PARTITIONS OF PRIMES DEFINED BY CHEBYSHEV AND LUCAS POLYNOMIALS

MACIEJ P. WOJTKOWSKI

Abstract. Partitions of the set of primes are introduced based on the Lucas numbers. The role of primitive partitions is revealed, which touches on the work of Lagarias, Ballot, Moree and Stevenhagen, on prime densities of the divisors of Lucas numbers. Two conjectures are formulated augmenting their results. Crude, but explicit description of the Ballot’s trichotomy is established. The exposition puts Chebyshev polynomials on the center stage.

1. Introduction

For every $2 \times 2$ matrix $A$ with determinant 1 (and complex elements if needed) we have $A^2 = TA - I$, where $T$ is the trace of $A$, and $I$ is the identity matrix. It follows that for any integer $n$ the power $A^n = U_n(T)A - U_{n-1}(T)I$, for some polynomials $U_k(T), k \in \mathbb{Z},$ of degree $|k| - 1,$ with integer coefficients, which are called the Chebyshev polynomials of the second kind. The traces of the powers $A^n$ are also polynomials in $T$ with integer coefficients, $C_n(T) = U_{n+1}(T) - U_{n-1}(T),$ which are called the Chebyshev polynomials of the first kind. Here is the list of the first sixteen
of them.

\[ C_0 = 2, \quad U_{16} = T^{15} - 14T^{13} + 78T^{11} - 220T^9 + 330T^7 - 252T^5 + 84T^3 - 8T \]

\[ C_1 = T, \quad U_{15} = T^{14} - 13T^{12} + 66T^{10} - 165T^8 + 210T^6 - 126T^4 + 28T^2 - 1 \]

\[ C_2 = T^2 - 2, \quad U_{14} = T^{13} - 12T^{11} + 55T^9 - 120T^7 + 126T^5 - 56T^3 + 7T \]

\[ C_3 = T^3 - 3T, \quad U_{13} = T^{12} - 11T^{10} + 45T^8 - 84T^6 + 70T^4 - 21T^2 + 1 \]

\[ C_4 = T^4 - 4T^2 + 2, \quad U_{12} = T^{11} - 10T^9 + 36T^7 - 56T^5 + 35T^3 - 6T \]

\[ C_5 = T^5 - 5T^3 + 5T, \quad U_{11} = T^{10} - 9T^8 + 28T^6 - 35T^4 + 15T^2 - 1 \]

\[ C_6 = T^6 - 6T^4 + 9T^2 - 2, \quad U_{10} = T^9 - 8T^7 + 21T^5 - 20T^3 + 5T \]

\[ C_7 = T^7 - 7T^5 + 14T^3 - 7T, \quad U_9 = T^8 - 7T^6 + 15T^4 - 10T^2 + 1 \]

\[ C_8 = T^8 - 8T^6 + 20T^4 - 16T^2 + 2, \quad U_8 = T^7 - 6T^5 + 10T^3 - 4T \]

\[ C_9 = T^9 - 9T^7 + 27T^5 - 30T^3 + 9T, \quad U_7 = T^6 - 5T^4 + 6T^2 - 1 \]

\[ C_{10} = T^{10} - 10T^8 + 35T^6 - 50T^4 + 25T^2 - 2, \quad U_6 = T^5 - 4T^3 + 3T \]

\[ C_{11} = T^{11} - 11T^9 + 44T^7 - 77T^5 + 55T^3 - 11T, \quad U_5 = T^4 - 3T^2 + 1 \]

\[ C_{12} = T^{12} - 12T^{10} + 54T^8 - 112T^6 + 105T^4 - 36T^2 + 2, \quad U_4 = T^3 - 2T \]

\[ C_{13} = T^{13} - 13T^{11} + 65T^9 - 156T^7 + 182T^5 - 91T^3 + 13T, \quad U_3 = T^2 - 1 \]

\[ C_{14} = T^{14} - 14T^{12} + 77T^{10} - 210T^8 + 294T^6 - 196T^4 + 49T^2 - 2, \quad U_2 = T \]

\[ C_{15} = T^{15} - 15T^{13} + 90T^{11} - 275T^9 + 450T^7 - 378T^5 + 140T^3 - 15T, \quad U_1 = 1 \]

The polynomials \( C_n \) and \( U_n \) satisfy the same recursive relations, which can be put concisely into the following matrix identities.

\[
\begin{bmatrix}
-C_{n-1} & \phantom{-}U_n \\
\phantom{C_{n-1}} & -U_{n+1}
\end{bmatrix}
= 
\begin{bmatrix}
0 & 1 \\
-1 & T
\end{bmatrix}^n
\begin{bmatrix}
0 & 1 \\
-1 & T
\end{bmatrix}
\begin{bmatrix}
2 & 0 \\
\phantom{2} & \phantom{0}
\end{bmatrix}.
\]

These simple algebraic facts seem to be a part of the mathematical folklore, which were nevertheless re-discovered repeatedely, \[D\], \[A\]. One possible reason for this relative obscurity is that in most applications the Chebyshev polynomials are considered as functions of \( t = \frac{x}{2} \), namely they are defined as \( \frac{C_n(2t)}{2} \) and \( U_n(2t) \). As a result the polynomials from the list look quite different from the classical Chebyshev polynomials, \[Wk\].

We consider two more sequences of polynomials

\[ V_{2k+1} = U_{k+1} - U_k, \quad W_{2k+1} = U_{k+1} + U_k, \quad k \in \mathbb{Z}. \]

These polynomials are sometimes called the \textit{Chebyshev polynomials of the third and fourth kind}, respectively, \[Y\].

They satisfy the same recursive relations as Chebyshev polynomials.

\[
\begin{bmatrix}
-V_{2k} & \phantom{-}W_{2k-1} \\
\phantom{V_{2k}} & -W_{2k+1}
\end{bmatrix}
= 
\begin{bmatrix}
0 & 1 \\
-1 & T
\end{bmatrix}^k
\begin{bmatrix}
1 & 0 \\
1 & \phantom{1}
\end{bmatrix}.
\]
The number-theoretic properties of the values of Chebyshev polynomials for integer $T$ were studied by many authors, in particular Schur, [S], and Rankin, [R]. The subject goes back to Lucas, [L], whose approach was also more general. We admit that our bibliography is very limited, due to the volume of the literature. Further sources can be found in the papers that we cite. We adhere to the point of view of Schur and Rankin.

We consider the Chebyshev polynomials for $n \geq 1$, and only for natural values of the variable $T$. Let us denote by $\Pi$ the set of odd primes. Fixing $T \geq 3$ we introduce the subsets of odd primes $\Pi_s = \Pi_s(T) \subset \Pi, s = 0, 1, 2, \ldots$. An odd prime $p \in \Pi_0(T)$ if there is a natural $k$ such that $p$ divides $U_{2k+1}(T)$. An odd prime $p \in \Pi_s(T), s \geq 1$, if there is an odd $d$ such that $p$ divides $C_n(T)$ for $n = 2s-1d$.

Further we introduce the subsets $\Pi_\pm = \Pi_\pm(T) \subset \Pi_0$. An odd prime $p$ belongs to $\Pi_-(T)(\Pi_+(T))$ if there a natural $k$ such that $p$ divides $V_{2k+1}(T)(W_{2k+1}(T))$. Since $V_{2k+1}W_{2k+1} = U_{2k+1}$ we have clearly $\Pi_0 = \Pi_- \cup \Pi_+$.

**Theorem 1.** For every $T \geq 3$ the sets $\Pi_s(T), s = -, +, 1, 2, \ldots$, are disjoint, and the set of odd primes $\Pi$ is partitioned by them,

$$\Pi = \Pi_- \cup \Pi_+ \cup \bigcup_{s=1}^{\infty} \Pi_s.$$ 

Hence we get for every $T \geq 3$ a partition of odd primes which we call the $T$-partition. In general these partitions are different for different $T$ with the following exceptions.

**Theorem 2.** If $\tilde{T} = C_d(T)$, for an odd $d$, then the $\tilde{T}$-partition is equal to the $T$-partition.

For every $T \geq 3$ and $T_2 = T^2 - 2 = C_2(T)$ we have $\Pi_k(T_2) = \Pi_{k+1}(T), k = 1, 2, \ldots$, and

$$(3) \quad \Pi_+(T_2) = \Pi_0(T) = \Pi_-(T) \cup \Pi_+(T), \quad \Pi_-(T_2) = \Pi_1(T).$$

Theorems 1 and 2 are not necessarily new in the strict sense, however we failed to find such formulations elsewhere.

We say that $T \geq 3$ is a primitive trace if there is no natural $\tilde{T} \geq 3$ such that $C_2(T) = \tilde{T}^2 - 2 = \tilde{T}$. By Theorem 2 it is enough to study the $T$-partitions only for primitive traces $T$. The first four natural $T \geq 3$ which are not primitive traces are $7, 14, 23, 34$. Clearly the primitive traces have density $1$ in the set of all natural numbers.

For a subset $S$ of primes the prime density of $S$ is defined as

$$\delta(S) = \lim_{n \to +\infty} \frac{\#\{p \in S|p \leq n\}}{\#\{p \in \Pi|p \leq n\}}.$$ 

We define the lower and upper densities accordingly. Stevenhagen and Lenstra, [S-L], gave an elementary introduction to the methods of calculating prime densities, with an outline of the history of the subject.

The calculation of prime densities of the sets in a $T$-partition is a difficult task. Lagarias [L], and Moree and Stevenhagen, [M-S], obtained prime densities of some sets in the $T$-partitions. The machinery used in [M-S] is probably sufficient to obtain the prime densities of all the sets in a $T$-partition for primitive traces $T \geq 3$, however we were unable to achieve this. The results in [M-S] are consistent with the following conjecture.
Conjecture 1 For any primitive trace \( T \geq 3 \) the prime densities of the \( T \)-partition \( 1 = \delta(\Pi_-) + \delta(\Pi_+) + \delta(\Pi_1) + \delta(\Pi_2) + \ldots \) are equal to 
\[
\frac{2}{2^7 + \frac{3}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \ldots}, \quad \text{when } T = 2(y^2 - 1) \text{ for a natural } y. \quad \text{In every other case they are equal to } \frac{1}{3} + \frac{1}{3} + \frac{1}{3} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \ldots.
\]

In [M-S], page 404, several prime densities are given. In particular the special case \( d = 2 \) corresponds to the 6-partition, which is exceptional, \( 6 = 2(2^2 - 1) \). The authors obtained in this case that \( \delta(\Pi_-) = \frac{7}{24} \). For other exceptional values of \( T \) the density listed there is \( \delta(\Pi_- \cup \Pi_+) = \frac{7}{24} \). In all non-exceptional cases the densities they obtained are either \( \delta(\Pi_- \cup \Pi_+) = \frac{2}{3} \), or \( \delta(\Pi_-) = \frac{1}{7} \). All of these densities agree with Conjecture 1.

Lagarias, [L], page 450, states that (in our language) \( \delta(\Pi_-) = \delta(\Pi_+) = \frac{1}{3} \), for primitive \( T \neq x^2 + 2 \), for some natural \( x \). Apparently some conditions where left out, since for the exceptional cases [M-S] gives \( \delta(\Pi_- \cup \Pi_+) = \frac{7}{24} \).

Ballot and Elia, [B-E], page 62, state that (in our language) the same trichotomy \( \delta(\Pi_-) = \delta(\Pi_+) = \frac{1}{3} \) holds for a primitive trace \( T = x^2 + 2 \), for some natural \( x \neq 2 \). The readers are referred to previous work for details. This also agrees with Conjecture 1, because the exceptional value \( T = x^2 + 2 = 2y^2 - 2 \) is primitive only for \( x = 2 \), which is explicitly excluded from the claim.

Let us outline the contents of the paper. In Section 1 we prove Theorems 1 and 2. The highlight of the proofs is that they follow directly from appropriate identities satisfied by Chebyshev polynomials. On the way we establish all the necessary identities.

In Section 2 we introduce the Fibonacci polynomials, which arise from powers of \( 2 \times 2 \) matrices with determinant \(-1\). We show in Theorem 8 that the partitions of primes they define coincide with the \( T \)-partitions.

In Section 3 we proceed to the general case of a \( 2 \times 2 \) matrix \( A \), with the trace \( T \) and the determinant \( Q \). We obtain the Lucas polynomials \( K_n, L_n \),
\[
A^n = L_n(T, Q)A - QL_{n-1}(T, Q)I,
\]
\[
K_n(T, Q) = \text{trace}(A^n) = L_{n+1}(T, Q) - QL_{n-1}(T, Q), \quad n \geq 1.
\]

The basic properties of Lucas polynomials are encoded in the matrix identities corresponding to (1).
\[
\begin{bmatrix}
-QL_{n-1} & L_n \\
-QL_n & L_{n+1}
\end{bmatrix}
= \begin{bmatrix} 0 & 1 \\ -Q & T \end{bmatrix}^n,
\]
\[
\begin{bmatrix}
K_n & L_n \\
K_{n+1} & L_{n+1}
\end{bmatrix}
= \begin{bmatrix} 0 & 1 \\ -Q & T \end{bmatrix}^n \begin{bmatrix} 2 & 0 \\ T & 1 \end{bmatrix}.
\]

The Lucas polynomials are rigidly connected, by homogenization, to Chebyshev polynomials. For example
\[
C_0(T) = T^9 - 9T^7 + 27T^5 - 30T^3 + 9T,
\]
\[
K_0(T, Q) = T^9 - 9T^7Q + 27T^5Q^2 - 30T^3Q^3 + 9TQ^4.
\]

In general every identity for Chebyshev polynomials can be translated into the respective identity for Lucas polynomials, with the provision that we may get in the process polynomials in \( T \) and \( \sqrt{Q} \). For example the Chebyshev polynomials of the third and fourth kind, \( V_n \) and \( W_n \), turn into polynomial functions of \( T \) and \( \sqrt{Q} \).
A pair of integer numbers \((T, Q)\) is called admissible if they are different from zero and relatively prime, and not equal to \((\pm 1, 1)\) or \((\pm 2, 1)\). For an admissible pair \((T, Q)\) we proceed with the definition of a \((T, Q)\)-partition using Lucas polynomials, in complete parallel to the \(T\)-partitions.

The proofs of the analogs of Theorems 1 and 2 for \((T, Q)\)-partitions are obtained by repeating every step of the proofs in the Chebyshev Section 2, with the provision that every polynomial identity employed needs translation into Lucas polynomials. For the sake of clarity we actually split the proofs between Sections 2, 3 and 4, most facts are proven for the special case of Chebyshev and Fibonacci polynomials, while some are left to the general case of Lucas polynomials, and other are done twice.

Clearly Sections 2 and 3 cover just special cases of Section 4, \(Q = 1\) and \(Q = -1\). However the notation is significantly simpler with the Chebyshev or Fibonacci polynomials. And we want to demonstrate that the general case of Lucas polynomials does not require any additional ideas.

In Section 5 we briefly introduce Lehmer polynomials \(J_n(Z, Q), H_n(Z, Q), n \geq 1\), which in our language correspond to positive powers of a \(2 \times 2\) matrix \(A\) with the determinant \(Q\) and the trace \(T = \sqrt{Z}\). We have

\[
A^n = \sqrt{Z^{\epsilon_n}}H_n(Z, Q)A - Q\sqrt{Z^{\epsilon_{n-1}}}H_{n-1}(Z, Q)I,
\]
\[
tr \ A^n = \sqrt{Z^{\epsilon_n}}J_n(Z, Q) = \sqrt{Z^{\epsilon_n}}(H_{n+1}(Z, Q) - QH_{n-1}(Z, Q))I,
\]

where \(\epsilon_n\) is 0 or 1, depending on the parity of \(n\), \(\epsilon_n = n - 1 \mod 2\).

Lehmer polynomials are again, by homogenization, rigidly connected with Chebyshev polynomials. For example

\[
U_{10} = T^9 - 8T^7 + 21T^5 - 20T^3 + 5T,
\]
\[
H_{10}(Z, Q) = Z^4 - 8Z^3Q + 21Z^2Q^2 - 20ZQ^3 + 5Q^4.
\]

We establish that Lehmer polynomials do not define any new partitions, all such partitions are already covered in Section 4. This may come as a surprise to experts since the Lehmer numbers are a nontrivial generalization of Lucas numbers. The explanation is contained in the following identities

\[
J_{2k+1}(Z, Q) = V_{2k+1}(Z - 2Q, Q), \quad H_{2k+1}(Z, Q) = W_{2k+1}(Z - 2Q, Q).
\]

for \(k \geq 1\), which are direct translations of the respective identities from Section 3 connecting Chebyshev and Fibonacci polynomials. Hence the role of Lehmer polynomials can be understood as augmenting the Chebyshev polynomials of the first and second kind, \(C_n, U_n\), by the polynomials of the third and fourth kind, \(V_{2k+1}, W_{2k+1}\). This connection appears in the work of Laxton, [Lax], although it is not discussed explicitly.

Finally in Section 6 we discuss the prime densities of the sets in the general \((T, Q)\)-partitions of Section 4. We formulate and prove several estimates of the densities of some of the sets, under some restrictions on \((T, Q)\).

In particular we establish by elementary considerations the following “poorman’s trichotomy”. We use the Legendre symbol \((n|p)\), for integer \(n\) and \(p\) an odd prime. Let \(\Pi_{even} = \Pi_{even}(T, Q) = \bigcup_{k=2}^{\infty} \Pi_k(T, Q)\).
Theorem 3. If \( Q \) and \(-D = -(T^2 - 4Q)\) are not rational squares then
\[
\{ p \in \Pi \mid (Q|p) = 1, (-D|p) = -1 \} \subseteq \Pi_0 \subseteq \{ p \in \Pi \mid (Q|p) = 1 \},
\]
\[
\{ p \in \Pi \mid (Q|p) = -1, (-D|p) = -1 \} \subseteq \Pi_1 \subseteq \{ p \in \Pi \mid (Q|p)(-D|p) = 1 \},
\]
\[
\{ p \in \Pi \mid (Q|p) = -1, (-D|p) = 1 \} \subseteq \Pi_{\text{even}} \subseteq \{ p \in \Pi \mid (-D|p) = 1 \}.
\]

It follows by the Frobenius Theorem, [S-L], that if additionally \(-Q\) or \( D\) is not a rational square then the prime densities \( \delta(\Pi_0)\), \( \delta(\Pi_1)\) and \( \delta(\Pi_{\text{even}})\), are all between \( \frac{1}{4} \) and \( \frac{1}{2} \).

Following Ballot, [B2], we say that a pair \((T, Q)\) is special if
\[
Q = \pm z^2, \text{ or } Q = \pm 2z^2, \text{ or } D = \pm z^2, \text{ or } D = \pm 2z^2, \quad z \in \mathbb{N}.
\]

Ballot, [B1], and Moree, [M], effectively calculated the prime densities of all the subsets in a \((T, Q)\)-partition for pairs \((T, Q)\) which are not special. We conjecture that his result can be extended to all subsets in a \((T, Q)\)-partition.

Conjecture 2 For admissible pairs \((T, Q)\) which are not special the prime densities of the \((T, Q)\)-partition are equal to
\[
1 = \delta(\Pi_0) + \delta(\Pi_1) + \delta(\Pi_2) + \delta(\Pi_3) + \cdots = \frac{1}{3} + \frac{1}{3} + \frac{1}{6} + \frac{1}{24} + \frac{1}{48} + \cdots.
\]

Ballot, [B1], and Moree, [M], effectively calculated the prime densities of all the subsets in a \((T, Q)\)-partition in the reducible case, i.e., \( T = a+b, Q = ab \), for integer \( a, b \). Their formulas can be simplified by considering only primitive pairs \((T, Q)\), for which no gluing, as in (3) of Theorem 2, is present.

Theorem 4. For any primitive reducible pair \((T, Q)\) the prime densities of the \((T, Q)\)-partition are equal to
\[
(5) \quad 1 = \delta(\Pi_0) + \delta(\Pi_1) + \delta(\Pi_2) + \delta(\Pi_3) + \cdots = \frac{7}{24} + \frac{7}{24} + \frac{1}{3} + \frac{1}{24} + \frac{1}{48} + \cdots,
\]
when \( Q = 2y^2 \) for a natural \( y \). In every other case they are equal to
\[
(6) \quad 1 = \delta(\Pi_0) + \delta(\Pi_1) + \delta(\Pi_2) + \delta(\Pi_3) + \cdots = \frac{1}{3} + \frac{1}{3} + \frac{1}{6} + \frac{1}{12} + \frac{1}{24} + \frac{1}{48} + \cdots.
\]

Let us note that in the reducible case \( Q \) cannot be a rational square for a primitive pair \((T, Q)\), and then \( \Pi_0 \) cannot be split further into \( \Pi_- \) and \( \Pi_+ \).

It follows from the estimates in Section 6 that there must be other splittings of the prime densities, different from the two appearing above, for special primitive pairs \((T, Q)\). In particular for the \((2,5)\)-partition we get \( \delta(\Pi_0 \cup \Pi_1) \leq \frac{1}{2} \), which is less than \( \frac{3}{8} \) from the splitting (6), and less than \( \frac{7}{12} \) from the splitting (5).

We are aware that most of the material covered in this paper can be found in the literature, at least implicitly. Nevertheless we chose to give an elementary direct presentation.

2. Chebyshev polynomials and the proof of Theorems 1 and 2

The Chebyshev polynomials are given by the following expansions, which can be proven by induction.
\[
(7) \quad C_n = \sum_{s=0}^{[n/2]} (-1)^s \frac{n-s}{n-s} \left( \begin{array}{c} n-s \\ s \end{array} \right) T^{n-2s}, \quad U_{n+1} = \sum_{s=0}^{[n/2]} (-1)^s \left( \begin{array}{c} n-s \\ s \end{array} \right) T^{n-2s}.
\]
The Chebyshev polynomial $C_n(T)$ contains only even powers of $T$ for even $n$, and only odd powers for odd $n$. Hence $T$ is a factor of the polynomial $C_n(T)$ for odd $n$. Similarly $U_n(T)$ contains only odd powers for even $n$, and only even powers for odd $n$.

The coefficients in these polynomials can be obtained from the Pascal triangle, by taking the “diagonal” $(\binom{n}{s})$, $s = 0, 1, 2, \ldots$. It transpires from the first formula that for a prime $p$ all the coefficients of $C_p(T)$ are divisible by $p$, except for the leading one (equal to 1). This gives us the following Proposition.

**Proposition 5.** For integer $T$, and any prime $p$, $C_p(T) = T^p = T \mod p$.

The paper [St] gives the history of several generalizations of this fact. For any $2 \times 2$ matrix $A$ with the determinant 1 and trace $T$ we have for $\tilde{A} = A - tI, 2t = T$, that $\tilde{A}^2 = (t^2 - 1)I$. This leads via binomial expansion to the formula $A^n = (tI + \tilde{A})^n = \frac{1}{2}C_nI + U_n\tilde{A}$, where

\[ C_n = 2 \sum_{s=0}^{\left\lfloor \frac{n}{2} \right\rfloor} \binom{n}{2s} t^{n-2s}(t^2 - 1)^s, \quad U_n = \sum_{s=0}^{\left\lfloor \frac{n}{2} \right\rfloor} \binom{n}{2s+1} t^{n-2s-1}(t^2 - 1)^s. \]

It follows from (8) that for any odd prime $p$ the coefficients in the expansion of $U_p$ are multiples of $p$ except for the last term, where $s = \frac{n-1}{2}$, equal to $(t^2 - 1)^\frac{n-1}{2}$. This gives us the following Proposition.

**Proposition 6.** For integer $T$, and any odd prime $p$,

\[ U_p(T) = (D \mid p) \mod p, \quad \text{where} \quad D = T^2 - 4. \]

We proceed with the proof of Theorems 1 and 2. The interpretation of $C_n(T)$ as the trace of the $n$-th power of a matrix with trace $T$ yields immediately that

\[ \text{tr } A^{nm} = C_{nm} = C_m(C_n) = C_n(C_m). \]

We have by (1) that

\[ A^{nm} = U_m(C_n)A^n - U_{m-1}(C_n)I = U_m(C_n)U_nA - (U_m(C_n)U_{n-1} + U_{m-1}(C_n))I. \]

It follows that

\[ U_{nm} = U_m(C_n)U_n = U_n(C_m)U_m. \]

Now we can claim for integer $k, l$ that $C_{(2l+1)k} = C_{2l+1}(C_k)$ is divisible by $C_k$, and $U_{(2l+1)k} = U_k(C_{2l+1})U_{2l+1}$ is divisible by $U_{2l+1}$.

Taking determinants of both sides of the second line in (1) we obtain

\[ U_{n+1}C_n - U_nC_{n+1} = 2. \]

It follows that for a natural $T$ the greatest common divisor $gcd(C_n(T), U_n(T))$ is either 1 or 2.

Since $gcd(C_{(2l+1)k}(T), U_{(2l+1)k}(T))$ is either 1 or 2, we get the desired conclusion that $gcd(C_k(T), U_{2l+1}(T))$ is either 1 or 2.

We have proven that $\Pi_0$ is disjoint from the union $\bigcup_{s=1}^{\infty} \Pi_s$.

To continue with the proof we need more Chebyshev identities. We put them into the following Lemma.
Lemma 7. For any integers \( n \) and \( k \)
\[
U_{2n+1} = U_{n+1}^2 - U_n^2 = V_{2n+1}W_{2n+1}.
\]
(11)
\[
C_{2n+1} - 2 = (T - 2)W_{2n+1}^2, \quad C_{2n+1} + 2 = (T + 2)V_{2n+1}^2,
\]
\[
W_{(2n+1)(2k+1)} = W_{2n+1}(C_{2k+1})W_{2k+1} = W_{2k+1}(C_{2n+1})W_{2n+1},
\]
\[
V_{(2n+1)(2k+1)} = V_{2n+1}(C_{2k+1})V_{2k+1} = V_{2k+1}(C_{2n+1})V_{2n+1}.
\]

Proof.
(12)
\[
\begin{bmatrix}
C_{2n} & U_{2n} \\
C_{2n+1} & U_{2n+1}
\end{bmatrix} = \begin{bmatrix}
0 & 1 \\
-1 & T
\end{bmatrix}^n \begin{bmatrix}
0 & 1 \\
-1 & T
\end{bmatrix} \begin{bmatrix}
2 & 0 \\
T & 1
\end{bmatrix} =
\end{bmatrix}
\[
\begin{bmatrix}
-1 & U_n \\
U_{n+1}
\end{bmatrix}
\begin{bmatrix}
C_n & U_n \\
C_{n+1} & U_{n+1}
\end{bmatrix} = \begin{bmatrix}
C_{n+1}U_n - C_nU_{n-1} & C_nU_n \\
C_{n+1}U_{n+1} - C_nU_n & U_{n+1} - U_n
\end{bmatrix}
\]

We get immediately the first line of our Lemma. Further
\[
C_{n+1} - C_n = U_{n+2} - U_n - U_{n+1} + U_{n-1} =
\]
\[
TU_{n+1} - 2U_n - 2U_{n+1} + TU_n = (T - 2)W_{2n+1}.
\]

Further using (12) we obtain
\[
(T - 2)W_{2n+1}^2 = (C_{n+1} - C_n)(U_{n+1} + U_n) =
\]
\[
(C_{n+1}U_{n+1} - C_nU_n) - (C_nU_{n+1} - C_{n+1}U_n) = C_{2n+1} - 2.
\]

Since \( W_n(-T) = (-1)^nV(T) \), substituting \(-T\) for \( T \) in the last equality we obtain \((T + 2)V_{2n+1}^2 = C_{2n+1} + 2\).

We get from these
\[
(T + 2)V_{(2n+1)(2k+1)}^2(T) = C_{(2n+1)(2k+1)} + 2 = C_{2n+1}(C_{2k+1}) + 2 =
\]
\[
(C_{2k+1}(T) + 2)V_{2n+1}^2(C_{2k+1}) = (T - 2)V_{2k+1}^2(T)V_{2n+1}^2(C_{2k+1}).
\]

The equation (13) gives us the last line of (11) up to a sign, which is easily established because all the polynomials are monic, i.e., with the leading coefficient equal to 1.

Again substituting \(-T\) for \( T \) in (13) gives us the third line of (11). \( \square \)

We proceed with the proof that \( \Pi_+(T) \) and \( \Pi_-(T) \) are disjoint.

Taking determinants of both sides of (2) we get that
\[
W_{2n+1}V_{2n-1} - W_{2n-1}V_{2n+1} = 2,
\]
so that for a fixed \( T = 3, 4, \ldots \), \( \gcd(W_{2n+1}(T)V_{2n+1}(T)) \) is equal to 1 or 2.

Using Lemma 7 we can claim that for any natural \( n \) and \( k \) the number \( W_{2n+1}(T) \) divides \( W_{(2n+1)(2k+1)}(T) \), and the number \( V_{2k+1}(T) \) divides \( V_{(2n+1)(2k+1)}(T) \). Hence \( \gcd(W_{2n+1}(T), V_{2k+1}(T)) \) is either 1 or 2.

To finish the proof that the sets \( \Pi_s, s \geq 0 \), are disjoint we will first prove (3) of Theorem 2. Let us note that in these claims it is not necessary to have the partition: (3) is a claim about the equality of well defined subsets.

We need more Chebyshev identities.
\[
\begin{bmatrix}
-U_{2n-1} & U_{2n} \\
-U_{2n} & U_{2n+1}
\end{bmatrix} = \begin{bmatrix}
0 & 1 \\
-1 & T
\end{bmatrix}^{2n} = \begin{bmatrix}
-1 & T \\
-T & T^2 - 1
\end{bmatrix}^n =
\]
\[
U_n(T^2 - 2)\begin{bmatrix}
-1 & T \\
-T & T^2 - 1
\end{bmatrix} - U_{n-1}(T^2 - 2)I.
\]
We get from this the following identities.

\[ U_{2n}(T) = TU_n(C_2(T)), \]

\[ U_{2n-1}(T) = U_n(C_2(T)) + U_{n-1}(C_2(T)) = W_{2n-1}(C_2(T)). \]  

Finally

\[ TV_{2n-1} = TV_n(C_2(T)) - TU_{n-1}(C_2(T)) = U_{2n}(T) - U_{2n-2}(T) = C_{2n-1}(T). \]

Combining (14) with Lemma 7 we get

\[ W_{2n-1}(T)V_{2n-1}(T) = W_{2n-1}(C_2(T)), \]

which leads to \( \Pi_+(T_2) = \Pi_-(T) \cup \Pi_+(T), \) where \( T_2 = C_2(T). \)

(15) implies that \( \Pi_1(T) = \Pi_-(T_2), \) except for the divisors of \( T, \) which are taken care of by the following observation. If an odd prime \( p \) divides \( T, \) then \( C_2(T) = T^2 - 2 = -2 \mod p, \) so that \( V_p(C_2(T)) = V_p(-2) \mod p. \)

Since \( V_p(-2) = W_p(2) = p \) it follows that \( p \in \Pi_-(C_2(T)). \) On the other hand such a prime \( p \) divides \( C_d(T) \) for any odd \( d. \)

It follows from (9) that for \( s \geq 1 \) we have \( \Pi_s(T_2) = \Pi_{s+1}(T). \)

These equalities allow us to conclude that for any \( s \geq 2, \) and any \( T \geq 2, \) the sets \( \Pi_1(T) \) and \( \Pi_s(T) \) are disjoint. Now we have that for any \( s \geq 2 \) the sets \( \Pi_1(T_2) \) and \( \Pi_s(T_2) \) are disjoint as well, and so for \( s \geq 2 \) the sets \( \Pi_s(T) \) are also disjoint. We conclude the proof by induction. We have proved that the sets \( \Pi_s(T), s \geq 1, \) are disjoint.

It remains to prove the first part of Theorem 2. We will achieve it by proving that \( \Pi_s(T_d) \subset \Pi_s(T) \) for \( s = \pm 1, 2, \ldots. \) The equality of these sets is an immediate consequence, since they constitute two partitions of \( \Pi. \) For \( s = 1, 2, \ldots, \) this conclusion is obvious in view of (9): the values of the respective polynomials at \( T_d \) form a subsequence of the values at \( T. \)

For \( s = \pm, \) we use the last part of Lemma 7. Indeed if \( p \in \Pi_-(T_d) \) then there is a natural \( k \) such that \( p \) divides \( V_{2k+1}(T_d), \) but \( V_{d(2k+1)}(T) = V_{2k+1}(T_d)V_d(T) \) and hence \( p \) divides \( V_{d(2k+1)}(T). \) The argument in case of \( s = + \) is identical.

**Summary of the proof of Theorem 1:** \( C_n(T) \) and \( U_n(T) \) have no common divisors (except for 2), because they are part of a \( 2 \times 2 \) matrix with determinant 2. For \( C_n(T) \) and \( U_k(T), k \neq n, \) we consider \( C_{nk}(T) \) and \( U_{nk}(T). \) We have that \( U_{nk}(T) \) is always divisible by \( U_k(T), \) while \( C_{nk}(T) \) is divisible by \( C_n(T), \) provided that \( k \) is odd. The polynomials \( V_{2k+1} \) and \( W_{2k+1} \) behave similarly to the polynomials \( U_n, \) which allows the same proof of no common divisors. The proof that every odd prime belongs to one of the sets \( \Pi_s(T), s = 0, 1, 2, \ldots, \) is postponed until the general case of Lucas polynomials in Section 4.

The assumption that \( U_n \) is considered for odd index \( n \) only is substantial, which is seen clearly from the following factorization, which is a consequence of \( U_{2n} = C_kU_n, \) see (12). For an odd \( d \) and any natural \( k \)

\[ U_{2k-1}d = C_dC_{2d}C_{4d} \ldots C_{2k-1}dU_d = C_dC_{2d} \ldots C_{2k-1}dV_dW_d. \]

### 3. Fibonacci Polynomials

We turn our attention to another classical family of polynomials, the *Fibonacci polynomials*. 
For every $2 \times 2$ matrix $B$ with determinant $-1$ we have $B^2 = SB + I$, where $S$ is the trace of $B$. Again we get that $B^n = F_n(S)B + F_{n-1}(S)I$, where the polynomials $F_k(T)$ are called the Fibonacci polynomials of the second type. Choosing special matrix $B$ we get

$$
\begin{bmatrix}
0 & 1 \\
1 & S
\end{bmatrix}^n = \begin{bmatrix}
F_{n-1} & F_n \\
F_n & F_{n+1}
\end{bmatrix}.
$$

The Fibonacci polynomials of the first kind $G_n(S)$ are the traces of the powers, $G_n(S) = F_{n+1}(S) + F_{n-1}(S)$. One can obtain the Fibonacci polynomial $F_n(S)$ from the Chebyshev polynomial $U_n(T)$ by replacing $T$ with $S$ and changing all the minus signs into pluses in the coefficients. The same applies to the traces $G_n(S)$ and $C_n(T)$. It follows from the following identities.

$$
I^n \begin{bmatrix}
0 & 1 \\
1 & S
\end{bmatrix}^n = I^n \left( F_n(S) \begin{bmatrix}
0 & 1 \\
1 & S
\end{bmatrix} + F_{n-1}(S)I \right) = 
$$

$$
= I^n \begin{bmatrix}
0 & i \\
i & Si
\end{bmatrix} = U_n(Si) \begin{bmatrix}
0 & i \\
i & Si
\end{bmatrix} - U_{n-1}(Si)I.
$$

The formulas (17) lead to $F_n(S) = (-i)^{n-1}U_n(Si)$ and $G_n(S) = (-i)^nC_n(Si)$.

The Chebyshev polynomials of the third and fourth kind, $V_{2n+1}(T)$ and $W_{2n+1}(T)$, do not have a counterpart for the Fibonacci polynomials. In particular $F_{2n+1} = F_{n+1}^2 + F_n^2$ does not have the corresponding factorization.

For every $S \geq 1$ we can use Fibonacci polynomials to define a partition of primes. However these are just the $T$-partitions, for $T = G_2(S) = S^2 + 2$.

**Theorem 8.** For any $S \geq 1$ and $T = G_2(S) = S^2 + 2$ we have

(i) $p \in \Pi_+(T)$ if and only if there is an odd $d$ such that $G_d(S) = 0 \mod p$,

(ii) $p \in \Pi_-(T)$ if and only if there is an odd $d$ such that $F_d(S) = 0 \mod p$,

(iii) $p \in \Pi_k(T), k \geq 1$, if and only if there is an odd $d$ such that $G_{nd}(S) = 0 \mod p$, for $n = 2^kd$.

The proof of Theorem 8 follows from special identities connecting the Fibonacci polynomials of the variable $S$ with the Chebyshev polynomials of the variable $T = S^2 + 2 = G_2(S)$.

**Proposition 9.** For any natural $k$

$$
G_{2k}(S) = C_k(G_2(S)), \quad F_{2k}(S) = S U_k(G_2(S)),
$$

$$
G_{2k+1}(S) = S W_{2k+1}(G_2(S)), \quad F_{2k+1}(S) = V_{2k+1}(G_2(S)).
$$

These identities can be obtained from the respective properties of Chebyshev polynomials, formulated in (14) and (15). We choose to give an independent proof.

**Proof.** We have for natural $k$

$$
\begin{bmatrix}
F_{2k-1} & F_{2k} \\
F_{2k} & F_{2k+1}
\end{bmatrix}^k = \begin{bmatrix}
0 & 1 \\
1 & S
\end{bmatrix}^{2k} = \begin{bmatrix}
1 & S \\
S & S^2 + 1
\end{bmatrix}^k =
$$

$$
U_k(S^2 + 2) \begin{bmatrix}
1 & S \\
S & S^2 + 1
\end{bmatrix} - U_{k-1}(S^2 + 2)I.
$$

The trace of the second matrix is equal to $G_{2k}(S)$ and the trace of the third matrix is equal to $C_k(S^2 + 2)$. 

Further it follows from (19) that $F_{2k}(S) = SU_k(G_2(S))$. Hence

$SW_{2k-1}(G_2(S)) = SU_{k+1}(G_2(S)) + SU_k(G_2(S)) = F_{2k+2}(S) + F_{2k}(S) = G_{2k+1}(S)$. It follows also from (19) that

$$V_{2k-1}(G_2(S)) = U_k(G_2(S)) - U_{k-1}(G_2(S)) = F_{2k-1}(S).$$

□

Theorem 8 follows from Proposition 9, except for the status of the divisors of $S$. If an odd prime $p$ divides $S$, then $G_2(S) = S^2 + 2 = 2 \mod p$, so that $W_p(G_2(S)) = W_p(2) = p \mod p$. It follows that $p \in \Pi_+(G_2(S))$. On the other hand such a prime $p$ divides $G_d(S)$ for any odd $d$.

4. Lucas polynomials

Let us turn to a general $2 \times 2$ matrix with the trace $T$ and the determinant $Q$. We have $A^2 = TA - QI$ which leads to $A^n = L_n A - QL_{n-1} I$, where $L_k(T, Q)$, $k = 1, 2, \ldots$, are the Lucas polynomials. In particular

$$
\begin{bmatrix}
0 & 1 \\
-Q & T
\end{bmatrix}^n = 
\begin{bmatrix}
-QL_{n-1} & L_n \\
-QL_n & L_{n+1}
\end{bmatrix}.
$$

Since the determinant of a matrix can be rescaled to 1, the Lucas polynomials can be recovered from the Chebyshev polynomials by the following procedure. We consider the homogenization of the Chebyshev polynomials $U_n(T, R) = R^{n-1}U_n(T/R)$. Since the Chebyshev polynomials contain terms of only odd powers, or only even powers, in the resulting homogeneous polynomial $U_n(T, R)$ the variable $R$ appears in even powers alone. Hence $U_n(T, \sqrt{Q})$ is a polynomial in $T$ and $Q$, and it is equal to the Lucas polynomial $L_n(T, Q)$.

For negative values of the determinant $Q$ it may be convenient to start from Fibonacci polynomials to obtain first the homogeneous polynomials $F_n(T, R) = R^{n-1}F_n(T/R)$ and then $L_n(T, -Q) = F_n(T, \sqrt{Q})$.

Similarly the trace of $A^n$ is also a polynomial in $T$ and $Q$, and we denote it by $K_n(T, Q) = L_{n+1}(T, Q) - QL_{n-1}(T, Q)$, it is the companion Lucas polynomial. Let us remind the reader that $L_n$ is of degree $n - 1$ and $K_n$ is of degree $n$.

All the identities developed for Chebyshev polynomials can be translated to Lucas polynomials by the above procedure of homogenization. As a result we get polynomial identities in the variables $(T, \sqrt{Q})$ which may or may not be polynomial in the variables $(T, Q)$. In particular in accordance with the first line of Lemma 7 we have $L_{2k-1}(T, Q) = L_k^2(T, Q) - QL_{k-1}^2(T, Q)$, but the polynomial cannot be split further, as it is done for $Q = 1$. We can split it though after the substitution $Q = R^2$. The polynomials $W_{2k-1}(T)$ and $V_{2k-1}(T)$ turn into $W_{2k-1}(T, R)$ and $V_{2k-1}(T, R)$ by the homogenization and we get

$$
W_{2k-1}(T, R) = L_k(T, R^2) + RL_{k-1}(T, R^2),
$$

$$
V_{2k-1}(T, R) = L_k(T, R^2) - RL_{k-1}(T, R^2),
$$

$$
L_{2k-1}(T, R^2) = W_{2k-1}(T, R)V_{2k-1}(T, R).
$$
The values of Lucas polynomials for fixed integer values of $T, Q$ give rise to a partition of odd primes similar to the one defined for the Chebyshev polynomials. First we need to exclude the trivial cases. We assume that both $T$ and $Q$ are different from 0, and relatively prime. Moreover we consider only values of $T \geq 1$. With these restrictions in place we need to exclude only two more cases $(T, Q) = (1, 1)$ and $(T, Q) = (2, 1)$. Any pair of integers $(T, Q)$ satisfying all these restrictions will be called admissible.

For an admissible pair $(T, Q)$ we define the subsets of odd primes $\Pi_k = \Pi_k(T, Q) \subset \Pi, k = 0, 1, 2, \ldots$. An odd prime $p \in \Pi_0(T, Q)$ if there is an odd $d$ such that $p$ divides $L_d(T, Q)$. For $k \geq 1$, an odd prime $p \in \Pi_k(T, Q)$ if there is an odd $d$ such that $p$ divides $K_n(T, Q)$ for $n = 2^{k-1}d$.

Further when $Q$ is a square, $Q = R^2$, we define the splitting of $\Pi_0(T, R^2) = \Pi_+(T, R) \cup \Pi_-(T, R)$ by the condition that an odd prime $p \in \Pi_+(T, R)$ if there is a natural $k$ such that $p$ divides $W_{2k+1}(T, R) (V_{2k+1}(T, R))$.

**Theorem 10.** For any admissible $(T, Q)$ the family of subsets $\Pi_k(T, Q) \subset \Pi, k = 0, 1, 2, \ldots$ is a partition of $\Pi \setminus \mathcal{D}(Q)$, where $\mathcal{D}(Q)$ is the set of prime divisors of $Q$. Further if $Q$ is a square, $Q = R^2$, then $\Pi_+(T, R)$ and $\Pi_-(T, R)$ are disjoint.

The proof that all these sets of primes are disjoint follows the lines of the proof of its special case, Theorem 1, outlined in Section 1. Every identity for Chebyshev polynomials used in that proof can be turned into an identity involving Lucas polynomials, which then can be used to the same effect. We will prove now the part that every prime appears in these subsets, with the exception of the divisors of $Q$. This was the part of the proof of Theorem 1 which was postponed to this general case.

We start with a general fact that is probably part of the math folklore.

**Theorem 11.** For any $2 \times 2$ matrix $A$ with integer elements, with the determinant $Q$ and the trace $T$, for any odd prime $p$, and $D = T^2 - 4Q$

\[
A^p = A \mod p, \quad \text{if } (D|p) = 1,
\]
\[
A^{p+1} = QI \mod p, \quad \text{if } (D|p) = -1,
\]
\[
A^p = T^2 I \mod p, \quad \text{if } (D|p) = 0.
\]

**Proof.** Proposition 5 can be extended to the Lucas polynomials $K_n$ by using the homogenized version of (7). Hence we have that for any prime $p$

\[
K_p(T, Q) = T^p \equiv T \mod p.
\]

Since

\[
K_p = L_{p+1} - QL_{p-1} = T \mod p, \quad L_{p+1} + QL_{p-1} = TL_p,
\]
we get

\[
(22) \quad 2L_{p+1} = T (L_p + 1), \quad 2QL_{p-1} = T (L_p - 1) \mod p.
\]

Also the expansion (8) can be extended to Lucas polynomials $L_n$ by homogenization, so that $L_p(T, Q) = (T^2 - 4Q)^{p-1} \mod p$. It leads to the generalization of Proposition 6.

In the case $L_p = 1 \mod p$ we get by (22) that $QL_{p-1} = 0 \mod p$. Consequently $A^p = L_p A - QL_{p-1} I = A$.

Similarly, if $L_p = -1 \mod p$ then $L_{p+1} = 0 \mod p$. Consequently $A^{p+1} = L_{p+1} A - QL_p I = QI$. 


In the final case, \( L_p = 0 \mod p \), we get \( 2QL_{p-1} = -T \mod p \) which leads to \( A' = L_pA - QL_{p-1}I = \frac{T}{2}I \).

It transpires in the last proof that for any odd prime \( p \) either \( QL_{p-1} = 0 \), or \( L_{p+1} = 0 \), or \( L_p = 0 \mod p \). Using the factorization (16), translated to Lucas polynomials, we conclude that for every odd prime, except for the divisors of \( Q \), either \( L_d = 0 \mod p \) for an odd \( d \), or some trace \( K_n = 0 \mod p \). To finish the proof of Theorem 10 we still need to use the admissibility of the pair \((T, Q)\) to rule out the possibility that \( L_d \) or \( K_n \) vanish in \( \mathbb{Z} \), rather than only in \( \mathbb{F}_p \). Theorem 10 is proven. Theorem 1 is clearly a special case of Theorem 10.

For an admissible pair \((T, Q)\) the partition appearing in Theorem 10 will be called the \((T, Q)\)-partition. To be precise a \((T, Q)\)-partition contains \( \Pi_0(T, Q) \) if \( Q \) is not a square. Otherwise, if \( Q = R^2, R \in \mathbb{N} \), it contains two sets instead, \( \Pi_+(T, R) \) and \( \Pi_-(T, R) \). In the next theorem it is convenient to allow negative values for \( R \). Such a change of sign leads to \( \Pi_\pm(T, R) = \Pi_\pm(T, -R) \).

In general for different values of admissible \((T, Q)\) we get different \((T, Q)\)-partitions, with the following exceptions.

**Theorem 12.** For an admissible \((T, Q)\), if \( \hat{T} = K_d(T, Q) \), for an odd \( d \), then the \( (\hat{T}, Q^d)\)-partition is equal to the \((T, Q)\)-partition.

Further, for \( T_2 = T^2 - 2Q = K_2(T, Q) \)

\[
\Pi_k(T_2, Q^2) = \Pi_{k+1}(T, Q), \quad k = 1, 2, \ldots,
\]

(23)

\[
\Pi_0(T_2, Q) = \Pi_0(T, Q) \cup \Pi_1(T, Q),
\]

\[
\Pi_-(T_2, Q) = \Pi_1(T, Q), \quad \Pi_+(T_2, Q) = \Pi_0(T, Q).
\]

If the determinant \( Q \) is a square, \( Q = R^2 \), then

(24)

\[\Pi_+(T_2, Q) = \Pi_-(T, R) \cup \Pi_+(T, R).\]

The proof of this theorem is obtained in the same way as the proof of Theorem 2. It follows by the application of the same polynomial identities translated from the Chebyshev to Lucas polynomials. To get (23) we use the Lucas version of the polynomial identities from Proposition 9. For clarity we reproduce here some details. The identities in (14) and (15) translate to Lucas polynomials as

(25) \[ TV_{2k+1}(T_2, Q) = K_{2k+1}(T, Q), \quad W_{2k+1}(T_2, Q) = L_{2k+1}(T, Q).\]

These identities imply immediately the second line in (23), except for the role of the factor \( T \) which is handled exactly as before. If an odd prime \( p \) divides \( T \), then \( T_2 = K_2(T, Q) = S^2 - 2Q = -2Q \mod p \), so that for \( p = 2k + 1 \) we have

\[
V_p(T_2, Q) = V_p(-2Q, Q) = L_{k+1}(-2Q, Q^2) - QL_{k-1}(-2Q, Q^2) = Q^kV_p(-2) = Q^kW_p(2) = Q^kp \mod p.
\]

It follows that \( p \in \Pi_+(T_2, Q) \). On the other hand such a prime \( p \) divides \( K_d(T, Q) \) for any odd \( d \).

(24) follows from (21).
It follows from Theorem 12 that if $Q$ is not a square then the $(T, Q)$-partition and the $(T_2, Q_2^2)$-partition coincide, except that one contains $\Pi_0$, and the other $\Pi_+$ and $\Pi_-$. For example $\Pi_1(3, 2) = \Pi_-(5, 2)$, $\Pi_0(3, 2) = \Pi_+(5, 2)$. Further, $\Pi_1(3, -2) = \Pi_-(13, -2) = \Pi_+(13, 2)$, $\Pi_0(3, -2) = \Pi_+(13, -2) = \Pi_-(13, 2)$.

Hence the $(3, 2)$- and $(5, 4)$-partitions, and also $(3, -2)$- and $(13, 4)$-partitions, coincide up to the indexing of their sets.

More generally Theorem 12 implies that it is enough to study the $(T, Q)$-partitions for $T \geq 1, Q \geq 1$. Indeed for $Q \leq -1$ we have by (23) that

$$\Pi_1(T, Q) = \Pi_+(T^2 + 2|Q|, |Q|), \quad \Pi_0(T, Q) = \Pi_-(T^2 + 2|Q|, |Q|).$$

Overall if $Q \leq -1$ then the $(T, Q)$-partition is equal to the $(T^2 + 2|Q|, Q^2)$-partition.

Further, for any admissible $(T, Q)$, the $(-T, Q)$- and $(T, Q)$-partitions coincide.

Nevertheless it may be beneficial to use admissible pairs $(T, Q)$ with negative values of $Q$. There is a clear difference between negative and positive values of $Q$ from the point of view of algebraic number theory. It will be demonstrated in Section 6.

We are thus lead to the following definition. An admissible pair $(T, Q)$ is primitive if $T \geq 1, Q \geq 1$ and there are no natural numbers $S, R$ such that $T = \pm G_2(S, R) = \pm (S^2 - 2R), Q = R^2, R \geq 1$.

For example any pair $(T, 2)$, $T$ odd, is primitive, because 2 is not a power of any integer. The pair $(T, 1), T \geq 3$, is primitive if $T$ is a primitive trace, as defined before. The pair $(3, 4)$ is not primitive because $G_2(1, 2) = -3$.

We have established in this Section that it is sufficient to study $(T, Q)$-partitions for primitive admissible pairs only. The connection to the general case is spelled out in Theorem 12. For example if $T = 6^4 - 1, Q = -6^4$, then the $(T, Q)$-partition can be obtained in the following way from the primitive $(7, 6)$-partition. First the $(T, Q)$-partition is equal to the $(6^6 + 1, 6^6)$-partition. By applying Theorem 12 three times we have

$$\Pi_0(T, Q) = \Pi_-(6^8 + 1, 6^8) = \Pi_1(6^4 + 1, 6^4) = \Pi_2(6^2 + 1, 6^2) = \Pi_3(7, 6),$$

$$\Pi_1(T, Q) = \Pi_+(6^8 + 1, 6^8) = \Pi_0(7, 6) \cup \Pi_1(7, 6) \cup \Pi_2(7, 6),$$

$$\Pi_k(T, Q) = \Pi_{k+2}(7, 6), \quad k \geq 2.$$  \hspace{1cm} (26)

5. Lehmer polynomials

Lehmer polynomials appear when we take powers of a $2 \times 2$ matrix with the trace $T = \sqrt{Z}$ and the determinant $Q$. Clearly the traces are polynomials in $\sqrt{Z}$, namely $K_n(\sqrt{Z}, Q)$. They are polynomials in $Z, Q$ for even powers $n$. The Lehmer polynomials are defined for $k \geq 1$ as

$$J_{2k}(Z, Q) = K_{2k}(\sqrt{Z}, Q), \quad J_{2k-1}(Z, Q)\sqrt{Z} = K_{2k-1}(\sqrt{Z}, Q).$$  \hspace{1cm} (27)

Similarly we define the companion Lehmer polynomials for $k \geq 1$

$$H_{2k-1}(Z, Q) = L_{2k-1}(\sqrt{Z}, Q), \quad H_{2k}(Z, Q)\sqrt{Z} = L_{2k}(\sqrt{Z}, Q).$$  \hspace{1cm} (28)
PARTITIONS OF PRIMES DEFINED BY CHEBYSHEV AND LUCAS POLYNOMIALS

The polynomials $H_n, J_n$ are homogeneous of degree $\frac{n-1}{2}$ and $\frac{n}{2}$ (integer parts when needed), respectively. They have only integer coefficients and can be easily obtained from the Chebyshev, or Lucas, polynomials. For example

$$C_7(T) = T^7 - 7T^5 + 14T^3 - 7T,$$

$$K_7(T, Q) = T^7 - 7T^5Q + 14T^3Q^2 - 7TQ^3,$$

$$J_7(Z, Q) = Z^3 - 7Z^2Q + 14ZQ^2 - 7Q^3.$$  

Identities for Lucas polynomials can be translated with the help of (27) and (28) into formulas satisfied by Lehmer polynomials. We will use the following equivalents of (14), and (15), or (18).

$$J_{2k}(Z, Q) = K_k(Z - 2Q, Q^2), \quad H_{2k}(Z, Q) = L_k(Z - 2Q, Q^2),$$

$$J_{2k+1}(Z, Q) = V_{2k+1}(Z - 2Q, Q), \quad H_{2k+1}(Z, Q) = W_{2k+1}(Z - 2Q, Q).$$

Lehmer polynomials can be used to partition the set of odd primes, however we obtain only some of the $(T, Q)$-partitions, defined previously.

**Proposition 13.** For any $Q \geq 1$ and $Z$ such that $(T, Q^2)$ is admissible, where $T = Z - 2Q$, we have:

(i) an odd prime $p \in \Pi_+(T, Q)$ if and only if there is an odd $d$ such that $H_d(Z, Q) = 0 \mod p$,

(ii) an odd prime $p \in \Pi_-(T, Q)$ if and only if there is an odd $d$ such that $J_d(Z, Q) = 0 \mod p$,

(iii) an odd prime $p \in \Pi_k(T, Q^2), k \geq 1$, if and only if there is an odd $d$ such that $J_{n}(Z, Q) = 0 \mod p, \text{ for } n = 2^kd$.

The proof is a straightforward application of (29).

Motivated by Proposition 13 we introduce for the $(T, R^2)$-partition, $R \geq 1$, its Lehmer values, which are the natural numbers $(T + 2R, R)$. For example, the $(6, 1)$-partition has Lehmer values $(8, 1)$, and $(1, 25)$-partition has Lehmer values $(11, 5)$. The meaning of this notion is that by (29) the values of Lucas polynomials for $(T, R^2)$ coincide with the values of Lehmer polynomials for the Lehmer values $(T + 2R, R)$. It may or may not be a coincidence that the exceptional values of the trace $T$ in Conjecture 1 can be described as the pairs $(T, 1)$ with Lehmer values equal to $(2y^2, 1)$, for a natural $y$.

6. THE PROOF OF THEOREM 3 AND PRIME DENSITIES

We now look at the size of the sets in a $(T, Q)$-partition, measured by their prime densities. We will denote by $\delta_s = \delta_s(T, Q) = \delta(\Pi_s(T, Q)), s = \pm, 0, 1, 2, \ldots$, the prime densities of the sets in a $(T, Q)$-partition, if they exist, or lower, or upper densities, as appropriate.

We are going to prove Theorem 3 by fairly elementary tools.

It follows from Theorem 11 that for any odd prime $p$ there is the smallest $\xi = \xi(p) \geq 1$ such that $L_{\xi}(T, Q) = 0 \mod p$. It is called the index of appearance of $p$. The basic recurrence relation gives us $L_{\xi+1} = -QL_{\xi-1} \mod p$, and using (20) we get

$$A^\xi = \begin{bmatrix} 0 & 1 \\ -Q & T \end{bmatrix}^\xi = \begin{bmatrix} -QL_{\xi-1} & 0 \\ 0 & L_{\xi+1} \end{bmatrix} = L_{\xi+1}I \mod p.$$
Hence calculating the determinants at both ends we arrive at $Q^\xi = L_{\xi+1}^2 \mod p$. It follows that if $\xi$ is odd, which is equivalent to $p \in \Pi_0$, then $Q$ must be a square residue $\mod p$. We obtain the following Proposition.

**Proposition 14.** If $Q$ is not a rational square then $\Pi_0 \subset \{ p \in \Pi \mid (Q|p) = 1 \}$, and $\delta_0(T, Q) \leq \frac{1}{2}$.

**Proof.** By the theorem of Frobenius, [S-L], for a fixed integer $Q$, which is not a rational square, the prime density of the set of primes $p$, for which the polynomial $\lambda^2 - Q$ splits over the field $\mathbb{F}_p$, is equal to $\frac{1}{2}$. □

In particular we get that $\delta_0(T, Q) \leq \frac{1}{2}$ for all $Q \leq -1$.

If the index of appearance is even, $\xi = 2m$, then $L_{\xi+1} = \pm Q^m \mod p$. Somewhat surprisingly we can determine the sign in this equality without making any assumptions, beyond $Q \not\equiv 0 \mod p$.

**Lemma 15.** If $\xi = 2m$ then $L_{\xi+1} = -Q^m$ and $K_m = 0 \mod p$.

**Proof.** From (30) we get $A^m = L_{\xi+1} I \mod p$, and consequently $\lambda^2 - Q$ splits over the field $\mathbb{F}_p$, is equal to $\frac{1}{2}$. □

Since $T L_{m+1} = L_{m+1} + Q L_{m-1}$, we get, using Lemma 15, that $2L_{m+1} = 2Q L_{m-1} = T L_m$. Further

$$2A^m = \left[ \begin{array}{cc} -TL_m & 2L_m \\ -2QL_m & TL_m \end{array} \right] \mod p.$$

Again calculating the determinants of both sides we arrive at

$$4Q^m = -(T^2 - 4Q) L_m^2 \mod p.$$  

Since $A^\xi$ is the first power which is a multiple of $I \mod p$ then by Theorem 11 we have the following alternative. If $(D|p) = 1$, where $D = T^2 - 4Q$, then there is a natural $h$ such that $2mh = p - 1$ and $I = A^{p-1} = A^h = (-Q^m)^h I$. Hence we get

$$(-1)^h Q^{\frac{p-1}{2}} = 1 \mod p.$$  

If $(D|p) = -1$ then there is a natural $h$ such that $2mh = p + 1$ and $Q I = A^{p+1} = A^h = (-Q^m)^h I$, and we get again (32).

Note that although in both cases we arrive at (32), we have $2hm = p - 1$ if $(D|p) = 1$, and $2hm = p + 1$ if $(D|p) = -1$.

It follows from (32) and Proposition 14 that

**Lemma 16.** If $(Q|p) = -1$ then $p \not\in \Pi_0$ and $h$ in (32) is odd.

We proceed to explore the consequences of (31).
Proposition 17. If the determinant $Q$ and $-D = -(T^2 - 4Q)$ are not rational squares then

1. if $(Q|p) = 1$ and $(-D|p) = -1$ then $p \in \Pi_0(T, Q)$,
2. if $p \in \Pi_1(T, Q)$ then $(Q|p)(-D|p) = 1$,
3. if $p \in \Pi_{even}(T, Q)$ then $(-D|p) = 1$,
4. if $(Q|p) = -1$ and $(-D|p) = 1$ then $p \in \Pi_{even}(T, Q)$.

Proof. (1) If $Q$ is a square residue mod $p$ and $-D$ is a square non-residue mod $p$ then (31) is impossible, which means that $\xi$ is odd, and $p \in \Pi_0(T, Q)$.

(2) If $p \in \Pi_1(T, Q)$ then $m$ in (31) is odd and hence the quadratic residue status of $Q$ and $-D$ must be the same.

(3) If $p \in \Pi_{even}(T, Q)$ then $m$ in (31) is even, and then clearly $-D$ must be a square residue.

(4) Conversely if $Q$ is a square non-residue mod $p$ and $-D$ is a square residue mod $p$ then $m$ in (31) must be even. □

Now Theorem 3 follows readily from Propositions 14 and 17.

We can further get estimates of the prime densities of the sets.

Proposition 18. If $Q$ and $-D = -(T^2 - 4Q)$ are not rational squares, and also $-Q$ or $D$ are not rational squares, then the prime densities of the three sets $\Pi_0$, $\Pi_1$ and $\Pi_{even}$ are all between $1/4$ and $1/2$.

All the densities are understood as upper for the inequalities $\delta \leq$, and lower for the inequalities $\delta \geq$.

Proof. We have

\begin{align*}
\{ p \in \Pi_0 \mid (Q|p) = 1, (-D|p) = -1 \} &\subset \Pi_0 \subset \{ p \in \Pi_1 \mid (Q|p) = 1 \}, \\
\{ p \in \Pi_1 \mid (Q|p) = -1, (-D|p) = -1 \} &\subset \Pi_1 \subset \{ p \in \Pi_1 \mid (Q|p)(-D|p) = 1 \}, \\
\{ p \in \Pi_{even} \mid (Q|p) = -1, (-D|p) = 1 \} &\subset \Pi_{even} \subset \{ p \in \Pi_1 \mid (-D|p) = 1 \}.
\end{align*}

It follows from the theorem of Frobenius, $\mathbb{S}$-$\mathbb{L}$, that the sets on the left have all prime density $\frac{1}{4}$, and the sets on the right have all density $\frac{1}{2}$. There is the exceptional case when both $-Q$ and $D$ are rational squares, so it needs to be excluded. □

It remains to analyze the cases when $\pm Q$ or $\pm D$ is a rational square.

Proposition 19. (i) If $Q$ is a rational square, $-D$ is not a rational square, and $p \notin \Pi_0$ then $(-D|p) = 1$, and $\delta_0 \geq \frac{1}{2}$.

(ii) If $-D$ is a rational square, $Q$ is not a rational square, and $p \in \Pi_1$ then $(Q|p) = 1$, and $\delta(\Pi_{even}) \geq \frac{1}{4}$.

(iii) If $-Q$ and $D$ are rational squares, and $(-1|p) = -1$ then $p \in \Pi_1$, and $\delta_1 \geq \frac{1}{2}$.

Proof. The proof is similar to the proofs of Propositions 14 and 17.

The case (i) follows directly from (31).

In the case (ii) on top of (31) we use also Proposition 14 to get that $\Pi_0 \cup \Pi_1 \subset \{ p \in \Pi_1 \mid (Q|p) = 1 \}$.

To get (iii) we first observe that if $p \in \Pi_0$ then by Proposition 14 $(Q|p) = 1$, which forces $(-1|p) = 1$. Hence under the assumptions in (iii) we have that $p \notin \Pi_0$ and we can apply (31).
Secondly we write (31) as $4(-1)^{m-1}(-Q)^m = DL_m^2$. We conclude now that if $-1$ is a quadratic non-residue $\mod p$ then $m - 1$ must be even, and hence $p \in \Pi_1$. □

Let us note that the unusually large densities in Proposition 19 can be explained in the case (i) by the fact that in this case $Q = R^2$ and $\Pi_0(T, R^2) = 1$. Similarly in the case (iii) we have $Q = -R^2$ and $T^2 + 4R^2 = D = X^2$ for some natural $X$. Now by Theorem 12 we get

$$\Pi_1(T, -R^2) = \Pi_+(T^2 + 2R^2, R^2) = \Pi_+(X^2 - 2R^2, R^2) = \Pi_+(X, R) \cup \Pi_-(X, R).$$

However in the case (ii) we do not have such a splitting, and the assumptions allow $(T, Q)$ to be primitive. For example $(T, Q) = (2, 5)$ is primitive and we have $D = -16$.

Note that when both $Q$ and $-D$ are rational squares we do not have Proposition 14, and (31) does not work as above.

We will now use Lemma 15. Let us then assume that $Q$ and $-D$ are not rational squares so that the set

$$\Gamma := \{ p \in \Pi \mid (Q|p) = -1, (-D|p) = 1 \} \subset \Pi_{\text{even}}.$$ We are going to split the set $\Gamma$ using the $(T, Q)$ partition. To proceed we need to exclude more values of $(T, Q)$. For that purpose we invoke the definition of a special pair $(T, Q)$ from the Introduction, the concept derived from [B2].

**Proposition 20.** If $(T, Q)$ is not special then for $k \geq 2$ the prime density

$$\delta(\Gamma \cap \Pi_k) = \frac{1}{2^{k+1}}.$$

**Proof.** By Proposition for $p \in \Gamma$ we have $\xi = 2m$, and $h$ is odd. We consider the disjoint sets $\Gamma_1$ and $\Gamma_-$, $\Gamma = \Gamma_1 \cup \Gamma_-.$

$$\Gamma_1 = \Gamma \cap \{ p \mid (-1|p) = 1 \} = \{ p \mid (Q|p) = -1, (D|p) = 1, (-1|p) = 1 \},$$

$$\Gamma_- = \Gamma \cap \{ p \mid (-1|p) = -1 \} = \{ p \mid (Q|p) = -1, (D|p) = -1, (-1|p) = -1 \}.$$ If $p \in \Gamma_1 \cap \Pi_k$, for $k \geq 2$, we get that $p - 1 = 2mh$, $2^{k-1}||m$. Since $h$ is odd it follows that $2^k||p - 1$. Since we work with a partition we can conclude that $\Gamma_1 \cap \Pi_k = \{ p \mid (Q|p) = -1, (D|p) = 1, p = 2^k + 1 \mod 2^{k+1} \}.

If the primitive pair $(T, Q)$ is not special then the conditions describing the last set are “independent”, as explained in [B2], and the prime density

$$\delta(\Gamma_1 \cap \Pi_k) = 2^{-(k+2)}.$$

If $p \in \Gamma_- \cap \Pi_k$, for $k \geq 2$, we get that $p + 1 = 2mh$, $2^{k-1}||m$. We get again that $2^k||p + 1$.

Further $\Gamma_- \cap \Pi_k = \{ p \mid (Q|p) = -1, (D|p) = 1, p = 2^k - 1 \mod 2^{k+1} \}.

Again because we assume that the primitive pair $(T, Q)$ is not special then the conditions describing the last set are “independent”, and again the prime density

$$\delta(\Gamma_- \cap \Pi_k) = 2^{-(k+2)}.$$

Finally the prime density

$$\delta(\Gamma \cap \Pi_k) = 2^{-(k+1)}.$$

Let us note that the assumption that $(T, Q)$ is not special is essential. If $Q$ and $-D$ are not rational squares, and $Q = 2z^2$, $z \in \mathbb{N}$, then $\Gamma \subset \Pi_2$. Indeed $(Q|p) = -1$ if and only if $p = 3 \mod 8$ or $p = 5 \mod 8$. In both cases we conclude that $2mh = 4 \mod 8$, which means that $p \in \Pi_2$. 


Further, if $Q$ and $-D$ are not rational squares, and $D = -2z^2, z \in \mathbb{N}$, then $\Gamma \cap \Pi_2 = \emptyset$. Indeed $(-D|p) = 1$ if and only if $p = 1 \mod 8$ or $p = 7 \mod 8$. In both cases $2mh = 0 \mod 8$, and hence $p \notin \Pi_2$.

Ballot,[B1], and Moree,[M], obtained prime densities of $\Pi_0$ in the reducible case, without assuming (in our language) the primitivity of $(T, Q)$. Hence their formulas allow, by Theorem 12, to obtain the prime densities of all the subsets in a $(T, Q)$-partition, when $D$ is a rational square. The result is surprisingly simple, it is given in Theorem 4. The translation is straightforward. We present it by applying Theorem 4 to obtain the densities $\delta_0$ given by Ballot,[B1], page 26, for several non-primitive values of $(T, Q)$. The main tool is Theorem 12, and we proceed as in (26). We use the shorthand notation $(\delta_i + \delta_j)(T, Q) = \delta_i(T, Q) + \delta_j(T, Q)$. First we treat the general cases ($Q \neq 2x^2$).

\[
\begin{align*}
\delta_0(2^4 + 3^4, 6^4) &= (\delta_0 + \delta_1)(2^2 + 3^2, 6^2) = (\delta_0 + \delta_1 + \delta_2)(5, 6) = 5/6, \\
\delta_0(-12^2 + 1, -12^2) &= \delta_-(12^4 + 1, 12^2) = \delta_1(12^2 + 1, 12^2) = \delta_2(13, 12) = 1/6 \\
\delta_0(-6^4 + 1, -6^4) &= \delta_3(7, 6) = 1/12.
\end{align*}
\]

In the exceptional cases ($Q = 2x^2$) we have

\[
\begin{align*}
\delta_0(2^3 + 1, 2^3) &= 7/24, \quad \delta_0(-2 + 1, -2) = \delta_-(2^2 + 1, 2) = \delta_1(3, 2) = 7/24, \\
\delta_0(18 + 1, 18) &= 7/24, \quad \delta_0(18^2 + 1, 18^2) = (\delta_0 + \delta_1)(19, 18) = 7/12, \\
\delta_0(2^4 + 3^4, 18^4) &= (\delta_0 + \delta_1)(2^2 + 3^2, 18^2) = (\delta_0 + \delta_1 + \delta_2)(11, 18) = 11/12, \\
\delta_0(-2^2 + 1, -2^2) &= \delta_-(2^4 + 1, 2^2) = \delta_1(2^2 + 1, 2^2) = \delta_2(3, 2) = 1/3, \\
\delta_0(-2^4 + 1, -2^4) &= \delta_-(2^8 + 1, 2^4) = \delta_1(2^4 + 1, 2^4) = \delta_3(3, 2) = 1/24.
\end{align*}
\]

References

[A] V.I. Arnold, *Fermat Dynamics, Matrix Arithmetics, Finite Circles, and Finite Lobachevsky Planes*. Funct. Analysis Appl. 38 (2004), 1-13.

[B1] C. Ballot, *Density of prime divisors of linear recurrences*. Mem. Amer. Math. Soc. 551 (1995).

[B2] C. Ballot, *On the $\frac{1}{4}$ density of odd ranked primes in Lucas sequences*. Unif. Distrib. Theory 3 (2008), 129-145.

[B-E] C. Ballot, M. Elia, *Rank and Period of Primes in the Fibonacci sequence. A Trichotomy*. Fibonacci Quart. 45 (2007), 56-63.

[D] P. Damphousse, *The arithmetic of power and root in $GL_2(\mathbb{C})$ and $SL_2(\mathbb{C})$*. Fibonacci Quart. 27 (1989), 386-401.

[Lag] J.C. Lagarias, *The set of primes dividing the Lucas numbers has density $\frac{2}{\varphi^2}$*. Pacific J. Math. 118 (1985), 449-461.

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

[L] E. Lucas *Theorie des fonctions numeriques simplement periodiques*. Amer. J. Math. 1 (1878), 184-240, 289-321.

[M] P. Moree, *On the divisors of $a^k + b^k$*. Acta Arithmetica (1997), 197-212.

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

[R] R.A. Rankin, *Chebyshev polynomials and the modulary group of level p*. Math.Scand. 2 (1954), 315-326.

[S] I. Schur, *Arithmetisches uber die Tschebysheffschen Polynome*. Gesammelte Abhandlungen, Springer, (1973), Bd. 3, 422-453.
[St] H. Steinlein, *Fermat's Little Theorem and Gauss Congruence: Matrix Versions and Cyclic Permutations*. Amer. Math. Monthly, 124, 548-553.

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

[Wiki] Chebyshev polynomials. Wikipedia.

[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

E-mail address: mwojtkowski@uni.opole.pl