ON SEQUENCE GROUPS

ZBIGNIEW LIPIŃSKI AND MACIEJ P. WOJTKOWSKI

Abstract. Linear second order recursive sequences with arbitrary initial conditions are studied. For sequences with the same parameters a ring and a group is attached, and isomorphisms and homomorphisms are established for related parameters. In the group, called the sequence group, sequences are identified if they differ by a scalar factor, but not if they differ by a shift, which is the case for the Laxton group.

Prime divisors of sequences are studied with the help of the sequence group mod $p$, which is always cyclic of order $p \pm 1$.

Even and odd numbered subsequences are given independent status through the introduction of one rational parameter in place of two integer parameters. This step brings significant simplifications in the algebra.

All elements of finite order in Laxton groups and sequence groups are described effectively.

A necessary condition is established for a prime $p$ to be a divisor of a sequence: the norm (determinant) of the respective element of the ring must be a quadratic residue mod $p$. This leads to an upper estimate of the set of divisors by a set of prime density $1/2$. Numerical experiments show that the actual density is typically close to 0.35.

A conjecture is formulated that the sets of prime divisors of the even and odd numbered elements are independent for a large family of parameters.

1. Introduction

We present some new results about linear recursive sequences of order 2. There is a vast literature of the subject. The book by Everest, van der Poorten, Shparlinski and Ward, [E-P-S-W], gives a broad panorama of problems and results with an exhaustive bibliography. Another source is the book of Williams, [W], where the themes developed in our work are brought into focus. We will refer only to papers which are most relevant to our work. Our study is rooted in the work of Laxton, [L1, L2] who associated an abelian group structure to recursive sequences, to study the sets of their prime divisors.

For rational $Q \neq 0$ and $T \neq 0$ let $D = D_{T,Q} = \begin{bmatrix} 0 & -Q \\ 1 & T \end{bmatrix}$ be the matrix defining recursive sequences $\{x_n\}_{n \in \mathbb{Z}}$ by the formula

$$[x_n \ x_{n+1}] = [x_0 \ x_1]D^n.$$

We choose to consider all rational initial conditions $x_0, x_1$. Non-integer values are actually unavoidable even if we consider integer parameter pairs.

Date: October 31, 2024.

2010 Mathematics Subject Classification. 11B37, 11B39.
ZBIGNIEW LIPIŃSKI AND MACIEJ P. WOJTKOWSKI

$(T, Q)$ and integer initial values. Indeed powers of $Q$ appear in the denominators of the elements with negative indices. In general the denominators are similarly “poor”, while the numerators are “rich”, in prime divisors. More precisely for every sequence the denominators have only finitely many prime divisors. This allows the use of the modular arithmetic with rational numbers. A fully reduced simple fraction $\frac{a}{b} = 0 \mod p$, for a prime $p$ not dividing $b$, if $a$ is divisible by $p$. It works well if we avoid the prime divisors of the denominators, which are only finitely many for a specific sequence.

We propose to separate the even and odd terms of a recursive sequence as recursive sequences in their own right. More precisely one sequence $\{x_n\}_{n \in \mathbb{Z}}$ for the parameter pair $(T, Q)$ is split into two sequences $\{y_k = Q^{1-k}x_{2k}\}_{k \in \mathbb{Z}}$ and $\{z_k = Q^{1-k}x_{2k-1}\}_{k \in \mathbb{Z}}$ for the parameters $(t, 1), t = T^2/Q-2$, essentially the even and odd numbered elements of the original sequence. The idea to allow the rational parameter $t$, and achieve $Q = \det D = 1$, appeared first in [Wo], and it lead to substantial simplifications. In this paper we find further applications of this method. We mostly use the one parameter language, due to its simplicity, and translate the results into the language of two parameters $(T, Q)$.

The interest in Laxton groups was recently revived by Aoki and Kida, [A-K], and Suwa, [S1, S2].

In Section 2 we introduce a ring of $2 \times 2$ matrices associated with recursive sequences. In general this ring is a quadratic field extension of $\mathbb{Q}$. Similar construction appeared in the work of Hall, [H1]. We use it to compare sequences for the parameters $t$ and $t_r = C_r(t)$, where $C_r(t) = tr D_r^t$ are the Chebyshev polynomials of the first kind. In Proposition 3 we show that the sequences for $t$ can be disintegrated into $r$ sequences for $t_r$. It brings forward the concept of a primitive parameter $t$ which is not equal to $C_r(u)$ for any prime $r$ and rational $u$.

In Section 3 we discuss the phenomenon of recombination: two sequences for a parameter pair $(T, Q)$ become sequences for another parameter pair $(\hat{T}, \hat{Q})$, after essentially the exchange of odd terms. The two parameter pairs are rigidly connected, and we call them twins. For example the twin of the Fibonacci parameters $(1, -1)$ is $(5, 5)$. The phenomenon of twins was discovered in [Wo] in a more restricted setting of special sequences.

We proceed looking for rational $t \neq a$ and a prime $r$ such that $C_r(t) = C_r(a)$, which is essential for extending the recombination to other sets of parameters. It turns out to be exceedingly rare, limited to $r = 2$ (the twin case), $r = 4$ (the circular case) and $r = 3$ (the cubic case). The parameter $a$ will be called an associate parameter of $t$.

In Section 4 we introduce the sequence group $L(t)$, which is an extraction of the multiplicative structure of the ring up to scalar factors. Further we consider $L_p(t)$, the sequence group mod $p$, which turns out to be always cyclic of order $p \pm 1$ (Theorem 10).

In Section 5 we arrive at the Laxton group $G(t)$, [L1], which is the quotient of the sequence group by the cyclic subgroup generated by the element $D$. While the finite order elements in $G$ are of significant interest, the sequence groups $L$ provide a good environment for calculations.
We are able to list all torsion elements in sequence groups and Laxton groups for all parameters. It was attempted in [L2], we give a more explicit description. For primitive parameters \( t \) there are only 3 finite order elements in the Laxton group under additional assumption of primitivity, namely that not only \( t \) is primitive but also its associate parameters are primitive. This stronger condition is called twin, circular or cubic primitivity.

The special sequences which are of finite order in the circular and cubic cases were studied in detail in a remarkable paper of Ballot, [B], in the language of the parameter pairs \( (T, Q) \).

In Section 6 we briefly describe the structure of all the torsion subgroups of the Laxton groups. However we must admit that we did not find any application for this information.

In Section 7 we proceed with the study of the sets of prime divisors of recursive sequences, mostly in the language of one rational parameter \( t \). We reformulate the old theorem of Hall, [H2], into the language of \( \mathcal{L}_p(t) \) (Proposition 29).

In his paper, [L1], Laxton states that “One problem of perennial interest is that of prime divisors of a recurrence. ... The divisor problem is the chief interest in this article.”

The study of the sets of prime divisors for recursive sequences for arbitrary initial conditions was the subject of only few papers, Laxton was preceded by Ward, [Wa], where he proves that for most sequences this set is infinite. The exclusions are only in parameters, and not the initial conditions. In our one parameter language they correspond to \( t \neq 0, \pm 1, \pm 2 \). This result can be also traced back to the paper of Polya, [P], [L]. The results of Stephen, [St], and Moree and Stevenhagen, [M-S], suggest that the sets have positive prime density. The state of the art is presented comprehensively by Moree in his survey paper [M], Chapter 8.4.

In the final Section 8 we formulate a conjecture that for a large family of sequences, for the parameter pair \( (T, Q) \), the sets of divisors of even and odd terms are independent, i.e., the prime density of their intersection is the product of their prime densities. This conjecture has two motivations. One is the simple criterion (Theorem 31) that for most sequences if an odd prime \( p \) is a divisor then the determinant (or the norm) of the sequence is a quadratic residue \( \mod p \). This implies that for most sequences of one parameter \( t \) the set of divisors is contained in a set of prime density \( 1/2 \). As a consequence we arrive at two independent sets for the even and odd terms of the sequence for the respective parameter pair \( (T, Q) \).

The other motivation comes from numerical experiments which give a tentative confirmation of the conjecture.

2. The ring of recursive sequences

Let \( \mathcal{R} = \mathcal{R}(T, Q) \) be the ring of \( 2 \times 2 \) matrices with rational entries which commute with \( D = D_{T, Q} = \begin{bmatrix} 0 & -Q \\ 1 & T \end{bmatrix} \). In particular \( D \in \mathcal{R} \).

Lemma 1.

\[
\mathcal{R} = \left\{ X \mid X = \begin{bmatrix} -Qx_1 & -Qx_0 \\ x_0 & x_1 \end{bmatrix}, x_1 = Tx_0 - Qx_{-1}, x_0, x_1 \in \mathbb{Q} \right\}
\]
For ease of notation we will denote an element $X \in \mathcal{R}$ by the second row $[x_0 \ x_1]$. We put the recursive sequences $\{x_n\}_{n \in \mathbb{Z}}$ into $1 - 1$ correspondence with the elements of $\mathcal{R}$ by the formula $X = [x_0 \ x_1]$. Alternatively we associate with $\{x_n\}_{n \in \mathbb{Z}}$ the sequence of matrices $\{X D^n\}_{n \in \mathbb{Z}}$ in $\mathcal{R}$, where

$$X D^n = \begin{bmatrix} -Qx_{n-1} & -Qx_n \\ x_n & x_{n+1} \end{bmatrix}. $$

The determinant of the matrices in $\mathcal{R}$ will play an important role. For $[x_0 \ x_1] = X \in \mathcal{R}$

$$\det X = x_1^2 - T x_1 x_0 + Q x_0^2,$$

As long as the discriminant $\Delta = T^2 - 4Q$ is not a rational square there are no zero divisors in the ring, and it is actually isomorphic to the quadratic field $\mathbb{Q}(\sqrt{\Delta})$. Under this isomorphism the determinant becomes the norm of a field element. The canonical field automorphism of $\mathbb{Q}(\sqrt{\Delta})$ translates into $\mathcal{R}(T, Q)$ as $X \mapsto (\det X)X^{-1}$. If $X$ represents a recursive sequence $\{x_n\}_{n \in \mathbb{Z}}$ then $(\det X)X^{-1}$ represents the sequence $\{-Q^n x_{-n}\}_{n \in \mathbb{Z}}$.

We are ready to introduce the crucial step in our paper, namely the separation of even and odd terms of a recursive sequence as recursive sequences in their own right.

**Proposition 2.** For any pair of rational nonzero parameters $(T, Q)$ and $t = T^2 Q^{-1} - 2$ there is a canonical ring isomorphism $\Phi : \mathcal{R}(T, Q) \rightarrow \mathcal{R}(t, 1)$, defined by the conjugation $\Phi(X) = A^{-1} X A \in \mathcal{R}(t, 1)$, where $X = [x_0 \ x_1]$,

$$A = \begin{bmatrix} Q & -Q \\ 0 & T \end{bmatrix} \quad \text{and} \quad T \Phi(X) = \begin{bmatrix} x_2 - t Q x_0 & -Q x_0 \\ Q x_0 & x_2 \end{bmatrix}. $$

In particular $\Phi(D_{T, Q}^2) = Q D_{t, 1}$, and $\Phi(Q^{-k} X D_{T, Q}^{2k}) = \Phi(X) D_{t, 1}^k$.

Since $t^2 - 4 = (T^2 - 4Q)T^2/Q^2$ the respective quadratic fields coincide, and the proof of this Proposition is obtained by direct calculation. However its meaning can be elucidated further. For a recursive sequence $\{x_n\}_{n \in \mathbb{Z}} = X \in \mathcal{R}(T, Q)$ and $W = T \Phi(D_{T, Q}^{-1}) = [-1 \ 1] \in \mathcal{R}(t)$ we have

$$\Phi(X) = \{T^{-1} Q^{1-n} x_{2n}\}_{n \in \mathbb{Z}} = Z \in \mathcal{R}(t), \quad \{Q^{1-n} x_{2n-1}\}_{n \in \mathbb{Z}} = T \Phi(D_{T, Q}^{-1} X) = W Z \in \mathcal{R}(t). $$

Note that these formulas are consistent with the recursive relation

$$T x_{2n-1} = Q x_{2n-2} + x_{2n}. $$

In particular we substitute $X = [0 \ 1] = \{L_n\}_{n \in \mathbb{Z}}$ in the formula (1), i.e., the identity matrix in $\mathcal{R}(T, Q)$, or in other words the Lucas sequence. [Wi]. We obtain that for $I = [0 \ 1] = \{u_n\}_{n \in \mathbb{Z}} \in \mathcal{R}(t)$ and $W = \{w_{2n-1}\}_{n \in \mathbb{Z}} \in \mathcal{R}(t)$ we have

$$u_n = \frac{1}{T Q^n-1} L_{2n}, \quad w_{2n-1} = \frac{1}{Q^{-n-1}} L_{2n-1}. $$

(The choice of indexing for the sequence $W$ has some advantages that will be illuminated later on.)

Hence one recursive sequence $\{x_n\}_{n \in \mathbb{Z}}$ for the parameter pair $(T, Q)$ is split into two recursive sequences $\{Q^{1-k} x_{2k}\}_{k \in \mathbb{Z}}$ and $\{Q^{1-k} x_{2k-1}\}_{k \in \mathbb{Z}}$ for
the parameters \((t, 1)\), essentially the even and odd numbered elements of the original sequence.

We say that parameter pairs \((T, Q)\) and \((\hat{T}, \hat{Q})\) are similar if \(T^2 \hat{Q} = \hat{T}^2 Q\). Clearly the similarity is an equivalence relation. In particular \((T, Q)\) and \((aT, a^2 Q)\) are similar for any rational \(a\). Note that \((T, Q)\) and \((-T, Q)\) are always similar, while \((T, Q)\) and \((T, -Q)\) are never similar (we exclude the values \(T = 0\) or \(Q = 0\) from consideration).

Similar parameter pairs give the same parameter \(t = T^2/Q - 2\), and hence in view of Proposition 2 they produce essentially the same recursive sequences. More precisely if \(\{x_n\}_{n \in \mathbb{Z}}\) is a recursive sequence for the parameters \((T, Q)\) then the sequence \(\{\bar{x}_n = a^n x_n\}_{n \in \mathbb{Z}}\) is a recursive sequence for the parameters \((\hat{T}, \hat{Q}) = (aT, a^2 Q)\). In particular the sequence \(\{(-1)^n x_n\}_{n \in \mathbb{Z}}\) is a recursive sequence for the parameters \((-T, Q)\).

We say that a parameter pair \((T, Q)\) is simple if \(T\) and \(Q\) are integers and for any prime divisor \(p\) of \(T\) the parameter \(Q\) is not divisible by \(p^2\). Every \((T, Q)\) is similar to exactly two simple pairs of the form \((\pm aP, aR)\) with co-prime integers \(P\) and \(R\), and \(R\) and \(a\). It is obtained directly by simplifying the fraction \(\frac{T^2}{Q^2} = \frac{aP^2}{R^2}\), with a square-free \(a\). In the rest of the paper we will consider either simple pairs \((T, Q) = (aP, aR)\) or one rational parameter \(t\).

The idea to allow the rational parameter \(t\), and achieve determinant 1, appeared first in \([Wo]\), and it lead to substantial simplifications. In this paper we find further applications of this method. For any rational \(t\) we introduce the notation \(D_t = D_{t, 1}\), and \(\mathcal{R}(t) = \mathcal{R}(t, 1)\). We will study mainly the sequences in \(\mathcal{R}(t)\), \(t = 4P^2/R^2 - 2\). The information obtained can be then translated into the original space \(\mathcal{R}(T, Q)\).

There is a hidden symmetry of the problem, which is revealed by the passage to the parameter \(t\). The following proposition is established by inspection.

**Proposition 3.** For any rational \(t\) there is a canonical ring isomorphism \(\Psi: \mathcal{R}(t) \rightarrow \mathcal{R}(-t)\) given by the transposition \(\Psi(X) = X^T\).

In particular \(D_{-t} = -D_t^T\), and for a recursive sequence \(\{x_n\}_{n \in \mathbb{Z}}\) represented by \(X\) in \(\mathcal{R}(t)\), the sequence \(\{(-1)^n x_n\}_{n \in \mathbb{Z}}\) is represented by \(\Psi(X)\) in \(\mathcal{R}(-t)\).

We say that the parameters \(t\) and \(-t\) are twins, and that two parameter pairs \((T, Q)\) and \((\hat{T}, \hat{Q})\) are twins if the respective parameters \(t\) and \(\hat{t}\) are twins. It is straightforward that two simple parameter pairs are twins if and only if they are equal to \((aP, aR)\) and \((bS, bR)\), respectively, satisfying \(aP^2 + bS^2 = 4R\). Every simple parameter pair has a simple twin, essentially unique. For example the twin of the Fibonacci pair \((1, -1)\) is \((5, 5)\). In general with \(\Delta = T^2 - 4Q\) the parameter pairs \((T, Q)\) and \((\Delta, -\Delta Q)\) are twins (here we do not assume or claim their simplicity).

Proposition 2 can be generalized to “higher powers”. We recall that a recursive sequence \(\{x_n\}_{n \in \mathbb{Z}}\) of \(D_t\) can be written in terms of the Chebyshev polynomials of the second kind \(U_n(t)\), \([Wo]\),

\[
D_t^n = \begin{bmatrix}
-U_{n-1}(t) & -U_n(t) \\
U_n(t) & U_{n+1}(t)
\end{bmatrix}, \quad x_n = U_n(t) x_1 - U_{n-1}(t) x_0.
\]
In particular the identity matrix $I$ of the ring $\mathcal{R}(t)$ represents the sequence $\{U_n(t)\}_{n \in \mathbb{Z}}$. The Chebyshev polynomials of the first kind are equal to $C_n(t) = \text{tr } D^n_t$. We denote by $C = [2 \, t]$ the sequence $\{C_n(t)\}_{n \in \mathbb{Z}}$.

It is useful to introduce also the Chebyshev polynomials of the third and fourth kind, $[Y]$, namely $W_{2k-1} = U_k + U_{k-1}$ and $V_{2k-1} = U_k - U_{k-1}$. The sequence $\{W_{2k-1}(t)\}_{n \in \mathbb{Z}}$ is equal to $W = [-1 \, 1]$ and the sequence $\{V_{2k-1}(t)\}_{n \in \mathbb{Z}}$ is equal to $V = [1 \, 1]$. The special indexing of these polynomials simplifies the formulation of their properties, cf. $[W]$. It is not hard to prove that the only rational zeroes of the polynomials $U_n$ are $t = 0, \pm 1, \pm 2$, $[W]$. We will exclude these values of the parameter $t$ from further considerations.

**Proposition 4.** For any natural $r$ there is a canonical ring isomorphism $\Phi_r : \mathcal{R}(t) \to \mathcal{R}(t_r)$, where $t_r = C_r(t)$, given by the conjugation $\Phi_r(X) = A^{-1} X A \in \mathcal{R}(t_r)$, where $X = [x_0 \, x_1]$, 

$$A = \begin{bmatrix} 1 & -U_{r-1}(t) \\ 0 & U_r(t) \end{bmatrix} \quad \text{and} \quad U_r(t)\Phi_r(X) = \begin{bmatrix} x_r - t_r x_0 - x_0 & -x_0 \\ x_0 & x_r \end{bmatrix}. $$

In particular $\Phi_r(D^r_t) = D_{t_r}$ and $\Phi_r(X D^k_{t_r}) = \Phi_r(X) D^k_{t_r}$.

**Proof.** For a recursive sequence $\{x_n\}_{n \in \mathbb{Z}}$ of the matrix $D_t$ the sequence $\{x_{kr}\}_{k \in \mathbb{Z}}$ is a recursive sequence of the matrix $D_{t_r}$. Indeed we have 

$$[x_0 \, x_r] = [x_0 \, x_1] \begin{bmatrix} 1 & -U_{r-1}(t) \\ 0 & U_r(t) \end{bmatrix}, \quad [x_r \, x_{2r}] = [x_0 \, x_r] A^{-1} D^r_t A, $$

It follows that $A^{-1} D^r_t A = D_{t_r}$.

Clearly $\Phi_r$ is a ring monomorphism into $\mathcal{R}(t_r)$. Since for $X = [x_0 \, x_1]$ we have $U_r(t)\Phi_r(X) = [x_0 \, x_r]$ and for a given $x_0$ the element $x_r$ assumes arbitrary rational value, then $\Phi$ is onto $\mathcal{R}(t_r)$.

It follows from this Proposition that splitting a recursive sequence $\{x_n\}_{n \in \mathbb{Z}}$ of the parameter $t$ into $r$ subsequences $\{x_{kr+j}\}_{k \in \mathbb{Z}}, j = 0, 1, \ldots, r - 1$, we obtain recursive sequences of the parameter $t_r$.

We say that a parameter $t$ is $r$-primitive if there is no rational $u$, such that $t = C_r(u)$, and it is primitive if it is $r$-primitive for all natural $r \geq 2$.

In view of Proposition 4 we will mostly restrict our attention to primitive parameters (excluding again the values $t = 0, \pm 1, \pm 2$, which are not primitive).

We look now at matrices in $\mathcal{R}(t)$ with determinant 1.

**Lemma 5.** Given a rational $t$, for a rational $b$ there is a matrix $X \in \mathcal{R}(t)$ with $\text{tr } X = b$, $\det X = 1$ if and only if $\frac{b^2 - 4}{t^2 - 4}$ is a rational square.

The matrix $X$, if it exists, is unique up to the automorphism of $\mathcal{R}(t)$.

**Proof.** We seek an element $X = [x_0 \, x_1] \in \mathcal{R}(t)$ with $\det X = 1$ and $\text{tr } X = b$. By a direct calculation we arrive at the equivalent conditions of the form $x_0^2 = \frac{b^2 - 4}{t^2 - 4}$ and $2x_1 = tx_0 + b$.

When there is such a rational $x_0$ then $-x_0$ gives us another matrix $X^{-1}$ with the same trace $b$, and there are no other in $\mathcal{R}(t)$.

Clearly the condition in the Lemma is equivalent to the rings $\mathcal{R}(t)$ and $\mathcal{R}(a)$ being isomorphic.
3. Recombination of sequences

We have seen that a recursive sequence can be split into two, or more, recursive sequences for a new parameter. In this section we will inspect the opposite, how to recombine two, or more sequences of one parameter, into recursive sequences of another parameter.

For a simple parameter pair \((T, Q)\) and \(t = T^2/Q - 2\) let us recall the special sequences in \(\mathcal{R}(t)\) we have introduced earlier

\[
C = [2 \ t] = \frac{T}{Q} \Phi([2 \ T]), \ W = [-1 \ 1] = T \Phi(D_{T,Q}^{-1}), \ V = [1 \ 1] = \frac{1}{t+2} WC.
\]

The following Proposition appeared originally in the paper of Laxton, \([L1]\) (Theorem 4.3), for a parameter pair \((T, Q)\). It is markedly simpler in the language of one rational parameter \(t\).

**Proposition 6.** For any \([x_0 \ x_1] = X \in \mathcal{R}(t)\) we have

\[
X^2 = \begin{bmatrix}
x_1 - tx_0 & -x_0 \\
x_0 & x_1
\end{bmatrix}^2 = \begin{bmatrix}
x_0(x_1 - x_0) & (x_1 + x_0)(x_1 - x_0)
\end{bmatrix},
\]

\[
CX = [x_1 - x_{-1} \ x_{-2} - x_0], \ WX = [x_0 + x_{-1} \ x_1 + x_0], \ VX = [x_0 - x_{-1} \ x_1 - x_0].
\]

Let us note that if \(X \in \mathcal{R}(t)\) represents the sequence \(\{x_k\}_{k \in \mathbb{Z}}\) then \(CX, WX, VX\) represent, respectively, \(\{x_{k+1} - x_{k-1}\}_{k \in \mathbb{Z}}, \{x_k + x_{k-1}\}_{k \in \mathbb{Z}}, \{x_k - x_{k-1}\}_{k \in \mathbb{Z}}\). The role of this proposition comes from the fact that all elements of the sequence \(X^2\) are factored into the elements of the sequences \(X, CX, WX, VX\). More precisely the even numbered elements are factored into the elements of \(X, CX\), and odd numbered elements into the elements of \(WX\) and \(VX\) (note that \((t + 2)VX = WCX\)).

It follows from the formula (1) that the sequences \(X \in \mathcal{R}(t)\) and \(WX\) can be recombined to give a sequence in \(\mathcal{R}(T, Q)\) with even-numbered elements essentially equal to the elements of \(X\), and odd-numbered elements essentially equal to the elements of \(WX\).

For the isomorphism \(\Psi : \mathcal{R}(t) \to \mathcal{R}(-t)\) of Proposition 3 we have

\[
\Psi(C_t) = -C_{-t}, \ \Psi(W_t) = V_{-t}, \ \Psi(V_t) = W_{-t}.
\]

It follows that while sequences \(X\) and \(WX\) from \(\mathcal{R}(t)\) can be recombined into one sequence \(Z \in \mathcal{R}(T, Q)\), the sequences \(X\) and \(VX\) can be recombined into one sequence \(\hat{Z} \in \mathcal{R}(\hat{T}, \hat{Q})\), where \((\hat{T}, \hat{Q})\) is the twin simple pair, in particular \(\hat{T}^2/\hat{Q} = 2 - t\). More precisely we have the following Proposition.

**Proposition 7.** For any recursive sequence \(\{z_n\}_{n \in \mathbb{Z}}\) in \(\mathcal{R}(t)\), the sequences \(\{x_n\}_{n \in \mathbb{Z}}\) and \(\{y_n\}_{n \in \mathbb{Z}}\) given by

\[
x_{2k} = TQ^{k-1}z_k, \quad x_{2k-1} = Q^{k-1}(z_k + z_{k-1}),
\]

\[
y_{2k} = Q^{k-1}(z_{k+1} - z_{k-1}), \quad y_{2k-1} = Q^{k-2}T(z_k - z_{k-1}), \quad k = 0, \pm 1, \ldots,
\]

belong to \(\mathcal{R}(T, Q)\). Further the sequences \(\{\hat{x}_n\}_{n \in \mathbb{Z}}\) and \(\{\hat{y}_n\}_{n \in \mathbb{Z}}\) given by

\[
\hat{x}_{2k} = (-1)^kTQ^{k-1}z_k, \quad \hat{x}_{2k-1} = (-1)^kQ^{k-1}(z_k - z_{k-1}),
\]

\[
\hat{y}_{2k} = (-1)^{k+1}Q^{k-1}(z_{k+1} - z_{k-1}), \quad \hat{y}_{2k-1} = (-1)^kTQ^{k-2}(z_k + z_{k-1}),
\]

\(k = 0, \pm 1, \ldots\), belong to \(\mathcal{R}(\hat{T}, \hat{Q})\).
Proof. The form of the even-numbered elements follows directly from the formula (1) and Proposition 3. Once these are established we get the odd-numbered elements from the recursion relation for a sequence \( \{a_n\}_{n \in \mathbb{Z}} \in \mathcal{R}(T, Q) \)

\[
Ta_{2k-1} = Qa_{2k-2} + a_{2k}, \quad k = 0, \pm 1, \ldots.
\]

We also need the following identity for any \( \{z_n\}_{n \in \mathbb{Z}} \in \mathcal{R}(t) \)

\[
z_{n+1} + z_n - z_{n-1} - z_{n-2} = (2 + t)(z_n - z_{n-1}) = \frac{T^2}{Q}(z_n - z_{n-1}).
\]

\( \square \)

The pairs of sequences \( X, WX \) and \( CX, VX \in \mathcal{R}(t) \) correspond to two sequences in \( \mathcal{R}(T, Q) \). Laxton calls them polar sequences, [L1]. It transpires from Proposition 7 that essentially exchanging odd numbered elements in polar sequences in \( \mathcal{R}(T, Q) \) gives us polar sequences in \( \mathcal{R}(T, Q) \).

Guided by this recombination phenomenon we want to consider two rational parameter values \( t \neq \pm a \) such that \( C_r(t) = \pm C_r(a) \), for a prime \( r \). It turns out that it is fairly rare.

**Lemma 8.** The equation \( C_r(t) = \pm C_r(a) \), for a prime \( r \), has a rational solution \( t = \pm a \) if and only if \( r = 2 \) or 3.

The equation \( C_2(t) = -C_2(a) \) is equivalent to \( t^2 + a^2 = 4 \).

The equation \( C_3(t) = C_3(a) \) is solvable if and only if \( t^2 - 4 = -3f^2 \), for some rational \( f \), with \( a = \frac{1 \pm \sqrt{3}}{2}f \).

Proof. It is a direct check that the solutions listed are indeed solutions. In particular we have \( C_3(t) - C_3(a) = (t - a)(t^2 + ta + a^2 - 3) \), and solving the quadratic equation gives us the answer above.

Let us now assume that there is such a rational solution \( t \neq a \) for a prime \( r \). We substitute \( x = t \) and \( x = a \) into the following identity valid for Chebyshev polynomials for any natural \( n \), to obtain

\[
C_n^2(x) - (x^2 - 4)U_n^2(x) = 4, \quad \frac{a^2 - 4}{t^2 - 4} = \frac{U_n^2(t)}{U_n^2(a)}.
\]

Hence by Lemma 8 we get an element \( X = [x_0 \ x_1] \in \mathcal{R}(t) \) with \( \det X = 1 \) and \( tr X = a \). We have that \( X^r \) and \( D_f^r \) have the same traces, and determinant 1. It follows by Lemma 5 that \( X^{\pm r} = D_f^r \), and further \( (X^{\pm 1}D_1)^r = I \).

It is well known that there are roots of unity of order \( n \) in \( SL(2, \mathbb{Q}) \) only for \( n = 2, 3, 4 \) and \( n = 6 \), which ends the proof. (We will give an independent proof of a more general fact in Proposition 17)

Note that the equation \( C_2(t) = -C_2(a) \) is effectively equivalent to \( C_4(t) = C_4(a) \).

We will refer to the \( r = 2 \) case as circular, and \( r = 3 \) as cubic, jointly as cyclotomic cases. Both cases appear explicitly in Ballot, [B], in the language of two parameters. For a given parameter \( t \), the other parameters \( a \), if present, will be called the associate parameters. Note that the circular case and the cubic case are exclusive; a parameter \( t \) cannot be circular and cubic at the same time. By the above identity for Chebyshev polynomials we get that for any natural \( n \) and rational \( t \) the parameter \( C_n(t) \) is cyclotomic if
and only if \( t \) is cyclotomic, with the preservation of the circular and cubic type.

For associate parameters \( t \) and \( a \) there is a canonical ring isomorphism \( \Theta = \Theta_{t,a} : \mathcal{R}(t) \to \mathcal{R}(a) \), which is defined on the basis of Propositions 3 and 4. So \( \Theta_{t,a} = \Phi_2^{-1} \circ \Psi \circ \Phi_2 \) in the circular case, and \( \Theta_{t,a} = \Phi_3^{-1} \circ \Phi_3 \) in the cubic case.

The next Proposition details the relation between the sequences represented by \( X \) and \( \Theta(X) \) in the circular case.

**Proposition 9.** In the circular case for the associate parameters \( t \) and \( a \), for any \( X \in \mathcal{R}(t) \) representing the sequence \( \{x_n\}_{n \in \mathbb{Z}} \) we have
\[
\Theta(X) = t^{-1}[-ax_0 \; tx_1 - 2x_0] = t^{-1}[-ax_0 \; x_2 - x_0].
\]
In particular
\[
\Theta(C_t) = -at^{-1}C_a, \quad \Theta(D_tC_t) = -aD_a, \quad \Theta(D_t^2) = -D_a^2.
\]
Further, if \( CX \) represents \( \{y_n\}_{n \in \mathbb{Z}} \) and \( \Theta(X) \) represents \( \{\hat{x}_n\}_{n \in \mathbb{Z}} \) then
\[
\hat{x}_{2k} = (-1)^{k-1}at^{-1}x_{2k}, \quad \hat{x}_{2k+1} = (-1)^{k}a^{-1}(x_{2k+2} - x_{2k}), \quad k = 0, \pm 1, \ldots.
\]

The proof is by a straightforward calculation. It follows that the sequences \( X \) and \( \Theta(X) \) share essentially the same odd-numbered elements, while \( CX \) and \( \Theta(X) \) share essentially the same odd-numbered elements. Since \( C^2 = (t^2 - 4)I \) we can say that essentially exchanging the subsequences in \( X \) and \( CX \) we obtain two recursive sequences in \( \mathcal{R}(a) \).

Let us note that the last formulas in Proposition 9 are consistent with the fact that for any recursive sequence \( \{\hat{x}_n\}_{n \in \mathbb{Z}} \) in \( \mathcal{R}(a) \), we have \( \hat{x}_{2k+1} = a^{-1}(\hat{x}_{2k} + \hat{x}_{2k+2}), \quad k = 0, \pm 1, \ldots \) Using this observation we can state the following simpler version of Proposition 9.

**Proposition 10.** In the circular case for the associate parameters \( t \) and \( a \), for any recursive sequence \( \{x_n\}_{n \in \mathbb{Z}} \) in \( \mathcal{R}(t) \), the sequence \( \{\hat{x}_n\}_{n \in \mathbb{Z}} \) given by
\[
\hat{x}_{2k} = (-1)^{k-1}x_{2k}, \quad \hat{x}_{2k+1} = (-1)^{k}a^{-1}(x_{2k+2} - x_{2k}), \quad k = 0, \pm 1, \ldots.
\]
is a recursive sequence for the parameter \( a \).

The recombination phenomenon is more complicated in the cubic case in which \( \mathcal{R}(t) \) is isomorphic to \( \mathbb{Q}(\sqrt{-3}) \). To describe it we employ the two roots of unity of order 3, \( S = S_t = -\frac{1}{\sqrt[3]{2}}[2 \; t + f] \) and \( R = R_t = \frac{1}{\sqrt[3]{2}}[2 \; t - f] \) in \( \mathcal{R}(t) \). We have \( \det S = 1 = \det R, \; \text{tr} \; S = -1 = \text{tr} \; R, \; S^3 = I = R^3 \) and \( SR = I \).

**Proposition 11.** In the cubic case for the associate parameters \( t \) and \( a \), for any \( X \in \mathcal{R}(t) \) representing the recursive sequence \( \{x_n\}_{n \in \mathbb{Z}} \) we have
\[
(t^2 - 1) \Theta(X) = [(a^2 - 1)x_0 \; (a - t)x_0 + (t^2 - 1)x_1] = [(a^2 - 1)x_0 \; ax_0 + x_3].
\]
In particular
\[
\Theta(D_tS_t) = D_a, \quad \Theta(D_t^{-1}R_t) = D_a^{-1}.
\]
Further if \( SX, RX \) and \( \Theta(X) \) represent the recursive sequences \( \{y_n\}_{n \in \mathbb{Z}}, \{z_n\}_{n \in \mathbb{Z}}, \{\hat{x}_n\}_{n \in \mathbb{Z}} \), respectively, then
\[
\hat{x}_{3k} = c_3x_{3k}, \quad \hat{x}_{3k+1} = cy_{3k+1}, \quad \hat{x}_{3k-1} = cz_{3k-1}, \quad c = \frac{a^2 - 1}{t^2 - 1}, \quad k = 0, \pm 1, \ldots.
\]
Proof. The element $D^3_t \in \mathcal{R}(t)$ has exactly three roots of order 3, namely $D_1, D_tS, D_tR$. Since $\Phi(D^3_t) = D_{t3} = D_{a3} = \Phi(D^3_a)$, where $t3 = C_3(t) = C_3(a) = a_3$, we conclude that

$$\{\Theta(D_1), \Theta(D_tS_t), \Theta(D_tR_t)\} = \{D_a, D_aS_a, D_aR_a\}.$$

Since all of these matrices have determinant 1, and $\Theta$ preserves traces, it remains to compare $tr D_tS_t$ and $tr D_a$. We have $tr D_tS_t = \frac{t^2-t-1}{2} = \frac{3t^2-t-1}{2} = a$. Hence $\Theta(D_tS_t) = D_a$. It follows that $\Theta(D_t^{-1}R_t) = \Theta((D_tS_t)^{-1}) = D_a^{-1}$, since $\Theta$ is a ring isomorphism.

The first equality is obtained by direct calculation. Taking into account that $\Theta(D^3_t) = D^3_a$ and $\Theta(D^3_tX) = D^3_a\Theta(X)$ we obtain $\hat{x}_{3k} = cx_{3k}$.

To get $\hat{x}_{3k+1} = cy_{3k+1}$ we observe that

$$\Theta(X)D^3_{a(k+1)} = \Theta(X)\Theta(D_tS_t)\Theta(D^3_t) = \Theta(S_tXD^3_t).$$

In a similar fashion we arrive at $\hat{x}_{3k-1} = cz_{3k-1}$. \qed

A proof of the last equality in the Proposition by direct calculation requires the application of the following surprising identity $\frac{-2x^2}{x-1} = -\frac{x^2-1}{t^2-1}$.

Note that for any recursive sequence $\{x_n\}_{n \in \mathbb{Z}}$ in $\mathcal{R}(t)$, we have

$$(t^2-1)x_{3k+1} = (tx_{3k} + x_{3k+3}), \ (t^2-1)x_{3k-1} = (x_{3k-3} + tx_{3k}), \ k = 0, \pm 1, \ldots.$$ Using these identities we can reformulate the last Proposition somewhat differently.

**Proposition 12.** In the cubic case for the associate parameters $t$ and $a$, for any $X \in \mathcal{R}(t)$ representing the recursive sequence $\{x_n\}_{n \in \mathbb{Z}}$, the sequence $\{\hat{x}_n\}_{n \in \mathbb{Z}}$ given by

$$\hat{x}_{3k} = x_{3k}, \ \hat{x}_{3k+1} = \frac{1}{a^2-1}(ax_{3k} + x_{3k+3}), \ \hat{x}_{3k-1} = \frac{1}{a^2-1}(x_{3k-3} + ax_{3k}),$$

$k = 0, \pm 1, \ldots$ belongs to $\mathcal{R}(a)$. Further if $SX$ and $RX$ represent the recursive sequences $\{y_n\}_{n \in \mathbb{Z}}$ and $\{z_n\}_{n \in \mathbb{Z}}$, respectively, then

$$\hat{x}_{3k+1} = y_{3k+1}, \ \hat{x}_{3k-1} = z_{3k-1}, \ k = 0, \pm 1, \ldots.$$ Hence in the cubic case $X$ and $\Theta(X)$ essentially share the same elements with indices divisible by 3. Further, essentially exchanging appropriate subspaces in the sequences $X, SX$ and $RX$ in $\mathcal{R}(t)$ we obtain three recursive sequences $\Theta(X), \Theta(SX)$ and $\Theta(RX)$ in $\mathcal{R}(a)$.

4. **SEQUENCE GROUPS**

The following constructions depend on the choice of $T, Q \neq 0$, which are fixed. We will not show this dependence explicitly in notation unless it may cause ambiguity.

We are going to identify recursive sequences which differ by a scalar rational factor. To that end we projectivize the ring $\mathcal{R}$, i.e., we consider two elements of $\mathcal{R} \setminus \{0\}$, $[x_0 \ x_1]$ and $[y_0 \ y_1]$, equivalent if there are integers $k \neq 0, l \neq 0$, such that $k[x_0 \ x_1] = l[y_0 \ y_1]$. Clearly it is an equivalence relation and we consider the space of equivalence classes, with the exclusion of elements $X$ with $\det X = 0$. We denote the resulting space by $\mathcal{L}$.

**Lemma 13.** The multiplication of matrices is well defined for the equivalence classes in $\mathcal{L}$, and $\mathcal{L}$ becomes a commutative group.
We will call the group \( \mathcal{L} = \mathcal{L}(T, Q) \) the \textit{sequence group}.

Let us note that every equivalence class in \( \mathcal{L} \) contains a matrix \( X = [x_0 \ x_1] \) with integer, relatively prime \( x_0 \) and \( x_1 \). We call such a matrix a \textit{reduced} representative. Clearly every equivalence class has exactly two reduced representatives, differing by the sign.

We address now the problem of taking square roots in the sequence group \( \mathcal{L} \).

\textbf{Proposition 14.} An element \([y_0 \ y_1]=Y \in \mathcal{L}(T, Q)\) is a square if and only if \( \det Y \) is a square, \( \det Y = \lambda^2, \lambda \in \mathbb{Q} \). The solutions \([x_0 \ x_1]=X \in \mathcal{L}(T, Q)\) of the equation \( bX^2 = Y \) are the row eigenvectors of the matrix

\[
\begin{bmatrix}
-y_1 & Qy_0 - Ty_1 \\
y_0 & y_1
\end{bmatrix}
\]

with the eigenvalues \( \pm \lambda \). Moreover if \( y_0 \neq 0 \) then the square roots are equal to \([y_0 \ y_1 \pm \lambda] \).

\textit{Proof.} We are going to solve the matrix equation \( bX^2 = Y \), for a rational \( b \). We rewrite the equation as \( bX = YX^{-1} \). Changing the free rational parameter \( b \) to another one \( \lambda \) we get

\[
\lambda \begin{bmatrix}
-Qx_{-1}-Qx_0 \\
x_0
\end{bmatrix} = \begin{bmatrix}
y_1 - Ty_0 & -Qy_0 \\
y_0 & y_1
\end{bmatrix}\begin{bmatrix}
x_1 & Qx_0 \\
-x_0 & x_1 - Tx_0
\end{bmatrix}.
\]

Clearly if the problem has a solution then \( \det Y = \lambda^2 \). Further, since this is an equation in the sequence group \( \mathcal{L}(T, Q) \), it is equivalent to the equality of the second rows of the matrices on the left, and on the right. That gives us the eigenvalue problem

\[
[x_0 \ x_1]\begin{bmatrix}
y_1 - Ty_0 & -Qy_0 \\
y_0 & y_1
\end{bmatrix} = \lambda[x_0 \ x_1]
\]

The characteristic equation is \( \lambda^2 = \det Y \), so that the rational square roots of \( \det Y \) are the eigenvalues. \( \square \)

This proposition will facilitate our calculations. It also has an interesting corollary.

\textbf{Corollary 15.} For the group homomorphism \( \Upsilon : \mathcal{L} \rightarrow \mathcal{L}, \ U(X) = X^2 \) the image \( \Upsilon(\mathcal{L}) \) contains exactly those \( Y \in \mathcal{L} \) for which there is a matrix \( A \in SL(2, \mathbb{Q}) \) and integers \( k \neq 0, l \neq 0 \) such that \( kY = lA \).

\textit{Proof.} If \( Y \in \Upsilon(\mathcal{L}) \) then \( Y = X^2 \) for a matrix \( X \in \mathcal{R} \), so that \( \det Y = \lambda^2, \lambda = \det X \). The sought after element \( A \in SL(2, \mathbb{Q}) \) is equal to \( A = \frac{1}{\lambda}Y \).

Conversely we start with the equation \( kY = lA \) for a matrix \( A \in SL(2, \mathbb{Q}) \). It implies that \( \det Y = \left( \frac{1}{\lambda} \right)^2 \). By Proposition 14 it follows that there is an element \( X \in \mathcal{L} \) such that \( bX^2 = Y \) for some \( b \in \mathbb{Q} \). Hence \( Y \in \Upsilon(\mathcal{L}) \). \( \square \)

From now on we restrict our attention to the one parameter sequence group \( \mathcal{L} = \mathcal{L}(t) \). For \( X = [x_0 \ x_1], Z = [x_0 \ x_{-1}] \) in \( \mathcal{R}(t) \) we have \( XZ = - (\det X)I \), which gives us the inverse elements in \( \mathcal{L}(t) \). It follows that if \( X \) in \( \mathcal{L}(t) \) represents the sequence \( \{x_k\}_{k \in \mathbb{Z}} \) then \( X^{-1} \) can be represented by the sequence \( \{x_{-k}\}_{k \in \mathbb{Z}} \).

To study the number-theoretic properties of recursive sequences we introduce another kind of sequence groups. For a fixed \( t \in \mathbb{Q}, t \neq 0, \pm 1, \pm 2 \), let \( \Pi_t \) be the set of odd primes not dividing the numerator, or denominator of \( t \) and
\[ \delta = t^2 - 4 \] (\( t \) is assumed to be a fully reduced simple fraction). For a prime \( p \in \Pi_t \) we consider the subgroup \( \widetilde{\mathcal{L}}_p(t) \subset \mathcal{L}(t) \) of equivalence classes with the determinant of the reduced representative \( \neq 0 \mod p \). There is the canonical homomorphism \( \mathcal{M} : \widetilde{\mathcal{L}}_p(t) \to \widetilde{GL}(2, \mathbb{F}_p) \), where \( GL(2, \mathbb{F}_p) \) is the projectivization of \( GL(2, \mathbb{F}_p) \), i.e., the quotient group \( GL(2, \mathbb{F}_p)/\mathbb{F}_p^* \). We define the sequence group \( \mod p, \mathcal{L}_p(t) \), as a subgroup of \( \widetilde{GL}(2, \mathbb{F}_p) \), \( \mathcal{L}_p(t) = \mathcal{M}\widetilde{\mathcal{L}}_p(t) \).

Let us note that one can equivalently introduce the group \( \mathcal{L}_p(t) \) by repeating the construction of \( \mathcal{R}(t) \) with the replacement of recursive sequences with rational elements by recursive sequences with elements in \( \mathbb{F}_p \).

**Theorem 16.** The sequence group \( \mathcal{L}_p(t) \) is cyclic of order \( p-1 \) if \( \delta = t^2 - 4 \) is a square residue \( \mod p \), and of order \( p+1 \) if \( \delta \) is a square non-residue \( \mod p \).

**Proof.** For the proof we will trace back the construction of \( \mathcal{L}(t) \), repeating it \( \mod p \). So we consider the matrix \( D_t \) as an element in \( SL(2, \mathbb{F}_p) \), and we obtain \( \mathcal{R}_p \), the ring of \( 2 \times 2 \) matrices with entries from \( \mathbb{F}_p \), commuting with \( D_t \). If \( \delta = t^2 - 4 \) is a square residue \( \mod p \) then the matrix \( D_t \) has two different eigenvalues, and it can be diagonalized. The ring \( \mathcal{R}_p \) is then isomorphic to the ring \( \mathbb{F}_p^2 \times \mathbb{F}_p^2 \). The projectivization of \( \mathcal{R}_p \) has \( p+1 \) elements, however two of them have zero determinants. It leads to the cyclic group \( \mathcal{L}_p \) of order \( p - 1 \).

If \( \delta \) is a square non-residue \( \mod p \) then the matrix \( D_t \) has no eigenvalues, and it is well known that in such a case the ring of matrices of the form \( aI + bD_t \), \( a, b \in \mathbb{F}_p \) is isomorphic to the finite field \( \mathbb{F}_{p^2} \). The projectivization \( \mathcal{L}_p \) is then isomorphic to the quotient group \( \mathbb{F}_{p^2}^*/\mathbb{F}_p^* \), which is cyclic of order \( p+1 \). \( \square \)

As an application of the sequence groups \( \mathcal{L}_p \) we prove the following useful fact.

**Proposition 17.** For any rational \( t \) there are no elements of finite order \( k \geq 2 \) in \( \mathcal{L}(t) \), except for \( k = 2, 3, 4, 6 \).

**Proof.** If there is such an element \( X = [x_0 \ x_1] \) then, assuming that \( X \) is a reduced representative, for all odd primes \( p \in \Pi_t \) not dividing \( x_0 \) and \( \det X \neq 0 \mod p \), the homomorphism \( \mathcal{M} : \widetilde{\mathcal{L}}_p(t) \to \mathcal{L}_p \) takes \( X \) into an element of order \( k \). It follows that \( k \) divides the order of \( \mathcal{L}_p \), equal to \( p \pm 1 \). Hence \( p = \pm 1 \mod k \) for all \( p \) with only finitely many exceptions. It is a contradiction except when \( k = 2, 3, 4, 6 \). \( \square \)

We end this section with a discussion of the torsion subgroup of \( \mathcal{L}(t) \). Let us note that all the isomorphisms of the rings discussed in Section 2 translate into isomorphisms of respective sequence groups.

Using Proposition 14 we can easily enumerate elements of order \( 2^k \). First of all we calculate square roots of identity in \( \mathcal{L}(t) \) to conclude that there is exactly one element of order 2, which we denote by \( C = [2 \ t] \). We have \( C^2 = (t^2 - 4)I \).

To get elements of order 4 we need to take square roots of \( C \). Since \( \det C = 4 - t^2 \) it is possible only in the circular case.
Proposition 18. There are elements of order 4 in $L(t)$ only in the circular case, i.e., for $t$ such that $t^2 - 4 = -a^2$, for a rational $a$. The elements of order 4 are then $G = [2 \ t + a]$ and $H = [2 \ t - a]$.

For any rational $t$ there are no elements of order 8 in $L(t)$.

Proof. Elements of order 4 must be square roots of $C$. Assuming $4 - t^2 = a^2$, for a rational $a$, we solve the matrix equation $aX^2 = C$ using Proposition 14. We obtain the only two elements of order 4 in $L(t)$, $G = [2 \ t + a]$ and $H = [2 \ t - a]$. We have $G^2 = 2aC$, $H^2 = -2aC$ and $GH = -2a^2I$.

Since $\det G = 2a^2 = \det H$, these elements do not have square roots. □

In the circular case the torsion subgroup of $L(t)$ is isomorphic to $\mathbb{Z}_4$.

We now address the elements of odd order $r$.

Proposition 19. There are elements of odd order $r$ in $L(t)$ only in the cubic case, i.e., for $r = 3$ and $t$ such that $t^2 - 4 = -3f^2$ for a rational $f$. The elements are $S = [2 \ t + f]$ and $R = [2 \ t - f]$. Furthermore, in this case there are also two elements of order 6, $Y = [2 \ t + 3f]$ and $Z = [2 \ t - 3f]$.

Proof. By Proposition 17 we only need to find all elements of order 3.

Let $X = [x_0 \ x_1] \in L(t)$ be an element of order 3. It means that there is $\lambda \in \mathbb{Q}$ such that $X^3 = \lambda I$. It follows that $(\det X)^3 = \lambda^2$, and hence $\det X = \lambda^2(\det X)^{-2}$ is a rational square. So without loss of generality we can assume that $X \in SL(2, \mathbb{Q})$ and $X^3 = I$. The trace of $X$ must be a solution of the polynomial equation $C_3(u) = 2$, and hence it is equal to $-1$.

We arrive at the equations

$$\det X = x_1^2 - tx_1x_0 + x_0^2 = 1, \quad tr X = 2x_1 - tx_0 = -1.$$ 

Substituting $x_1$ in the first equation using the second equation we obtain

$$(t^2 - 4)x_0^2 = -3.$$ 

If we put $t^2 - 4 = -3f^2$ then $x_0 = \pm \frac{f}{\sqrt{3}}$, $x_1 = \frac{t + f}{\sqrt{3}}$. That gives us the only two elements of order 3, $S = [2 \ t + f]$ and $R = [2 \ t - f]$.

Elements of order 6 must be square roots of the elements of order 3. Since $\det S = 4f^2 = \det R$ we obtain by Proposition 14 two elements of order 6 $Y = [2 \ t + 3f]$ and $Z = [2 \ t - 3f]$, with $\det Y = 12f^2 = \det Z$. □

We have $S^2 = 2fR, R^2 = -2fS, SR = -4f^2I$. Further $Y^2 = 6fS, Z^2 = -6fR, and YZ = -12f^2I$. In the cubic case the torsion subgroup of $L(t)$ is isomorphic to $\mathbb{Z}_6$.

5. The Laxton group and its torsion subgroup

Let $D$ be the cyclic subgroup of $L$ generated by the element $D$. The Laxton group is the quotient group $\mathcal{G} = L/D$. The meaning of this definition is that while elements of $L$ can be thought of as recursive sequences, considered up to a multiplicative factor, in the Laxton group we also identify sequences that differ by a shift.

The conjugacy of Proposition 2 becomes the homomorphism of $\mathcal{G}(t)$ onto $\mathcal{G}(T, Q)$, a 2 to 1 mapping. We denote the homomorphism by $\Xi : \mathcal{G}(t) \to \mathcal{G}(T, Q)$. However it seems that there is no canonical isomorphic embedding.
of $\mathcal{G}(T,Q)$ into $\mathcal{G}(t)$. The explanation for this is that for the recursive sequence $\{x_n\}_{n \in \mathbb{Z}}$ of the matrix $D_{T,Q}$ there is no canonical choice between the two recursive sequences $\{x_{2k}Q^{1-k}\}_{k \in \mathbb{Z}}$ and $\{x_{2k-1}Q^{1-k}\}_{k \in \mathbb{Z}}$, which comprise the complete preimage under the homomorphism $\Xi$.

The kernel of the homomorphism $\Xi$ is comprised of two elements, identity $I$ and $W = [-1, 1]$. Indeed using the notation of Proposition 2 we get

$$TA^{-1}D_{T,Q}A = Q\begin{bmatrix}1 & -1 \\ 1 & t+1\end{bmatrix} = Q\begin{bmatrix}t+1 & 1 \\ -1 & 1\end{bmatrix}\begin{bmatrix}0 & -1 \\ 1 & t\end{bmatrix} = QWD_t.$$

Similarly it follows from Proposition 4 that for any natural $n$ we have the homomorphism of $\mathcal{G}(t_n)$ onto $\mathcal{G}(t)$, which we denote by $\Xi_n : \mathcal{G}(t_n) \to \mathcal{G}(t)$. The kernel of $\Xi_n$ is obtained from the image of the set of powers of $D_t$ by the ring isomorphism $\Phi_n$ of Proposition 4.

We are going to list all elements of finite order in a Laxton group $\mathcal{G}(t)$. Clearly they come from solutions of the matrix equation $X^r = \lambda D^k$ for natural $r$, integer $k$ and rational $\lambda$. We already know all the solutions for $k = 0$.

To get all the elements of order 2 in $\mathcal{G}(t)$ we need to solve the equation $X^2 = \lambda D^{2m-1}$ for integer $m$. For $Y = XD^{-m}$ we get the equation $Y^2 = \lambda D^{-1}$. By Proposition 14 it is solvable because $\det D = 1$ and we obtain two elements, $W = [-1, 1]$ and $V = [1, 1]$. We have $W^2 = (t+2)D^{-1}$ and $V^2 = (t-2)D^{-1}$. Moreover $WC = (t+2)V$.

Further, $\det W = 2 + t$ and $\det V = 2 - t$, so that by Proposition 14 $W$ and $V$ do not have square roots if and only if both $t$ and $-t$ are 2-primitive. In such a case we say that $t$ is twin primitive.

**Proposition 20.** For a primitive and twin primitive $t$, which is not cyclic, the torsion subgroup of the Laxton group $\mathcal{G}(t)$ contains only 4 elements $I, C, W$ and $V$, and it is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

**Proof.** We continue the search for solutions of the matrix equation $X^r = \lambda D^n$ for an odd prime $r$, rational $\lambda$ and integer $n \neq 0$. We have $(\det X)^r = \lambda^2$, and hence $\det X = \frac{\lambda^2}{(\det X)^r}$ is a rational square. It is enough then to solve the equation $X^r = D^n$ for $X \in \mathcal{R}(t)$, $\det X = 1$, and $n \neq 0$. If $n = mr$ is divisible by $r$ then $(XD^{-m})^r = I$, and the solutions are shifts by $D^m$ of the elements of odd order $r$ in the sequence group $\mathcal{L}(t)$. By the assumption that $t$ is not cubic there are no such solutions.

If $r$ does not divide $n$ there are integers $k, l$ such that $ln = kr + 1$. It follows that $X^{kr} = D^{k+1}$, or equivalently $(X^lD^{-k})^r = D$. It follows that $t = C_r(u)$, where $u = tr \ X^lD^{-k}$. Hence contrary to the assumption $t$ is not primitive. We arrive at the conclusion that under the assumptions of this Proposition there are no elements of odd prime order in the Laxton group.

To find all elements of order 4 we need only to take square roots of the elements of order 2, namely $C, W$ and $V$. Taking the square roots in the Laxton group $\mathcal{G}(t)$ is equivalent by Proposition 14 to taking square roots in $\mathcal{L}(t)$. Since $t$ is twin primitive $W$ and $V$ do not have square roots. Further, $\det C = 4 - t^2$ is a rational square only if $t$ is circular, which we have excluded. Hence there are no elements of order 4. $\square$
Definition 1. A cyclotomic $t$ is circular (cubic) primitive if $t$ and its associate values are 2-primitive (3-primitive).

Let us note that for a circular $t$ and any odd prime $r$ the $r$-primitivity is automatically shared by $t$ and its associate value. Indeed if $t^2 + a^2 = 4$ then for $\bar{C} = -a^{-1}C$ we have that $\det \bar{C} = 1$ and $tr \bar{C}D = a$. Hence the associate value $a$ is $r$-primitive if and only if $\bar{C}D$ has no $r$-th root in $L(t)$. However, $\bar{C}^r = \pm C$ so that $\bar{C}$ has always the trivial $r$-th root.

Similarly for a cubic $t$ the $r$-primitivity is shared by $t$ and its associate values for any prime $r$ with the exception of $r = 3$. In this case the associate values of $t$ are the traces of the matrices $SD$ and $RD$ of determinant 1. The matrices $S$ and $R$ have trivial $r$-th roots in $L(t)$ except for $r = 3$. Indeed, for example the 5-th root of $S$ is $R$, and the 5-th root of $R$ is $S$.

Proposition 21. In the circular case if $t$ is primitive and circular primitive then the torsion subgroup of the Laxton group $G(t)$ is isomorphic to $Z_2 \times Z_4$. The elements $I, C, G, H$ form a subgroup isomorphic to $Z_4$. The other four elements are obtained by the translation by $W$.

Proof. The torsion subgroup of $L(t)$ gives us the subgroup $Z_4$ of $G(t)$. The translations by $W$ produce the subgroup isomorphic to $Z_2 \times Z_4$.

By the argument in the proof of Proposition \[20\] there are no elements of odd prime order in $G(t)$. It remains to check if the elements $WG$ and $WH$ of order 4 can have square roots. We have $\det WG = 2(2 + t)a^2 = \det WH$, where $a$ is the associate value. Since for $t^2 + a^2 = 4$ we have $2(2 + t)(2 + a) = (2 + t + a)^2$ we conclude that $2(2 + t)$ is a rational square if and only if $a$ is 2-primitive. We conclude by Proposition \[14\] that under the assumption of circular primitivity there are no elements of order 8. \[\square\]

Let us note that we have established in the proof a simple criterion of circular primitivity, namely a circular $t$ is circular primitive if and only if $2 + t$ and $2(2 + t)$ are not rational squares.

Proposition 22. In the cubic case if $t$ is primitive and cubic primitive then the torsion subgroup of the Laxton group $G(t)$ is isomorphic to $Z_2 \times Z_6$. The elements $I, C, S, R, Y, Z$ form a subgroup isomorphic to $Z_6$. The other six elements are obtained by the translation by $W$.

Proof. The 6 elements comprising the torsion subgroup of $L(t)$ from Proposition \[19\] give us also a subgroup, when treated as elements of $G(t)$.

The argument in the proof of Proposition \[20\] applies, and we can conclude that there are no elements of odd prime order $r$ in $G(t)$, which do not come from finite order elements in $L(t)$.

We still need to look for roots in $G(t)$ of the elements of the torsion subgroup of $L(t)$. Since cubic case excludes the circular case there are no elements of order 4.

We proceed to study the matrix equations $X^r = \lambda R D^n, X^r = \lambda S D^n$ for an odd prime $r$, rational $\lambda$ and a natural $n$. Since for $r \neq 3$ the elements $S$ and $R$ have trivial $r$-th roots in $L(t)$ it is enough to consider the case of $r = 3$. By the argument in the proof of Proposition \[20\] we may further reduce our attention to $\lambda = 1$ and $n = 1$. By the assumption of circular primitivity the equations $X^3 = \lambda S D, X^3 = \lambda R D$ have no solutions in $L(t)$. 


It remains to observe that the elements $Y$ and $Z$ of order 6 do not have square roots in $\mathcal{G}(t)$ because $\det YD^n = \det ZD^n = 12f^2$ and Proposition 14 applies.

The list of finite order elements in the Laxton group $\mathcal{G}(t)$ is completed by the multiplication of two elements of order 3 and three elements of order 2 to get four additional elements of order 6.

We have $(WS)^2 = 2f(2 + t)D^{-1}R$, $(WR)^2 = -2f(2 + t)D^{-1}S$, $(WY)^2 = 6f(2 + t)D^{-1}S$, $(WZ)^2 = -6f(2 + t)D^{-1}R.
\square$

For a given $t = C_m(u)$, for some natural $m$, and a rational primitive $u$, we have the homomorphism $\Xi : \mathcal{G}(t) \to \mathcal{G}(u)$. The kernel of this homomorphism is a cyclic subgroup of order $m$, consisting of the equivalence classes of the matrices $\Phi_m(D_k^u), k = 0, 1, 2, \ldots, m - 1$. The torsion subgroup of $\mathcal{G}(t)$ is the preimage of the torsion subgroup of $\mathcal{G}(u)$ under the homomorphism $\Xi$, hence it is $m$ times larger. Since $W_a^u = D_u$ in $\mathcal{L}(u)$ then $\Phi_m(W_a)$ is an element of order $2m$ in $\mathcal{G}(t)$. It follows that the torsion subgroup of $\mathcal{G}(t)$ in the non-cyclotomic case is isomorphic to $\mathbb{Z}_{2m} \times \mathbb{Z}_2$. For the same reason in the cyclotomic case the torsion subgroup of $\mathcal{G}(t)$ is isomorphic to $\mathbb{Z}_{2m} \times \mathbb{Z}_4$ if $u$ is circular and circular primitive, and to $\mathbb{Z}_{2m} \times \mathbb{Z}_6$ if $u$ is cubic and cubic primitive.

In terms of torsion sequences $\{x_n\}_{n \in \mathbb{Z}}$ of $\mathcal{G}(u)$ the torsion elements in $\mathcal{G}(t)$ are the subsequences $\{x_{km}\}_{k \in \mathbb{Z}}$.

Finally we consider a cubic and cubic primitive $u$, and $t = C_{3m}(u)$ for a natural $m$, and an associate value $a$ of $t$, which by necessity is cubic but not cubic primitive. Due to our definitions $t' := C_3(t) = C_3(a)$. The sequence groups for all of these parameters are naturally isomorphic, and we choose to identify them with $\mathcal{L}(t')$. Under such an identification we have $D_{t'} = D_{3t}$ and $D_a = D_{t'S}$. The Laxton groups $\mathcal{G}(t)$ and $\mathcal{G}(a)$ are factor groups $\mathcal{G}(t')/\{D_t\}$ and $\mathcal{G}(a)/\{D_a\}$, respectively. The torsion subgroup of $\mathcal{G}(t')$ is isomorphic to $\mathbb{Z}_{6m} \times \mathbb{Z}_6$. To get the torsion subgroups of $\mathcal{G}(t)$ and $\mathcal{G}(a)$ we factor $\mathbb{Z}_{6m} \times \mathbb{Z}_6$ by the elements $(3, 0)$ and $(3, 2)$, respectively. Hence we obtain that the torsion subgroup of $\mathcal{G}(a)$ is isomorphic to $\mathbb{Z}_{6m} \times \mathbb{Z}_2$, while it is isomorphic to $\mathbb{Z}_{2m} \times \mathbb{Z}_6$ for $\mathcal{G}(t)$.

In the circular case of a primitive and circular primitive $u$, and $t = C_{2m}(u)$ and the associate value $a$ of $t$, we obtain by a similar argument that the torsion subgroup of $\mathcal{G}(a)$ is isomorphic to $\mathbb{Z}_{4m} \times \mathbb{Z}_2$, while the torsion subgroup of $\mathcal{G}(t)$ is isomorphic to $\mathbb{Z}_{2m} \times \mathbb{Z}_4$.

6. The sets of prime divisors of recursive sequences

Let us recall that for a fixed rational $t \neq 0, \pm 1, \pm 2$, we denote by $\Pi_t$ the set of all odd primes with the exclusion of the divisors of the denominators and numerators of $t$ and $\delta(t) = t^2 - 4$. Not all of these exclusions are necessary for some of the forthcoming theorems. However they are only finite, and they simplify the formulations.

For a sequence $X \in \mathcal{L}(t)$ with the reduced representative $[x_0, x_1] = X$, we define the set $\Gamma_X$ of prime divisors of $X$ by
$$\Gamma_X = \{p \in \Pi_t \mid \exists n \in \mathbb{Z}, \ x_n = 0 \mod p\}.$$
We have that \( p \in \Gamma_X \) if and only if there is an integer \( k \) such that \( XD^k = x_{k+1}I \mod p \). Let us recall that if \( X \) represents the sequence \( \{x_k\}_{k\in\mathbb{Z}} \), then \( X^{-1} \) represents the sequence \( \{x_{-k}\}_{k\in\mathbb{Z}} \). It follows immediately that \( \Gamma_X = \Gamma_{X^{-1}} \). Similarly \( \Gamma_X = \Gamma_{XD^k} \) for any integer \( k \).

We turn to some general facts about the sets of prime divisors of the recursive sequences.

**Proposition 23.** For any \( X, Y \in \mathcal{L}(t) \), \( \Gamma_X \cap \Gamma_Y \subset \Gamma_{XY} \). Further

\[
\Gamma_X \cap \Gamma_{XY} = \Gamma_Y \cap \Gamma_{XY} = \Gamma_X \cap \Gamma_Y.
\]

**Proof.** For \( p \in \Gamma_X \cap \Gamma_Y \) there are integers \( k \) and \( l \) such that \( XD^k = x_{k+1}I \mod p \) and \( YD^l = y_{l+1}I \mod p \). Hence \( XYD^{k+l} = x_{k+1}y_{l+1}I \mod p \), which proves the first part.

To prove the second part we note that \( \Gamma_X \cap \Gamma_{XY} = \Gamma_{X^{-1}} \cap \Gamma_{XY} \subset \Gamma_Y \). The rest follows by the symmetric role played by \( X \) and \( Y \).

It follows directly from Proposition 6 that \( \Gamma_{X^2} \) is the union of the following four subsets.

**Proposition 24.** For any \( X \in \mathcal{L}(t) \),

\[
\Gamma_{X^2} = \Gamma_X \cup \Gamma_{CX} \cup \Gamma_{W_X} \cup \Gamma_{V_X}.
\]

We give another proof which makes no reference to the factorizations of Proposition 6.

**Proof.** Let us note that for any \( p \in \Pi_t \) the element \( X^2 \) in the cyclic group \( \mathcal{L}_p(t) \) has exactly two square roots, \( X \) and \( CX \). Further the element \( D^{-1} \) also has exactly two square roots, \( W \) and \( V \).

\( p \in \Gamma_{X^2} \) if and only if there is an integer \( k \) such that \( X^2 = D^k \) in \( \mathcal{L}_p(t) \).

If \( k = 2l \) then \( (D^l)^2 = X^2 \), and hence in the cyclic group \( \mathcal{L}_p(t) \) the element \( D^l \) is a square root of \( X^2 \). It follows immediately that either \( D^l = X \) or \( D^l = CX \) in \( \mathcal{L}_p(t) \).

If \( k = 2l - 1 \) then \( (XD^{-l})^2 = D^{-1} \) in \( \mathcal{L}_p(t) \) and, since we know two square roots of \( D^{-1} \) in \( \mathcal{L}(t) \), we conclude that \( XD^{-l} = W \) or \( XD^{-l} = V \) in \( \mathcal{L}_p(t) \).

The four sets in the last Proposition are not disjoint. Actually the sum of any three of them will give the whole \( \Gamma_{X^2} \). In general four sets produce a partition into 16 subsets. It turns out that in our case only 6 elements of the partition may be nonempty, Figure 1.

**Proposition 25.** For any \( X \in \mathcal{L}(t) \) the following six sets are disjoint

\[
\Gamma_X \cap \Gamma_{CX}, \Gamma_X \cap \Gamma_{W_X}, \Gamma_X \cap \Gamma_{V_X}, \Gamma_{W_X} \cap \Gamma_{V_X}, \Gamma_{CX} \cap \Gamma_{W_X}, \Gamma_{CX} \cap \Gamma_{V_X},
\]

and their union is all of \( \Gamma_{X^2} \). Further

\[
\Gamma_X \cap \Gamma_{CX} = \Gamma_C \cap \Gamma_{CX}, \Gamma_X \cap \Gamma_{W_X} = \Gamma_W \cap \Gamma_{W_X}, \Gamma_X \cap \Gamma_{V_X} = \Gamma_V \cap \Gamma_{V_X}, \Gamma_{W_X} \cap \Gamma_{V_X} \subset \Gamma_C, \Gamma_{CX} \cap \Gamma_{W_X} \subset \Gamma_V, \Gamma_{CX} \cap \Gamma_{V_X} \subset \Gamma_W.
\]

In the proof we need the following Proposition.

**Proposition 26.** \( \Gamma_W, \Gamma_V \) and \( \Gamma_C \) are disjoint and their union is all of \( \Pi_t \).

It was established in [Wo], we will give an independent proof later on.
Figure 1. Sets of prime divisors of $X, WX, VX, CX$.

Proof. To check that the union is all of $\Gamma_{X^2}$ we observe that by Proposition 23 we have the following equalities

$$\Gamma_X \cap \Gamma_{CX} = \Gamma_C \cap \Gamma_X, \quad \Gamma_X \cap \Gamma_{WX} = \Gamma_W \cap \Gamma_X, \quad \Gamma_X \cap \Gamma_{VX} = \Gamma_V \cap \Gamma_X.$$  

By Proposition 26 we conclude that these sets partition $\Gamma_X$. Replacing $X$ successively with $CX, WX$ and $VX$ we will arrive at their partitions as well.

One needs to recall that $WV = CD^{-1}$, $WC = V, VC = W$ in $L(t)$. For example replacing $X$ with $VX$ we get

$$\Gamma_{VX} \cap \Gamma_{CVX} = \Gamma_{VX} \cap \Gamma_{WX} = \Gamma_C \cap \Gamma_{VX},$$

$$\Gamma_{VX} \cap \Gamma_{WVX} = \Gamma_{VX} \cap \Gamma_{CX} = \Gamma_W \cap \Gamma_{VX},$$

$$\Gamma_{VX} \cap \Gamma_{V^2X} = \Gamma_{VX} \cap \Gamma_X = \Gamma_V \cap \Gamma_{VX}.$$  

□

Proposition 26 generalizes to the following Corollary.

Corollary 27. If $\Gamma_{X^2} = \Gamma_X$ then the sets $\Gamma_{CX}, \Gamma_{WX}$ and $\Gamma_{VX}$ are disjoint and their union is all of $\Gamma_{X^2}$. Moreover

$$\Gamma_{CX} = \Gamma_C \cap \Gamma_X, \quad \Gamma_{WX} = \Gamma_W \cap \Gamma_X, \quad \Gamma_{VX} = \Gamma_V \cap \Gamma_X.$$  

Proof. It follows directly from Proposition 25 when we observe that

$$\Gamma_{X^2} \setminus \Gamma_X = (\Gamma_{WX} \cap \Gamma_{VX}) \cup (\Gamma_{CX} \cap \Gamma_{WX}) \cup (\Gamma_{CX} \cap \Gamma_{VX}).$$  

□

In the cubic case $S^2 = S^{-1} = R$, and $CS = Y, VS = WZ$ in $L(t)$ which gives us yet another Corollary.

Corollary 28. In the cubic case $\Gamma_{WS}, \Gamma_Y$ and $\Gamma_{WY}$ are disjoint and their union is all of $\Gamma_S$.

Ballot, [B], established, under some genericity condition $s$, that the prime density of $\Gamma_S$ is $3/4$ and for $\Gamma_Y \cup \Gamma_{WY}$ it is $1/2$. Assuming these genericity conditions for both $t$ and the twin parameter $-t$ it follows, using the last Corollary and the recombination of Propositions 11 and 12, that the prime densities of the three disjoint sets $\Gamma_{WS}, \Gamma_Y$ and $\Gamma_{WY}$ are each equal to $1/4$. Indeed the sequences $WS$ in $L(t)$ and $VS = WY$ in $L(-t)$ have essentially the same primes divisors, and hence $\Gamma_{WS}$ and $\Gamma_{WY}$ have the same prime densities. The same claim can be made about $VS = WY$ in $L(t)$ and $WS$ in
\( \mathcal{L}(t) \). It follows by simple arithmetic that the three sets have equal prime densities.

The sets of divisors can be described in terms of the groups \( \mathcal{L}_p(t) \), which are cyclic by Theorem [10]. For an element \( X \) of the sequence group \( \mathcal{L}(t) \) let us denote by \( \text{ord}_p(X) \) the order of \( X \) in the group \( \mathcal{L}_p(t) \), if \( \det X \neq 0 \mod p \).

The following Proposition is essentially equivalent to the theorem of Hall, [12]. Let us observe first that if for a reduced sequence \( \det X = 0 \mod p \) then \( p \notin \Gamma_X \). Indeed, since \( \det X = x_1^2 - tx_1x_0 + x_0^2 \), in such a case if \( p \mid x_0 \) then \( p \mid x_1 \), contradicting the assumption that the sequence is reduced. Further, by the same argument, for the shifted sequence \( XD^k \), for any integer \( k \), if \( x_k = 0 \mod p \) then \( x_{k+1} = 0 \mod p \). But then all elements of the sequence vanish \mod p, which is again the contradiction.

**Proposition 29.** For any \( X \in \mathcal{L}(t) \)

\[
\Gamma_X = \{ p \in \Pi_t \mid \text{ord}_p(X) \mid \text{ord}_p(D_t) \}.
\]

**Proof.** As noted before \( p \in \Gamma_X \) if and only if there is an integer \( k \) such that \( X = x_{k+1}D^{-k} \mod p \). The last equality can be considered as the equality in the cyclic group \( \mathcal{L}_p(t) \). Now our Proposition is a consequence of the following property of cyclic groups. For two elements \( x, y \) of a finite cyclic group \( \text{ord}(x) \mid \text{ord}(y) \) if and only if \( x \) is contained in the subgroup generated by \( y \). \( \square \)

As an application of this criterion we prove the following more detailed version of Proposition [29] and Corollary [28]. Let us define the index of appearance \( \xi = \xi(t, p) = \text{ord}_p(W) \). This definition is justified by the fact that \( \xi(t, p) \) is actually the classical index of appearance for the Lucas sequence \( \{L_n\}_{n \in \mathbb{Z}} \) for the two parameters \((T, Q)\), i.e., it is the smallest natural index \( n \) such that \( L_n = 0 \). Indeed, let us denote \( W = \{w_{2n+1}\}_{n \in \mathbb{Z}} \) and \( D = \{u_{n+1}\}_{n \in \mathbb{Z}} \).

If \( \xi = 2k - 1 \) then \( W^\xi = I = W^{-\xi} = D^kW \) which leads by formula (2) to \( 0 = w_\xi = Q^{-1} - L_\xi \). If \( \xi = 2k \) then \( W^\xi = I = W^{-\xi} = D^k \) which leads by formula (2) to \( 0 = u_\xi = T^{-1}Q^{-1} - L_\xi \). The rest of the argument is routine.

**Proposition 30.** For any \( t \neq 0, \pm 1, \pm 2 \)

\[
\Gamma_W = \{ p \in \Pi_t \mid \xi = 1 \mod 2 \}, \Gamma_V = \{ p \in \Pi_t \mid \xi = 2 \mod 4 \},
\]

\[
\Gamma_C = \{ p \in \Pi_t \mid \xi = 0 \mod 4 \}.
\]

For any cubic \( t \)

\[
\Gamma_{WS} = \{ p \in \Pi_t \mid \xi = 3 \mod 6 \}, \Gamma_{VS} = \{ p \in \Pi_t \mid \xi = 6 \mod 12 \},
\]

\[
\Gamma_{CS} = \{ p \in \Pi_t \mid \xi = 0 \mod 12 \}.
\]

The first part appeared as “trichotomy” in [B-E]. It was also proven in [Wo], where the sets are denoted as \( \Pi_0, \Pi_1, \Pi_+ \). The second part was essentially proven in [B3].

**Proof.** The cyclic group \( \mathcal{L}_p(t) \) is isomorphic to the additive group \( \mathbb{Z}_N \) for the appropriate \( N = p \pm 1 \). We do not have any canonical isomorphism of the two, nevertheless we find it convenient to do calculations in \( \mathbb{Z}_N \).

Since \( C \) is of order 2 in \( \mathcal{L}_p \) then \( C = \frac{N}{2} \in \mathbb{Z}_N \). Let \( W = w \in \mathbb{Z}_N \). Since we do calculations in a cyclic group without loss of generality we can assume
that $\xi = \text{ord}_p(W) = \frac{N}{\omega}$. Since $W^2 = D^{-1} = V^2$ in $\mathcal{L}_p$, then $D^{-1} = 2w \in \mathbb{Z}_N$ and $V = w + \frac{N}{2} \in \mathbb{Z}_N$.

We get then that $\text{ord}_p(D^{-1}) = \text{ord}_p(D)$ is equal to $\xi$, if $\xi$ is odd, and to $\xi/2$, if $\xi$ is even. It follows that $p \in \Gamma_W$ if and only if $\xi$ is odd.

Further $p \in \Gamma_C$ if and only if $2 = \text{ord}_p(C)$ divides $\text{ord}_p(D)$, which is $\xi$ or $\xi/2$. It follows that $p \in \Gamma_C$ if and only if $\xi = 0 \mod 4$.

Since $V = \frac{1}{2}w(2 + \xi)$ we get that if $\xi$ is odd then $\text{ord}_p(V) = 2\xi$ and $p \notin \Gamma_V$. If $\xi$ is even and $1 + \frac{\xi}{2}$ is odd then $\text{ord}_p(V) = \xi$ and $p \notin \Gamma_V$. If $\xi$ is even and $1 + \frac{\xi}{2}$ is even then $\text{ord}_p(V) = \xi/2$ and $p \in \Gamma_V$. We can now conclude that $p \in \Gamma_V$ if and only if $\xi = 2 \mod 4$.

In the cubic case $S = \frac{N}{3}$ and $WS = \frac{1}{3}w(3 + \xi)$. If $3 \nmid \xi$ then $\text{ord}_p(WS) = 3\xi$ and hence $p \notin \Gamma_{WS}$. If $3 \nmid \xi$ then $\text{ord}_p(WS) = \xi$ and hence $p \in \Gamma_{WS}$ if and only if $\xi$ is odd.

We have $CS = \frac{N}{2} + \frac{N}{4}$ and hence $\text{ord}_p(CS) = 6$. Since $\text{ord}_p(D)$ is $\xi$ or $\xi/2$ then clearly $p \in \Gamma_{CS}$ if and only if $\xi = 0 \mod 12$.

Finally $VS = w + \frac{N}{2} + \frac{N}{4} = \frac{1}{2}w(6 + 5\xi)$. It follows that if $\xi$ is odd then $\text{ord}_p(VS)$ must be even and hence it cannot divide $\text{ord}_p(D) = \xi$. If $3 \nmid \xi$ then $3 \nmid \text{ord}_p(VS)$ and then also $p \notin \Gamma_{VS}$. If $6 \nmid \xi$ then $VS = w\left(1 + \frac{5\xi}{6}\right)$ and $\text{ord}_p(VS) = \xi$ if $\xi/6$ is even, and $\text{ord}_p(VS) = \xi/2$ if $\xi/6$ is odd. Hence $p \in \Gamma_{VS}$ if and only if $\xi = 6 \mod 12$. 

## 7. Density estimates and Independence Conjecture

**Theorem 31.** If $\det X$ is not a rational square then

$$\Gamma_X \subset \{p \in \Pi | \det X \text{ is a quadratic residue } \mod p\}.$$  

The upper prime density of $\Gamma_X$ does not exceed $1/2$.

**Proof.** If $p \in \Gamma_X$ then there is integer $k$ such that $XD^k = x_{k+1}I \mod p$. Taking determinants of both sides we obtain $\det X = x_{k+1}^2 \mod p$. \hfill $\square$

It follows from this Theorem that for two sequences $X, Y \in \mathcal{L}(t)$, we have the following table, where we indicate the location of the elements of $\Gamma_X$ and $\Gamma_Y$.

In particular by the Frobenius Density Theorem, if $\det X, \det Y$ and $\det XY$ are not rational squares then the upper prime densities of $\Gamma_X \cap \Gamma_Y$ and $\Gamma_X \cup \Gamma_Y$ do not exceed $1/4$ and $3/4$, respectively.

For a sequence $[x_0, x_1] = \tilde{X} \in \mathcal{L}(T, Q)$, with simple integer parameters $T, Q$, we consider the sets of prime divisors of the even numbered elements, and the odd numbered elements. As observed previously for the sequence $[Q\hat{x}_0, \hat{x}_2] = X \in \mathcal{L}(t), \ t = \frac{T^2}{Q} - 2$, the sets $\Gamma_X$ and $\Gamma_{WX}$ are the sets of divisors of even and odd numbered elements of $\tilde{X}$, respectively.

| $\det Y$ | $\det X = \Box$ | $\det X \neq \Box$ |
|----------|----------------|----------------|
| $\Gamma_X \cup \Gamma_Y$ | $\Gamma_Y$ | $\emptyset$ |

| $\det Y \neq \Box$ | $\Gamma_X$ | $\emptyset$ |
| $\det Y \neq \Box$ | $\Gamma_X$ | $\emptyset$ |
We have $\det X = T^2 \det \tilde{X}$ and $\det W = 2 + t = \frac{T^2}{Q}$ (cf. Proposition 6). Under the assumption that $\det \tilde{X}, Q$ and $Q \det \tilde{X}$ are not rational squares we get an approximate “independence” of the sets of divisors, which can be illustrated in the following table.

**Table 2. The sets of divisors for the sequences $X, WX$**

| $Q = \Box$ | $\Gamma_X \cup \Gamma_{WX}$ | $\emptyset$ |
|------------|-------------------------------|-------------|
| $Q \neq \Box$ | $\Gamma_X$ | $\Gamma_{WX}$ |

More precisely, as observed above the upper prime densities of $\Gamma_X$, $\Gamma_{WX}$ and $\Gamma_X \cap \Gamma_{WX}$ do not exceed $1/2$ and $1/4$, respectively.

For a subset of odd primes $A$ we denote by $|A|$ the prime density of the set, if it exists.

**Conjecture on the exact independence of even and odd numbered elements of some recursive sequences**

For any “generic” $t$ and a sequence $X$ of infinite order in the Laxton group $\mathcal{S}(t)$, such that any of the sequences $X, WX, CX$ and $VX$ is not a power in $\mathcal{S}(t)$ then the sets of primes $\Gamma_X$ and $\Gamma_{WX}$ have prime densities and are “independent”

$$|\Gamma_X \cap \Gamma_{WX}| = |\Gamma_X||\Gamma_{WX}|.$$  

The condition of not being a power in $\mathcal{S}(t)$ can be effectively checked. To show that, we invoke the ring of integers in the quadratic field $\mathcal{R}(t)$. The reduced representative of $X$ is automatically such an integer. We consider the factorization of this integer into primes, and we can assume that $X$ is not divisible by a rational prime (if there is such a prime we can remove it, without changing $X$ as an element of $\mathcal{S}(t)$). Producing a similar factorization for the matrix $D$ we can then establish by inspection if some product $D^kX$ is actually a power. In view of the nonuniqueness of the factorizations, while we can fix a factorization of $D$, we still need to consider all the possible factorizations of $X$.. This scheme looks laborious but it can be implemented numerically.

If the conjecture is valid then it applies equally well to $CX$ and hence we get also the independence of $\Gamma_{CX}$ and $\Gamma_{VX}$. Further we also get the independence for the respective sequences in $\mathcal{L}(-t)$. Hence by the recombination of Proposition 7 we would obtain that independence applies also to the pairs of sets $\Gamma_X, \Gamma_{WX}$ and $\Gamma_{CX}, \Gamma_{WX}$. It turns out that the independence of the four pair of sets implies that

$$|\Gamma_X \cap \Gamma_W| = |\Gamma_X \cap \Gamma_V| = |\Gamma_{CX} \cap \Gamma_{WX}| = |\Gamma_{CX} \cap \Gamma_{VX}|,$$

and in view of Table 1 this leads to

$$|\Gamma_X| = |\Gamma_{CX}|, \quad |\Gamma_{WX}| = |\Gamma_{VX}|.$$
To prove it let us denote the prime densities of the six subsets shown in Table 1 as

\[
a = |\Gamma_X \cap \Gamma_W|, b = |\Gamma_X \cap \Gamma_V|, c = |\Gamma_X \cap \Gamma_{CX}|
\]

\[
\alpha = |\Gamma_{CX} \cap \Gamma_{VX}|, \beta = |\Gamma_{CX} \cap \Gamma_{WX}|, \gamma = |\Gamma_{WX} \cap \Gamma_{VX}|
\]

The independence of the four pairs \((\Gamma_X, \Gamma_{WX}), (\Gamma_X, \Gamma_{VX}), (\Gamma_{CX}, \Gamma_{VX})\) and \((\Gamma_{CX}, \Gamma_{WX})\) give us the equalities

\[
\begin{align*}
(1) & \quad (a + b + c)(a + \beta + \gamma) = a, \\
(2) & \quad (a + b + c)(\alpha + b + \gamma) = b, \\
(3) & \quad (\alpha + \beta + c)(\alpha + b + \gamma) = \alpha, \\
(4) & \quad (\alpha + \beta + c)(a + \beta + \gamma) = \beta.
\end{align*}
\]

Dividing (1) by (2) we obtain \(b(a + \beta + \gamma) = a(\alpha + b + \gamma)\), which yields

\[
5) \quad b(\beta + \gamma) = a(\alpha + \gamma).
\]

Dividing (3) by (4) we get \(\beta(\alpha + b + \gamma) = \alpha(a + \beta + \gamma)\), which leads to

\[
6) \quad \beta(b + \gamma) = \alpha(a + \gamma).
\]

Subtracting (6) from (5) gives us \(\gamma(\beta - b) = \gamma(\alpha - a)\), or equivalently

\[
7) \quad a - b = \alpha - \beta.
\]

Dividing (1) by (4) we get \(\beta(a + b + c) = a(\alpha + \beta + c)\) or

\[
8) \quad \beta(b + c) = a(\alpha + c).
\]

Dividing the (2) by (3) delivers \(b(\alpha + \beta + c) = \alpha(a + b + c)\) or

\[
9) \quad b(\beta + c) = \alpha(a + c).
\]

Subtracting (8) from (9) produces \(c(b - \beta) = c(\alpha - a)\) or

\[
10) \quad a + b = \alpha + \beta.
\]

Now (7) and (10) imply

\[
11) \quad a = \alpha, \quad b = \beta.
\]

Substituting (11) into (1) and (2) we conclude that \(a = b\), so that finally \(a = b = \alpha = \beta\).

Numerical experiments support the conjecture, which is shown in the following Table 3.

| (T,Q) | x₀ x₁ | |Γₓ| | |Γₓ| | |Γₓ∩Γwx| | |Γₓ| | |Γwx| |
|---|---|---|---|---|---|---|---|---|---|---|
| (5,3) | [17 11] | 0.356 | 0.356 | 0.126 | 0.127 |
| (4,11) | [3 8] | 0.328 | 0.334 | 0.111 | 0.110 |
| (3,7) | [2 5] | 0.357 | 0.355 | 0.123 | 0.127 |
| (3,-2) | [4 15] | 0.353 | 0.340 | 0.116 | 0.120 |
| (7,11) | [3 2] | 0.340 | 0.340 | 0.115 | 0.116 |
| (2,-5) | [3 14] | 0.343 | 0.339 | 0.111 | 0.116 |
Table 4. The prime density of $|\Gamma_{X^2}|$ calculated for the first 1200 primes

| $(T,Q)$ | $X^2 = [x_0, x_1]$ | $|\Gamma_{Y^2}|$ | $|\Gamma_{WY^2}|$ | $|\Gamma_{Y^2 \cap \Gamma_{WY^2}}|$ | $|\Gamma_{Y^2}|$ | $|\Gamma_{WY^2}|$ |
|---------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|
| (5,3)   | [-1071, -746]   | 0.722699        | 0.316931        | 0.261885        | 0.228909        |
| (4,11)  | [12, -35]       | 0.670559        | 0.289408        | 0.231026        | 0.194065        |
| (3,7)   | [8, -3]         | 0.70392         | 0.297478        | 0.237698        | 0.209591        |
| (3,-2)  | [72, 257]       | 0.692244        | 0.296914        | 0.230192        | 0.205537        |
| (7,11)  | [-51, -95]      | 0.688073        | 0.30442         | 0.237698        | 0.209463        |
| (2,-5)  | [66, 241]       | 0.686405        | 0.297748        | 0.226856        | 0.204376        |

Table 5. The prime density of $|\Gamma_{X^3}|$ calculated for the first 1200 primes

| $(T,Q)$ | $X^3 = [x_0, x_1]$ | $|\Gamma_{Y^3}|$ | $|\Gamma_{WY^3}|$ | $|\Gamma_{Y^3 \cap \Gamma_{WY^3}}|$ | $|\Gamma_{Y^3}|$ | $|\Gamma_{WY^3}|$ |
|---------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|
| (5,3)   | [66572, 46415]  | 0.39            | 0.39116         | 0.13333         | 0.15255         |
| (4,11)  | [-153, -676]    | 0.37            | 0.37782         | 0.12594         | 0.13979         |
| (3,7)   | [-14, -127]     | 0.3975          | 0.39783         | 0.14095         | 0.15814         |
| (3,-2)  | [1244, 4431]    | 0.3958          | 0.37917         | 0.1275          | 0.15009         |
| (7,11)  | [684, 1493]     | 0.385           | 0.38365         | 0.13            | 0.14771         |
| (2,-5)  | [1251, 4364]    | 0.3883          | 0.37615         | 0.12344         | 0.14607         |

We also inspected the sets of divisors for squares (Table 4) and third powers (Table 5) of $X$.

In both cases we see deterioration of independence. There is a striking phenomenon for the sets $\Gamma_{X^2}$ and $\Gamma_{WX^2}$: while the first is quite large, consistent with Proposition 24, the density of the second set is smaller than the values for generic sequences of Table 1. Let us note that it has to be smaller than 1/2 by Theorem 31, yet it does not explain why it is much smaller than typical.

In Table 5 we see that the densities are larger than in Table 3, which is easily explained by the fact that $\Gamma_X \subset \Gamma_{X^3}$. They cannot exceed 1/2 because of the constraint of Theorem 31 which applies equally well to $\Gamma_{X^3}$ and $\Gamma_{WX^3}$. There is also not much difference between the two. That can be explained by the fact that $WX^3 = (WX)^3$ in $\mathcal{J}(t)$, since $W^3 = D^{-1}W$.

The vague requirement in the Conjecture that $t$ is “generic” comes from the example of the circular case where the intersections of $\Gamma_X$ and $\Gamma_{WX}$ are unusually small, and the conjecture fails. Non-primitivity of $t$ most probably also affects the independence. In the cubic case the situation is not clear.

References

[A-K] M. Aoki, M. Kida, On the Laxton group. Res. Number Theory 5 (2019), No. 13.
[B] C. Ballot, Lucas sequences with cyclotomic root field. Dissertationes Math. 490 (2013).
[B-E] C. Ballot, M. Elia, Rank and Period of Primes in the Fibonacci sequence. A Tri- chotomy. Fibonacci Quart. 45 (2007), 56 - 63.
[E-P-Sh-W] G. Everest, A. van der Poorten, I. Shparlinski, T. Ward, Recurrence Sequences. Mathematical Surveys and Monographs 104 (2003).
[H1] M. Hall, *An Isomorphism between linear recurring sequences and algebraic rings.* Trans. Amer. Math. Soc. **44** (1938), 196 - 218.

[H2] M. Hall, *Divisors of second-order sequences.* Bull. Amer. Math. Soc. **43**, (1937), 78 - 80.

[L1] R. R. Laxton, *On Groups of Linear Recurrences I.* Duke Math. J. **26** (1969), 721-736.

[L2] R. R. Laxton, *On groups of linear recurrences, II.* Elements of finite order. Pacific J. Math. **32**, (1970), 173 - 179.

[L] J. van Leeuwen, *Reconsidering a Problem of M. Ward.* A collection of manuscripts related to the Fibonacci sequence, The Fibonacci Association, (1980), 45 - 46.

[M] P. Moree, *Artin’s primitive root conjecture - a survey.* J. Number Theory 12 (2012), 1305-1416.

[M-S] P. Moree, P. Stevenhagen, *Prime divisors of the Lagarias sequence.* Journal de Théorie des Nombres de Bordeaux **13** (2001), 241 - 251.

[P] G. Polya, *Arithmetische Eigenschaften der Reihenentwicklungen rationaler Funktionen.* J. Reine Angew. Math. **151** (1920), 1–31.

[S-L] P. Stevenhagen, H.W. Lenstra,Jr., *Chebotarev and his density theorem.* Math. Intelligencer **18** (1996), 26 - 37.

[St] P.J. Stephens, *Prime divisors of second order linear recurrences. II.* Journal of Number Theory **8** (1976), 333 - 345.

[S1] N. Suwa, *Geometric aspects of Lucas sequences, I.* Tokyo J. Math. **43** (2020), 75 - 136.

[S2] N. Suwa, *Geometric aspects of Lucas sequences, II.* Tokyo J. Math. **43** (2020), 383 - 454.

[Wa] M. Ward, *Prime divisors of second order recurring sequences.* Duke Math. J. **21** (1954), 607 - 614.

[Wi] H. C. Williams, *Edouard Lucas and Primality Testing.* Canad. Math. Soc. Ser. Monogr. Adv. Texts, Wiley, (1998).

[Wo] M. P. Wojtkowski, *Partitions of primes by Chebyshev polynomials.* arXiv:1806.09446 [math.NT]

[Y] M. Yamagishi, *A note on Chebyshev polynomials, cyclotomic polynomials and twin primes.* J. Number Theory **133** (2013), 2455 - 2463.

University of Opole, Opole, Poland

Email address: zlipinski@uni.opole.pl

The University of Arizona, Tucson, Arizona 85721, USA

Email address: maciejw@math.arizona.edu