Uniform Distribution Theory **3** (2008), no.2, 129–145

uniform distribution theory

ON THE 1/3 DENSITY OF ODD RANKED PRIMES IN LUCAS SEQUENCES

Christian Ballot

ABSTRACT. It seems that companion Lucas sequences often have a two-third density of prime divisors. Is it indeed the case? And if so, why? In this paper we present heuristics that predict this 2/3 proportion before actually proving that 2/3 is the correct prime density for almost all companion Lucas sequences.

Communicated by Florian Luca

1. Introduction

We say that a set of primes S has a prime density if it has an asymptotic density within the set of all primes, i.e., if

$$\lim_{x\to\infty} \frac{\#\{p \le x\ ;\ p \in S\}}{\pi(x)} \text{ exists.}$$

If (x_n) is a sequence of rational integers then we define the associated set S of prime divisors of (x_n) as

$$S = \{p \text{ prime } ;\ p \text{ divides } x_n, \text{ for some } n\}.$$

We often write that $p \in S$ as $p \mid (x_n)$. If S has a prime density d, we say the sequence (x_n) has prime density d.

To a monic quadratic polynomial $f = X^2 - PX + Q \in \mathbb{Z}[X]$ with non-zero roots α and β, we associate the pair of Lucas sequences $\{(U_n),\ (V_n)\}$ defined for $n \ge 0$ by

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

We will also write $V_n = V_n(P,Q)$ and $U_n = U_n(P,Q)$ since these sequences are determined by the integers P and Q. The rank $\rho(p)$ of a prime p in (U_n) is the

2000 Mathematics Subject Classification: 11B39, 11B05.
Keywords: Prime density, Lucas sequence, Legendre symbol, number field.

smallest index $t > 0$ for which $p \mid U_t$. This rank always exists if $p \nmid Q$. This means that the prime density of (U_n) is always 1. Moreover we have that $p \mid U_n$ if and only if $\rho \mid n$. Because $U_{2n} = U_n V_n$ and $V_n^2 - DU_n^2 = 4Q^n$, where $D = P^2 - 4Q$ is the discriminant of f, we have for primes p not dividing $2Q$ that

$$2 \mid \rho(p) \iff p \mid (V_n). \tag{1}$$

The (V_n)-sequence is called the *companion Lucas sequence* and its prime density always exists [8]. In fact, for many choices of f it is known that the prime density of the associated (V_n)-sequence is equal to $2/3$. If α and β are rational integers and their ratio is not $\pm$ a square in $\mathbb{Q}$, or $\pm$ twice a square in $\mathbb{Q}$, then this density is equal to $2/3$ (see for instance [1], Theorem 3.1.3). As a consequence of the preceding facts, we have

$$\lim_{x \to +\infty} (4x^2)^{-1} \times \#\{(a,b) \in [-x,x]^2 \cap \mathbb{Z}^2;\ \delta(a^n + b^n) = 2/3\} = 1, \tag{2}$$

that is, $\delta(V_n) = 2/3$ for almost all reducible polynomials $f \in \mathbb{Z}[X]$.

For irreducible polynomials f, after Lagarias [8] computed the case of $f = X^2 - X - 1$, only specific families of recursions have been studied in [12] and [14]. Theorem 2 of [14] implies that for almost all integers P the prime density of the (V_n)-sequence associated to $f = X^2 - PX - 1$ is $2/3$. But the question of whether the $2/3$ density holds almost always for general f has not been settled. Note that (1) says that up to finitely many primes the divisors of (V_n) are the primes of even rank. All heuristics and proofs actually work out the density δ of odd ranked primes. This explains the title of the paper. Then of course one has that the density of the complementary set is $1 - \delta$.

Besides this introduction, the paper contains three sections. Section 2 and 3 deal with heuristics, while Section 4 proves a general density result. Section 2 is devoted to what we may call 'general heuristics' because the densities they yield are expected to be correct on average, or for most companion sequences. These heuristics are based on making general assumptions on the roots of f that hold for most f, but not for every f. Section 2 is divided into two subsections. Section 2.1 treats the case of reducible characteristic polynomials f. Section 2.2 treats the irreducible case.

Section 3 illustrates on three examples the fact that general heuristics can be adapted to specific companion Lucas sequences. Thus we present heuristics that yield correctly the prime densities of the three sequences $(2^n + 1)$, $\big((-4)^n + 1\big)$ and, how could we not?, the sequence of Lucas numbers $L_n = \varepsilon^n + \bar{\varepsilon}^n$, where $\varepsilon = (1 + \sqrt{5})/2$. The last two do have the expected $2/3$ density but do not obey the general heuristic. We note in passing that the $2/3$ density of the Lucas numbers, proved by Lagarias [8], was then shown to extend to a whole class of companion Lucas sequences associated to fundamental units ε of norm -1 in real

quadratic number fields [14]. The Lucas numbers correspond to the field $\mathbb{Q}(\sqrt{5})$. The 2/3 prime density associated with these fundamental units was given several interpretations in [4], where the set of primes was partitioned into three disjoint subsets B_1, B_2 and B_3 each of density 1/3. These three sets were described in various ways and the prime divisors of $\varepsilon^n + \bar{\varepsilon}^n$ are given by the union of B_1 and B_3.

We believe our probabilistic arguments often make these density results more transparent than rigorous proofs do. Indeed we strove to use only elementary arithmetic facts and language, i.e., mostly the arithmetic of $\mathbb{Z}/p\mathbb{Z}$ and the Dirichlet density theorem for primes in arithmetic progressions. Recall here that given integers m and a, $m \geq 2$ and $\gcd(a, m) = 1$, this theorem gives that the set of primes p congruent to $a \pmod m$ has prime density $\big(\varphi(m)\big)^{-1}$, where φ is the Euler totient function. We use the symbol $\square$ to mark the end of a heuristic argument although it is not a proof in the usual sense. The author has developped this heuristic approach in relation to various sets of primes [3]. Also it is worth mentioning here that Moree [13] has obtained asymptotic formulas for the function that counts primes $\leq x$ that divide a given companion Lucas sequence (in the reducible case), and that these formulas, albeit shown to be exact, were obtained first via heuristic reasonings.

In Section 4 we provide a proof that almost all companion Lucas sequences have a 2/3 prime density. By 'almost all' we mean that, as $x \to \infty$, the number of pairs (P, Q), $|P| \leq x$, $|Q| \leq x$, such that the prime density of $V_n(P, Q)$ is 2/3, is asymptotically equal to $4x^2$. The route we use is plain. The Hasse-Lagarias method [6, 7, 8] expresses that a prime p has odd rank in (U_n), i.e., that p does not divide the (V_n)-sequence, by the fact that p satisfies some splitting conditions in a number field $K_j = K_j(P, Q)$, where 2^j is the exact power of 2 in either $p-1$, or $p+1$. Primes satisfying splitting conditions in a given number field have a prime density which, in principle, can always be obtained by application of the Frobenius density theorem [9]. Here we identify a set of pairs (P, Q), which represents most polynomials f, such that the j-th partial prime densities of a companion Lucas sequence depend only on the degree of K_j over $\mathbb{Q}$ for each $j \geq 1$. Moreover, the degree of $K_j(P, Q)$ over $\mathbb{Q}$ is, for each $j \geq 1$, independent of the particular choice of the pair (P, Q) within that set. That is, the degree K_j over $\mathbb{Q}$ is a function of j only. The prime density of the companion Lucas sequence $V_n(P, Q)$, obtained by summing partial densities over all j's, is then the same for any choice of (P, Q) in that general set and it is 2/3.

We introduce some notation. The ratio α/β of the roots of f is denoted by r throughout the paper. The letter p always denotes a rational prime. The expression $(n \mid p)$ stands for the value of the Legendre symbol of the integer n

with respect to p. We write $p^k \,||\, n$ to signify that the p-adic valuation of n with respect to p is equal to k. If S is a finite set, then $\sharp S$ denotes the cardinality of S. The Vinogradov symbol $\ll$ is used with its usual meaning. For $a \in \mathbb{N}$, ζ_a denotes the complex number $e^{2\pi i/a}$.

Prime density results are unchanged if we remove or add finitely many primes from a given set. Thus we are satisfied to say that a result holds if it holds up to finitely many primes whether we mention the exceptional primes or not.

Before getting started we rephrase the problem in terms of primitive divisors. It is known [5] that if $n > 30$ and $(U_t)_{t\geq 0}$ is any Lucas sequence then U_n has a *primitive prime divisor*, i.e., U_n has a prime factor p, which is not a prime factor of any U_m with $0 < m < n$. So why would even-indexed terms U_{2n} have twice as many primitive prime factors as odd-indexed terms U_{2n+1}?

2. General Heuristics

2.1. The reducible case.

We begin by addressing the case of a reducible polynomial f.

By (1), our problem reduces to estimating the probability that $\rho(p)$ be odd. Let r be the ratio of the roots of f. For all but finitely many primes p, the rank $\rho(p)$ is the order of $r \pmod p$.

Assume that r is not the k-th power of a rational number for any $k \geq 2$. Then we make the assumption that, as p varies through the primes not dividing Q, the value of $r \pmod p$ is as likely to be any non-zero residue class $\pmod p$ as any other. If $2^j \,||\, p-1$, then there are precisely $(p-1)/2^j$ non-zero residue classes of odd order $\pmod p$. Thus the probability that $\rho(p)$ be odd is 2^{-j}. By Dirichlet's theorem for primes in arithmetic progressions, primes $p \equiv 1 + 2^j \pmod{2^{j+1}}$ have prime density $d_j = 2^{-j}$ so that the probability that $\rho(p)$ be odd as p varies is estimated by the weighted sum

$$\sum_{j\geq 1} d_j \times \ \mathrm{Prob}_{\nu_2(p-1)=j}\{\rho(p) \text{ is odd}\} = \sum_{j\geq 1} 2^{-j} \times 2^{-j} = 1/3, \tag{3}$$

where $\mathrm{Prob}_{\nu_2(p-1)=j}\{\rho(p) \text{ is odd}\}$ stands for the probability that the order of $r \pmod p$ be odd given that $2^j \,||\, p-1$. □

2.2. The irreducible case.

Here we assume the root ratio r to not be a k-th power of an algebraic number in $\mathbb{Q}(\alpha)$. If D is a square $\pmod p$, then $\mathbb{Z}/p\mathbb{Z}$ contains the square roots of D, the roots of f and therefore r. So the heuristic of Section 2.1 can be reiterated

with d_j representing instead the prime density of the set S_j^+ of primes p with $p-1=2^j m$, m odd, *and* $(D \mid p)=1$. Having in mind that D is not a square integer since f is irreducible and using the reciprocity properties of the Legendre and the Jacobi symbols, one can see that the condition $(D \mid p)=1$ is satisfied for half the residues in $(\mathbb{Z}/D^0\mathbb{Z})^*$, where D^0 is either the squarefree part of $|D|$, or four times the squarefree part of $|D|$. Hence by the Dirichlet density theorem (mod D^0), the density of primes p for which $(D \mid p)=1$ is $1/2$. If we assume that the condition $(D \mid p)=1$ is 'independent' of the condition $p \equiv 1+2^j \pmod{2^{j+1}}$, for each $j \geq 1$, then the density d_j is $2^{-1} \times 2^{-j}$. Thus as in (3) the sum

$$\sum_{j\geq 1} d_j \times \operatorname*{Prob}_{\substack{\nu_2(p-1)=j \\ (D|p)=1}} \{\rho(p) \text{ is odd}\} = \sum_{j\geq 1} 2^{-j-1} \times 2^{-j} = 1/6\,,$$

yields an expected prime density of $1/6$ for primes p with $\rho(p)$ odd and $(D \mid p)=1$.

It is important to note that our independence assumption can be false. For instance, one easily checks it is false for $D=-4$ and $j=1$, or for $D=8$ and $j=2$. Using the arguments in the proof of Theorem 1 of Section 4 giving the degree of the number field $\mathbb{Q}(\sqrt{D},\zeta_{2^j})$, it is easily seen that the prime density of S_j^+ is 2^{-j-1} whenever $D \neq \pm z^2,\ \pm 2z^2$ for any $z \in \mathbb{N}$. Proving it by elementary means is longer to write down. There are four cases according to whether the squarefree part, Δ, of D is odd and >0, odd and <0, even and >0, or even and <0. We will only detail the simplest of the four cases, i.e., Δ odd >0. Since $D \neq z^2$ for any $z \in \mathbb{N}$, Δ is odd and ≥ 3. Note that for any squarefree odd $m \geq 3$ the groups

$$\big(\mathbb{Z}/m\big)^* \quad \text{and} \quad \bigotimes_{\substack{q\mid m \\ q \text{ prime}}} \big(\mathbb{Z}/q\big)^*$$

are isomorphic and $(p \mid q)=1$ for $(q-1)/2$ values of $p \pmod q$, so that the Jacobi symbol $(p \mid m)=1$ if and only if $p \pmod m$ belongs to a set $\mathcal{R}$ of reduced residues (mod m) of cardinality $\varphi(m)/2$. We seek to show that S_j^+ has a prime density of value 2^{-j-1} for each $j \geq 1$. If $\Delta \equiv 1 \pmod 4$, then $(D \mid p)=1$ if and only if the Jacobi symbol $(p \mid \Delta)=1$. But $(p \mid \Delta)=1$ holds for p belonging to a set $\mathcal{R}$ of reduced residues (mod Δ) of cardinality $\varphi(\Delta)/2$. Using the Chinese Remainder theorem and the Dirichlet density theorem, we find that S_j^+ has prime density $\#\mathcal{R}/\varphi(2^{j+1}\Delta) = 2^{-j-1}$. Assume now that $\Delta \equiv 3 \pmod 4$. For primes $p \equiv 1 \pmod 4$ again $(D \mid p)=1$ if and only if $(p \mid \Delta)=1$, a condition that holds for p belonging to a set $\mathcal{R}$ of reduced residues (mod Δ) of cardinality $\#\mathcal{R}=\varphi(\Delta)/2$. On the other hand for primes $p \equiv 3 \pmod 4$, $(D \mid p)=1$ if and only if $(p \mid \Delta)=-1$, which holds for $p \pmod \Delta$ belonging to $\mathcal{S} = \big(\mathbb{Z}/\Delta\big)^* \backslash \mathcal{R}$.

If $j = 1$, then $p \in S_1^+$ if and only if $p \pmod 4$ is 3 and $p \pmod \Delta \in \mathcal{S}$. By the Chinese Remainder theorem and the Dirichlet density theorem, S_1^+ has a prime density equal to $\#\mathcal{S}/\varphi(4\Delta) = 1/4 = 2^{-j-1}$. If $j \geq 2$, primes in S_j^+ are all $1 \pmod 4$ so $p \in S_j^+$ if and only if $p \pmod{2^{j+1}}$ is $1 + 2^j$ and $p \pmod \Delta \in \mathcal{R}$. Therefore the prime density of S_j^+ is

$$\#\mathcal{R}/\varphi(2^{j+1}\Delta) = \varphi(\Delta)/2\varphi(2^{j+1})\varphi(\Delta) = 2^{-j-1}.$$

If D is not a square $\pmod p$, then $\mathbb{Z}[\sqrt{D}]/(p)$ is a field with p^2 elements. Thus, if $p \nmid Q$, then the order of $r \pmod{(p)}$ divides $p^2 - 1$. Using elementary Lucas theory (the binomial formula and Fermat's little theorem suffice), one gets that $U_p \equiv (D \mid p) \pmod p$ and $V_p \equiv P \pmod p$. But we have $2U_{p+1} = U_pV_1 + U_1V_p \equiv (D \mid p) \cdot P + P = 0 \pmod p$. Thus if p is odd $\rho(p)$ divides $p + 1$ and so $r \pmod{(p)}$ belongs to the cyclic subgroup C_{p+1} of order $p + 1$ of $\big(\mathbb{Z}[\sqrt{D}]/(p)\big)^*$. The set of primes p satisfying $2^j || p + 1$ has prime density 2^{-j} by Dirichlet's density theorem for primes in arithmetic progressions, while the set of primes p satisfying $(D \mid p) = -1$ has density $1/2$. If we assume independence of the conditions $2^j || p + 1$ and $(D \mid p) = -1$, the intersection of these two sets has density $d_j = 2^{-j-1}$. This independence is met whenever $D \neq \epsilon z^2$ for any $\epsilon \in \{\pm 1, \pm 2\}$ and $z \in \mathbb{N}$. Fixing $j \geq 1$ such that $2^j || p + 1$ and assuming that $r \pmod{(p)}$ is as likely to be any residue in C_{p+1} as any other, the probability that $\rho(p)$ be odd is $(p + 1)/2^j$ divided by $p + 1$, i.e., 2^{-j}. Therefore we expect primes p with $(D \mid p) = -1$ and $\rho(p)$ odd to have a prime density equal to

$$\sum_{j \geq 1} d_j \times \operatorname*{Prob}_{\substack{\nu_2(p+1)=j \\ (D|p)=-1}} \{\rho(p) \text{ is odd}\} = 2^{-1} \sum_{j \geq 1} 4^{-j} = 1/6.$$

Thus the expected prime density of primes with $\rho(p)$ odd is twice $1/6$, that is again $1/3$. □

3. Adapting the general heuristics to specific sequences

The heuristics presented to compute the prime density of divisors of generic (V_n) Lucas sequences in Section 2 may be valid on average, as in the sense of (2), yet produce the wrong density for specific (V_n)-sequences. Here, we stress the fact that one can often adjust the heuristic to specific (V_n)-sequences. For instance, $\delta(2^n + 1) = 17/24$, not $2/3$. Indeed, taking into account a few arithmetic facts the heuristic of Section 2.1 leads to the correct density. These arithmetic facts are

i) if $2^1 \,||\, p-1$, then either $p \equiv 3 \pmod 8$, or $p \equiv 7 \pmod 8$. But only when p is congruent to 7 (mod 8) do we have that 2 is a quadratic residue (mod p) and its order (mod p) is odd. By the Dirichlet density theorem such primes have density 1/4,

ii) if $2^2 \,||\, p-1$, then 2 is a quadratic non-residue (mod p) so that the order of 2 (mod p) must be even, and

iii) if $2^3 \mid p-1$, then 2 is a quadratic residue (mod p) so that the probability that the order of 2 (mod p) be odd is $2^{-j+1} = \big(2^{-j}(p-1)\big)/\big(2^{-1}(p-1)\big)$ instead of 2^{-j} for $j \geq 3$.

Hence, the sum evaluated in (3) becomes

$$\sum_{j\geq 1} d_j \times \text{ Prob}_{\nu_2(p-1)=j}\{\text{order of } 2 \pmod p \text{ is odd }\} =$$

$$= 4^{-1} + 0 + \sum_{j\geq 3} 2^{-j} \times 2^{-j+1} = \frac{1}{4} + 2 \times \frac{1}{4^3} \times \frac{1}{1-1/4} = 7/24.$$

□

Theorem 3.1.3 of [1] gave the value of the asymptotic density of $\delta(a^n + b^n)$ for any choice of integers a and b. We contend that our heuristic can be adjusted so as to yield the correct density for each such sequence. Let us give another example. We know that $\delta((-4)^n + 1) = 2/3$. Let us again estimate the probability that $r = -4$ be of odd order (mod p) for primes p with $\nu_2(p-1) = j \geq 1$. For $j = 1$ observe that r is a quadratic non-residue so that the order of r (mod p) is never odd. If $j = 2$, then -1 is a square but not a fourth power (mod p). Also since 2 is a quadratic non-residue, 4 is a square but not a fourth power (mod p). Thus $-4 = x^2y^2$, with x and y quadratic non-residues (mod p). Hence -4 is a fourth power which implies that its order (mod p) is odd. So far our arguments are proofs. For $j \geq 3$, 4 and -1 are both at least fourth powers (mod p) so that -4 is at least a fourth power and Prob $_{\nu_2(p-1)=j}\{-4 \,(\text{mod } p) \text{ has odd order}\} = 2^{2-j}$. Thus with d_j still standing for the prime density of $\{p \,;\, \nu_2(p-1) = j\}$

$$\sum_{j\geq 1} d_j \times \text{ Prob}_{\nu_2(p-1)=j}\{\text{order of } -4 \pmod p \text{ is odd }\} =$$

$$= 0 + \sum_{j\geq 2} 2^{-j} \times 2^{2-j} = 4 \times \frac{1}{4^2} \times \frac{1}{1-1/4} = 1/3.$$

□

Let us now treat the case of the Lucas numbers, i.e., the case of $V_n = L_n = \varepsilon^n + \bar{\varepsilon}^n$, where $\varepsilon = (1+\sqrt{5})/2$ and $\bar{\varepsilon} = (1-\sqrt{5})/2$. The associated (U_n)-sequence is the sequence of Fibonacci numbers (F_n). We know that $\delta(L_n) = 2/3$ [8]. The polynomial $f = X^2 - X - 1$ is irreducible over $\mathbb{Z}$ and we may think that

the heuristic of Section 2.2 apply. However, this heuristic does not predict a distinct behavior for primes congruent to $\pm 1 \pmod 5$ and primes congruent to $\pm 2 \pmod 5$. But the density of primes $\pm 1 \pmod 5$ that do not divide (L_n) is only $1/12$ whereas the density of primes $\pm 2 \pmod 5$ not dividing any Lucas number is $1/4$, i.e., three times more. Again we will adjust the heuristic of Section 2.2 and come up with a heuristic argument that predicts these two partial densities. In fact for primes $\pm 2 \pmod 5$ there is no need for a probabilistic point of view since a very simple proof is available. We will try to make the argument as elementary as can be.

Observe that the rank $\rho(p)$ of a prime p in (F_n) is the order of $\varepsilon/\bar{\varepsilon} = -\varepsilon^2$ in the ring $\mathbb{Z}[\varepsilon]$ modulo the ideal (p) generated by p.

First assume that $p \equiv \pm 2 \pmod 5$ so that by the quadratic reciprocity law 5 is a quadratic non-residue (mod p). Hence $X^2 - X - 1$ has no roots in $\mathbb{Z}/p\mathbb{Z}$. These roots lie in a quadratic extension of $\mathbb{Z}/p\mathbb{Z}$ and the quotient ring $\mathbb{Z}[\varepsilon]/(p)$ is isomorphic to the finite field of p^2 elements. Note that $0 = (\varepsilon^2 - \varepsilon - 1)^p \equiv \varepsilon^{2p} - \varepsilon^p - 1 \pmod{(p)}$ in $\mathbb{Z}[\varepsilon]$. So ε^p must be congruent to one of the two roots of $X^2 - X - 1 \pmod{(p)}$. It cannot be ε since it would say that $\varepsilon^{p-1} \equiv 1 \pmod{(p)}$ implying that ε lies in the subgroup $(\mathbb{Z}/p\mathbb{Z})^*$ of the cyclic group $\big(\mathbb{Z}[\varepsilon]/(p)\big)^*$. So $\varepsilon^p \equiv \bar{\varepsilon} \pmod{(p)}$. Hence

$$(-\varepsilon^2)^{(p+1)/2} = (-1)^{(p+1)/2}\varepsilon^{p+1} \equiv (-1)^{(p+1)/2}\varepsilon\bar{\varepsilon} = (-1)^{(p-1)/2} \pmod{(p)}.$$

If $p \equiv 1 \pmod 4$, then $(p+1)/2$ is odd so $\rho(p)$ is odd. If $p \equiv 3 \pmod 4$, then $(-\varepsilon^2)^{(p+1)/2} \equiv -1 \pmod{(p)}$ and $p \mid L_{(p+1)/2}$. Thus $\rho(p)$ is odd for primes in $\{p\ ;\ p \equiv \pm 2 \pmod 5 \text{ and } p \equiv 1 \pmod 4\}$, which by the Chinese remainder theorem corresponds to all primes in two arithmetic progressions (mod 20), a set of prime density $1/4$ by the Dirichlet density theorem.

Consider now primes p congruent to $\pm 1 \pmod 5$ so that $\mathbb{Z}/p\mathbb{Z}$ contains square roots of 5 and roots of $X^2 - X - 1$. Write j for $\nu_2(p-1)$.

For the case of $j = 1$ we use an old argument of Ward [15]. Recall that for all $n \geq 0$

$$L_n^2 - 5F_n^2 = 4(-1)^n. \tag{4}$$

Assume $\rho(p)$ odd and put $n = \rho(p)$ in (4). One gets

$$L_{\rho(p)}^2 \equiv -4 \pmod p,$$

so -1 is a quadratic residue (mod p). This contradicts the hypothesis $p \equiv 3 \pmod 4$ so $\rho(p)$ must be even.

Assume $j \geq 2$. Then -1 being a square (mod p), so is $-\varepsilon^2$. We make the probabilistic assumption that, on average as p varies through primes that satisfy $\nu_2(p-1) = j$, $-\varepsilon^2 \pmod p$ is as likely to be any of the $(p-1)/2$ quadratic residues (mod p) as any other. Since $2^{-j}(p-1)$ quadratic residues (mod p) have

odd order, $\rho(p)$ is odd with probability $P_j = \big(2^{-j}(p-1)\big)/\big(2^{-1}(p-1)\big) = 2^{-j+1}$. By the Dirichlet density theorem the primes p congruent to $\pm 1 \pmod 5$ and congruent to $1+2^j \pmod{2^{j+1}}$ have prime density $d_j = 2^{-j-1}$. Hence as we did in earlier heuristics the density of primes $p \equiv \pm 1 \pmod 5$ having odd rank $\rho(p)$ is evaluated by the sum

$$\sum_{j\geq 2} d_j \times P_j = \sum_{j\geq 2} 4^{-j} = 1/12.$$

□

4. An 'almost all' proof.

Given a real number $x > 1$, we define B_x as the plane square box

$$B_x = \{(P,Q) \in \mathbb{Z} \times \mathbb{Z}\ ;\ |P| \leq x,\ |Q| \leq x\}.$$

Since $\sharp B_x$ is asymptotic to $4x^2$ as $x \to \infty$, we say that a property that depends on (P,Q) holds for almost all (P,Q)'s if the ratio of the number of pairs (P,Q) in B_x satisfying the property to $4x^2$ tends to 1 as $x \to \infty$. For a subset S of $\mathbb{Z} \times \mathbb{Z}$, we denote the intersection $S \cap B_x$ by $S(x)$ and say that S is *negligible* if $\sharp S(x)$ is $o(x^2)$ as $x \to \infty$.

Theorem 1. *For almost all integer pairs (P,Q), the prime density of the companion Lucas sequence $V_n(P,Q)$ is 2/3.*

We will establish several lemmas before giving a proof of Theorem 1. The first lemma is trivial.

Lemma 2. *Let I be a real interval of length $\ell > 1$ and ν be the number of square integers in I. Then $\nu \ll \sqrt{\ell}$ as $\ell \to \infty$.*

Proof. There is no loss of generality assuming that I is an interval of the form $]a,b]$ where $0 < a < a+1 \leq b$. Then ν is the difference between the number of square integers in $]0,b]$ and the number of square integers in $]0,a]$. Therefore

$$\nu \leq \sqrt{b} - \lfloor \sqrt{a}\ \rfloor \leq \sqrt{b} - \sqrt{a} + 1 \leq \ell/(\sqrt{a} + \sqrt{b}\ ) + 1 < \ell/\sqrt{\ell} + 1 \ll \sqrt{\ell}.$$

□

Lemma 3. *The three sets S_1, S_2 and S_3 of pairs $(P,Q) \in \mathbb{Z}\times\mathbb{Z}$ defined respectively by one of the three conditions below*

$$\begin{aligned} &i) \quad Q = \pm z^2 \quad &or \quad \pm 2z^2, \qquad &z \in \mathbb{N}\,; \\ &ii) \quad D = \pm z^2 \quad &or \quad \pm 2z^2, \qquad &z \in \mathbb{N}\,; \\ &iii) \quad D = \pm Qy^2 \quad &or \quad \pm 2Qy^2, \qquad &y \in \mathbb{Q}\,, \end{aligned}$$

where $D = P^2 - 4Q$, are each negligible.

Proof. We show first that S_1 is negligible. Fix a positive real number x. If $(P,Q) \in S_1(x)$, then Q is associated with a $z \in \mathbb{N}$ with either z^2 in $[0,x]$, $-z^2$ in $[-x,0]$, z^2 in $[0,x/2]$, or $-z^2$ in $[-x/2,0]$. Applying Lemma 2 four times we get at once that

$$\sharp\{Q\,;\ |Q| \le x \ \text{ such that } \ \exists P \in \mathbb{Z},\ (P,Q) \in S_1(x)\} \ll \sqrt{x}.$$

Therefore $\sharp S_1(x) \ll x\sqrt{x}$.

To show that S_2 is negligible we fix again $x > 0$. Let P be an integer in $[-x,x]$ and let ν_P be the number of integers $Q \in [-x,x]$ such that there are a $z \in \mathbb{N}$ and an $\epsilon \in \{\pm 1, \pm 2\}$ with $D = P^2 - 4Q = \epsilon z^2$. Then $\epsilon z^2 \in [P^2 - 4x, P^2 + 4x]$, and so z^2 belongs to an interval I_P of length $8x/|\epsilon|$ for each of the four values of ϵ. Lemma 2 gives that the number of square integers in I_P is $\ll \sqrt{x}$ so that $\nu_P \ll \sqrt{x}$ and $\sharp S_2(x) \ll x\sqrt{x}$. We have shown that S_2 is negligible.

Fix $x > 0$ and assume (P,Q) belongs to $S_3(x)$. Then $P^2 - 4Q = \epsilon Q y^2$ for some $y \in \mathbb{Q}$ and some $\epsilon \in \{\pm 1, \pm 2\}$. Putting $y = a/b$, where a and b are coprime integers, we obtain

$$b^2 P^2 = Q\epsilon\big(4b^2/\epsilon + a^2\big).$$

Since b^2 and $(4b^2/\epsilon) + a^2$ are two coprime integers, we have that

$$b^2 \mid Q\epsilon \quad \text{ and } \quad Q\epsilon \mid b^2 P^2,$$

so that $Q\epsilon$ is of the form $\pm dz^2$ with d a positive divisor of P^2 and z a natural number. Fixing such a d the number $\nu_d(x)$ of integers Q, $|Q| \le x$, $Q\epsilon = \pm dz^2$ for some z is $\ll\sqrt{x}$ since $z^2 \le 2|Q|/d \le 2x/d \le 2x$. Therefore

$$\sharp S_3(x) \ll \sqrt{x} \sum_{|P|\le x} \tau(P^2),$$

where $\tau(n)$ denotes the number of positive divisors of the integer n. Note that if $P = \prod p^{\alpha_p}$ is the prime factorisation of P, then $\tau(P^2) = \prod_{p|P}(2\alpha_p + 1) < 2^{\omega(P)} \prod_{p|P}(\alpha_p + 1) = 2^{\omega(P)}\tau(P)$, where $\omega(n)$ is the number of distinct prime

factors of the integer n. Knowing that $\omega(n) \ll \log n/\log\log n$ we have for all $P \in [-x, x]$, $\omega(P) \ll \log x/\log\log x$. Hence

$$\tau(P^2) \ll 2^{\log x/\log\log x}\tau(P) < e^{\log x/\log\log x}\tau(P) = x^{1/\log\log x}\tau(P),$$

and using the well known estimate $\sum_{n\le x}\tau(n) \sim x\log x$ we conclude that for every $\eta > 0$

$$\begin{aligned}\sqrt{x}\sum_{|P|\le x}\tau(P^2) &\ll \sqrt{x}\,x^{1/\log\log x}\sum_{|P|\le x}\tau(P)\\ &\ll \sqrt{x}\,x^{1/\log\log x}x\log x \ll x^{3/2+\eta},\end{aligned}$$

so that $\sharp S_3(x) = o(x^2)$. [1] □

To prove Theorem 1 we will only consider irreducible polynomials X^2-PX+Q since Lemma 3 tells us that reducible polynomials with $D \in \mathbb{N}^2$ are negligible. The Hasse method as adapted by Lagarias [8] distinguishes primes that split in $\mathbb{Q}(\sqrt{D}\,)$ from inert primes. This method is sketched in the proofs of the following lemmas, but we refer the reader to [8] for details on the Hasse-Lagarias method.

Define for $j \ge 1$ the sets of primes

$$\begin{aligned}S_j^+ &= \{p\,;\,(D\mid p) = 1 \text{ and } 2^j \mid\mid p-1\},\\ D_j^+ &= \{p \in S_j^+\,;\,\rho(p) \text{ exists and is odd }\},\\ S_j^- &= \{p\,;\,(D\mid p) = -1 \text{ and } 2^j \mid\mid p+1\},\\ D_j^- &= \{p \in S_j^-\,;\,\rho(p) \text{ exists and is odd }\},\end{aligned}$$

and the two number fields

$$L_j = \mathbb{Q}\big(\zeta_{2^j}, \sqrt{D}, \sqrt[2^j]{r}\big)$$

and

$$K_j = L_j\big(\zeta_{2^{j+1}}\big).$$

Lemma 4. *The field extensions $L_j/\mathbb{Q}$ and $K_j/\mathbb{Q}$ are normal.*

Proof. It suffices to show that the algebraic conjugates of $\sqrt[2^j]{r}$ all lie in L_j. Note that $\sqrt[2^j]{r}$ is a root of the polynomial $M(X) = X^{2^{j+1}}-(r+\bar r)X^{2^j}+1 \in \mathbb{Q}[X]$, where $\bar r = \bar\alpha/\alpha$. The roots of $M(X)$ are all of the form $\zeta_{2^j}^k\sqrt[2^j]{r}$ or $\zeta_{2^j}^k\sqrt[2^j]{\bar r}$ for $k = 1, 2, 3, \ldots, 2^j$, where $\sqrt[2^j]{r}$ is a 2^j-th root of r and $\sqrt[2^j]{\bar r} = \big(\sqrt[2^j]{r}\big)^{-1}$. These roots all lie in the number field generated by ζ_{2^j} and $\sqrt[2^j]{r}$; thus they lie in L_j. □

[1] This last proof can be somewhat shortened by noting that $\tau(P^2) \le \tau(P)^2$ and then by using the estimate $\sum_{n\le x}\tau(n)^2 = O(x\log^3 x)$.

Lemma 5. *Let p be a prime not dividing $2Q$. We have for any $j \geq 1$,*

$$p \in D_j^+ \text{ if and only if } p \text{ splits completely in } L_j, \text{ but not in } K_j\,;$$

for primes $p \in S_j^-$, we have $p \in D_j^-$ if and only if

$$p \text{ is inert in } \mathbb{Q}(\sqrt{D}) \text{ and splits completely from } \mathbb{Q}(\sqrt{D}) \text{ to } K_j\,,$$
$$\text{and the congruence } r^{(p+1)/2^j} \equiv 1 \pmod{(p)}, \text{ in } \mathbb{Q}(\sqrt{D}), \text{ holds.}$$

Sketch of proof. Denote by O_D the ring of integers of $\mathbb{Q}(\sqrt{D})$. For a split prime p let $(p) = \pi\bar{\pi}$ be the prime ideal decomposition of (p) in O_D. Since the algebraic conjugate $\bar{r}$ of $r = \alpha/\bar{\alpha}$ is its inverse r^{-1}, we claim that the order of $r \pmod{\pi}$ is equal to $\rho(p)$, the order of $r \pmod{(p)}$. Indeed, $r^n \equiv 1 \pmod{\pi} \implies (r^{-1})^n \equiv 1 \pmod{\pi}$, which by algebraic conjugation gives $r^n \equiv 1 \pmod{\bar{\pi}}$. But $(p) = \pi\bar{\pi} = \pi \cap \bar{\pi}$ so the claim follows. Indeed, the reverse direction '$r^n \equiv 1 \pmod{(p)} \implies r^n \equiv 1 \pmod{\pi}$' holds because $(p) \subset \pi$.

Thus we have for primes $p \in S_j^+$ that $\rho(p)$ is odd if and only if $r^{(p-1)/2^j} \equiv 1 \pmod{\pi}$, a congruence in O_D which holds if and only if, by Euler's criterion, $X^{2^j} - r = 0$ is solvable $\pmod{\pi}$. Since $p \equiv 1 \pmod{2^j}$, the solvability of the foregoing equation gives via the Kummer-Dedekind theorem that p splits completely in L_j, but not in K_j since $p \not\equiv 1 \pmod{2^{j+1}}$. The converse follows at once using the Kummer-Dedekind theorem in the reverse direction.

Now let p be a prime in S_j^- and $\mathcal{P}$ be a prime ideal above p in K_j. Since $K_j/\mathbb{Q}$ is normal, we may consider the Frobenius automorphism ψ of $\mathcal{P}$ over p. Because $(D \mid p) = -1$, p is inert in $\mathbb{Q}(\sqrt{D})$ so that the restriction of ψ to $\mathbb{Q}(\sqrt{D})$ acts as the non-trivial automorphism of $\mathbb{Q}(\sqrt{D})$ over $\mathbb{Q}$. Therefore we have $r^{-1} = \bar{r} = \psi(r) \equiv r^p \pmod{(p)}$ implying that $r^{p+1} \equiv 1 \pmod{(p)}$. Hence $\rho(p)$ is a divisor of $p+1$. Thus for primes in S_j^-, $\rho(p)$ is odd if and only if $r^{(p+1)/2^j} \equiv 1 \pmod{(p)}$, which says that r is at least a 2^j-th power $\pmod{(p)}$. Hence $X^{2^j} - r = 0$ is solvable $\pmod{(p)}$ in $\mathbb{Q}(\sqrt{D})$ and, by the Kummer-Dedekind theorem, (p) in O_D splits completely in L_j. Therefore the restriction of ψ^2 to L_j is the identity. But $p \equiv -1 + 2^j \pmod{2^{j+1}}$ implies that $p^2 \equiv 1 \pmod{2^{j+1}}$, so that $\psi^2(\zeta_{2^{j+1}}) \equiv \zeta_{2^{j+1}} \pmod{\mathcal{P}}$. But since $p \neq 2$ we have $\psi^2(\zeta_{2^{j+1}}) = \zeta_{2^{j+1}}$. Because $K_j = L_j(\zeta_{2^{j+1}})$, ψ^2 is the identity on K_j as well. Hence the ideal (p) in $\mathbb{Q}(\sqrt{D})$ splits completely in K_j. □

Lemma 6. *The sets D_j^+ and D_j^- have a prime density for each $j \geq 1$. Their values δ_j^+ and δ_j^- satisfy*

$$\begin{aligned}\delta_j^+ &= [L_j : \mathbb{Q}]^{-1} - [K_j : \mathbb{Q}]^{-1};\\ \delta_j^- &= [K_j : \mathbb{Q}]^{-1}, \text{ if } [K_j : \mathbb{Q}] = 2 \cdot 4^j.\end{aligned}$$

P r o o f. Because L_j and K_j are normal over $\mathbb{Q}$ and D_j^+ is the set difference between primes that split completely in L_j and primes that split completely in K_j, the Chebotarev density theorem yields the existence and the value claimed for δ_j^+.

To alleviate notation we will write r_j instead of $\sqrt[2^j]{r}$. We write O_{K_j} for the ring of integers of K_j. Assume p is a prime in D_j^- and $\mathcal{P}$ a prime ideal in K_j lying above p. Denote by ψ the Frobenius automorphism of $\mathcal{P}$ over p. Note that $p \equiv -1 + 2^j \pmod{2^{j+1}}$ if and only if $\psi(\zeta_{2^{j+1}}) \equiv \zeta_{2^{j+1}}^{-1+2^j} = -\zeta_{2^{j+1}}^{-1} \pmod{\mathcal{P}}$ so that $\psi(\zeta_{2^{j+1}}) = -\zeta_{2^{j+1}}^{-1}$. Because ψ is an automorphism of K_j over $\mathbb{Q}$ that maps a root of $X^{2^j} - r$ to a root of $X^{2^j} - r^{-1}$, $\psi(r_j) = \zeta_{2^j}^k r_j^{-1}$ for some $k \in \{1, 2, \ldots, 2^j\}$. Since, by Lemma 5, ψ has order 2, we have $r_j = \psi^2(r_j) = \zeta_{2^j}^{-2k} r_j$ so that k must be either 2^{j-1} or 2^j. Thus $\psi(r_j) = \pm r_j^{-1}$. However the case $\psi(r_j) = -r_j^{-1}$ does not occur. Indeed, r_j is not integral, but for p not dividing Q, $r_j \pmod{\mathcal{P}}$ belongs to $\left(O_{K_j}/\mathcal{P}\right)^*$ so that we may write $\psi(r_j) \equiv r_j^p = r_j^{-1} r_j^{p+1} \pmod{\mathcal{P}}$. But $r_j^{p+1} = r^{(p+1)/2^j} \equiv 1 \pmod{\mathcal{P}}$ and therefore $\psi(r_j) \equiv r_j^{-1} \pmod{\mathcal{P}}$. If $p \neq 2$, $-r_j^{-1} \not\equiv r_j^{-1} \pmod{\mathcal{P}}$ and we conclude that $\psi(r_j) = r_j^{-1}$. Thus, the Frobenius automorphism of $\mathcal{P}$ over p is a determined element of the Galois group, G_j, of K_j over $\mathbb{Q}$, since elements of this group are fully determined by their action on $\zeta_{2^{j+1}}$ and r_j. Moreover, it is independent of the choice of the ideal $\mathcal{P}$ above p in K_j. This means that ψ is a central element of that group. (This can also be checked by direct calculation. If σ is an element of G_j, then σ is determined by a triplet (a, b, ν) where $\sigma(\zeta_{2^{j+1}}) = \zeta_{2^{j+1}}^a$, $\sigma(r_j) = \zeta_{2^j}^b r_j^\nu$, with a, b integers, a odd, $1 \leq a < 2^{j+1}$, $1 \leq b \leq 2^j$ and $\nu = \pm 1$. Then $\sigma\psi\sigma^{-1}$ acts on $\zeta_{2^{j+1}}$ and r_j as ψ does. Hence $\sigma\psi\sigma^{-1} = \psi$.)

Conversely, assume p is a prime with an associated Frobenius automorphism $\psi = \psi(\mathcal{P}/p)$ that satisfies

$$\psi(r_j) = r_j^{-1} \quad \text{and} \quad \psi(\zeta_{2^{j+1}}) = -\zeta_{2^{j+1}}^{-1}. \tag{5}$$

As seen before the second condition in (5) above says that $p \in S_j^-$. Also (5) implies that $\psi^2 = id$ and that the restriction of ψ to $\mathbb{Q}(\sqrt{D})$ is the non-trivial automorphism of $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$, since $\psi(r) = \psi(r_j)^{2^j} = r_j^{-2^j} = r^{-1}$. Thus p is inert in $\mathbb{Q}(\sqrt{D})$ and splits completely from there on to K_j. Moreover, $1 = r_j r_j^{-1} =$

$r_j\psi(r_j) \equiv r_j r_j^p = r^{(p+1)/2^j} \pmod{\mathcal{P}}$, for any $\mathcal{P}$ above (p) in K_j, so that $\rho(p)$ is odd. Hence $p \in D_j^-$.

However, without our condition on the degree of K_j over $\mathbb{Q}$, there would be no guarantee that D_j^- is not empty. Indeed, for example, as shown in Section 3 for the case of $V_n = L_n$, the sequence of Lucas numbers, there are no primes in D_j^-, for any $j \geq 2$. The condition $[K_j : \mathbb{Q}] = 2 \cdot 4^j$ is sufficient to ensure the existence of a ψ in G_j that satisfies the conditions in (5). Indeed, an element of G_j must map $\zeta_{2^{j+1}}$ to one of its 2^j conjugates and map r_j to one of the 2^{j+1} numbers $\zeta_{2^j}^k \cdot r_j^\nu$, where k is defined (mod 2^j) and $\nu = \pm 1$. Thus G_j may contain up to $2^j \times 2^{j+1} = 2 \cdot 4^j$ elements. If G_j does have that many elements, then, by the Chebotarev density theorem, there is a set of primes whose Frobenius ψ satisfies (5), and that set of primes has a positive density δ_j^- equal to $[K_j : \mathbb{Q}]^{-1} = 2^{-1} \cdot 4^{-j}$, since ψ is unique in its conjugacy class. □

We are now ready for a proof of Theorem 1.

P r o o f o f T h e o r e m 1. To prove the theorem we assume the pair (P, Q) to lie outside $S_1 \cup S_2 \cup S_3$, where S_1, S_2 and S_3 are the sets defined in Lemma 3. We will show that the prime density of $V_n(P, Q)$ is then equal to $2/3$. Since the sets S_1, S_2 and S_3 are negligible, this will prove the theorem. By Lemma 6, the prime density of D_j^+ exists and equals $[L_j : \mathbb{Q}]^{-1} - [K_j : \mathbb{Q}]^{-1}$. Since D is not $\pm$ the square of an integer, nor $\pm$ twice the square of an integer, $\sqrt{D}$ does not belong to any of the three number fields $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{-2})$. For $j \geq 3$ these three fields are the only quadratic subfields of $\mathbb{Q}(\zeta_{2^j})$, since the Galois group of $\mathbb{Q}(\zeta_{2^j})$, isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{j-2}\mathbb{Z}$, has three subgroups of index 2. Thus $[\mathbb{Q}(\sqrt{D}, \zeta_{2^j}) : \mathbb{Q}] = 2 \times 2^{j-1} = 2^j$. The conditions on Q linked to the fact that $(P, Q) \notin S_1$ imply immediately that $\sqrt{Q} \notin \mathbb{Q}(\zeta_{2^j})$ for any $j \geq 1$. Because $(P, Q) \notin S_3$, $\sqrt{Q} \notin \mathbb{Q}(\sqrt{\epsilon D})$ for $\epsilon \in \{\pm 1, \pm 2\}$ and therefore $\sqrt{Q} \notin \mathbb{Q}(\sqrt{D}, \zeta_{2^j})$. But $r = \alpha/\bar{\alpha} = \alpha^2/Q$ so $\sqrt{r}$ belongs to $\mathbb{Q}(\sqrt{D}, \zeta_{2^j})$ if and only if $\sqrt{Q}$ does. Thus the degree of the Kummer extension $[L_j : \mathbb{Q}(\sqrt{D}, \zeta_{2^j})] = 2^j$ and $[K_j : \mathbb{Q}] = 2 \times [L_j : \mathbb{Q}] = 2 \times 2^j \times [\mathbb{Q}(\sqrt{D}, \zeta_{2^j}) : \mathbb{Q}] = 2 \times 4^j$. Using Lemma 6, we get, for each $j \geq 1$, $\delta_j^+ = \delta_j^- = 2^{-1} \cdot 4^{-j}$. We refer the reader to [8], p. 454, to legitimate the fact that the prime density of odd ranked primes is indeed given by the sum $\sum_{j \geq 1}(\delta_j^+ + \delta_j^-) = \sum_{j \geq 1} 4^{-j} = 1/3$. □

Definition 1. We will say that $f = X^2 - PX + Q$, (P, Q), $V_n(P, Q)$ or $U_n(P, Q)$ are 'generic' whenever (P, Q) is a pair of rational integers that does not satisfy any of the three conditions i), ii) or iii) of Lemma 3.

We wish to stress a few properties of generic Lucas sequences that are easy consequences of our proof of Theorem 1.

We first state an immediate corollary.

Theorem 7. *If (P,Q) is a generic pair of rational integers, then the prime density of the Lucas sequence $V_n(P,Q)$ is $2/3$ with split primes and inert primes accounting each for $1/3$ in this density.*

As mentioned in the introduction the uneven $1/3 - 2/3$ partition of the set of primes into respectively non-divisors and divisors of the Lucas numbers can be replaced by a $1/3 - 1/3 - 1/3$ trichotomy of the set of primes into three sets B_1, B_2 and B_3 which was given several interpretations in [4]. In particular we had $B_1 = \{p\ ;\ \nu_2(\rho) = 1\}$, $B_2 = \{p\ ;\ \nu_2(\rho) = 0\}$ and $B_3 = \{p\ ;\ \nu_2(\rho) \geq 2\}$, where ρ is the rank of p in the Fibonacci sequence. Perhaps the most satisfactory interpretation was to view B_1, B_2 and B_3 as the sets of prime divisors of three recurring sequences representing the three order 2 elements of a Klein group associated with the polynomial $f = X^2 - 3X + 1$.

This trichotomy and the above two interpretations of B_1, B_2 and B_3 hold for any generic recursion.

Theorem 8. *Let $f = X^2 - PX + Q = (X - \alpha)(X - \bar{\alpha})$ be a generic polynomial and $V_n = V_n(P,Q)$, $U_n = U_n(P,Q)$ be the two associated Lucas sequences. Define B_1 as $\{p\ ;\ \nu_2(\rho) = 1\}$, B_2 as $\{p\ ;\ \nu_2(\rho) = 0\}$ and $B_3 = \{p\ ;\ \nu_2(\rho) \geq 2\}$, where ρ is the rank of p in U_n. Then the three sets B_i, $i = 1,2,3$, each have prime density equal to $1/3$. Moreover, the three recurring sequences (V_{2n+1}), (U_{2n+1}) and (V_{2n}) represent the three order 2 elements of a Klein subgroup of the Laxton group associated to $g = X^2 - (P^2 - 2Q)X + Q^2 = (X - \alpha^2)(X - \bar{\alpha}^2)$. Note that*

$$\begin{aligned} B_1 &= \{p\ ;\ p \mid V_{2n+1} \text{ for some } n\},\\ B_2 &= \{p\ ;\ p \mid U_{2n+1} \text{ for some } n\},\\ B_3 &= \{p\ ;\ p \mid V_{2n} \text{ for some } n\}. \end{aligned}$$

Proof. Clearly the three sets B_i, $i = 1,2,3$, are pairwise disjoint and we have that $B_1 \cup B_3$, being the set of prime divisors of the V_n sequence, has prime density $2/3$. Note that the order of $r^2 \pmod{(p)}$ is odd if and only if the order of $r \pmod{(p)}$ is either odd or divisible by 2, but not by 4. Thus the set of primes p with order of $r^2 \pmod{(p)}$ an odd number is $B_1 \cup B_2$. The proofs of Lemmas 5, 6 and of Theorem 1 hold with r^2 in place of r if we replace, for each $j \geq 1$, L_j and K_j, respectively, by the number fields L'_j and K'_j, where $L'_j = \mathbb{Q}\big(\zeta_{2^j}, \sqrt{D}, \sqrt[2^{j-1}]{r}\big)$ and $K'_j = L'_j\big(\zeta_{2^{j+1}}\big)$. The condition $[K_j : \mathbb{Q}] = 2 \cdot 4^j$ in Lemma 6 needs to be replaced by $[K'_j : \mathbb{Q}] = 4^j$. The degrees of L'_j and K'_j over $\mathbb{Q}$ are half the degrees of (resp.) L_j and K_j for each $j \geq 1$. Thus the prime density of $B_1 \cup B_2$ is twice $1/3$, i.e., is $2/3$. Therefore the complementary set B_3 has density $1/3$. Thus each B_i has density $1/3$.

For the second part of the theorem, we refer the reader to the original papers [10], [11] where Laxton studies a group structure built on classes of second order recurring sequences that share the same characteristic polynomial. This group is relevant to prime division and a generalization of it was given for higher order recurrences in [1] and in [2]. In fact to date it remains true that only torsion sequences in this group have had their prime density shown to exist in an unconditional way. Laxton showed, in particular, that if h is of the form $X^2 - PX + R^2$, with P and R in $\mathbb{Z}$, then this group contains three classes of sequences that form, with the group identity represented by the Lucas sequence $U_n(P, R^2)$, a Klein subgroup. These three sequences of characteristic polynomial h are, besides the companion Lucas sequence $V_h(n) = V_n(P, R^2)$, the two sequences $A_h(n)$ and $B_h(n)$ defined by their initial values $A_h(0) = B_h(0) = 1$, $A_h(1) = P + R$ and $B_h(1) = P - R$. Laxton had already observed that $V_h(n)$, $A_h(n)$ and $B_h(n)$ have disjoint sets of prime divisors and that every prime divides one of the three sequences. Thus here we may consider $A_g(n)$ and $B_g(n)$. Noting that $U_f(2n+1)$ and $V_f(2n+1)$ have characteristic polynomial g, and comparing initial values shows that $A_g(n) = U_f(2n+1)$ and $B_g(n) = P^{-1}V_f(2n+1)$ and the theorem is proved since $V_g(n) = V_f(2n)$. □

REFERENCES

[1] BALLOT, C.: *Density of prime divisors of linear recurrences*, Mem. Amer. Math. Soc. **115** (1995), no. 551, pp. 102.

[2] BALLOT, C.: *Group structure and maximal division for cubic recursions with a double root*, *Pacific J. Math.* **173** (1996), no. 2, 337-355.

[3] BALLOT, C.: *Simple heuristics yielding prime densities*, (preprint in progress).

[4] BALLOT, C. – ELIA, M.: *Rank and Period of Primes in the Fibonacci sequence. A Trichotomy*, Fibonacci Quart. **45** (2007), no. 1, 56–63.

[5] BILU, Y. – HANROT, G. – VOUTIER, P.: *Existence of primitive divisors of Lucas and Lehmer numbers* J. Reine Angew. Math. **539** (2001), 75–122.

[6] HASSE, H.: *Über die Dichte der Primzahlen p für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von durch eine vorgegebene primzahl $l \neq 2$ teilbarer bzw. unteilbarer Ordnung mod. p ist*, Math. Ann. **162** (1965), 74–76.

[7] HASSE, H.: *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.

[8] LAGARIAS, J.: *The set of primes dividing the Lucas numbers has density 2/3*, Pacific J. Math. **118** (1985), no. 2, 449–461; Errata: Pacific J. Math. **162** (1994), 393–397.

[9] LAGARIAS, J.: *Sets of primes determined by systems of polynomial congruences*, Illinois J. Math. **27** (1983), no. 2, 224–239.

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

[11] LAXTON, R.: *On groups of linear recurrences II. Elements of finite order*, Pacific J. Math. **32** (1970), 173–179.

[12] MOREE, P.: *On the prime density of Lucas sequences*, J. Théor. Nombres Bordeaux **8** (1996), 449–459.
[13] MOREE, P.: *Asymptotically exact heuristics for prime divisors of the sequence* $\{a^k + b^k\}_{k=1}^{\infty}$, J. Integer Seq. **9** (2006), no. 2, pp. 15. Article 06.2.8, (electronic).
[14] MOREE, P. – STEVENHAGEN, P.: *Prime divisors of Lucas sequences*, Acta Arith. **82** (1997), no. 4, 403–410.
[15] WARD, M.: *The prime divisors of Fibonacci numbers*, Pacific J. Math. **11** (1961), 379–386.

Received July 30, 2008
Accepted March 10, 2009

Christian Ballot
Laboratoire Nicolas Oresme
Université de Caen
F14032 Caen Cedex, France
E-mail: christian.ballot@math.unicaen.fr