+1})$.

Assume $j \geq 3$ is fixed and p is a prime in $\mathcal{P}_j^+$. Since $p \equiv 1 \pmod{2^j}$ and $p \equiv 1 \pmod{12}$, p splits completely in F_j. Since F_j contains $\mathbb{Q}(\zeta_8)$, which contains $\sqrt{2}$, we see by (11) that F_j contains the algebraic integer $\sqrt{\alpha}$. Hence, the minimal polynomial of $\sqrt[2^{j-1}]{\alpha}$ over F_j is $f(x)$, where $f(x) := x^{2^{j-2}} - \sqrt{\alpha}$.

Given any prime ideal π in $\mathbb{Z}[\sqrt{3}]$ above p, we know $p \mid (\bar{U}_{2n+1})$ if and only if

$$\alpha^{(p-1)/2^{j-1}} \equiv 1 \pmod{\pi}, \text{ but } \alpha^{(p-1)/2^j} \equiv -1 \pmod{\pi}.$$

If P is a prime ideal above p in F_j, then the above congruences hold modulo P. Thus, $\sqrt{\alpha}$ is a 2^{j-2}th power residue modulo P. As F_j contains primitive 2^jth roots of unity, it follows that $f(x)$ factorizes into linear factors modulo P. By the Kummer-Dedekind theorem, p must split completely in K_j. However, since $\alpha^{(p-1)/2^j} \equiv -1 \pmod{P}$, p does not split completely in $K_j(\sqrt[2^j]{\alpha})$, nor in $K_j(\zeta_{2^{j+1}})$ since $2^{j+1} \nmid p-1$. By inclusion-exclusion and the Kronecker-Frobenius density theorem, primes in $\mathcal{P}_j^+$ that divide $(\bar{U}_{2n+1})$ have the density

$$d_j^+ = \frac{1}{[K_j : \mathbb{Q}]}\left(1 - (\frac{1}{2} + \frac{1}{2}) + \frac{1}{4}\right) = \frac{1}{4} \cdot \frac{1}{[K_j : \mathbb{Q}]}.$$

As $\sqrt{\alpha} \in F_j$, we see that $[K_j : \mathbb{Q}] = 2 \cdot 2^{j-1} \cdot 2^{j-2} = 4^{j-1}$. By a standard argument [6, p. 451], we find that d_1 exists and is equal to the sum

$$\sum_{j \geq 3} d_j^+ = \sum_{j \geq 3} \frac{1}{4^j} = \frac{1}{4^3} \cdot \frac{1}{1 - \frac{1}{4}} = \frac{1}{48}.$$

Case 2. Density of divisors among primes congruent to $-1 \pmod{12}$.

By the Dirichlet density theorem, primes $p \equiv -1 \pmod{12}$ have density $1/4$. Since $2 \,||\, p-1$, either h is odd or $2 \,||\, h$. Now h is odd if and only if α is a quadratic residue of π, i.e., if and only if $x^2 - \alpha$ factors modulo π. By the Kummer-Dedekind theorem, we see that primes $-1 \pmod{12}$ such that h is odd split from $\mathbb{Q}$ to $\mathbb{Q}(\sqrt{3}, \sqrt{\alpha}) = \mathbb{Q}(\sqrt{\alpha})$. Since $4 \nmid p-1$, they do not split further in $\mathbb{Q}(\sqrt{\alpha}, i)$. Thus, by the Kronecker-Frobenius density theorem, their density exists and is equal to

$$\frac{1}{[\mathbb{Q}(\sqrt{\alpha}) : \mathbb{Q}]} - \frac{1}{[\mathbb{Q}(\sqrt{\alpha}, i) : \mathbb{Q}]} = \frac{1}{4}\left(1 - \frac{1}{2}\right) = \frac{1}{8}.$$

The complementary set within primes $-1 \pmod{12}$ consists of the primes that satisfy $2 \,||\, h$. Hence, $d_{-1} = \frac{1}{4} - \frac{1}{8} = \frac{1}{8}$. Alternatively, as for primes $p \equiv -1 \pmod{12}$, $2 \,||\, p-1$, the necessary condition (10) for ρ to be odd is also a sufficient condition. Primes congruent to $-1 \pmod{12}$ are congruent to $-1 \pmod 3$ and $-1 \pmod 4$. The latter condition means congruent to 3 or $7 \pmod 8$. Hence, as $(-1 \,|\, p) = -1$, $p \mid (\bar{U}_{2n+1})$ if and only if $(2 \,|\, p) = -1$, i.e., if and only if $p \equiv 3 \pmod 8$. We conclude by the Dirichlet density theorem since primes congruent to $-1 \pmod 3$ and to $3 \pmod 8$ have prime density $1/8$.

In the remaining cases, the rank ρ of p in $\bar{U}$ divides $p+1$. Indeed, we know, by Proposition 1, that $p \mid \bar{U}_{p-\varepsilon\eta}$, where $\varepsilon = (D \,|\, p) = (6 \,|\, p)$ and $\eta = (R \,|\, p) = (2 \,|\, p)$. Therefore, $\varepsilon\eta = (3 \,|\, p) = -1$ and $p \mid \bar{U}_{p+1}$. Thus, a necessary condition for p to divide $(\bar{U}_{2n+1})$ is that ρ divides $(p+1)/2$. Moreover, by (9), we must have

$$\alpha^\rho \equiv -1 \pmod{(p)}, \ h = 2\rho \ \text{ and } \ h \mid p+1.$$

Case 3. Density of divisors among primes congruent to $5 \pmod{12}$.

Suppose p is a prime congruent to $5 \pmod{12}$, i.e., congruent to $-1 \pmod 3$ and to $1 \pmod 4$.

Since $2 \,||\, p+1$, ρ is odd if and only if $\rho \mid (p+1)/2$. By the Euler criterion for $\bar{U}$, $p \mid \bar{U}_{(p+1)/2}$ if and only if $(2 \,|\, p) = (-1 \,|\, p) = 1$. Hence, p divides $(\bar{U}_{2n+1})$ if and only if $p \equiv 1 \pmod 8$. But, by the Dirichlet density theorem, primes congruent to $-1 \pmod 3$ and to $1 \pmod 8$ have density $\frac{1}{2} \cdot \frac{1}{4} = \frac{1}{8}$. Thus, $d_5 = 1/8$.

Case 4. Density of divisors among primes congruent to $-5 \pmod{12}$.

For $j \geq 2$, define $\mathcal{P}_j^-$ as the set of primes $\{p;\ 2^j \,||\, p+1 \text{ and } 3 \mid p-1\}$. The union of all $\mathcal{P}_j^-$, $j \geq 2$, is the set of primes $-5 \pmod{12}$. Suppose $j \geq 3$ and $p \in \mathcal{P}_j^-$. Then $8 \mid p+1$. Therefore, $(2 \,|\, p) = 1$ and $(-1 \,|\, p) = -1$. Thus, these primes do not satisfy the necessary condition (10) for p to divide $(\bar{U}_{2n+1})$. Hence, none divides $(\bar{U}_{2n+1})$.

Let $j = 2$ and $p \in \mathcal{P}_2^-$. Thus, $p \equiv 3 \pmod 8$. Since p is inert in $\mathbb{Q}(\sqrt{3})$ and $(p+1)/4$ is odd, we see that $p \mid (\bar{U}_{2n+1})$ if and only if

$$\alpha^{(p+1)/4} \equiv -1 \pmod{(p)},$$

where (p) is the ideal generated by p in $\mathbb{Z}[\sqrt{3}]$.

Consider the normal number field $L = \mathbb{Q}(\zeta_8, \sqrt[4]{\alpha}) = \mathbb{Q}(\zeta_8, \sqrt{3}, \sqrt[4]{\alpha})$. Since $\sqrt{2} \in \mathbb{Q}(\zeta_8)$ and, by (11), $\sqrt{\alpha} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, the degree of L over $\mathbb{Q}$ is $4 \cdot 2 \cdot 2 = 16$.

Suppose $p \in \mathcal{P}_2^-$ divides $(\bar{U}_{2n+1})$. If $\mathcal{P}$ is a prime ideal in the ring of integers of L lying above p, then the Frobenius automorphism $\psi = \psi(\mathcal{P} \,|\, p)$ satisfies the conditions

$$\psi(\alpha_4) = -\alpha_4^{-1} \quad \text{and} \quad \psi(\zeta_8) = -\zeta_8^{-1}, \tag{12}$$

where $\alpha_4 = \sqrt[4]{\alpha} = \sqrt[4]{2+\sqrt{3}} > 0$. Indeed, $\psi(\alpha_4) \equiv \alpha_4^p = \alpha_4^{-1} \cdot \alpha^{(p+1)/4} \pmod{\mathcal{P}}$. But, $\alpha^{(p+1)/4} \equiv -1 \pmod{(p)}$, so that, in particular, we have $\psi(\alpha_4) \equiv -\alpha_4^{-1} \pmod{\mathcal{P}}$, which implies $\psi(\alpha_4) = -\alpha_4^{-1}$. Also, $\psi(\zeta_8) \equiv \zeta_8^p = \zeta_8^{-1}(\zeta_8^4)^{(p+1)/4} = -\zeta_8^{-1} \pmod{\mathcal{P}}$ implying the second condition in (12). If the Galois group G of L over $\mathbb{Q}$ contains an element satisfying the conditions in (12), then this element is unique since α_4 and ζ_8 generate L. Moreover, ψ does not depend on $\mathcal{P}$, meaning it is a central element of G. The conjugacy class of ψ contains only ψ. Thus, by the Cebotarev density theorem, primes in $\mathcal{P}_2^-$ dividing $(\bar{U}_{2n+1})$ have density $1/|G|$, i.e., $1/16$. Hence, $d_{-5} = 1/16$. We now check that G contains an element that satisfies the conditions in (12). The minimal polynomial of α_4 over $\mathbb{Z}$ is $g(x) := x^8 - 4x^4 + 1$. It factorizes over $\mathbb{Z}[\sqrt{2}]$ into $g_1(x)g_2(x) := (x^4 - \sqrt{2}x^2 - 1)(x^4 + \sqrt{2}x^2 - 1)$. Here, α_4 is a zero of $g_1(x)$. Any $\Phi \in G$ sends ζ_8 to ζ_8^k for some k in $\{\pm 1, \pm 3\}$. If $k = \pm 1$, then Φ fixes $\sqrt{2}$. Thus, α_4 can only be mapped onto one of the four zeros of $g_1(x)$. These eight possibilities account for at most eight elements of G. If $k = \pm 3$, then $\sqrt{2}$ is moved to $-\sqrt{2}$ and α_4 has to be mapped onto one of the four zeros of $g_2(x)$. Since $|G| = 16$, we have just described all sixteen elements of G. The element ψ defined by (12) does belong to G; it corresponds to $k = 3$ and $\alpha_4 \mapsto -\alpha_4^{-1}$. We readily check that $g_2(-\alpha_4^{-1}) = (2 - \sqrt{3}) + \sqrt{2} \cdot \frac{\sqrt{3}-1}{\sqrt{2}} - 1 = 0$.

We conclude that prime divisors of $(\bar{U}_{2n+1})$ possess a density equal to

$$d_1 + d_{-1} + d_5 + d_{-5} = \frac{1}{48} + \frac{1}{8} + \frac{1}{8} + \frac{1}{16} = \frac{1}{3}.$$

Thus, the complementary sets within the four congruence classes modulo 12 have the prime densities

$$\left(\frac{1}{4} - \frac{1}{48}\right) + \left(\frac{1}{4} - \frac{1}{8}\right) + \left(\frac{1}{4} - \frac{1}{8}\right) + \left(\frac{1}{4} - \frac{1}{16}\right),$$

yielding, respectively, the four announced sub-densities. Also, the companion Lehmer sequence $\bar{V}(2,-1)$ has prime density $1-1/3=2/3$. □

Remark 1. We found that out of the first 200 primes exactly 68 divide $(\bar{U}_{2n+1})$. There are 1,229 primes less than 10,000 and 410 of them divide $(\bar{U}_{2n+1})$. These proportions match very closely the 1/3 asymptotic density. Checking the four sub-densities d_1, d_{-1}, d_5 and d_{-5}, the least 1920 primes were tested for division of $(\bar{U}_{2n+1})$. We chose 1920 for the practical reason that it is a multiple of 48, (it is 40×48), which gives an integral number of expected divisors for each sub-density. (By 'expected,' we mean the number of prime divisors if the asymptotic proportion were to be respected.) We got the table:

$p \pmod{12}$	1	-1	5	-5
found	44	241	249	119
'expected'	40	240	240	120

Table 1: Number of prime divisors among the first 1920 primes

3. Did We Get Lucky in the Previous Two Cases?

The Hasse-Lagarias method provides the correct prime density provided it is applied with sufficient care, in particular in evaluating the degrees of the number field extensions involved. Assessing prime densities to whole families of recurrences is prone to errors. It was not necessarily obvious that $\alpha = 2+\sqrt{3}$ is a nonresidue of primes 13 (mod 24), i.e., primes 1 (mod 3) and 5 (mod 8). Yet, the remark was helpful in getting the right value for the sub-density d_1. Thus, we will be satisfied here with knowing whether one can, in principle, apply the Hasse-Lagarias method in all cases of $\bar{V}(R,Q)$. Did we merely get lucky in the examples treated in Section 2?

Laxton [7, Thm. 4.4] investigated the set of elements of order 2 in the group $G(f)$. Suppose $f(x)=x^2-Px+Q$. The class of $V(P,Q)$ is always an order-two element in $G(f)$. If Q is not a square in $\mathbb{Z}$, then the class of $V(P,Q)$ is the only order-two element. If $Q=S^2$, S an integer, there are exactly three elements of order 2, namely the class of the companion Lucas sequence V and the classes of $A=(A_n)_{n\geq 0}$ and $B=(B_n)_{n\geq 0}$, where $A_0=B_0=1$, $A_1=P+S$ and $B_1=P-S$. That is, using $U=U(P,Q)$,

$$\begin{aligned} A_n &= U_{n+1}+SU_n, \\ B_n &= U_{n+1}-SU_n. \end{aligned} \tag{13}$$

By (13) and $U_{2n+1} = U_{n+1}^2 - QU_n^2$, we see that

$$U_{2n+1} = A_n B_n, \text{ for all integers } n \geq 0.$$

Hence, the prime divisors of A and B are the primes of odd rank in $U(P,Q)$. The sets of prime divisors of A and B are essentially disjoint [7, Thm. 4.6]; a prime dividing both A and B would divide V since the classes of the four sequences form a copy of the Klein group and prime division is preserved by the group operation. Because the prime divisors of V are the primes of even rank, we see that the set of all primes is partitioned into three (disjoint) subsets according to whether they divide V, A or B.

Proposition 3. *Suppose $Q = S^2$, S an integer. The sequences A and B, defined above, are amenable to the Hasse-Lagarias method. In fact, both sequences A and B satisfy the Lagarias conditions (5) with $\varphi = \alpha/S = (P + \sqrt{D})/(2S)$, $\epsilon = 1$, $k = 2$, $\zeta = \pm 1$ and $j = -1$, where $\zeta = -1$ for A and $\zeta = 1$ for B.*

Proof. We only treat the case of the A sequence. Noting that the discriminant D of $x^2 - Px + S^2$ is $P^2 - 4S^2$, we see that

$$\frac{\alpha}{\beta} = \frac{P + \sqrt{D}}{P - \sqrt{D}} = \frac{(P + \sqrt{D})^2}{P^2 - D} = \left(\frac{P + \sqrt{D}}{2S}\right)^2 = \left(\frac{\alpha}{S}\right)^2 = \varphi^2.$$

The nth term of the sequence A has the closed form

$$A_n = \frac{(P + S - \beta)\alpha^n - (P + S - \alpha)\beta^n}{\alpha - \beta}.$$

Thus, with the notation of (5), we get $\bar{c}/c = -(P + S - \alpha)/(P + S - \beta)$. It remains to verify the identity $\bar{c}/c = -\varphi^{-1} = -S/\alpha$ which holds if and only if $(P + S)\alpha - \alpha^2 = PS + S^2 - \beta S$, i.e., as $PS + S^2 - \beta S = S^2 + \alpha S$, if and only if, $P\alpha - \alpha^2 = S^2$. But both sides of this latter equation are equal to $\alpha\beta$. □

The complementary set within the set of primes of the prime divisors of $\bar{V}(R,Q)$ consists of the prime divisors of $(\bar{U}_{2n+1}(R,Q))$. Remarkably, the sequence $(\bar{U}_{2n+1}(R,Q))$ turns out to be the A torsion sequence associated with the recursion $x^2 - (R - 2Q)x + Q^2$.

Theorem 3. *Suppose $f(x) = x^2 - (R - 2Q)x + Q^2$. Then we find that for all $n \geq 0$,*

$$\bar{U}_{2n+1}(R,Q) = A_n, \text{ for all } n \geq 0,$$

where A is the order-two linear recurrence in $G(f)$ defined in (13).

Proof. By Equation (1), $(\bar{U}_{2n+1}(R,Q))$ admits $f(x)$ as its characteristic polynomial. The recurrence A has initial values 1 and $(R - 2Q) + Q = R - Q$, which, by (2), correspond to the initial values of the second-order linear recurrence $(\bar{U}_{2n+1}(R,Q))$. □

Consequently, by Proposition 3, the prime density of $(\bar{U}_{2n+1}(R,Q))$ is amenable to the Hasse-Lagarias method, and hence we can always find out the prime density of a companion Lehmer sequence $\bar{V}(R,Q)$.

4. An Unsuspected Conclusion with Remarks

As recalled in the previous section, if $f(x) = x^2 - Px + S^2$, where P and S are nonzero integers, then the torsion subgroup $T(f)$ of the Laxton group $G(f)$ contains a copy $K(f)$ of the Klein group $\mathbb{Z}_2 \times \mathbb{Z}_2$ given by the classes of the recurrences $U = U_f$, $V = V_f$, $A = A_f$ and $B = B_f$. The prime density of each sequence V, A and B is amenable to the Hasse-Lagarias method and, thus, can be computed.

Theorem 4. *Given two nonzero integers R and Q, the four second-order linear recurrences $(\bar{U}_{2n}(R,Q))$, $(\bar{V}_{2n}(R,Q))$, $(\bar{U}_{2n+1}(R,Q))$ and $(\bar{V}_{2n+1}(R,Q))$ are, respectively, the four sequences U_f, V_f, A_f and B_f whose classes form the Laxton subgroup $K(f)$, where $f(x) = x^2 - (R-2Q)x + Q^2$.*

Proof. By Equation (1), $(\bar{U}_{2n}(R,Q))$, $(\bar{V}_{2n}(R,Q))$, $(\bar{U}_{2n+1}(R,Q))$ and $(\bar{V}_{2n+1}(R,Q))$ are second-order linear recurrences with characteristic polynomial $f(x)$. We already saw in Theorem 3 that $(\bar{U}_{2n+1}(R,Q))$ is A_f. Since $\bar{U}_0(R,Q) = 0$ and $\bar{U}_2(R,Q) = 1$, we find that $(\bar{U}_{2n}(R,Q))$ is U_f. The initial values of $(\bar{V}_{2n}(R,Q))$ are 2 and $R-2Q$ so that $\bar{V}_{2n}(R,Q) = V_f(n)$. The values of $\bar{V}_{2n+1}(R,Q)$ for $n=0$ and $n=1$ are, respectively, 1 and $R-3Q = (R-2Q)-Q$. Thus, we see that $\bar{V}_{2n+1}(R,Q) = B_f(n)$. □

The content of Theorem 4 is summarized in Table 2.

$\bar{X}(R,Q)$	$f(x) = x^2 - (R-2Q)x + Q^2$
$\bar{U}_{2n}$	$U_f(n)$
$\bar{V}_{2n}$	$V_f(n)$
$\bar{U}_{2n+1}$	$A_f(n)$
$\bar{V}_{2n+1}$	$B_f(n)$

Table 2: Correspondence between Lehmer sub-sequences and elements of $K(f)$

There is an obvious converse to Theorem 4: Given a Laxton Klein group $K(f)$, i.e., a quadratic polynomial $f(x) = x^2 - Px + S^2$, the two Lehmer pairs $(\bar{U}, \bar{V})$ with $(R, Q) = (P \pm 2S, \pm S)$ make the correspondence in Table 2 hold. Changing S into $-S$ permutes the roles of A and B, but does not alter the Lucas sequences U and V, and both choices give the same Klein group. Define a pair of Lehmer sequences with parameters R and Q to be *equivalent* to the pair with parameters R', Q' if, and only if, $R' = R - 4Q$ and $Q' = -Q$. This relation is symmetric. Then, we may say the correspondence between equivalent pairs of Lehmer sequences and Laxton Klein groups is one-to-one. Because of Theorem 4, the study of the arithmetic of Lehmer sequences is intricately linked to the arithmetic of the four Lucas-Laxton sequences U, V, A and B.

A particular case of Theorem 4 had already been discovered in [3, Sects. 5 and 6] with no reference to the Lehmer sequences. Indeed, if $\sqrt{R} = R = 1$ and $Q = -1$, then the corresponding Lehmer sequences $\bar{U}(1, -1)$ and $\bar{V}(1, -1)$ are simply the famous pair of Lucas sequences (F, L) of Fibonacci and Lucas numbers. By Table 2, we see that $f(x) = x^2 - 3x + (-1)^2$, $A_f(n) = F_{2n+1}$, $B_f(n) = L_{2n+1}$ and $V_f(n) = L_{2n}$. The prime partition, or trichotomy, of the set of all primes into divisors of A_f, B_f and V_f mentioned at the end of Section 3, is then *well-balanced* in the sense that each block has prime density $1/3$ as was shown in [3]. The three blocks of the trichotomy were described in many interesting ways in [3, Thm. 5.1]. One way is readily seen to be in terms of Fibonacci rank:

- Odd ranked primes,
- Primes of even rank not divisible by 4,
- Primes of rank divisible by 4.

It was observed in [3, Section 6] that the trichotomy remained well-balanced for $f(x) = x^2 - (4a^2 + 2) + (-1)^2$, where $a = \frac{1}{2}(\varepsilon + \bar{\varepsilon})$, $a > 0$, if the fundamental unit $\varepsilon = a + b\sqrt{d}$ of $\mathbb{Q}(\sqrt{d})$, $d \geq 5$ square-free, has norm -1. Here, $(R, Q) = (4a^2, -1)$ and the associated Lehmer sequences $\bar{U}$ and $\bar{V}$ are essentially, i.e., up to a factor of $2a$ for even-indexed terms of $\bar{U}$ and odd-indexed terms of $\bar{V}$, the pair of Lucas sequences (U, V) with parameters $(P, S^2) = (4a^2 + 2, (-1)^2)$. Note in passing that the pair of Lehmer sequences with parameters $(1, -1)$ that corresponds to $a = 1/2$ and $\varepsilon = (1 + \sqrt{5})/2$ is equivalent to the pair with parameters $(5, 1)$ which was the object of Theorem 1.

Theorem 4 tells us the description of the prime trichotomy in terms of Fibonacci or Lucas ranks generalizes in terms of their ranks in the Lehmer sequence $\bar{U}(R, Q)$, when R is not a square integer. Indeed, prime divisors of $\bar{V}_{2n}$ are the primes of Lehmer rank divisible by 4, prime divisors of $\bar{V}_{2n+1}$ have rank exactly divisible by 2 (not by 4), and prime divisors of $\bar{U}_{2n+1}$ have odd rank.

We calculated the prime density of $\bar{V}(2, -1)$ in Section 2 to be $2/3$. We could have computed its prime density by calculating separately the prime density of

$(\bar{V}_{2n})$ and that of $(\bar{V}_{2n+1})$. The sequence $(\bar{V}_{2n})$ is the companion Lucas sequence

$$V_n(4,1) = (2+\sqrt{3})^n + (2-\sqrt{3})^n.$$

Since $2+\sqrt{3}(= a+b\sqrt{3})$ is the fundamental unit of $\mathbb{Q}(\sqrt{3})$, with norm 1 and $a-1$ is a square, we know from the main theorem of [11], that its prime density is $1/3$. Since we found that the prime density of $(\bar{U}_{2n+1})$ is $1/3$, we see that $(\bar{V}_{2n+1})$ must have prime density $1/3$. The prime trichotomy associated with $(R,Q) = (2,-1)$ is well-balanced.

We end the paper with an open question: Is it true that for almost all choices of R and Q, in the sense of [2], the associated prime trichotomy is well-balanced?

Acknowledgments. We are thankful to an anonymous referee for turning in a positive report very quickly and making a few remarks that improved our text.

References

[1] C. Ballot, Density of Prime Divisors of Linear Recurrences, *Mem. Amer. Math. Soc.* **551** (1995), 102 pages.

[2] C. Ballot, On the 1/3 density of odd ranked primes in Lucas sequences, *Unif. Distrib. Theory* **3** (2008), 129–145.

[3] C. Ballot and M. Elia, Rank and period of primes in the Fibonacci sequence. A trichotomy, *Fibonacci Quart.* **45** (2007), 56–63.

[4] C. Ballot and H. C. Williams, *The Lucas Sequences: Theory and Applications*, CMS/CAIMS Books in Mathematics, Springer, 2023.

[5] H. Hasse, Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von gerader bzw. ungerader Ordnung mod.p ist, *Math. Ann.* **166** (1966), 19–23.

[6] J. Lagarias, The set of primes dividing the Lucas numbers has density 2/3, *Pacific J. Math.* **118** (1985), 449–461; Errata: *Pacific J. Math.* **162** (1994), 393–397.

[7] R. Laxton, On groups of linear recurrences I, *Duke Math. J.* **26** (1969), 721–736.

[8] D. H. Lehmer, An extended theory of Lucas' functions, *Annals of Math.* **31** (1930), 419–448.

[9] D. H. Lehmer, On Lucas's test for the primality of Mersenne's numbers, *J. London Math. Soc.* **10** (1935), 162–165.

[10] D. A. Marcus, *Number Fields*, Springer-Verlag, 1977.

[11] P. Moree and P. Stevenhagen, Prime divisors of Lucas sequences, *Acta Arith.* **82** (1997), 403–410.

[12] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, first edition, 1982.