ACTA ARITHMETICA
LXXXIX.3 (1999)

Strong arithmetic properties of the integral solutions of $X^3 + DY^3 + D^2Z^3 - 3DXYZ = 1$, where $D = M^3 \pm 1$, $M \in \mathbb{Z}^*$

by

Christian Ballot (Caen)

0. Introduction. Lucas sequences have many number-theoretic applications. Not surprisingly, several generalizations have been made and examined. It is the purpose of this paper to show that under certain conditions two, a priori unrelated, generalizations of Lucas sequences merge into one. When this occurs the generalized sequences we obtain truly have very rich arithmetic properties.

The first of these generalizations, although encountered by earlier authors, was studied in detail by H. Williams in his doctoral thesis [Wi1]. This generalization is natural in several respects. As D. H. Lehmer [Le1] once noted Lucas sequences V_n, U_n are the integral solutions, up to constants, of the Fermat–Pell equation $X^2 - DY^2 = 1$. The Williams sequences, as we shall name them here, W_n, V_n, U_n are, up to constants, the integral solutions of the cubic norm equation $X^3 + DY^3 + D^2Z^3 - 3DXYZ = 1$ that we will call the Mathews equation [Ma]. These sequences satisfy many Lucas-like identities [Wi1], [Wi2]. Also they were auxiliary tools in primality tests for certain types of numbers (cf. [Wi1], Ch. 5, or [Wi2], pp. 49–50).

The second generalization of interest here was examined by the author in [Ba1]. This generalization is intricately linked to properties of prime divisors in Lucas sequences (we say that a prime p divides a sequence of integers if it divides a number in the sequence). These are group, rank and density properties.

Indeed, Lucas sequences are torsion elements of a group structure, relevant to divisibility by primes (see Laxton's paper [Lax]), of which V_n, U_n form a cyclic subgroup of order 2. This group is infinite, of infinite rank, but finite torsion. Secondly, there is coincidence between the prime divisors p of the Lucas V_n-sequence and the primes of even rank $r = r(p)$.

1991 *Mathematics Subject Classification*: 11B37, 11B83, 11B05.

Here, r is the first positive term number n for which $p \mid U_n$. Thirdly, Hasse's method, an algebraic method that can be used to compute *exactly* the Dirichlet density of the set of prime divisors of certain sequences, applies successfully to the Lucas V_n-sequences. But sequences for which we know how to apply the method are few and exceptional. Consequently, such sequences have aroused interest, particularly the Lucas V_n-sequences, which are among the exceptional ones (see [Ha], [Lag1], [Ba1], Chapter 3, [Mo] and [M-S]).

In Chapter 5 of [Ba1] a general group structure, the Laxton–Ballot group, is defined on the set of recurring sequences having a characteristic polynomial $f \in \mathbb{Z}[X]$, where f has arbitrary degree. This group is related to the notion of maximal prime division, a notion which generalizes the usual division for quadratic recurring sequences. Also, a notion of rank of a prime with respect to maximal division is defined which includes the former notion as a particular case. Moreover, the density of maximal divisors of some of the few torsion sequences in the group is computed using an extended version of Hasse's method. Also, the set of primes whose rank of maximal division is a multiple of a given prime q is assessed a density through the same method. Thus, in this context, the author's generalized Lucas sequences were precisely those torsion sequences of the Laxton–Ballot group.

This paper shows that for certain values of D in the Mathews equation, the integral solutions are generalizations of ordinary Lucas sequences from *both* points of view. More precisely, these solutions, the Williams sequences W_n, V_n, U_n, are also torsion elements of the Laxton–Ballot group (they form a 3-cyclic group). It is almost true that the maximal divisors of the W_n, V_n-sequences are the primes whose rank of maximal division is divisible by 3. The adverb "almost" will be attributed a precise meaning. Also, density results about prime maximal divisors and primes of rank divisible by 3 are established.

Hence, whenever $D = M^3 \pm 1$ in the Mathews equation, the Williams sequences represent an extraordinarily rich arithmetic realm in which a great deal of the number theory of the usual Lucas sequences is preserved, and perhaps some applications of interest are to be expected. Throughout the paper, the Williams sequences will be referred to as *WB-sequences* (Williams–Ballot) whenever $D = M^3 \pm 1$ in the Mathews equation.

Section 1 is preliminary. Notation and former results are presented. In Section 2, a brief presentation of the Laxton–Ballot group is made and it is shown that the WB-sequences are torsion sequences of the group. Section 3 is concerned with the special rank property of the maximal prime divisors of WB-sequences, while Section 4 is devoted to computing the density of these maximal divisors and the density of primes having a rank multiple of 3. Some final remarks are given in the fifth section.

The density calculation of Section 4 is an interesting addition to earlier work, and particularly to the author's work. For cubic linear recurring sequences (i.e. linear recurring sequences having a degree three characteristic polynomial f), maximal division means division of two consecutive terms. The density of maximal prime divisors of some such sequences was computed in [Ba1], Chap. 4, but always in the case of a *non-degenerate* f having only *rational* roots. (A polynomial f is non-degenerate if the ratio of any two roots is not a root of unity.) Thus, for instance, $(5^n + 2 \cdot 3^n - 1)$ has a $2/7$ density of maximal divisors. In [Ba2], a simple class of *degenerate* cubic characteristic polynomials is treated, but their roots are still all rational. As an example, we know that maximal prime divisors of $(n2^n - 1)$ have density $17/24$. A first instance of a sequence associated with a cubic polynomial with irrational roots is studied in [Ba3]. It is $(1 + F_n)$, with a $2/3$ density of maximal divisors (where F_n is the nth Fibonacci number). However, the characteristic polynomial $(X-1)(X^2-X-1)$ has one rational and two irrational roots. Here, the roots of the polynomial associated with the WB-sequences are *all irrational.* Hence, this paper, among other results, demonstrates the existence of non-trivial integral linear recurring sequences with *irreducible* characteristic polynomial for which the Dirichlet density of prime maximal divisors is computable and computed exactly. For instance, the sequence $(\alpha^n + \beta^n + (\overline{\beta})^n)$, where $\alpha = 4 + 2\sqrt[3]{7} + \sqrt[3]{49}$, $\beta = 4 + 2\omega^2\sqrt[3]{7} + \omega\sqrt[3]{49}$, $\overline{\beta}$ is the complex conjugate of β and $\omega = e^{2\pi i/3}$, has an asymptotic proportion of prime maximal divisors of 51 to 104.

For the definition of the Lucas V_n and U_n-sequences, we refer the reader to Lucas's famous original work [Lu] as well as to the recent fine book [Wi3], Chapter 4.

1. Notation and preliminaries. Let $\omega = e^{2\pi i/3} \in \mathbb{C}$. Let $D \in \mathbb{Z}^*$ and $\delta = \sqrt[3]{D}$.

Definition 1.1 (Williams sequences). Let $f(X) = X^3 - PX^2 + QX - R \in \mathbb{Z}[X]$, $R \neq 0$, where the highest common factor of P, Q and R is 1. If (α, β, γ) is a permutation of the roots of $f(X)$ such that

$$\begin{cases} w_n = \alpha^n + \beta^n + \gamma^n, \\ v_n = \delta^{-1}(\alpha^n + \omega\beta^n + \omega^2\gamma^n), \\ u_n = \delta^{-2}(\alpha^n + \omega^2\beta^n + \omega\gamma^n) \end{cases}$$

are integers for all $n \in \mathbb{N}$, then the sequences $W = (w_n)$, $V = (v_n)$ and $U = (u_n)$ are called *Williams sequences.* H. Williams called them the extended Lucas functions of order 3 associated with the polynomial $f(X)$ (see [Wi1], p. 62). A set of extended Lucas functions of order q was further defined and studied for any prime $q \geq 2$; see [Wi2].

We now assume that D is not a cube in $\mathbb{Z}$. Let G be the Galois group of the Galois extension $\mathbb{Q}(\delta,\omega)$ over $\mathbb{Q}$. Let σ be the automorphism in G such that $\sigma(\delta)=\delta\omega^2$ and $\sigma(\omega)=\omega$, and let τ represent complex conjugation. Let $\alpha=x+y\delta+z\delta^2\in\mathbb{Z}[\delta]$, $\alpha\notin\mathbb{Z}$. The two conjugates of α are $\beta=\sigma(\alpha)=x+y\delta\omega^2+z\delta^2\omega$ and $\gamma=\sigma^2(\alpha)=x+y\delta\omega+z\delta^2\omega^2$. Note that $\gamma=\overline{\beta}=\tau(\beta)$. Let $f(X)=(X-\alpha)(X-\beta)(X-\gamma)=X^3-PX^2+QX-R$ be the minimal polynomial of α. Then the root field of f, $\mathbb{Q}(\alpha,\beta,\gamma)$, is $\mathbb{Q}(\delta,\omega)$. The ring of integers of $\mathbb{Q}(\delta,\omega)$ is denoted by $\mathcal{O}$.

PROPOSITION 1.2. *The sequences* $X=(x_n)_{n\geq 0}$, $Y=(y_n)_{n\geq 0}$ *and* $Z=(z_n)_{n\geq 0}$ *of rational integers defined by*

$$x_n+y_n\delta+z_n\delta^2=(x+y\delta+z\delta^2)^n=\alpha^n,\qquad \forall n\geq 0, \tag{1.1}$$

are linear recurring sequences with characteristic polynomial $f(X)$.

Proof. Apply σ and σ^2 to equation (1.1) and thus get two more equations. Linear combinations of these three equations yield

$$\begin{cases} x_n=\dfrac{1}{3}(\alpha^n+\beta^n+\gamma^n),\\ y_n=\dfrac{1}{3\delta}(\alpha^n+\omega\beta^n+\omega^2\gamma^n),\\ z_n=\dfrac{1}{3\delta^2}(\alpha^n+\omega^2\beta^n+\omega\gamma^n).\end{cases}$$

Now, α, β and γ being the roots of $f(X)$, the proposition follows. ■

REMARKS 1.3. (1) The sequences X, Y and Z of Proposition 1.2 are up to a factor of 3 equal to a set of Williams sequences.

(2) For any $n\geq 0$, (x_n,y_n,z_n) is a solution of the Mathews equation $X^3+DY^3+D^2Z^3-3DXYZ=R^n$, since $x_n^3+Dy_n^3+D^2z_n^3-3Dx_ny_nz_n=\operatorname{norm}(x_n+y_n\delta+z_n\delta^2)=\operatorname{norm}(\alpha^n)=R^n$.

(3) The recurring sequences X, Y and Z may be defined for negative indices by running the recursion backward. The computing of x_{-1}, y_{-1} and z_{-1} can be done using (1.1) and expressing $\beta\gamma$ in the basis $(1,\delta,\delta^2)$ of the $\mathbb{Z}$-module $\mathbb{Z}[\delta]$, since $x_{-1}+y_{-1}\delta+z_{-1}\delta^2=\alpha^{-1}=\beta\gamma/R$. This yields

$$\begin{gathered} x_{-1}=R^{-1}(x^2-Dyz),\quad y_{-1}=R^{-1}(Dz^2-xy),\\ z_{-1}=R^{-1}(y^2-xz). \end{gathered}\tag{1.2}$$

(4) Let the $\mathbb{R}^3$-vector $\begin{pmatrix}x_n\\ y_n\\ z_n\end{pmatrix}$ be denoted by A_n. Now the side-step formulas expressing x_{n+1}, y_{n+1} and z_{n+1} in terms of x_n,y_n and z_n can easily be computed since (1.1) implies

$$x_{n+1}+y_{n+1}\delta+z_{n+1}\delta^2=(x_n+y_n\delta+z_n\delta^2)(x+y\delta+z\delta^2). \tag{1.3}$$

One can then check that (1.3) corresponds to the matrix equation

$$A_{n+1} = BA_n, \quad \text{where} \quad B = \begin{pmatrix} x & Dz & Dy \\ y & x & Dz \\ z & y & x \end{pmatrix}. \tag{1.4}$$

Definition 1.4 (WB-sequences). Let $M \in \mathbb{Z}^*$, $\varepsilon \in \{\pm 1\}$ and $D = M^3 + \varepsilon \neq 0$. The fundamental unit α ($\alpha > 1$) of $\mathbb{Q}(\delta)$ is well known to be $\alpha = M^2 + M\delta + \delta^2$ (see [Na], pp. 24–25). In fact, $\alpha^{-1} = \varepsilon(\delta - M)$. Hence, all units in the ring of integers of $\mathbb{Q}(\delta)$ are of the form $\pm\alpha^n$, $n \in \mathbb{Z}$. And the units of norm 1 are the α^n, $n \in \mathbb{Z}$. So the integral solutions of the Mathews equation

$$X^3 + DY^3 + D^2Z^3 - 3DXYZ = 1, \qquad D = M^3 + \varepsilon, \tag{1.5}$$

are all triples $(x_n, y_n, z_n) \in \mathbb{Z}^3$ such that $x_n + y_n\delta + z_n\delta^2 = \alpha^n$ for all $n \in \mathbb{Z}$. We define the *WB-sequences* associated with (1.5) to be the sequences $X' = (x'_n)_{n\geq 0}$, $Y' = (y'_n)_{n\geq 0}$ and $Z' = (z'_n)_{n\geq 0}$, where $x'_n = x_{n-1}$, $y'_n = y_{n-1}$ and $z'_n = z_{n-1}$. By extension, the X, Y and Z sequences and the corresponding Williams sequences $W = 3X$, $V = 3Y$ and $U = 3Z$ will also be referred to as WB-sequences. Actually, these recurring sequences all have the same characteristic polynomial $f(X)$.

Lemma 1.5. *The WB-sequences associated with equation* (1.5) *have characteristic polynomial* $f(X) = X^3 - 3M^2X^2 - 3\varepsilon MX - 1$.

Proof. The coefficients P, Q and R of $f(X) = X^3 - PX^2 + QX - R$ are the symmetric functions of the roots α, β and γ. So we immediately get $P = 3M^2$ and $R = \operatorname{norm}(\alpha) = 1$, while $Q = \beta\gamma + \sigma(\beta\gamma) + \sigma^2(\beta\gamma) = \alpha^{-1} + \sigma(\alpha^{-1}) + \sigma^2(\alpha^{-1}) = \varepsilon(\delta - M) + \varepsilon(\delta\omega^2 - M) + \varepsilon(\delta\omega - M) = -3\varepsilon M$. One may also find $f(X)$ by computing the characteristic polynomial of the matrix B in (1.4), which is, up to sign, $f(X)$. ∎

Definition 1.6 (WB-recursion). A polynomial $f(X) = X^3 - 3M^2X^2 - 3\varepsilon MX - 1$, where $M \in \mathbb{Z}^*$, $\varepsilon \in \{\pm 1\}$ and $M^3 + \varepsilon \neq 0$ is called a *WB-recursion.*

Remark. We will assume throughout that $M \geq 1$ in (1.5). There is no loss of generality in making this assumption because if $D' = (M')^3 + \varepsilon'$ and $\delta' = (D')^{1/3}$, where $M' < 0$ and $\varepsilon' = \pm 1$, then $\mathbb{Q}(\delta) = \mathbb{Q}(\delta')$, with $D = M^3 + \varepsilon$, $M = -M'$ and $\varepsilon = -\varepsilon'$.

2. The WB-sequences are torsion sequences. First we briefly describe the main features of the Laxton–Ballot group for a polynomial of degree m with distinct roots. (See [Lax] for the case $m = 2$; [Ba1], Chapter 4, for the case $m = 3$ and [Ba1], Chapter 5, for the general case $m \geq 2$.)

Definition 2.1 (The Laxton–Ballot group). Let $f(X)\in\mathbb{Z}[X]$ be monic, of degree $m\ge 2$, and having m distinct non-zero roots $\alpha_1,\dots,\alpha_m\in\mathbb{C}$. Let $S(f)$ be the set of recurring sequences with integral terms and characteristic polynomial $f(X)$, which satisfy no recursion of order $< m$. If $U=(u_n)_{n\ge 0}\in S(f)$, then U is fully determined by its first m values and we write $U=[u_0,u_1,\dots,u_{m-1}]$. Now u_n can be expressed as

$$u_n=\sum_{i=1}^{m}A_i\frac{\alpha_i^n}{f'(\alpha_i)},\qquad \forall n\in\mathbb{N},\tag{2.1}$$

where A_i is an algebraic integer depending only on $u_0,u_1,\dots,u_{m-1}$ and $\alpha_1,\dots,\alpha_m$. (Expression (2.1) appears in M. Ward's article [Wa1] in which the notion of maximal divisor is first introduced.) Hence the sequence $U\in S(f)$ is determined by the m-tuple $(A_1,\dots,A_m)$. And we write U in *standard form* as

$$U=\langle A_1,\dots,A_m\rangle.$$

A product $U*V$ of $U=\langle A_1,\dots,A_m\rangle$ and $V=\langle B_1,\dots,B_m\rangle$ in $S(f)$ is defined via component-wise multiplication of the m-tuples $(A_1,\dots,A_m)$ and $(B_1,\dots,B_m)$. This product makes $(S(f),*)$ a semi-group with identity $I=\langle 1,\dots,1\rangle$, where $I=[0,0,\dots,0,1]$ (with $m-1$ zeros).

If p is a rational prime number, then p is said to be a *maximal divisor* of $U\in S(f)$ (we write $p\,|\,U$), if p divides $m-1$ consecutive terms of U, but never m consecutive terms. The product $*$ in $S(f)$ preserves division by any prime p, i.e. $p\,|\,U$ and $p\,|\,V\Rightarrow p\,|\,U*V$.

The density $d(U)$ of primes dividing U, if it exists, is the limit

$$d(U)=\lim\frac{\log x}{x}\cdot|\{p\,|\,U : p\le x\}|.$$

We then define $E(f)=S(f)/\sim$, where $\sim$ is the equivalence relation defined on $S(f)$ by

$$U\sim V\Leftrightarrow \exists s\in\mathbb{Z},\ \exists\lambda,\lambda'\in\mathbb{Z},\quad \lambda u_{n+s}=\lambda' v_n,\ \forall n\in\mathbb{N}.\tag{2.2}$$

If $\mathcal{U}\in E(f)$, then we say that a prime p *divides* $\mathcal{U}$ if there exists $U\in\mathcal{U}$ such that $p\,|\,U$. We know that for all $U\in\mathcal{U}$, the sets $P(U)$ and $P(\mathcal{U})$ of primes dividing respectively U and $\mathcal{U}$ differ by at most finitely many primes, so that, if $d(U)$ exists, then we define $d(\mathcal{U})$, the density of primes dividing $\mathcal{U}$, as $d(U)$. The product $*$ defined on $S(f)$ is well-defined on $E(f)$ and the structure $(E(f),*)$ forms a group, in which the inverse of the class of $\langle A_1,\dots,A_m\rangle$ is the class of $\langle\prod_{i\ne 1}A_i,\prod_{i\ne 2}A_i,\dots,\prod_{i\ne m}A_i\rangle$. Finally, if p is a prime, then the set $E(f,p)$ of classes divisible by p forms a subgroup of $(E(f),*)$.

As the reader will check for himself the WB-sequences could have been defined without reference to the Mathews equation or to equation (1.1). We do this in the following paragraph.

Definition 2.2 (Alternative definition of WB-sequences). Let $f(X) = X^3 - 3M^2X^2 - 3\varepsilon MX - 1$ be a WB-recursion. Then the *WB-sequences* are the sequences in $S(f)$ defined by their initial values

$$\begin{cases} X' = [-\varepsilon M, 1, M^2], \\ Y' = [\varepsilon, 0, M], \\ Z' = [0, 0, 1]. \end{cases} \tag{2.3}$$

We calculated that the discriminant Δ of $f(X)$ is $-27D^2$, where $D = M^3 + \varepsilon$.

We now give the main result of Section 2.

Theorem 2.3. *The WB-sequences* X', Y' *and* Z' *have standard forms*

$$\begin{cases} X' = \langle \delta^2, \delta^2\omega, \delta^2\omega^2 \rangle, \\ Y' = \langle \delta, \delta\omega^2, \delta\omega \rangle, \\ Z' = \langle 1, 1, 1 \rangle. \end{cases} \tag{2.4}$$

Hence, *the classes of the WB-sequences form a cyclic subgroup of order three of the Laxton–Ballot group* $E(f)$.

Proof. We show that $X' = \langle \delta^2, \delta^2\omega, \delta^2\omega^2 \rangle$. The standard forms for Y' and Z' can be obtained in a similar fashion. Now, if $X' = \langle A_1, A_2, A_3 \rangle$, then (see [Ba1], p. 35)

$$\begin{cases} A_1 = x_0'\beta\gamma - x_1'(\beta + \gamma) + x_2', \\ A_2 = \sigma(A_1), \qquad A_3 = \sigma(A_2). \end{cases}$$

But by (1.2), $x_0' = x_{-1} = M^4 - (M^3 + \varepsilon)M = -\varepsilon M$. Now $x_1' = x_0 = 1$ and $x_2' = x_1 = P/3 = M^2$. Also $\beta\gamma = \alpha^{-1} = \varepsilon(\delta - M)$ and $\beta + \gamma = 2M^2 - M\delta - \delta^2$. Hence, $A_1 = -\varepsilon M \cdot \varepsilon(\delta - M) - (2M^2 - M\delta - \delta^2) + M^2 = \delta^2$! But $\sigma(\delta) = \delta\omega^2 \Rightarrow A_2 = \sigma(A_1) = \sigma(\delta^2) = \delta^2\omega$ and $A_3 = \sigma(A_2) = \delta^2\omega^2$. Thus $X' = \langle \delta^2, \delta^2\omega, \delta^2\omega^2 \rangle$ and (2.4) holds.

Now observe that $Y' * Y' = X'$ and $Y' * X' = D \cdot Z' \sim Z' = I$, the identity of $S(f)$. Hence the class of Y' has order 1 or 3 in $E(f)$. If it is of order 1, then $Y' \sim I$ and there exist $s, \lambda, \lambda' \in \mathbb{Z}$ such that $\lambda\delta\alpha^s = \lambda'$. (See Definition 2.2 and note that shifting Y' by s places transforms B_1 into $\alpha^s B_1$, where $Y' = \langle B_1, B_2, B_3 \rangle$. Here $B_1 = \delta$.) Raising $\lambda\delta\alpha^s = \lambda'$ to the power 3, we see that the algebraic integer α^{3s} is rational, and so belongs to $\mathbb{Z}$. But its norm is 1, so $\alpha^{3s} = 1$, contradicting $\alpha > 1$. So the class of Y' has order 3. ∎

3. The rank of prime divisors of WB-sequences. For integers a and b let (a, b) denote the greatest common divisor of a and b. Let

$$f(X) = X^3 - PX^2 + QX - R = (X - \alpha)(X - \beta)(X - \gamma) \in \mathbb{Z}[X], \qquad R \neq 0.$$

We denote the discriminant of $f(X)$ by Δ.

First we recall some definitions and results.

Definition. Let U be a recurring sequence in $S(f)$ and p be a prime. Then we say that p is a maximal divisor of U *at* n if $p\,|\,(u_n, u_{n+1})$ and $p\nmid u_{n+2}$.

The definition of the rank of a prime relative to a polynomial f of degree $m = 3$ is redefined here. It generalizes the usual rank introduced by Lucas in the case $m = 2$ ([Lu], p. 290). The general definition, for f of arbitrary degree $m \geq 2$, is given on p. 457 of [Wa1] or p. 91 of [Ba1].

Definition. Let $I = \langle 1, 1, 1\rangle = [0, 0, 1] \in S(f)$ and p be a prime. Then we define the *rank* of p (relative to f) to be the smallest $r > 0$ such that $p\,|\,I$ at r (i.e. p is a maximal divisor of I at r). If $p\nmid R$, then the rank r of p exists.

Proposition 3.1. *Let $U = \langle A, B, C\rangle \in S(f)$ and p be a prime. If $p\nmid ABCR\Delta$, then we have the equivalences*

$$p\,|\,(u_n, u_{n+1}) \Leftrightarrow p\,|\,U \text{ at } n \Leftrightarrow A\alpha^n \equiv B\beta^n \equiv C\gamma^n \pmod{(p)},$$

where (p) is the ideal generated by p in the ring of integers $\mathcal{O}$ of the root field of f.

Proof. See Theorem 4.4.1 and its Corollary on pp. 39–40 of [Ba1]. ■

Corollary 3.2. *Let $p\nmid R\Delta$ be a prime of rank r. Then $p\,|\,I$ at $n \Leftrightarrow r\,|\,n$.*

Proof. ⇒ By Proposition 3.1, $\alpha^n \equiv \beta^n \equiv \gamma^n \pmod{(p)}$ and $\alpha^r \equiv \beta^r \equiv \gamma^r \pmod{(p)}$. But since $p\nmid R$, we must have $\alpha^{n-r} \equiv \beta^{n-r} \equiv \gamma^{n-r} \pmod{(p)}$ and by the same token we can get $\alpha^g \equiv \beta^g \equiv \gamma^g \pmod{(p)}$, where $g = (n, r)$. Now $1 \leq g \leq r \Rightarrow g = r$, by the minimality of the rank. Hence, $r\,|\,n$. For the converse use Proposition 3.1 and raise the congruences $\alpha^r \equiv \beta^r \equiv \gamma^r \pmod{(p)}$ to the power n/r. ■

We now assume that $f(X) = X^3 - 3M^2X^2 - 3\varepsilon MX - 1$, where $M \geq 1$, $\varepsilon = \pm 1$ and $D = M^3 + \varepsilon \neq 0$ and study some rank property of the maximal divisors of the WB-sequences X' and Y'.

Lemma 3.3. *Suppose $p\nmid 3D$ is a prime of rank r. Then $p\,|\,X'$ or $p\,|\,Y' \Rightarrow 3\,|\,r$.*

Proof. Assume $p\,|\,X'$ at n. Let $X' = \langle A, B, C\rangle$. Then by Theorem 2.3 we have $ABC = (\delta^2)^3 = D^2$. Moreover $R = 1$ and $\Delta = -27D^2$ so that $p\nmid 3D \Leftrightarrow p\nmid ABCR\Delta$. Thus by Proposition 3.1, we have

$$\delta^2\alpha^n \equiv \delta^2\omega\beta^n \equiv \delta^2\omega^2\gamma^n \pmod{(p)}. \tag{3.1}$$

Raising (3.1) to the power 3 and dividing out by D^2 yields $\alpha^{3n} \equiv \beta^{3n} \equiv \gamma^{3n} \pmod{(p)}$. That is, $p\,|\,I$ at $3n$. So, by Corollary 3.2, $r\,|\,3n$. But, (3.1) together with $p\nmid 3D$ implies that the congruence $\alpha^n \equiv \beta^n \equiv \gamma^n \pmod{(p)}$ does not hold. So $r \nmid n$. But $r \mid 3n$ and $r \nmid n \Rightarrow 3 \mid r$. The proof that $p \mid Y' \Rightarrow 3 \mid r$ is similar. ■

The study of the converse of Lemma 3.3 is more delicate. We have to distinguish primes according to their splitting type in $\mathcal{O}$.

Thus, let $p \nmid 3D$ be a rational prime. Then p is unramified in $\mathbb{Q}(\delta, \omega)$. And the ideal (p) generated by p in $\mathcal{O}$ factorizes as $\prod_{i=1}^{s} P_i$ where the P_i's are distinct prime ideals of $\mathcal{O}$. We denote by $\mathcal{P}$ the set $\{P_i : 1 \le i \le s\}$. We have three cases.

Case 1: $p \in S_1 = \{p : p \nmid 3D \text{ and } p \equiv 2 \pmod 3\}$. For these primes we have $s = |\mathcal{P}| = 3$.

Case 2: $p \in S_2 = \{p : p \nmid 3D$ and $p \equiv 1 \pmod 3$ and D is not a cube modulo $p\}$. Here $s = 2$.

Case 3: $p \in S_3 = \{p : p \nmid 3D$ and $p \equiv 1 \pmod 3$ and D is a cube modulo $p\}$. Here $s = 6$.

The Dirichlet densities of the sets S_1, S_2 and S_3 are respectively 1/2, 1/3 and 1/6.

First we need a lemma which will also be of use in Section 4.

Lemma 3.4. *Let $n \in \mathbb{N}$, $\zeta \in \{1, \omega, \omega^2\}$, p be a rational prime and $P \in \mathcal{P}$. Then the congruences $\alpha^n \equiv \zeta\beta^n \equiv \zeta^2\gamma^n$ hold modulo (p) if and only if they hold modulo P.*

Proof. $\Rightarrow$ Clear since $(p) \subset P$.

$\Leftarrow$ We have

$$\alpha^n \equiv \zeta\beta^n \equiv \zeta^2\gamma^n \pmod{P}. \tag{3.2}$$

Now applying τ to (3.2) yields the same congruences, but modulo $\tau(P)$. Also applying σ to (3.2) and multiplying the resulting congruences through by ζ yields again the same congruences but modulo $\sigma(P)$. But G is generated by σ and τ and the action of G on $\mathcal{P}$ is transitive, so that (3.2) holds for all $P \in \mathcal{P}$. Therefore, (3.2) holds true modulo (p). ■

Theorem 3.5. *Let $p \in S_1$ or $p \in S_2$ be a prime of rank $r = 3n$, where n is an integer ≥ 1. Then $p \mid X'$ at n or $p \mid Y'$ at n.*

Proof. By hypothesis, $p \mid I$ at $3n$. So $\alpha^{3n} \equiv \beta^{3n} \equiv \gamma^{3n} \pmod{(p)}$, or equivalently $\alpha^{3n} \equiv \beta^{3n} \equiv \gamma^{3n} \pmod{P_i}$ for $1 \le i \le s$. In particular, we have $\alpha^{3n} \equiv \beta^{3n} \pmod{P_1}$, where P_1 is arbitrary in $\mathcal{P}$. Therefore, there exists $\zeta \in \{1, \omega, \omega^2\}$ such that

$$\alpha^n \equiv \zeta\beta^n \pmod{P_1}. \tag{3.3}$$

Using appropriately the actions of σ and τ on $\alpha, \beta, \gamma, \omega$ and on $\mathcal{P}$, we will deduce that

$$\alpha^n \equiv \zeta\beta^n \equiv \zeta^2\gamma^n \pmod{P_1}. \tag{3.4}$$

But, by Lemma 3.4, congruence (3.4) implies that

$$\alpha^n \equiv \zeta\beta^n \equiv \zeta^2\gamma^n \pmod{(p)}. \tag{3.5}$$

This enables us to conclude the proof. Indeed, (3.5) $\Rightarrow \zeta \neq 1$, since $\zeta = 1$ would contradict $r = 3n$. So, either $\zeta = \omega$ and $p \mid X'$ at n, or $\zeta = \omega^2$ and $p \mid Y'$ at n.

Thus we need to prove (3.4). This is done separately according as $p \in S_1$ or $p \in S_2$.

Case 1. Consider the action of τ on $\mathcal{P}$. Here $\mathcal{P}$ is of size 3, so there exists a $P = P_1 \in \mathcal{P}$ such that $\tau(P_1) = P_1$. Now applying τ to (3.3) gives $\alpha^n \equiv \zeta^2\gamma^n \pmod{P_1}$, so that (3.4) holds.

Case 2. Since σ has order 3 in G, the orbits of the action of σ on $\mathcal{P}$ are either of size 1 or 3. But here $|\mathcal{P}| = 2$, so σ fixes both P_1 and P_2. Now applying σ to (3.3) gives $\beta^n \equiv \zeta\gamma^n \pmod{P_1}$, which yields (3.4). ■

Remark 3.6. The conclusion of Theorem 3.5 says that $p \mid X'$ at n or $p \mid Y'$ at n. Note that if $p \nmid 3D$, then $p \mid X'$ at $n \Rightarrow p \mid Y'$ at $2n$, and $p \mid Y'$ at $n \Rightarrow p \mid X'$ at $2n$.

Remark 3.7. For primes in S_3, Theorem 3.5 does not hold. For instance, for $D = 7 = 2^3 - 1$, the smallest prime for which the theorem fails is $p = 811$. (The rank of $p = 811$ is $r = 135$ which is a multiple of 3, but $p \nmid X'$, and consequently $p \nmid Y'$.) However, the set of primes for which the theorem fails is slim. The reader will see from the density results of Section 4 that Theorem 3.5 holds exactly 9 out of 10 times for primes in S_3! That is, asymptotically, out of ten primes in S_3 of rank divisible by 3, nine do divide the X and Y sequences. In fact, primes in S_3 are either 1, 4 or 7 modulo 9 and Theorem 3.5 holds for all primes congruent to 4 or 7 modulo 9 provided their rank is a multiple of 3.

Remark. As is often the case with number-theoretic facts linked to Lucas sequences, two types of proofs coexist: proofs based upon algebraic number-theoretic concepts and proofs based upon elementary Lucas arithmetic identities. (Thus note the two proofs of the Lucas–Lehmer primality test in [We] and [Le2]; or the two proofs that all primes $\pm 2 \pmod 5$ are maximal divisors of $(1 + F_n)$, where F_n is the nth Fibonacci number in [Ba3].) For our present subject, Hugh Williams showed me a very elementary proof of Theorem 3.5 based on the many Lucas-like identities that the Williams sequences satisfy (private communication).

4. Density results. The purpose of this section is twofold. First we show that the maximal prime divisors of the companion WB-sequences form a set having a Dirichlet density. (The *companion WB-sequences* are the X' and Y' sequences; their properties generalize those of the usual companion Lucas sequence, i.e. the V_n-sequence.) Secondly it is proved that the primes having a rank multiple of 3 in a WB-recursion also have a Dirichlet density.

In ordinary Lucas theory, the set of prime divisors of the companion Lucas sequence coincides with the set of primes of even rank (except possibly for divisors of $2Q$, where Q is the product of the two roots of the recursion). And the Dirichlet density of this set is always computable (cf. [Lag1], pp. 450–451). Here, for WB-recursions, our two sets of primes differ slightly, but remarkably both have a computable Dirichlet density.

We actually compute the density of these primes by calculating their density within each of the three subsets S_1, S_2 and S_3.

Notation and definitions. The ratios α/β, α/γ, β/γ are denoted respectively by $\varPsi_1$, $\varPsi_2$ and $\varPsi_3$. If j and k are fixed integers such that $j \ge k \ge 0$, then, for $i = 1, 2$ and 3, we define φ_i to be $\sqrt[3^{j-k}]{\varPsi_i}$.

Given $P \in \mathcal{P}$, $e_i = \mathrm{ord}_P \varPsi_i$ is the order of $\varPsi_i \pmod P$, $1 \le i \le 3$.

The 3-adic valuation of an integer n is denoted by $\mathcal{V}_3(n)$. If a is a positive integer, then the symbol ζ_a represents the complex number $e^{2\pi i/a}$.

We choose to write $p \mid X$ to mean that p is a maximal divisor of the companion WB-sequences. This is legitimate since the X, X', Y or Y' sequences share the same divisors, as long as $p \nmid 3D$. To be precise, we state a preliminary lemma.

Lemma 4.0. *Let p be a prime not dividing $3D$. Then*

$$p \mid X \Leftrightarrow p \mid X' \Leftrightarrow p \mid Y' \Leftrightarrow p \mid Y.$$

Proof. The sequences X and X' share the same divisors and so do Y and Y'. Now, the fact that $p \mid X' \Leftrightarrow p \mid Y'$, if $p \nmid 3D$, was stated in Remark 3.6. ■

We define the sets D_i and T_i for $1 \le i \le 3$ as $D_i = \{p \in S_i : p \mid X\}$ and $T_i = \{p \in S_i : 3 \mid r(p)\}$.

If S is a set of primes with Dirichlet density, then this density is denoted by $d(S)$.

Lemma 4.1. *Let j and k be integers such that $j \ge k \ge 0$. The extension $F = F_{j,k} = \mathbb{Q}(\delta, \zeta_{3^j}, \varphi_1, \varphi_2, \varphi_3)$ is a normal extension of the rationals of degree $2 \cdot 3^{3j-2k-1}$ if $j > k$, and of degree $2 \cdot 3^j$ if $j = k \ge 1$.*

Proof. The proof is left to the reader. Note that $\varphi_3 \in \mathbb{Q}(\delta, \zeta_{3^j}, \varphi_1, \varphi_2)$ and that $\mathbb{Q}(\delta, \zeta_{3^j}, \sqrt[3]{\varPsi_1})$ is normal over $\mathbb{Q}$, since $\sqrt[3]{\varPsi_1} \cdot \sqrt[3]{\varPsi_2} = \sqrt[3]{\alpha^3} \in \mathbb{Q}(\delta, \zeta_{3^j})$. ■

Lemma 4.2. *Let $p \nmid 3D$. Then*

$$p \mid X \Leftrightarrow \forall P \in \mathcal{P} : \mathcal{V}_3(e_1) = \mathcal{V}_3(e_2) = \mathcal{V}_3(e_3) \ge 1. \tag{4.1}$$

Proof. ⇒ By Theorem 2.3 and Proposition 3.1

$$p \mid X' \Rightarrow \exists n \in \mathbb{N},\ \forall P \in \mathcal{P},\ \alpha^n \equiv \omega\beta^n \equiv \omega^2\gamma^n \pmod{P}.$$

So, P being arbitrary in $\mathcal{P}$, there have to exist $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{N}$ such that

$$3n = \lambda_1 e_1 = \lambda_2 e_2 = \lambda_3 e_3, \quad \text{where} \quad \mathcal{V}_3(\lambda_i) = 0,\ \forall i.$$

Hence, the conclusion follows.

⇐ Let $P \in \mathcal{P}$. Then the hypothesis implies that there exist positive integers $\lambda_1,\ \lambda_2,\ \lambda_3$ such that

$$\begin{cases} e_1 = 3^k \cdot \lambda_1, \\ e_2 = 3^k \cdot \lambda_2, \\ e_3 = 3^k \cdot \lambda_3, \quad \text{where } k \geq 1 \text{ and } 3 \nmid \lambda_1\lambda_2\lambda_3. \end{cases}$$

Let n be equal to 3^{k-1} times the least common multiple of λ_1, λ_2 and λ_3. Then there exists $\zeta \in \{\omega, \omega^2\}$ such that $\alpha^n \equiv \zeta\beta^n \equiv \zeta^2\gamma^n \pmod{P}$. By Lemma 3.4, the last congruences hold (mod (p)) so that if $\zeta = \omega$, then $p \mid X'$, and if $\zeta = \omega^2$ then $p \mid Y'$. So by Lemma 4.0 in either case $p \mid X$. ■

LEMMA 4.3. *Let $p \nmid 3D$. Then*

$$3 \mid r(p) \Leftrightarrow \exists P \in \mathcal{P},\ \exists i \in \{1,2,3\},\ \mathcal{V}_3(e_i) \geq 1. \tag{4.2}$$

Proof. ⇒ Let $r = 3n$. Then there exists $P \in \mathcal{P}$ such that $\alpha^n \equiv \beta^n \equiv \gamma^n \pmod{P}$ does not hold. Hence, there exists $\Psi \in \{\Psi_1, \Psi_2, \Psi_3\}$ such that $\Psi^{3n} \equiv 1$, but $\Psi^n \not\equiv 1 \pmod{P}$. Therefore, $3 \mid \mathrm{ord}_P \Psi$.

⇐ By definition of r, we have $\alpha^r \equiv \beta^r \equiv \gamma^r \pmod{P}$. So $e_i \mid r$. And $3 \mid e_i \Rightarrow 3 \mid r$. ■

THEOREM 4.4. *We have $d(D_1) = 3/8$.*

Proof. Here we take $j \geq 1$ and $k = 0$. Thus, in the notation of Lemma 4.1, $F = F(j, 0)$. Let G^* denote the Galois group of $F(\zeta_{3^{j+1}})/\mathbb{Q}$. In this proof, for p a rational prime, $\mathcal{Q}$ and $\mathcal{R}$ denote the sets of prime ideals above p respectively in F and in $F(\zeta_{3^{j+1}})$.

Put $\overline{D}_1(j) = \{p \in S_1 \backslash D_1 : \mathcal{V}_3(p+1) = j\}$. Note that $\mathcal{V}_3(p+1) = j \Leftrightarrow$ the ideal generated by p is inert in the extension $\mathbb{Q}(\omega)/\mathbb{Q}$, splits completely in $\mathbb{Q}(\zeta_{3^j})/\mathbb{Q}(\omega)$ and its prime factors in $\mathbb{Z}[\zeta_{3^j}]$ are inert in $\mathbb{Q}(\zeta_{3^{j+1}})$. Also, let $p \in S_1 \backslash D_1$. By the contrapositive of Theorem 3.5, we have $3 \nmid r(p)$. So, by Lemma 4.3, for all $P \in \mathcal{P}$, and $i = 1, 2, 3$, $\mathcal{V}_3(e_i) = 0$, which is equivalent to Ψ_i being a 3^jth power (mod P) for all i, or by the Kummer–Dedekind theorem [1], to P splitting completely in $F/\mathbb{Q}(\omega, \delta)$. Hence,

$$\begin{aligned} p \in \overline{D}_1(j) \Leftrightarrow f(P \mid p) = f(Q \mid p) = 2& \\ \text{and } f(R \mid p) = 6,\ \forall P \in \mathcal{P},\ \forall Q \in \mathcal{Q},\ \forall R \in \mathcal{R},& \end{aligned} \tag{4.3}$$

[1] See Appendix A of [Ba1] for a statement of this theorem.

where $f(*\,|\,p)$ represents the inertial degree of $*$ over p. Next we show that there is a subset $\mathcal{A}$ of G^* such that

$$\text{(4.4)}\qquad p \text{ satisfies the condition in (4.3) } \Leftrightarrow \forall R\in\mathcal{R},\ \phi=\phi(R\,|\,p)\in\mathcal{A},$$

where ϕ is the Frobenius automorphism of R over p.

So let $p\in\overline{D}_1(j)$. Then $\mathcal{P}=\{P_0,P_1,P_2\}$, where, by the Kummer–Dedekind theorem, we may write

$$P_i=(p)+(\delta-\omega^i d),\quad i=0,1 \text{ or } 2,\quad \text{where}\quad d\in\mathbb{Z} \text{ and } d^3\equiv D \pmod p.$$

Suppose R lies above P_i. Because $\phi(x)\equiv x^p \pmod{P_i}$ for all $x\in\mathcal{O}$, and since $p\equiv 2 \pmod 3$ and $d^p\equiv d \pmod p$, we have

$$\phi(\delta)\equiv\delta^p\equiv(\omega^i d)^p\equiv\omega^{2i}d\equiv\omega^{2i}(\omega^{-i}\delta)=\omega^i\delta \pmod{P_i}.$$

Now, because $\phi(\delta)$ must be a cube root of D and $p\neq 3$, we deduce that $\phi(\delta)=\omega^i\delta$.

Assume for the moment that we choose R lying above P_0. Then $\phi(\delta)=\delta$ and so ϕ acts on $\{\alpha,\beta,\gamma\}$ as the transposition $(\beta\gamma)$. Hence, we must have

$$\text{(4.5)}\qquad \begin{cases}\phi(\varphi_1)=\xi_1\varphi_2,\\ \phi(\varphi_2)=\xi_2\varphi_1,\\ \phi(\varphi_3)=\xi_3\varphi_3^{-1},\end{cases}$$

where $\xi_1,\xi_2,\xi_3\in\{\zeta_{3^j}^l : l=1,2,\ldots,3^j\}$. We may assume that the roots $\varphi_i=\sqrt[3^j]{\Psi_i}$ have been chosen in such a way that $\varphi_1\varphi_2^{-1}\varphi_3=1$. Therefore $1=\phi(1)=\phi(\varphi_1\varphi_2^{-1}\varphi_3)=\xi_1\xi_2^{-1}\xi_3\cdot\varphi_1^{-1}\varphi_2\varphi_3^{-1}=\xi_1\xi_2^{-1}\xi_3\Rightarrow\xi_2=\xi_1\xi_3$. Now the restriction of ϕ to F has order 2 since $f(Q\,|\,p)=2$ for all $Q\in\mathcal{Q}$. Also the restriction of ϕ to $\mathbb{Q}(\zeta_{3^j})$ must be complex conjugation, the only order 2 automorphism of the extension $\mathbb{Q}(\zeta_{3^j})$ over $\mathbb{Q}$. So $\varphi_1=\phi^2(\varphi_1)=\phi(\xi_1\cdot\varphi_2)=\xi_1^{-1}\cdot(\xi_2\varphi_1)$, which implies $\xi_1=\xi_2$. Hence, $(\xi_1,\xi_2,\xi_3)=(\xi,\xi,1)$, for some $\xi=\zeta_{3^j}^l$. But $\varphi_1\varphi_2=\sqrt[3^{j-1}]{\alpha}$. So on the one hand, $\phi(\sqrt[3^{j-1}]{\alpha})=\eta\sqrt[3^{j-1}]{\alpha}$ with $\eta^{3^{j-1}}=1$, and on the other hand, $\phi(\varphi_1\varphi_2)=\xi^2\varphi_1\varphi_2$. Hence, $\xi^2=\eta$ and $\xi^{2\cdot 3^{j-1}}=1$ so that $3\,|\,l$. So $\xi=\zeta_{3^{j-1}}^n$, where $n\in\{1,2,\ldots,3^{j-1}\}$. Moreover, $\phi(\zeta_{3^{j+1}})=\zeta_{3^{j+1}}^m$, where $m\in\{m_1,m_2\}=\{-1\pm 3^j\}$, since $\mathcal{V}_3(p+1)=j\Leftrightarrow p\equiv -1\pm 3^j \pmod{3^{j+1}}$.

Hence, $\phi\in\mathcal{A}_0=\{g\in G^* : g=g(m,n)$, where $m\in\{m_1,m_2\}$ and $n\in\{1,2,\ldots,3^{j-1}\}\}$, and $g(m,n)$ satisfies

$$\text{(4.6)}\quad g(\delta)=\delta,\quad g(\zeta_{3^{j+1}})=\zeta_{3^{j+1}}^m,\quad g(\varphi_1)=\zeta_{3^{j-1}}^n\varphi_2,\quad g(\varphi_2)=\zeta_{3^{j-1}}^n\varphi_1.$$

Observe that there is exactly one element of G^* which satisfies (4.6) so that $\mathcal{A}_0$ is a subset of G^* of size $2\cdot 3^{j-1}$.

So by the Chebotarev density theorem, for each $g=g(m,n)\in\mathcal{A}_0$, there are infinitely many primes p such that $g=\phi=\phi(R\,|\,p)$, the Frobenius automorphism of R over p, for some $R\in\mathcal{R}$. We check that if $p\nmid 3D$, then $\phi=g\Rightarrow p$ satisfies condition (4.3). Note first that $g(\zeta_{3^{j+1}})=\zeta_{3^{j+1}}^m\equiv\zeta_{3^{j+1}}^p$

(mod R) $\Rightarrow p \equiv m \pmod{3^{j+1}}$, since $p \neq 3$. But $m = -1 \pm 3^j \Rightarrow p \equiv -1 \pmod{3^j}$ so that p has order 2 (mod 3^j) which means that the restriction of ϕ to $\mathbb{Q}(\zeta_{3^j})$ has order 2. Hence $\phi(\zeta_{3^j}) = \zeta_{3^j}^{-1}$, which in view of (4.5) yields $\phi^2(\varphi_1) = \varphi_1$ and $\phi^2(\varphi_2) = \varphi_2$. Therefore ϕ restricted to F is also of order 2. Hence $f(P\,|\,p) = f(Q\,|\,p) = 2$ where P and Q are the ideals respectively in $\mathcal{P}$ and $\mathcal{Q}$ lying under R. Finally, ϕ has order six so that $f(R\,|\,p) = 6$ and by the normality of $\mathbb{Q}(\delta, \omega)$, F and $F(\zeta_{3^{j+1}})$ condition (4.3) holds for all P, Q and R.

Note that to prove equivalence (4.4) we assumed that R lied above P_0. This assumption was made to alleviate our proof. Had we assumed R to lie above P_i, $i = 1$ or $i = 2$, a similar reasoning would have led to $\phi(R\,|\,p)$ satisfying conditions analogous to (4.5), but different. Eventually, we would obtain $\phi \in \mathcal{A}_1$ or $\mathcal{A}_2$, where $\mathcal{A}_1$ and $\mathcal{A}_2$ are subsets of G^* of the same size as $\mathcal{A}_0$. Hence, the set $\mathcal{A}$ introduced in (4.4) is the disjoint union $\mathcal{A}_0 \cup \mathcal{A}_1 \cup \mathcal{A}_2$ and has size $2 \cdot 3^j$. Now by equivalence (4.4) and because the Frobenius $\phi(R\,|\,p)$ describes a full conjugacy class in G^* as R varies, $\mathcal{A}$ must be a union of conjugacy classes [2]. So the Chebotarev density theorem gives

$$d(\overline{D}_1(j)) = \frac{|\mathcal{A}|}{|G^*|} = \frac{2 \cdot 3^j}{2 \cdot 3^{3j}},$$

since, by Lemma 4.1, the cardinality $|G^*|$ of G^* is $3 \cdot [F : \mathbb{Q}] = 2 \cdot 3^{3j}$. Hence,

$$d(D_1) = d(S_1) - \sum_{j \geq 1} d(\overline{D}_1(j)) = \frac{1}{2} - \sum_{j \geq 1} \frac{1}{3^{2j}} = \frac{1}{2} - \frac{1}{8} = \frac{3}{8}. \ \blacksquare$$

Numerical data. We found that 595 of the smallest 800 primes in S_1 divide X. The relative density of D_1 in S_1 is $(3/8)/(1/2) = 3/4$, which compares well to the experimental ratio of 595/800.

Theorem 4.5. *The set D_2 is empty so that $d(D_2) = 0$.*

Proof. We choose an elementary proof which uses Lucas-like identities satisfied by the X, Y and Z sequences. Suppose $p \in D_2$. Then there is an integer n such that $p\,|\,Y$ at n. So $p\,|\,(y_n, y_{n+1})$. Now equation (1.4) with $(x, y, z) = (M^2, M, 1)$ yields

$$\text{(4.7)} \qquad \begin{cases} x_{n+1} = M^2 x_n + D y_n + DM z_n, \\ y_{n+1} = M x_n + M^2 y_n + D z_n. \end{cases}$$

The second equation in (4.7) implies that $p\,|\,Mx_n + Dz_n$, so that the first equation in (4.7) implies $x_{n+1} \equiv Dy_n \pmod{p}$. But $p\,|\,y_n \Rightarrow p\,|\,x_{n+1}$.

[2] More precisely, $\mathcal{A}$ is an elementary Frobenius set since condition (4.3) says that primes in $\overline{D}_1(j)$ have determined splitting types in the subfields of $F(\zeta_{3^{j+1}})$ (cf. [Lag2], p. 227).

Now (1.5) $\Rightarrow x_{n+1}^3+Dy_{n+1}^3+D^2z_{n+1}^3-3Dx_{n+1}y_{n+1}z_{n+1}=1$. But x_{n+1} and y_{n+1} being divisible by p, we have $D^2z_{n+1}^3\equiv 1 \pmod p$, so that D^2 must be a cube modulo p and therefore D must also be a cube modulo p. This contradicts the hypothesis $p\in S_2$. Hence, D_2 is empty. ∎

Remark. Theorem 4.5 renders Lemma 3.4 and Theorem 3.5 vacuous for primes in S_2!

Remark. The proof of Theorem 4.5 is a generalization of the proof by M. Ward [Wa2] that no prime congruent to 1 (mod 4) such that 5 is not a square (mod p) ever divides a Lucas number. Here identity (1.5) plays the role of the Pythagorean identity $L_n^2-5F_n^2=4(-1)^n$, which links the nth Lucas number to the nth Fibonacci number.

Definitions. Let j,k be integers such that $j\ge k\ge 0$. We define $D_3(j,k)=\{p\in D_3:\mathcal{V}_3(p-1)=j,\ \mathcal{V}_3(e_1)=k\}$. Note that $p\in D_3(j,k)\Rightarrow p\mid X$, so that $\mathcal{V}_3(e_1)=\mathcal{V}_3(e_2)=\mathcal{V}_3(e_3)=k$. Also, the choice of $P\in\mathcal{P}$ used to define e_1, e_2 and e_3 does not alter the set $D_3(j,k)$.

Theorem 4.6. *We have* $d(D_3(j,k))=2/3^{3j-2k+2}$ *and* $d(D_3)=3/26$.

Proof. Assume that $j\ge k\ge 1$ are fixed integers and that F is as in Lemma 4.1.

Then we have the equivalence:

$$(4.8)\qquad p\in D_3(j,k)\Leftrightarrow p \text{ splits in } F,\text{ but is inert in the 4 extensions } F(\sqrt[3]{\varphi_i}),\ i=1,2,3 \text{ and } F(\zeta_{3^{j+1}}) \text{ over } F.$$

Indeed, for all i, $\mathcal{V}_3(e_i)=k\Leftrightarrow \Psi_i^{(p-1)/3^{j-k}}\equiv 1$, but $\Psi_i^{(p-1)/3^{j-k+1}}\not\equiv 1 \pmod P$. That is, using Euler's criterion, Ψ_i is a 3^{j-k}th power (mod P), but not a 3^{j-k+1}th power. This last condition added to the fact that $3^{j+1}\nmid p-1$ yields (4.8) by application of the Kummer–Dedekind theorem ([3]).

Let Π be a prime in $F(\sqrt[3]{\varphi_1},\sqrt[3]{\varphi_2})$ lying over Q, where Q is in F and lies above p. Let h be the Frobenius automorphism of Π over p. Because the inertial degree of Q over p is 1, the restriction of h to F is the identity. Thus h is in the Galois group G' of $F(\sqrt[3]{\varphi_1},\sqrt[3]{\varphi_2})$ over F.

Now if $j>k$, then G' has order 9 and exponent 3, so is isomorphic to $(\mathbb{Z}/3\mathbb{Z})^2$. Each g in G' is determined by $g(\sqrt[3]{\varphi_1})$ and $g(\sqrt[3]{\varphi_2})$. Since $\varphi_i\in F$, $g(\sqrt[3]{\varphi_i})$ is again a cube root of φ_i. So let $\xi_i\in\{1,\omega,\omega^2\}$ be defined by $h(\sqrt[3]{\varphi_i})=\xi_i\sqrt[3]{\varphi_i}$. The condition that Q be inert in each $F(\sqrt[3]{\varphi_i})$ imposes $\xi_i\ne 1$ for all i.

Indeed, the Frobenius h has the property that $h(\sqrt[3]{\varphi_i})\equiv(\sqrt[3]{\varphi_i})^p=(\sqrt[3]{\varphi_i})^{p-1}\sqrt[3]{\varphi_i} \pmod \Pi$. But $(\sqrt[3]{\varphi_i})^{p-1}=\Psi_i^{3^{k-1}\cdot l}$, where $p-1=3^j\cdot l$. Now

[3] See Appendix A of [Ba1] for a statement of the theorems or principles used in the proof.

$e_i \mid 3^k \cdot l$, but $e_i \nmid 3^{k-1} \cdot l$, so that $\Psi_i^{3^{k-1} \cdot l}$ is a primitive cube root of 1. Hence, $\xi_i \in \{\omega, \omega^2\}$.

With a choice of roots such that $\sqrt[3]{\varphi_2} = \sqrt[3]{\varphi_1}\sqrt[3]{\varphi_3}$, we have $h(\sqrt[3]{\varphi_2}) = h(\sqrt[3]{\varphi_1}\sqrt[3]{\varphi_3}) \Rightarrow \xi_2 = \xi_1\xi_3$. But $\xi_3 \neq 1 \Rightarrow (\xi_1, \xi_2) \in \{(\omega, \omega^2), (\omega^2, \omega)\}$. So there are two elements of G' that h can be equal to. Hence, because G' is abelian, the density of primes p that split in F and then are inert in each extension $F(\sqrt[3]{\varphi_i})$ over F, is $\frac{2}{9} \cdot \frac{1}{[F:\mathbb{Q}]}$ by the Chebotarev density theorem. A similar reasoning shows that the density of primes which split in $F(\zeta_{3^{j+1}})$ and are then inert in the three extensions $F(\zeta_{3^{j+1}}, \sqrt[3]{\varphi_i})$ is $\frac{2}{9} \cdot \frac{1}{[F(\zeta_{3^{j+1}}):\mathbb{Q}]}$, i.e. $\frac{2}{27} \cdot \frac{1}{[F:\mathbb{Q}]}$. Combining these results with the principle of Inclusion-Exclusion, we get the density of primes satisfying condition (4.8) as

$$(4.9) \quad d(D_3(j,k)) = \frac{1}{[F:\mathbb{Q}]} \cdot \left[1 - \left(\frac{7}{9} + \frac{1}{3}\right) + \frac{7}{27}\right], \qquad \text{where } j > k \geq 1.$$

For $j = k$, $\varphi_i = \Psi_i$, for all i, and because of the normality of $F(\sqrt[3]{\varphi_i})$, condition (4.8) becomes

$$p \text{ splits in } F, \text{ but does not split in either } F(\sqrt[3]{\varphi_1}) \text{ or } F(\zeta_{3^{j+1}}).$$

So using the Kronecker density theorem and the principle of Inclusion-Exclusion, we get

$$(4.10) \qquad d(D_3(j,j)) = \frac{1}{[F:\mathbb{Q}]} \cdot \left[1 - \left(\frac{1}{3} + \frac{1}{3}\right) + \frac{1}{9}\right].$$

Now using Lemma 4.1 and formulas (4.9) and (4.10), one obtains the density $d(D_3(j,k))$ claimed.

Hence, the density $d(D_3)$ is evaluated by summing up two geometric series:

$$d(D_3) = \sum_{j \geq k \geq 1} d(D_3(j,k)) = \frac{2}{9} \cdot \sum_{k \geq 1}\sum_{j \geq k} \frac{1}{3^{3j-2k}} = \frac{3}{26}. \ \blacksquare$$

Numerical remark. The set S_3 has Dirichlet density 1/6, while D_3 has density 3/26. So the relative density of primes in S_3 that divide X is 9/13. For $D = 7$, we found that 554 of the smallest 800 primes in S_3 divide X. This compares well to what the asymptotic ratio yields, i.e. $\frac{9}{13} \cdot 800 \sim 553.85$!

THEOREM 4.7. *The set of primes p such that $p \mid X$ has Dirichlet density $51/104 = 1/2 - 1/104$.*

Proof. By Theorems 4.4–4.6, we have $d(\{p : p \mid X\}) = 3/8 + 0 + 3/26$. $\blacksquare$

THEOREM 4.8. *The set of primes p such that $3 \mid r(p)$ has Dirichlet density $157/312 = 1/2 + 1/312$.*

Proof. We have $T_1 = D_1$ and $T_2 = D_2$. So we must determine $d(T_3)$, if it exists. What we do is show that $\overline{T}_3$, the complement of T_3 in S_3 has a density. Indeed, negating equivalence (4.2), we get

$$(4.11)\qquad 3\nmid r(p) \Leftrightarrow \forall P\in\mathcal{P},\ \mathcal{V}_3(e_1)=\mathcal{V}_3(e_2)=\mathcal{V}_3(e_3)=0.$$

Let $j\ge 1$ and $\overline{T}_3(j)=\{p\in\overline{T}_3 : \mathcal{V}_3(p-1)=j\}$. Using (4.11), we have $p\in\overline{T}_3(j)\Leftrightarrow \Psi_i^{(p-1)/3^j}\equiv 1 \pmod{P}$, for all i and P; that is, by Euler's criterion, each Ψ_i is a 3^jth power (mod P), and, by the Kummer–Dedekind theorem, p splits in F, but not in $F(\zeta_{3^{j+1}})$, where $F=\mathbb{Q}(\delta,\zeta_{3^j},\varphi_1,\varphi_2,\varphi_3)$ and $\varphi_i=\sqrt[3^j]{\Psi_i}$, $i=1,2,3$, as in Lemma 4.1. So,

$$d(\overline{T}_3(j))=\frac{1}{[F:\mathbb{Q}]}\cdot\left[1-\frac{1}{3}\right].$$

Now, since $k=0$ and $j>k$, Lemma 4.1 gives $[F:\mathbb{Q}]=2\cdot 3^{3j-1}$. Hence,

$$d(\overline{T}_3)=\sum_{j\ge1}d(\overline{T}_3(j))=\sum_{j\ge1}\frac{1}{3^{3j}}=\frac{1}{26}$$

and

$$d(T_3)=d(S_3)-d(\overline{T}_3)=\frac{1}{6}-\frac{1}{26}=\frac{5}{39}.$$

Thus,

$$d(\{p:3\,|\,r(p)\})=\frac{3}{8}+\frac{5}{39}=\frac{157}{312}.\ \blacksquare$$

Numerical remark. The relative density of T_3 in S_3 is $(5/39)/(1/6)=10/13$. For $D=7$, we found that 617 of the smallest 800 primes in S_3 have a rank multiple of 3, while the asymptotic ratio of 10/13 predicts $\frac{10}{13}\cdot 800\sim 615.4$.

Remark. Suppose $p\in T_3$, $\mathcal{V}_3(p-1)=j$ but that condition (4.2) holds with $\mathcal{V}_3(e_i)=j$ for some $i=1,2$ or 3 and some $P\in\mathcal{P}$, then condition (4.1) is also satisfied. Indeed, $\mathcal{V}_3(e_i)=j\Leftrightarrow p$ does not split in $F(\sqrt[3]{\Psi_i})$, where F is $\mathbb{Q}(\delta,\zeta_{3^j})$. But $F(\sqrt[3]{\Psi_1})=F(\sqrt[3]{\Psi_2})=F(\sqrt[3]{\Psi_3})\Rightarrow \mathcal{V}_3(e_1)=\mathcal{V}_3(e_2)=\mathcal{V}_3(e_3)=j$. Now if $\mathcal{V}_3(e_1)=\mathcal{V}_3(e_2)=\mathcal{V}_3(e_3)=j$ holds for some P, then it holds for all $P\in\mathcal{P}$. That is, p belongs to D_3. In particular, as mentioned in Section 3, all primes p congruent to 4 or 7 (mod 9) in T_3 belong to D_3.

5. Final remarks

Remark 5.1. In [M-S], the authors determine the density of prime divisors of the Lucas sequence $(\alpha^n+\overline{\alpha}^n)$, where α is the fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{D})$, $D\ge 2$, D squarefree integer. They found the set of possible densities to be limited to a few values and to depend in a simple manner on the norm and trace of α. We ask analogous questions for the cubic case.

In particular, besides the fields $\mathbb{Q}(\sqrt[3]{D})$ where $D=M^3\pm1$, are there other pure cubic fields with fundamental unit α for which $X=(\alpha^n+\beta^n+\overline{\beta}^n)$ has order 3 in the Laxton–Ballot group $E(f)$, where f is the minimal polynomial of α? If so, do the maximal divisors of X have a computable and predictable density? Or, do other sequences in $S(f)$ have such properties? Are there more families of pure cubic fields for which the density of primes having a rank r (relative to f) such that $3\,|\,r$ is determined? What would these densities be?

Remark. Although the WB-sequences may be viewed as a generalization of the pair $\{V_n, U_n\}$ of ordinary Lucas sequences, they can also be viewed as a generalization of the triplet $\{W_n^1, W_n^2, U_n\}$ of integral quadratic recurrences that exist whenever the discriminant Δ of $X^2 - PX + Q$ is of the form $-3F^2$.

The remark will make sense if one considers the theorem below.

Theorem 5.2. *Let $f(X) = X^2 - PX + Q = (X-\alpha)(X-\overline{\alpha}) \in \mathbb{Z}[X]$, $(P,Q) = 1$ and $\Delta = P^2 - 4Q = -3F^2$, $F \in \mathbb{N}$. Then the sequences (W_n^1) and (W_n^2) in $S(f)$ defined by their initial values as*

$$W^1 = \left[1, \frac{P-F}{2}\right] \quad \text{and} \quad W^2 = \left[1, \frac{P+F}{2}\right],$$

have the following properties, with $\alpha = (P + F\sqrt{-3})/2$:

(i) *$W^1 = \langle F\omega, F\omega^2\rangle$, $W^2 = \langle -F\omega^2, -F\omega\rangle$ and $U = \langle 1, 1\rangle$, so that the sequences W^1, W^2, U have classes in $E(f)$ forming a cyclic subgroup of order 3.*

(ii) *If $p \nmid 3FQ$, then*

$$\exists n \in \mathbb{N}, \quad r(p) = 3n \Leftrightarrow p\,|\,W^1 \text{ at } n \text{ or } p\,|\,W^2 \text{ at } n.$$

(iii) *If $\alpha/\overline{\alpha}$ is not a cube in $\mathbb{Q}(\omega)$, then $d(W^1) = d(W^2) = 3/4$.*

Proof. (i) Use (2.1) or (2.5) of [Ba1] to calculate $\langle A_1, A_2\rangle$.

(ii) This follows easily from the identity $F^2U_{3n} = 3U_nW_n^1W_n^2$.

(iii) One may follow the proof in the corrigendum of [Lag1] which treats the particular case $(P,Q) = (5,7)$. (The proof is in two parts according as $\mathcal{V}_3(p-1) \geq 1$ or $\mathcal{V}_3(p+1) \geq 1$. Note that the two sub-densities are $3/8$ and $3/8$, so that the density of prime divisors $\equiv 2 \pmod 3$ is equal to the density of maximal prime divisors $\equiv 2 \pmod 3$ found in companion WB-sequences.) ∎

Acknowledgments. Hugh Williams invited me for a week in Winnipeg, Canada, in December 1993 a couple months after I had noticed these mathematical facts. Hugh provided valuable documents and references concerning his work. John Brillhart did lend me a goose parka. The biting memory of this wondrous white week certainly contributed to my eventual completing of the work.

References

[Ba1] C. Ballot, *Density of prime divisors of linear recurrences*, Mem. Amer. Math. Soc. 551 (1995).

[Ba2] —, *Group structure and maximal division for cubic recursions with a double root*, Pacific J. Math. 173 (1996), 337–355.

[Ba3] —, *The density of primes p, such that -1 is a residue modulo p of two consecutive Fibonacci numbers, is* 2/3, Rocky Mountain J. Math., to appear.

[Ha] 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.

[Lag1] J. C. Lagarias, *The set of primes dividing the Lucas numbers has density* 2/3, Pacific J. Math. 118 (1985), 449–461; Errata: ibid. 162 (1994), 393–396.

[Lag2] —, *Sets of primes determined by systems of polynomial congruences*, Illinois J. Math. 27 (1983), 224–237.

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

[Le1] D. H. Lehmer, *On the multiple solutions of the Pell equation*, Ann. of Math. (2) 30 (1929), 66–72.

[Le2] —, *On Lucas's test for the primality of Mersenne's numbers*, J. London Math. Soc. 10 (1935), 162–165.

[Lu] E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math. 1 (1878), 184–240, 289–321.

[Ma] G. B. Mathews, *On the arithmetical theory of the form $x^3+ny^3+n^2z^3-3nxyz$*, Proc. London Math. Soc. 21 (1890), 280–287.

[Mo] P. Moree, *On the prime density of Lucas sequences*, J. Théor. Nombres Bordeaux 8 (1996), 449–459.

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

[Na] T. Nagell, *Über die Einheiten in reinen kubischen Zahlkörpern*, Skr. Norske Vid. Akad. Oslo Mat.-Naturv. Klasse 11 (1923), 1–34.

[Wa1] M. Ward, *The maximal prime divisors of linear recurrences*, Canad. J. Math. 6 (1954), 455–462.

[Wa2] —, *The prime divisors of Fibonacci numbers*, Pacific J. Math. 11 (1961), 379–386.

[We] A. E. Western, *On Lucas's and Pepin's tests for primeness of Mersenne numbers*, J. London Math. Soc. 7 (1932), 130–137.

[Wi1] H. C. Williams, *A generalization of the Lucas functions*, unpublished Ph.D. thesis, University of Waterloo, Waterloo, Ontario, 1969.

[Wi2] —, *On a generalization of the Lucas functions*, Acta Arith. 20 (1972), 33–51.

[Wi3] —, *Edouard Lucas and Primality Testing*, Canad. Math. Soc. Ser. Monographs Adv. Texts, Wiley, 1998.

Département de Mathématiques
Université de Caen, Campus 2
BP 5186
14032 Caen Cedex, France
E-mail: ballot@math.unicaen.fr

Received on 10.9.1998
and in revised form on 1.12.1998 (3461)