Journal of Integer Sequences, Vol. 21 (2018),
Article 18.7.2

On a Family of Sequences Related to Chebyshev Polynomials

Andrew N. W. Hone[1]
School of Mathematics, Statistics & Actuarial Science
Sibson Building
University of Kent
Canterbury CT2 7FS
UK
anwh@kent.ac.uk

L. Edson Jeffery
11918 Vance Jackson Road
San Antonio, TX 78230
USA
lejeffery2@gmail.com

Robert G. Selcoe
16214 Madewood Street
Cypress, TX 77429
USA
rselcoe@gmail.com

Abstract

We consider the appearance of primes in a family of linear recurrence sequences labelled by a positive integer n. The terms of each sequence correspond to a particular class of Lehmer numbers, or (viewing them as polynomials in n) dilated versions of the so-called Chebyshev polynomials of the fourth kind, also known as airfoil polynomials. We prove that when the value of n is given by a dilated Chebyshev polynomial of the first kind evaluated at a suitable integer, either the sequence contains a single prime,

[1]Corresponding author. Currently on leave in the School of Mathematics and Statistics, University of New South Wales, Sydney NSW 2052, Australia.

or no term is prime. For all other values of n, we conjecture that the sequence contains infinitely many primes, whose distribution has analogous properties to the distribution of Mersenne primes among the Mersenne numbers. Similar results are obtained for the sequences associated with negative integers n, which correspond to Chebyshev polynomials of the third kind, and to another family of Lehmer numbers.

1 Introduction

Consider the linear recurrence of second order given by

$$s_{k+2} - n\, s_{k+1} + s_k = 0, \tag{1}$$

together with the initial conditions

$$s_0 = 1, \qquad s_1 = n + 1. \tag{2}$$

For each integer n, this generates an integer sequence that begins

$$\begin{aligned}&1, n+1, n^2+n-1, n^3+n^2-2n-1, n^4+n^3-3n^2-2n+1,\\ &n^5+n^4-4n^3-3n^2+3n+1, \ldots .\end{aligned} \tag{3}$$

The sequence can also be extended backwards to negative indices k, so that in particular $s_{-1} = -1 = -s_0$, which implies that it has the symmetry

$$s_k(n) = -s_{-k-1}(n) \tag{4}$$

for all k. In this way we obtain a sequence that we denote by $(\, s_k(n)\,)_{k\in\mathbb{Z}}$, where the argument denotes the dependence on n.

We can also interpret this as a sequence of polynomials in the variable n, with the integer sequences being obtained by substituting particular values for the argument. From this point of view, it is apparent from the recursive definition that, for each $k \geq 0$, $s_k(n)$ is a monic polynomial of degree k in n with integer coefficients. In fact, these are rescaled (or dilated) versions of polynomials that are used to determine the pressure distribution in linear airfoil theory, being given by

$$s_k(n) = W_k(n/2), \qquad W_k(\cos\theta) = \frac{\sin\Big((2k+1)\theta/2\Big)}{\sin(\theta/2)}, \tag{5}$$

where W_k are known as the Chebyshev polynomials of the fourth kind [18], or the airfoil polynomials of the second kind (see [5], where the notation u_k is used in place of W_k). As a function of θ, the expression on the far right-hand side of (5) is known as the Dirichlet kernel in Fourier analysis, where it is usually denoted $D_k(\theta)$ [8]. Compared with those of the third and fourth kinds, the properties of Chebyshev polynomials of the first and second kinds are much better known, and in what follows we will make extensive use of connections with the latter two sets of polynomials.

The primary goal of this article is to describe the case where n is a positive integer, but before proceeding, we consider the sequences obtained for some particular small values of $|n| \leq 2$, which will mostly be excluded from subsequent analysis, but are relevant nevertheless. In the case $n = 0$, the sequence $(\, s_k(0)\,)$ begins

$$1, 1, -1, -1, \ldots, \tag{6}$$

and repeats with period 4; we mention this case because it is equivalent to the sequence $(\, s_k(n) \bmod n\,)$. When $n = 1$ the sequence has period 6, being specified by the six initial terms

$$1, 2, 1, -1, -2, -1, \ldots, \tag{7}$$

and for $n = -1$ the sequence repeats the values

$$1, 0, -1 \tag{8}$$

with period 3. For $n = 2$ the sequence grows linearly with k, beginning with

$$1, 3, 5, 7, 9, 11, \ldots, \tag{9}$$

and consists of the odd integers, that is

$$s_k(2) = 2k + 1, \tag{10}$$

while for $n = -2$ the sequence has period 2, being given by

$$s_k(-2) = (-1)^k. \tag{11}$$

For each integer $n \geq 3$ the sequence increases monotonically for $k \geq 0$ and grows exponentially with k (see below for details).

Sequence A269254 in the Online Encyclopedia of Integer Sequences (OEIS) [27] records the first appearance of a prime term in $(\, s_k(n)\,)$.

Definition 1. (Sequence A269254.) For each integer $n \geq 1$, if the sequence of terms $(\, s_k(n)\,)_{k\geq 0}$ with non-negative indices contains a prime, then let a_n be the smallest value of $k \geq 1$ such that $s_k(n)$ is prime; or otherwise, if there is no such term, let $a_n = -1$.

There is also sequence A269253, whose nth term is given by the first prime to appear in $(\, s_k(n)\,)_{k\geq 0}$, or by -1 if no prime appears.

To illustrate the above definition, let us start with $n = 1$: since the first prime term in the sequence (7) is $s_1(1) = 2$, it follows that $a_1 = 1$. Similarly, for $n = 2$, the first prime in (9) is $s_1(2) = 3$, so $a_2 = 1$; but for $n = 3$, the sequence $(\, s_k(3)\,)$ begins $1, 4, 11, \ldots$, so $a_3 = 2$. In cases where a prime term has appeared in the sequence $(\, s_k(n)\,)$, the value of

a_n is immediately determined. The sequence $(a_n)_{n\geq 1}$ begins with the following terms for $1 \leq n \leq 34$:

$$\begin{aligned}&1,1,2,1,2,1,-1,2,2,1,2,1,2,-1,2,1,3,1,2,2,2,1,-1,2,6,2,3,1,\\&3,1,2,9,9,-1,\ldots.\end{aligned} \tag{12}$$

All of the positive values above can be checked very rapidly, and it turns out that all values of $a_n > 0$ are of the form $(p-1)/2$, where p is an odd prime: this is a direct consequence of Lemma 26 below. What is less easy to verify is the negative values $a_7 = a_{14} = a_{23} = a_{34} = -1$ displayed above, indicating no primes. For instance, when $n = 7$, the sequence $(\, s_k(7)\,)$ begins with

$$1, 8, 55, 377, 2584, 17711, 121393, 832040, 5702887, \ldots, \tag{13}$$

and it can be verified that none of these first few terms are prime; but to show that $a_7 = -1$ it is necessary to prove that $s_k(7)$ is composite for all $k > 0$: a proof of this fact can be found in section 3, while another proof appears in section 5 in a broader setting.

In fact, in order to understand the family of sequences $(\, s_k(n)\,)$ with positive n, it will be natural to consider negative integer values of n as well. In that case, it is helpful to define the family of sequences $(\, r_k(n)\,)$ given by

$$r_k(n) = (-1)^k\, s_k(-n). \tag{14}$$

It is straightforward to show by induction that, for fixed n, the sequence $(\, r_k(n)\,)$ satisfies the same recurrence (1) but with different initial conditions, namely

$$r_{k+2} - n\, r_{k+1} + r_k = 0,$$

together with

$$r_0 = 1, \qquad r_1 = n - 1. \tag{15}$$

For integer n, this generates an integer sequence that begins

$$\begin{aligned}&1, n-1, n^2-n-1, n^3-n^2-2n+1, n^4-n^3-3n^2+2n+1,\\&n^5-n^4-4n^3+3n^2+3n-1, \ldots.\end{aligned} \tag{16}$$

Up to rescaling n by a factor of 2, this sequence of polynomials arises in describing the downwash distribution in linear airfoil theory, and in this context they are referred to as the airfoil polynomials of the first kind [5], denoted t_k; with the alternative notation V_k they are also referred to as the Chebyshev polynomials of the third kind [18], so that

$$r_k(n) = V_k(n/2), \qquad V_k(\cos\theta) = \frac{\cos\Big((2k+1)\theta/2\Big)}{\cos(\theta/2)}. \tag{17}$$

Since $n = 2\cos\theta$, the identity (14) can also be obtained immediately by taking $\theta \to \theta + \pi$ in (5), and comparing with (17).

There is another OEIS sequence that is relevant here, corresponding to the first appearance of a prime in the sequence defined by (14) for each positive integer n.

Definition 2. (Sequence A269252.) For each integer $n \geq 1$, if the sequence of terms $(\, r_k(n)\,)_{k\geq 0}$ with non-negative indices contains a prime, then let $\tilde{a}_n$ be the smallest value of $k \geq 1$ such that $r_k(n)$ is prime; or otherwise, if there is no such term, let $\tilde{a}_n = -1$.

There is also sequence A269251, whose nth term is given by the first prime to appear in $(\, r_k(n)\,)_{k\geq 0}$, or by -1 if no prime appears.

For comparison with A269254, note that the first few terms of A269252 for $1 \leq n \leq 34$ are given by

$$\begin{aligned}&-1,-1,1,1,2,1,2,1,2,2,2,1,3,1,3,2,2,1,14,1,2,2,3,1,2,5,2,36,\\&2,1,2,1,15,-1,\ldots.\end{aligned} \tag{18}$$

The two initial -1 values that appear above for $n = 1, 2$ clearly correspond to (8) and (11), respectively, while the first non-trivial case to consider is the value -1 that appears for $n = 34$, corresponding to the sequence $(\, r_k(34)\,)$, which begins with

$$1, 33, 1121, 38081, 1293633, 43945441, 1492851361, 50713000833, \ldots; \tag{19}$$

again it can be verified that none of these first few terms are prime, while a proof that all terms with $k > 0$ are composite for this and certain other values of n is given in section 5.

Aside from the connection with Chebyshev polynomials, the numbers $s_k(n)$ and $r_k(n)$ also correspond to particular instances of Lehmer numbers with odd index, which are closely related to sequences of Lucas numbers. Prime divisors in sequences of Lucas and Lehmer numbers have been studied for some time; see e.g., [1, 25, 26, 29] for some general results, or see [10] for a more elementary introduction to primitive divisors. However, to the best of our knowledge, the question of when such sequences are without prime terms, or of where the first prime appears in such sequences, has not been considered in detail before, except in the case $n = 6$.

The case $n = 6$ corresponds to the so-called NSW numbers, named after [19] (sequence A002315). An NSW number q can be characterized by there being some r such that the pair of positive integers (q, r) satisfies the Diophantine equation

$$q^2 + 1 = 2r^2.$$

The sequence of NSW numbers is given by $q = s_k(6)$ for $k \geq 0$, with the corresponding solution to the above equation being $(q, r) = (s_k(6), r_k(6))$. The subsequence of prime NSW numbers is of particular interest in relation to finite simple groups of square order: the symplectic group of dimension 4 over the finite field $\mathbb{F}_q$ has a square order if and only if q is a prime NSW number, with the order being $(q^2(q^2-1)r)^2$. The first prime NSW number is $s_1(6) = 7$, and the symplectic group of dimension 4 over $\mathbb{F}_7$ is of order 11760^2.

For an arbitrary linear recurrence relation of second order, that is

$$x_{k+2} = a\, x_{k+1} + b\, x_k, \qquad (a, b) \in \mathbb{Z}^2,$$

the general question of whether it generates a sequence without prime terms has been considered for some time. If either the coefficients a, b or the two initial values x_0, x_1 have a common factor then it is obvious that all terms x_k for $k \geq 2$ have the same common factor, so the main case of interest is where $\gcd(a, b) = 1 = \gcd(x_0, x_1)$. In the case of the Fibonacci recurrence with $a = b = 1$, the groundbreaking result was due to Graham, who found a sequence whose first two terms are relatively prime and which consists only of composite integers [11]. This result was generalized to arbitrary second-order recurrences by Somer [28] and Dubickas et al. [6].

An outline of the paper is as follows. The next section serves to set up notation and provide a rapid introduction to the properties of dilated Chebyshev polynomials of the first and second kinds, which will be used extensively in the sequel, and also contains the required definitions of the corresponding sequences of Lucas and Lehmer numbers that appear subsequently. Section 3 provides a very brief review of some standard facts about linear recurrence sequences and products of such sequences, before a presentation of examples and preliminary results about values of n for which the terms $s_k(n)$ factor into a product of two linear recurrence sequences; this serves to illustrate and motivate the results which appear in section 5. As preparation for the latter, section 4 contains a collection of various general properties of the sequences $(\, s_k(n)\,)$. The main results of the paper, on the factorization of $(\, s_k(n)\,)$ and $(\, r_k(n)\,)$ when n is a dilated Chebyshev polynomial of the first kind evaluated at integer argument (Chebyshev values), are presented in section 5. Section 6 considers the appearance of primes in these sequences in the case that n is not one of the Chebyshev values, and gives heuristic arguments and numerical evidence to support a conjecture to the effect that the behaviour is analogous to that of the sequence of Mersenne primes. Some conclusions are made in the final section, and there are two appendices: the first is a collection of data on prime appearances, and the second is a brief catalogue of related sequences in the OEIS.

This paper arose out of a series of posts to the `SeqFan` mailing list, with contributions from many people, both professional and recreational mathematicians. Our aim throughout has been to make the presentation as explicit as possible, and for the sake of completeness we have stated several standard facts and definitions, as well as providing direct, elementary proofs of almost every statement (even when some of them are particular cases of more general results in the literature). We hope that in this form it will be possible for our work to be appreciated by sequence enthusiasts of every persuasion.

2 Dilated Chebyshev polynomials and Lehmer numbers

The families of Chebyshev polynomials arise in the theory of orthogonal polynomials, and have diverse applications in numerical analysis [18]. There are four such families, and while the Chebyshev polynomials of the first and second kinds are well studied in the literature, those of the third and fourth kinds are not so well known, and some of their connections to arithmetical problems have only been considered quite recently [13].

In order to define scaled versions of the standard Chebsyhev polynomials in terms of trigonometric functions, let

$$n = 2\cos\theta = \lambda + \lambda^{-1},$$

so that we may write

$$\lambda = \frac{n + \sqrt{n^2 - 4}}{2} = e^{\mathrm{i}\theta}, \tag{20}$$

where $\mathrm{i} = \sqrt{-1}$. Then the formulae

$$\mathcal{T}_k(2\cos\theta) = 2\,\cos(k\theta), \qquad \mathcal{U}_k(2\cos\theta) = \frac{\sin\left((k+1)\theta\right)}{\sin\theta} \tag{21}$$

define $\mathcal{T}_k$, $\mathcal{U}_k$ as polynomials in n, for all $k \in \mathbb{Z}$. In [21, Chapter 18] these polynomials are referred to as the dilated Chebyshev polynomials of the first and second kinds, and they are denoted by C_k, S_k respectively. In standard notation, the classical Chebyshev polynomials of the first and second kinds are written as T_k and U_k, and their precise relationship with the dilated polynomials used here is as follows:

$$\mathcal{T}_k(n) = 2\,T_k\left(\frac{n}{2}\right), \qquad \mathcal{U}_k(n) = U_k\left(\frac{n}{2}\right).$$

It is straightforward to show from the definitions (21) that the dilated Chebyshev polynomials of the first and second kinds satisfy the same recurrence (1) as the sequence $(\,s_k(n)\,)$, but with different initial values. For example, to verify that the sequence $(\,\mathcal{U}_k(n)\,)$ satisfies the recurrence, it is sufficient to note that

$$\mathcal{U}_k(n) - n\,\mathcal{U}_{k-1}(n) + \mathcal{U}_{k-2}(n) \;=\; \frac{\sin((k+1)\theta) - 2\cos\theta\sin(k\theta) + \sin((k-1)\theta)}{\sin\theta}, \tag{22}$$

and then observe that the right-hand side above vanishes as a consequence of the addition formula for sine in the form

$$\sin(\theta+\phi) + \sin(\theta-\phi) = 2\sin\theta\cos\phi. \tag{23}$$

For comparison with other texts, we note that the sequence of dilated first kind polynomials begins thus:

$$(\,\mathcal{T}_k(n)\,): \qquad 2, n, n^2-2, n^3-3n, n^4-4n^2+2, n^5-5n^3+5n, \ldots. \tag{24}$$

In contrast, the sequence of dilated second kind polynomials begins as

$$(\,\mathcal{U}_k(n)\,): \qquad 1, n, n^2-1, n^3-2n, n^4-3n^2+1, n^5-4n^3+3n, \ldots. \tag{25}$$

For future reference, we note the standard identities

$$\mathcal{T}_{ab}(n) = \mathcal{T}_a(\mathcal{T}_b(n)) \tag{26}$$

and

$$\mathcal{U}_{ab-1}(n) = \mathcal{U}_{a-1}(\mathcal{T}_b(n))\,\mathcal{U}_{b-1}(n), \tag{27}$$

which follow from the trigonometric definitions above.

In order to get a formula for the coefficients of the polynomials $s_k(n)$, we present an explicit expansion for the dilated Chebyshev polynomials of the second kind. Although this can be found elsewhere in the literature (cf. equations (5.74) and (6.129) in [12]), for completeness we present an elementary proof.

Proposition 3. *The dilated Chebyshev polynomials of the second kind are given by*

$$\mathcal{U}_k(n) = \sum_{i=0}^{\lfloor \frac{k}{2} \rfloor} (-1)^i \binom{k-i}{i} n^{k-2i}. \tag{28}$$

Proof. First note that for $k = 0, 1$ the sum on the right-hand side of (28) agrees with the initial terms $\mathcal{U}_0 = 1$, $\mathcal{U}_1 = n$. Then, upon substituting the sum formula into the recurrence (22) and comparing powers of n, after dividing by $(-1)^i$ we see that the coefficient of n^{k-2i} yields the identity

$$\binom{k-i}{i} - \binom{k-i-1}{i} - \binom{k-i-1}{i-1} = 0$$

for binomial coefficients. Thus the sequences defined by the left-hand and right-hand sides of (28) satisfy the same recurrence with the same initial conditions, so they must coincide. $\square$

For use in what follows, we also define Lehmer numbers. Given a quadratic polynomial in X with roots α, β, that is

$$X^2 - \sqrt{R}\,X + Q = (X-\alpha)(X-\beta), \qquad Q, R \in \mathbb{Z}, \tag{29}$$

where it is assumed that Q, R are coprime and α/β is not a root of unity, there are two associated sequences of Lehmer numbers, which (adapting the notation of [9]) we denote by $L_k^-(\sqrt{R}, Q)$ and $L_k^+(\sqrt{R}, Q)$, where

$$L_k^-(\sqrt{R}, Q) = \begin{cases} \frac{\alpha^k - \beta^k}{\alpha - \beta}, & \text{if } k \text{ odd;} \\ \frac{\alpha^k - \beta^k}{\alpha^2 - \beta^2}, & \text{if } k \text{ even,} \end{cases} \tag{30}$$

and

$$L_k^+(\sqrt{R}, Q) = \begin{cases} \frac{\alpha^k + \beta^k}{\alpha + \beta}, & \text{if } k \text{ odd;} \\ \alpha^k + \beta^k, & \text{if } k \text{ even.} \end{cases} \tag{31}$$

The sequences of Lehmer numbers can be viewed as generalizations of Lucas sequences. Assuming that R is a perfect square, so $P = \sqrt{R} \in \mathbb{Z}$, the two types of Lucas sequences associated to the quadratic $X^2 - PX + Q = (X-\alpha)(X-\beta)$ are given by

$$\ell_k^-(P, Q) = \frac{\alpha^k - \beta^k}{\alpha - \beta}, \qquad \ell_k^+(P, Q) = \alpha^k + \beta^k; \tag{32}$$

the corresponding Lehmer numbers $L_k^{\pm}(P,Q)$ are obtained from the Lucas numbers $\ell_k^{\pm}(P,Q)$ by removing trivial factors.

From the above definitions, there is a clear link between Chebyshev polynomials and Lucas/Lehmer numbers, which can be summarized in the following

Proposition 4. *For integer values n, the sequences of dilated Chebyshev polynomials of the first and second kinds coincide with particular Lucas sequences, that is*

$$\mathcal{T}_k(n) = \ell_k^+(n,1), \qquad \mathcal{U}_{k-1}(n) = \ell_k^-(n,1), \tag{33}$$

while the sequences generated by (1) with initial values (15) and (2) consist of Lehmer numbers with odd index, namely

$$r_k(n) = L_{2k+1}^+\left(\sqrt{n+2},1\right), \quad s_k(n) = L_{2k+1}^-\left(\sqrt{n+2},1\right) \tag{34}$$

respectively, for all k.

Proof. The formulae for $\mathcal{T}_k$ and $\mathcal{U}_k$ follow immediately from comparison of (21) with (32), requiring from (20) that $\alpha = \lambda = e^{\mathrm{i}\theta} = \beta^{-1}$ in (29). For the proof of the second part of the statement, note that taking $k = 0,1$ gives $L_1^-(\sqrt{n+2},1) = 1$ and $L_3^-(\sqrt{n+2},1) = n+1$, while a short calculation shows that $L_{2k+1}^-(\sqrt{n+2},1)$ satisfies the same recurrence (1) as $s_k(n)$, and similarly for the other sequence given by $r_k(n) = (-1)^k s_k(-n)$; so for each equation in (34), the sequences given by their left/right-hand sides coincide. □

Remark 5. There are also expressions for $r_k(n)$ and $s_k(n)$ in terms of dilated Chebyshev polynomials of the first/second kinds, respectively, with argument $\sqrt{n+2}$: see (74) and (53) below.

By writing the roots of the polynomial $X^2 - \sqrt{n+2}\,X + 1$ as

$$\alpha^{\pm 1} = \frac{\sqrt{n+2} \pm \sqrt{n-2}}{2}, \tag{35}$$

we have an alternative way to identify the terms in sequence A269254.

Corollary 6. *(Alternative characterization of sequence A269254.) For each $n \geq 3$, if α is defined by (35), then a_n is that positive integer k yielding the smallest prime of the form*

$$\frac{\alpha^{2k+1} - \alpha^{-(2k+1)}}{\alpha - \alpha^{-1}}, \tag{36}$$

or $a_n = -1$ if no such k exists.

The sequence A269252 can be identified in terms of the characteristic roots of (35) in a similar way.

Corollary 7. *(Alternative characterization of sequence A269252.) For each $n \geq 3$, if α is defined by (35), then $\tilde{a}_n$ is that positive integer k yielding the smallest prime of the form*

$$\frac{\alpha^{2k+1} + \alpha^{-(2k+1)}}{\alpha + \alpha^{-1}}, \tag{37}$$

or $\tilde{a}_n = -1$ if no such k exists.

3 Some surprising factorizations

In this section we briefly recall some basic facts about sequences generated by linear recurrences, before looking at some special properties of the family of sequences $(\, s_k(n)\,)$. We assume that all recurrences are defined over the field $\mathbb{C}$ of complex numbers. (In the next section we will also consider recurrences in finite fields or residue rings.) For a broad review of linear recurrences in a more general setting, the reader is referred to [9].

For what follows, it is convenient to make use of the forward shift, denoted S, which is a linear operator that acts on any sequence (f_k) with index k according to

$$\mathrm{S}\, f_k = f_{k+1}.$$

With this notation, the fact that a sequence (x_k) satisfies a linear recurrence relation of order N with constant coefficients can be expressed in the form

$$F(\mathrm{S})\, x_k = 0, \tag{38}$$

where F (of degree N) is the characteristic polynomial of the recurrence.

Definition 8. A *decimation* of a sequence $(x_k)_{k\in\mathbb{Z}}$ is any subsequence of the form $(x_{i+dk})_{k\in\mathbb{Z}}$, for some fixed integers i, d, with $d \geq 2$. A particular name for the case $d = 2$ is a *bisection*, $d = 3$ is a *trisection*, and in general this is a decimation of order d.

Remark 9. The case of decimations of linear recurrences defined over finite fields is considered in [7].

Since, at least in the case that all the roots $\lambda_1, \lambda_2, \ldots, \lambda_N$ of F are distinct, the general solution of (38) can be written as a linear combination of kth powers of the λ_j, it is apparent that the terms of a decimation of order d are given by $x_{i+dk} = \sum_{j=1}^{N} A_j\, \lambda_j^{dk}$, for some coefficients A_j. Hence the decimation satisfies the linear recurrence

$$\prod_{j=1}^{N} (\mathrm{S} - \lambda_j^d)\, x_{i+dk} = 0. \tag{39}$$

(The recurrence for the decimation has the same form in the case of repeated roots.) Decimations of the sequence $(\, s_k(n)\,)$ will be considered in Proposition 23 in the next section.

Given two sequences (x_k), (y_k) that satisfy linear recurrences of order N, M respectively, the product sequence

$$(z_k) = (x_k y_k)$$

also satisfies a linear recurrence. The following result is well known.

Theorem 10. *The product $(z_k) = (x_k y_k)$ of two sequences that satisfy linear recurrences of order N, M satisfies a linear recurrence of order at most NM.*

To prove the theorem in the generic situation where the recurrences for (x_k), (y_k) both have distinct characteristic roots, given by λ_i, $1 \leq i \leq N$ and μ_j, $1 \leq j \leq M$ respectively, observe that each product $\nu_{i,j} = \lambda_i \mu_j$ is a characteristic root for the linear recurrence satisfied by (z_k), that is

$$\prod_{i,j} (\mathrm{S} - \nu_{i,j})\, z_k = 0, \tag{40}$$

where the sum is over a maximum set of i, j that give distinct $\nu_{i,j}$; so if the $\nu_{i,j}$ are all different from each other then the order of the recurrence is exactly MN, but the order could be smaller if some of the $\nu_{i,j}$ coincide. For the general situation with repeated roots, see [33].

We now consider an observation concerning the sequences $(\, s_k(n)\,)$ for the special values $n = j^2 - 2$ where $j \in \mathbb{Z}$, which includes the cases $n = 7, 14, 23, 34$ that have $a_n = -1$ in (12). The fact is that for all these values, there is a factorization of the form

$$s_k(j^2 - 2) = r_k(j) s_k(j), \tag{41}$$

where both factors on the right-hand side above satisfy a linear recurrence of second order. This is surprising, because in the light of Theorem 10 one would naively expect such a product to satisfy a recurrence of order 4.

Theorem 11. *For the values $n = j^2 - 2$, the terms of the sequence $(\, s_k(n)\,)$ admit the factorization (41), where $r_k(j)$ satisfies the same recurrence as $s_k(j)$, that is*

$$r_{k+2}(j) - j\, r_{k+1}(j) + r_k(j) = 0, \tag{42}$$

with the initial values

$$r_0(j) = 1, \qquad r_1(j) = j - 1. \tag{43}$$

Thus for all $j \in \mathbb{Z}$ the formula (41) expresses $s_k(j^2 - 2)$ as a product of two integers.

Proof. In the case $n = j^2 - 2$, the formula (35) fixes the characteristic roots of the recurrence (1) as $\lambda = \alpha^2$, $\lambda^{-1} = \alpha^{-2}$, where $\alpha = (j + \sqrt{j^2 - 4})/2$; so $\alpha + \alpha^{-1} = j$, and the square root of α can be fixed so that $\alpha^{1/2} + \alpha^{-1/2} = \sqrt{j+2}$. Then, by applying the difference of two squares to the numerator and denominator of (36), it follows that

$$s_k(j^2 - 2) = \left(\frac{\alpha^{(2k+1)/2} + \alpha^{-(2k+1)/2}}{\alpha^{1/2} + \alpha^{-1/2}} \right) \left(\frac{\alpha^{(2k+1)/2} - \alpha^{-(2k+1)/2}}{\alpha^{1/2} - \alpha^{-1/2}} \right) \tag{44}$$

which is the factorization (41) with $r_k(j)$ and $s_k(j)$ given by making the replacement $n \to j$ in (34). (For an alternative expression for these factors, see (55) in Remark 16 below.) Each of the factors above is a linear combination of kth powers of the characteristic roots α, α^{-1}, and $r_k(j) = (-1)^k s_k(-j)$ as in (14), so they each satisfy the same recurrence (42) with an appropriate set of initial values. $\square$

Remark 12. Generically, the product of any two solutions of the recurrence (42) would have three characteristic roots, namely $\alpha^2, \alpha^{-2}, 1$, giving a recurrence of order 3 in (40), but the potential root 1 cancels from the product (44), giving the second-order recurrence (1) with $n = j^2 - 2$. An inductive proof of the preceding result was given by Klee in a post to the Seqfan mailing list: see [16] for details. However, the factorization (44) in the form $L^-_{2k+1}(j,1) = L^+_{2k+1}(\sqrt{j+2},1)\, L^-_{2k+1}(\sqrt{j+2},1)$ appears to be well known in the literature on Lehmer numbers; see e.g., [4] and references.[2]

Example 13. In the case $n = 7$, there is the factorization

$$s_k(7) = r_k(3)\, s_k(3),$$

where the first terms of the factor sequences are

$$\begin{aligned} (\, r_k(3)\,) &: 1, 2, 5, 13, 34, 89, 233, 610, 1597, \ldots, \\ (\, s_k(3)\,) &: 1, 4, 11, 29, 76, 199, 521, 1364, 3571, \ldots, \end{aligned}$$

which multiply together to give the terms in (13). Since both $(\, r_k(3)\,)$ and $(\, s_k(3)\,)$ are strictly increasing sequences, it follows that $s_k(7)$ is composite for all $k \geq 1$, and hence $a_7 = -1$, as asserted previously.

As a consequence of the factorization (41), one can show similarly that for all integers $j \geq 3$, the terms $s_k(j^2-2)$ are composite for $k \geq 1$, and thus $a_{j^2-2} = -1$ for all $j \geq 3$ (for full details, see the proof of Theorem 38 below). In particular, Theorem 11 accounts for all the values $n = 7, 14, 23, 34$ with $a_n = -1$ that are shown in the list (12).

The question is now whether there are other cases with $a_n = -1$, for which $n \neq j^2 - 2$ for some j. It turns out that the answer to this question is affirmative, and the first case with $a_n = -1$ that does not fit into the above pattern is $n = 110$ [15].

Example 14. The sequence $(\, s_k(110)\,)_{k \geq 0}$, beginning with

$$\begin{aligned} &1, 111, 12209, 1342879, 147704481, 16246150031, 1786928798929, \\ &196545921732159, \ldots, \end{aligned} \tag{45}$$

appears as number A298677 in the OEIS. To see that none of the terms are prime, first of all note that the sequence $(\, s_k(110) \bmod 111\,)$ is periodic with period 3: it is equivalent to the sequence (8); this observation is a special case of Lemma 27 below. Thus it is helpful to consider the three trisections $(\, s_{3k+i}(110)\,)$ for $i = 0, 1, 2$, each of which satisfy the second-order recurrence

$$s_{3(k+2)+i}(110) - 1330670\, s_{3(k+1)+i}(110) + s_{3k+i}(110) = 0, \tag{46}$$

[2] In particular, see http://primes.utm.edu/top20/page.php?id=47 for a sketch of a proof of Theorem 11.

as follows by applying the formula (39). The easiest case is $i=1$, since $s_{3k+1} \equiv 0 \pmod{111}$ for all k; so in this subsequence, the first term $111 = 3 \times 37$ is composite, and subsequent terms $147704481 = 111 \times 1330671$, $196545921732159 = 111 \times 1770683979569$, etc. are all multiples of 111. The trisection $(\, s_{3k}(110)\,)$ is the subsequence beginning with $s_0(110) = 1$, and then $s_3(110) = 1342879 = 9661 \times 139$, $s_6(110) = 1786928798929 = 116876761 \times 15289$, and by induction it can be shown that each of these terms is divisible by the corresponding one for the sequence $(\, s_{3k}(5)\,) = 1, 139, 15289, \ldots$, so that

$$s_{3k}(110) = R_{3k}(5)\, s_{3k}(5), \tag{47}$$

where the integer sequence of prefactors satisfies the third order recurrence

$$R_{3(k+3)}(5) - 12099 \left(R_{3(k+2)}(5) - R_{3(k+1)}(5) \right) - R_{3k}(5) = 0. \tag{48}$$

Similarly, for the remaining trisection, namely $(\, s_{3k+2}(110)\,)$, one has

$$s_{3k+2}(110) = R_{3k+2}(5)\, s_{3k+2}(5), \tag{49}$$

where the prefactor sequence $(\, R_{3k+2}(5)\,)$ consists of integers and satisfies the same recurrence (48). In fact, it is not necessary to consider this trisection separately, since its properties follow immediately from extending $(\, s_{3k}(110)\,)$ to $k<0$ and using the symmetry (4). These observations show that all the terms in (45) are composite for $k>0$, confirming that $a_{110} = -1$ as claimed. Moreover, for all k there is a factorization

$$s_k(110) = R_k(5)\, s_k(5), \tag{50}$$

where

$$R_{k+3}(5) - 24 \left(R_{k+2}(5) - R_{k+1}(5) \right) - R_k(5) = 0, \tag{51}$$

but the prefactors making up the full sequence $(\, R_k(5)\,)_{k\geq 0}$, that is

$$1, \frac{37}{2}, 421, 9661, \frac{443557}{2}, 5091241, 116876761, \frac{5366148517}{2}, \ldots,$$

are only integers in the cases (47) and (49), and not when $k \equiv 1 \pmod 3$.

The values of n with $a_n = -1$ mentioned so far all have one thing in common: they correspond to values of dilated Chebyshev polynomials of the first kind. Indeed, the four -1 terms displayed in (12) appear at the index values

$$7 = \mathcal{T}_2(3), \quad 14 = \mathcal{T}_2(4), \quad 23 = \mathcal{T}_2(5), \quad 34 = \mathcal{T}_2(6),$$

and Theorem (11) implies that $s_k(n)$ is composite for all $k \geq 1$ when $n = \mathcal{T}_2(j)$, $j \geq 3$, while

$$110 = \mathcal{T}_3(5).$$

It turns out that for any Chebyshev value $n = \mathcal{T}_p(j)$ with $p > 1$, there is a factorization analogous to (41) or (50): see Theorem 37 below. Due to the identity (26), it is sufficient to consider the case of prime p only.

The curious reader might wonder why the values $n = 18 = \mathcal{T}_3(3)$ and $n = 52 = \mathcal{T}_3(4)$ are missing from the discussion. The reason is that, although there is a factorization analogous to (50) for these values of n, there are the prime terms $s_1(18) = 19$ and $s_1(52) = 53$, which imply that $a_{18} = 1 = a_{52}$; but it turns out that there are no other primes in the sequences $(\, s_k(n)\,)_{k\geq 0}$ for $n = 18$ or 52. See Theorem 38 for a more general statement which includes all these Chebyshev values.

4 General properties of the defining sequences

By writing the general solution of (1) in terms of the roots of its characteristic quadratic, and using various expressions for the dilated Chebyshev polynomials, as in section 2, we immediately obtain a number of equivalent explicit formulae for the sequence $(\, s_k(n)\,)$.

Proposition 15. *The terms of the sequence generated by (1) with the initial values (2) are given explicitly by*

$$s_k(n) = \frac{\lambda^{k+1} - \lambda^{-k}}{\lambda - 1} = \mathcal{U}_{k-1}(n) + \mathcal{U}_k(n), \tag{52}$$

where λ is given in terms of n according to (20), and by

$$s_k(n) = \mathcal{U}_{2k}(\sqrt{n+2}) = \frac{\sin\Big((2k+1)\theta/2\Big)}{\sin(\theta/2)}, \tag{53}$$

and they have the generating function

$$G(X, n) := \sum_{j=0}^{\infty} s_j(n)\, X^j = \frac{1 + X}{1 - nX + X^2}. \tag{54}$$

Proof. The first formula in (52) is equivalent to (36), with $\lambda = \alpha^2$, and the other one follows by rewriting the Chebyshev polynomials as linear combinations of λ^k and λ^{-k}, which generically provide two independent solutions of (1).[3] For the latter set of identities, let $m = \sqrt{n+2}$, and note that $\mathcal{T}_2(m) = n$, so θ can always be chosen such that $m = 2\cos(\theta/2)$. The expression on the far right-hand side of (53) is obtained by by applying (23) to the last equality in (52), or by setting $\alpha = e^{\mathrm{i}\theta/2}$ in (36), and this expression equals $\mathcal{U}_{2k}(2\cos(\theta/2)) = \mathcal{U}_{2k}(m)$. The generating function (54) follows from using the first formula in (52) and summing a pair of geometric series. $\square$

[3] The first equality is invalid when $n = \pm 2$, due to repeated roots $\lambda = \lambda^{-1} = \pm 1$, cf. (10) and (11).

Remark 16. The last formula in (52) together with (14) shows that the terms on the right-hand side of the factorization (41) in the case $n = \mathcal{T}_2(j) = j^2 - 2$ can also be written as

$$r_k(j) = \mathcal{U}_k(j) - \mathcal{U}_{k-1}(j), \qquad s_k(j) = \mathcal{U}_k(j) + \mathcal{U}_{k-1}(j). \tag{55}$$

If $5/2 < n \in \mathbb{R}$ then $\lambda > 2$, so $\lambda^{-k}/(\lambda - 1) < 1$ for all $k \geq 0$, and so we have

Corollary 17. *For all real $n > 5/2$, the terms $s_k(n)$ for $k \geq 0$ are given by*

$$s_k(n) = \left\lfloor \frac{\lambda^{k+1}}{\lambda - 1} \right\rfloor.$$

The recurrence (1) can also be rewritten in matrix form, as

$$\mathbf{v}_j = \mathbf{A}\,\mathbf{v}_{j-1}, \tag{56}$$

where

$$\mathbf{A} = \begin{pmatrix} 0 & 1 \\ -1 & n \end{pmatrix}, \qquad \mathbf{v}_j = \begin{pmatrix} s_j(n) \\ s_{j+1}(n) \end{pmatrix},$$

hence for all j the terms of the sequence are given in terms of the powers of $\mathbf{A}$ by

$$\mathbf{v}_j = \mathbf{A}^j\,\mathbf{v}_0.$$

By a standard method of repeated squaring, this allows rapid calculation of the terms of the sequence.

Proposition 18. *The jth power of the matrix $\mathbf{A}$ is given explicitly by*

$$\mathbf{A}^j = \begin{pmatrix} -\mathcal{U}_{j-2}(n) & \mathcal{U}_{j-1}(n) \\ -\mathcal{U}_{j-1}(n) & \mathcal{U}_j(n) \end{pmatrix}, \tag{57}$$

and this can be calculated in $O(\log j)$ steps.

Proof. The formula (57) follows by induction, noting that the columns of the matrix on the right-hand side satisfy the same recurrence (56) as the vector $\mathbf{v}_j$, and it is trivially true for $j = 0$. To calculate the powers of $\mathbf{A}$ quickly, compute the binary expansion $j = \sum_{i=0}^{d-1} b_i\, 2^i$, where $b_{d-1} = 1$ and $d = \log_2 j + 1$ is the number of bits, then use repeated squaring to obtain the sequence $\tilde{\mathbf{A}}_i = \mathbf{A}^{2^i}$ for $i = 0, 1, \ldots, d-1$, and finally evaluate $\mathbf{A}^j = \prod_{i=0}^{d-1} \tilde{\mathbf{A}}_i^{b_i}$. $\square$

There are other useful representations for the terms $s_k(n)$, two of which we record in the following

Proposition 19. *For $k \geq 0$, the terms of the sequence $(\, s_k(n)\,)$ admit the expansion*

$$s_k(n) = \sum_{i=0}^{\lfloor \frac{k}{2} \rfloor} (-1)^i \binom{k-i}{i} n^{k-2i} + \sum_{i=0}^{\lfloor \frac{k-1}{2} \rfloor} (-1)^i \binom{k-i-1}{i} n^{k-2i-1} \tag{58}$$

in powers of n, and the expansion

$$s_k(n) = \frac{1}{2}\mathcal{T}_0(n) + \sum_{i=1}^{k} \mathcal{T}_i(n) \tag{59}$$

in terms of dilated Chebyshev polynomials of the first kind.

Proof. The first expansion (58) follows from the expression on the far right-hand side of (52), together with equation (28). The second expansion (59) corresponds to a standard identity for the Dirichlet kernel; it can be proved by noting that dilated first/second kind Chebyshev polynomials are related via the identity $\mathcal{T}_k(n) = 2\mathcal{U}_k(n) - n\mathcal{U}_{k-1}(n)$, which is easily verified. Taken together with the recurrence (22), as well as the last expression in (52), this gives

$$s_k(n) - s_{k-1}(n) = \mathcal{T}_k(n). \tag{60}$$

Thus the expansion (59) is obtained by starting from $s_0 = 1 = \frac{1}{2}\mathcal{T}_0$ and then taking the telescopic sum of the first difference formula (60). □

Remark 20. A different form of series expansion for the airfoil polynomials of the second kind is given in [5].

Proposition 21. *For any odd integer p,*

$$s_{k+p}(n) - s_k(n) = \mathcal{T}_{k+\frac{p+1}{2}}(n)\, s_{(p-1)/2}(n). \tag{61}$$

Proof. This follows from the trigonometric expression on the far right-hand side of (53), by applying the addition formula (23). □

Remark 22. The formula (60) is the particular case $p = 1$ of the above identity.

Proposition 23. *Any decimation* $(\, s_{i+dk}(n)\,)$ *of the sequence of order d, satisfies the linear recurrence*

$$s_{i+d(k+1)}(n) - \mathcal{T}_d(n)\, s_{i+dk}(n) + s_{i+d(k-1)}(n) = 0. \tag{62}$$

Proof. By the first formula for $s_k(n)$ in (52), the terms of the decimated sequence can be written as linear combinations of kth powers of λ^d and λ^{-d}, so from the formula (39) we find

$$\Big(\mathrm{S}^2 - (\lambda^d + \lambda^{-d})\,\mathrm{S} + 1\Big)\, s_{i+dk}(n) = 0,$$

and by using (20) we see that $\lambda^d + \lambda^{-d} = 2\cos(d\theta) = \mathcal{T}_d(n)$, which verifies (62). □

It is worth highlighting some particular cases of the preceding two results, namely the formulae

$$s_{2j}(n) + 1 = s_j(n)\,\mathcal{T}_j(n), \qquad s_{2j+1}(n) - 1 = s_j(n)\,\mathcal{T}_{j+1}(n), \tag{63}$$

of which the first arises by setting $i = 0$, $k = 1$, $d = j$ in (62), while the second comes from taking $k = 0$, $p = 2j + 1$ in (61). For primality testing of a number q, it is often useful to have a factorization, or a partial factorization, of either $q - 1$ or $q + 1$ [2, 22], and each of the identities in (63) also has an analogue where the sign of the ± 1 term on the left-hand side is reversed.

Proposition 24. *For any integer j,*

$$s_{2j}(n) - 1 = (n+2)\, r_j(n)\, \mathcal{U}_{j-1}(n), \qquad s_{2j+1}(n) + 1 = (n+2)\, r_j(n)\, \mathcal{U}_j(n). \tag{64}$$

Proof. For the first identity in (64), using $\lambda = \alpha^2$ with $\alpha = e^{\mathrm{i}\theta/2}$ and $n = \lambda + \lambda^{-1}$ yields $n+2 = (\alpha + \alpha^{-1})^2$, and then from (37) and the definition of the dilated Chebyshev polynomials of the second kind it follows that $(n+2)r_j(n)\mathcal{U}_{j-1}(n)$ is equal to

$$(\alpha + \alpha^{-1})^2 \left(\frac{\alpha^{2j+1} + \alpha^{-(2j+1)}}{\alpha + \alpha^{-1}} \right) \left(\frac{\alpha^{2j} - \alpha^{-2j}}{\alpha^2 - \alpha^{-2}} \right) = \left(\frac{\alpha^{4j+1} - \alpha^{-(4j+1)}}{\alpha - \alpha^{-1}} \right) - 1$$

which is precisely $s_{2j}(n) - 1$, by (36). The proof of the second identity is similar. □

Another basic fact we shall use is that, with a suitable restriction on n, $s_k(n)$ is monotone increasing with k.

Proposition 25. *For each real $n \geq 2$, the sequence $(\, s_k(n)\,)$ is strictly increasing, and grows exponentially with leading order asymptotics*

$$s_k(n) \sim \frac{1}{2} \left(1 + \sqrt{\frac{n+2}{n-2}} \right) \left(\frac{n + \sqrt{n^2 - 4}}{2} \right)^k \qquad as \quad k \to \infty,$$

for all $n > 2$.

Proof. For real $n \geq 2$, from (20) we can set

$$\tau = \mathrm{i}\theta = \log \left(\frac{n + \sqrt{n^2 - 4}}{2} \right),$$

which defines a bijection from the interval $n \in [2, \infty)$ to $\tau \in [0, \infty)$. The inverse is

$$n = 2\cosh\tau \implies \frac{\mathrm{d}n}{\mathrm{d}\tau} = 2\sinh\tau > 0,$$

and we have

$$\mathcal{T}_k(n) = 2\cosh(k\tau) \implies \frac{\mathrm{d}}{\mathrm{d}\tau} \mathcal{T}_k(n) = 2k\sinh(k\tau) > 0$$

for $\tau > 0$; hence, for all fixed k, $\mathcal{T}_k(n)$ is a strictly increasing function of n for $n \geq 2$. Similarly, $\frac{\mathrm{d}}{\mathrm{d}k} \mathcal{T}_k(n) = 2\tau\sinh(k\tau)$ so for all fixed $n > 2$, the sequence $(\, \mathcal{T}_k(n)\,)_{k \geq 0}$ is also strictly increasing with k. Then since $\mathcal{T}_k(2) = 2$ for all k, it follows that, for all k,

$$\mathcal{T}_k(n) \geq 2 \qquad \forall n \geq 2, \tag{65}$$

so from (60) we have

$$s_k(n) - s_{k-1}(n) \geq 2.$$

Upon taking the leading term of the explicit expression in terms of λ in (52) and rewriting it as a function of n, the asymptotic formula results. □

We can now use the explicit formulae above to derive various arithmetical properties of the integer sequences defined by $s_k(n)$ for positive integers n. This will culminate in Lemma 29 below, which describes coprimality conditions on the terms, as well as Lemma 32 and its corollaries, which constrain where particular prime factors can appear. To begin with we describe where primes can appear in the sequence.

Lemma 26. *For all integers $n \geq 2$, if $s_k(n)$ is prime then $k = (p-1)/2$ for p an odd prime.*

Proof. If $2k+1 = ab$ is composite, for some odd integers $a, b \geq 3$, then the identity (27) can be applied to the middle expression in (53), to write $s_k(n)$ as the product

$$\begin{aligned} s_k(n) &= \mathcal{U}_{a-1}\left(\mathcal{T}_b(\sqrt{n+2})\right)\mathcal{U}_{b-1}(\sqrt{n+2}) \\ &= s_{(a-1)/2}\left(\mathcal{T}_b(\sqrt{n+2})^2 - 2\right)\, s_{(b-1)/2}(n). \end{aligned}$$

Then, since $\mathcal{T}_2(j) = j^2 - 2$, by using (26) we have

$$\begin{aligned} s_k(n) &= s_{(a-1)/2}\left(\mathcal{T}_{2b}(\sqrt{n+2})\right)\, s_{(b-1)/2}(n) \\ &= s_{(a-1)/2}\left(\mathcal{T}_b(n)\right)\, s_{(b-1)/2}(n), \end{aligned} \tag{66}$$

and each factor above is an integer greater than 1. $\square$

Henceforth we will consider only integer values of n. It is well known that all linear recurrence sequences defined over $\mathbb{Z}$ are eventually periodic mod m for any modulus m [32]; and for the recurrence (1) we can say further that it is strictly periodic mod m, because the linear map $(s_k, s_{k+1}) \mapsto (s_{k+1}, s_{k+2})$ defined by the matrix $\mathbf{A}$ in (56) is always invertible mod m (since $\det \mathbf{A} = 1$). However, in order to obtain coprimality conditions, we need a lemma that explicitly describes the periodicity of the terms $s_k(n) \bmod s_j(n)$ for fixed j.

Lemma 27. *For all integers $n \geq 2$ and any odd number $p \geq 3$, the sequence of residues $s_k(n) \bmod s_{(p-1)/2}(n)$ is periodic with period p, and $s_k(n) \equiv 0 \pmod{s_{(p-1)/2}(n)}$ if and only if $k \equiv (p-1)/2 \pmod{p}$.*

Proof. The identity (61) implies that, for all k,

$$s_{k+p}(n) \equiv s_k(n) \pmod{s_{(p-1)/2}(n)},$$

so the residues repeat with period p. By the monotonicity result in Proposition 25,

$$1 = s_0(n) < s_1(n) < \cdots < s_{(p-3)/2}(n) < s_{(p-1)/2}(n).$$

Then the symmetry (4) implies that the residues mod $s_{(p-1)/2}(n)$ are non-zero in the range $-(p-1)/2 \leq k \leq (p-3)/2$, so the rest of the statement follows from the periodicity. $\square$

Lemma 28. *For each integer $n \geq 2$ and any odd integer $p \geq 3$, $s_k(n)$ is coprime to $s_{(p-1)/2}(n)$ if and only if $(p-1)/2 - k$ is coprime to p.*

Proof. Once again, we drop the argument n for the purposes of the proof, and perform induction on the odd integers $p \geq 3$. With p fixed, for each k it will be convenient to consider

$$m = (p-1)/2 - k. \tag{67}$$

For the base case $p = 3$, note that the sequence of $s_k \bmod s_1$ repeats with period 3, by Lemma 27, and clearly $\gcd(s_0, s_1) = 1 = \gcd(s_{-1}, s_1)$ so the pattern is $s_k \equiv -1, 1, 0 \pmod{s_1}$ for $k \equiv -1, 0, 1 \pmod 3$; hence $\gcd(s_k, s_1) = 1$ if and only if the quantity $m = 1 - k \not\equiv 0 \pmod 3$, which is the required result in this case. Now we will assume that the result is true for all odd q with $3 \leq q < p$, and proceed to show that it is true for p.

Firstly, if for some k the corresponding value of m, given by (67), is not coprime to p, then there is some odd q with $3 \leq q \leq p$, $q|m$ and $q|p$. Therefore we have

$$(q-1)/2 - k = (q-p)/2 + m \equiv (q-p)/2 \equiv 0 \pmod q.$$

So by Lemma 27, both $s_k \equiv 0 \pmod{s_{(q-1)/2}}$ and $s_{(p-1)/2} \equiv 0 \pmod{s_{(q-1)/2}}$, hence s_k and $s_{(p-1)/2}$ are not coprime.

Thus it remains to show that

$$\gcd(m, p) = 1 \implies \gcd(s_{(p-1)/2-m}, s_{(p-1)/2}) = 1.$$

Observe that, by Lemma 27, it is sufficient to verify this for values of m between 1 and $p-1$ (i.e., the non-zero residue classes $\bmod\ p$). First consider $k = (p-1)/2 - m$ lying in the range $0 \leq k \leq (p-3)/2$: this can be written as $k = (q-1)/2$ for some odd positive integer q, and $\gcd(m, p) = 1$ is equivalent to the requirement that $\gcd(q, p) = 1$; so either $q = 1$ and $\gcd(s_0, s_{(p-1)/2}) = 1$ is trivially true, or $3 \leq q < p - 2$ and $\gcd(s_{(q-1)/2}, s_{(p-1)/2}) = 1$ holds by the inductive hypothesis. Now for the range $-(p-1)/2 \leq k \leq -1$, the result follows by the symmetry $k \to -1 - k$, using (4). Hence, by applying the shift $k \to k + p$ and using Lemma 27, the result is true for all integers k such that $\gcd((p-1)/2 - k, p) = 1$. □

In fact, it is possible to make a stronger statement about the common factors of the terms of the sequence.

Lemma 29. *For all integers $n \geq 2$ and $j, k \geq 0$,*

$$\gcd\Big(s_j(n), s_k(n)\Big) = s_m(n), \qquad \text{where} \quad 2m + 1 = \gcd(2j + 1, 2k + 1).$$

Proof. Given any j, k, suppose that $2m + 1 = \gcd(2j + 1, 2k + 1)$. The case $m = 0$ follows from Lemma 28, taking $p = 2j + 1$. If $m > 0$, then by writing $2j + 1 = (2m + 1)(2j' + 1)$, $2k + 1 = (2m + 1)(2k' + 1)$ with $\gcd(2j' + 1, 2k' + 1) = 1$, and applying (66), we have

$$\gcd\Big(s_j(n), s_k(n)\Big) = s_m(n)\ \gcd\Big(s_{j'}(\mathcal{T}_{2m+1}(n)), s_{k'}(\mathcal{T}_{2m+1}(n))\Big) = s_m(n),$$

by applying Lemma 28 once again. □

Remark 30. The preceding result is a special case of a result on the greatest common divisor of a pair of Lehmer numbers: see Lemma 3 in [29].

Remark 31. Since the argument n plays a passive role in most of the above, it is clear that, mutatis mutandis, Lemmas 27, 28 and 29 also apply to the sequence of polynomials $(\, s_k(n)\,)$ in $\mathbb{Z}[n]$. Analogous divisibility properties for the Chebyshev polynomials of the first kind are described in [23].

The preceding results allow the periodicity of the sequence modulo any prime to be described quite precisely. The notation $\left(\frac{\cdot}{\cdot}\right)$ is used below to denote the Legendre symbol.

Lemma 32. *Let $n \geq 2$ be fixed, and for any prime q let $\pi(q)$ denote the period of the sequence $(s_k(n) \bmod q)$. Then $\pi(2) = 3$ if and only if n is odd, in which case $s_k(n)$ is even $\iff k \equiv 1 \pmod 3$, while $\pi(2) = 1$ and all $s_k(n)$ are odd when n is even. Moreover, for q an odd prime, one of three possibilities can occur: (i) $\left(\frac{n^2-4}{q}\right) = \pm 1$ and $\pi(q)|q \mp 1$; (ii) $n \equiv 2 \pmod q$ and $\pi(q) = q$ with $s_k(n) \equiv 0 \pmod q \iff q|2k+1$; (iii) $n \equiv -2 \pmod q$ and $\pi(q) = 2$ with $s_k(n) \equiv (-1)^k \pmod q$.*

Proof. When n is even, then since $s_0(n) = 1$ and $s_1(n) = n+1$ are both odd, it follows from (1) that $s_k(n)$ is odd for all k, so $\pi(2) = 1$. For n odd, $s_1(n)$ is even, so by Lemma 28, $s_k(n)$ is even if and only if $k \equiv 1 \pmod 3$, and $\pi(2) = 3$.

Now let q be an odd prime. For case (i) it is most convenient to consider the behaviour of $(s_k \bmod q)$ in terms of the equivalent sequence defined by the recurrence (1) in the finite field $\mathbb{F}_q$. In that case we have $n > 2$, and when $\left(\frac{n^2-4}{q}\right) = 1$ it follows that n^2-4 is a quadratic residue mod q, so the first formula in (52), which can be rewritten as

$$s_k(n) = \frac{\lambda^{-k}(\lambda^{2k+1}-1)}{\lambda - 1}, \tag{68}$$

remains valid in terms of $\lambda \in \mathbb{F}_q$, with $\lambda \neq \pm 1$, and $\lambda^{q-1} = 1$ in $\mathbb{F}_q$ by Fermat's little theorem. The terms of the sequence repeat with period $\pi(q) = \mathrm{ord}(\lambda) > 2$, the multiplicative order of λ in the group $\mathbb{F}_q^*$, and this divides $q-1$ by Lagrange's theorem. The case $\left(\frac{n^2-4}{q}\right) = -1$ is similar, but now n^2-4 is a quadratic nonresidue mod q, so λ is not defined in $\mathbb{F}_q$ and the formula (68) should be interpreted in the field extension $\mathbb{F}_q[\sqrt{n^2-4}] \simeq \mathbb{F}_{q^2}$. The Frobenius automorphism $\lambda \to \lambda^q$ exchanges the roots of the quadratic $X^2 - n\,X + 1 = (X-\lambda)(X-\lambda^{-1})$, hence $\lambda^q = \lambda^{-1}$. Thus $\lambda^{q+1} = 1$, and now the sequence given by (68) repeats with period $\pi(q) = \mathrm{ord}(\lambda)$, the order of λ in $\mathbb{F}_{q^2}^*$, which divides $q+1$. In case (ii), the sequence $s_k(n) \bmod q$ is the same as the sequence (10) mod q, which first vanishes when $k = (q-1)/2$ and repeats with period q, and in case (iii) the sequence is equivalent to (11), which is never zero mod q. $\square$

At this stage it is convenient to introduce the notion of a primitive prime divisor (sometimes just referred to as a primitive divisor), which is a prime factor q that divides $s_k(n)$ but does not divide any of the previous terms in the sequence [10], and by convention does not divide the discriminant n^2-4 either [1, 26].

Definition 33. Let the product of the discriminant and the first k terms be denoted by

$$\Pi_k(n) = (n^2 - 4)\, s_1(n)s_2(n)\cdots s_k(n). \tag{69}$$

A *primitive prime divisor* of $s_k(n)$ is a prime $q|s_k(n)$ such that $q \not| \Pi_{k-1}(n)$.

Case (i) of Lemma 32 is the most interesting one. In that case it is clear from (68) that a prime $q|s_k(n)$ for some k whenever $\lambda^{2k+1} = 1$ in $\mathbb{F}_{q^2} \supset \mathbb{F}_q$, and then $\pi(q) = \mathrm{ord}(\lambda) = 2k^* + 1$ must be odd, where $k^* = (\pi(q) - 1)/2 > 0$ is the smallest k for which this happens; and if $\pi(q)$ is even then this cannot happen. If we include $q = 2$, then we can rephrase the latter by saying that the prime factors q appearing in the sequence $(\, s_k(n)\,)$ are precisely those q which have an odd period $\pi(q) > 1$, and this consequence of Lemma 32 can be restated in terms of primitive prime divisors.

Corollary 34. *A prime q is a primitive divisor of $s_k(n)$ if and only if $k = (\pi(q) - 1)/2$ where $\pi(q)$ is odd. Moreover, if q is odd and $\left(\frac{n^2-4}{q}\right) = \pm 1$ then $q = 2a\pi(q) \pm 1$ for some positive integer a.*

The latter statement just says that an odd primitive divisor of $s_k(n)$ has the form $q = 2a(2k+1)\pm 1$ for some $a \geq 1$, so the minus sign with $a = 1$ gives the lower bound $q \geq 4k+1$. Hence the primes that do not appear as factors in the sequence can also be characterized.

Corollary 35. *If a prime $q < 4k + 1$ is not a factor of $\Pi_{k-1}(n)$, then it never appears as a factor of $s_j(n)$ for $j \geq k$, and $\pi(q)$ is even.*

So far we have concentrated on properties of $s_k(n)$ for fixed n and allowed k to vary. However, if one is interested in finding factors of $s_k(n)$ for large n, then it may also be worthwhile to consider other values of n, as the following result shows.

Proposition 36. *Suppose that an integer $f|s_k(n)$ for some k, n. Then $f|s_k(m)$ whenever $m \equiv n \pmod f$.*

Proof. If $m \equiv n \pmod f$ then $m^j \equiv n^j \pmod f$ for any exponent $j \geq 0$, and since $s_k(m)$ is a polynomial in m with integer coefficients, it follows that $s_k(m) \equiv s_k(n) \equiv 0 \pmod f$, as required. $\square$

5 Generic factorization for Chebyshev values

The sequence $(\, s_k(n)\,)$ has special properties when n is given by a dilated Chebyshev polynomial of the first kind evaluated at an integer value of the argument.

Theorem 37. *For all integers $p \geq 2$, when $n = \mathcal{T}_p(j)$ for some integer j the terms of the sequence $(\, s_k(n)\,)$ can be factorized as a product of rational numbers, that is*

$$s_k(\mathcal{T}_p(j)) = R_k(j)\, s_k(j), \tag{70}$$

where the prefactors $R_k(j) \in \mathbb{Q}$ are given by

$$R_k(j) = \frac{\mathcal{U}_{p-1}(\mathcal{T}_{2k+1}(\sqrt{j+2}))}{\mathcal{U}_{p-1}(\sqrt{j+2})} \tag{71}$$

and satisfy a linear recurrence of order p. In particular, for $p = 2$ the prefactor is $R_k(j) = r_k(j) \in \mathbb{Z}$, as given in Theorem 11, while for all odd p the prefactor can be written as

$$R_k(j) = \frac{s_{(p-1)/2}(\mathcal{T}_{2k+1}(j))}{s_{(p-1)/2}(j)} \in \mathbb{Q}, \tag{72}$$

and satisfies the recurrence

$$(\mathrm{S} - 1) \prod_{i=1}^{(p-1)/2} (\mathrm{S}^2 - \mathcal{T}_{2i}(j)\,\mathrm{S} + 1)\, R_k(j) = 0. \tag{73}$$

Proof. Upon introducing ϕ such that $\ell = \sqrt{j+2} = 2\cos(\phi/2)$, the formula (53) gives

$$R_k(j) = \frac{s_k(\mathcal{T}_p(j))}{s_k(j)} = \frac{\sin\Big((2k+1)p\phi/2\Big)\sin(\phi/2)}{\sin(p\phi/2)\sin\Big((2k+1)\phi/2\Big)},$$

and the definition of the dilated Chebyshev polynomials of the second kind in (21) produces (71). For integer j, $R_k(j)$ is a ratio of integers, so it is a rational number (positive for $j \geq 2$). In the case $p = 2$, $R_k(j) = r_k(j)$, which can be written in the form

$$r_k(j) = \frac{\mathcal{T}_{2k+1}(\sqrt{j+2})}{\sqrt{j+2}}, \tag{74}$$

which is an integer, as follows from the fact that $\mathcal{U}_1(\ell) = \ell$, and this ratio is an even polynomial of degree $2k$ in ℓ with integer coefficients, hence it is a polynomial of degree k in j; and by (65) it is positive for real $j \geq 2$, and takes positive integer values for integers j in this range. In the case that p is odd, the expression (72) is found by applying the formula (53) to the numerator and denominator of (71).

To see that $R_k(j)$ satisfies a linear recurrence of order p, note that, upon setting $\mu = \exp(\mathrm{i}\phi)$ and applying the first formula in (52) with $\lambda = \mu^p$, the factorization (70) can be seen as a consequence of the elementary algebraic identity

$$\frac{\mu^{p(k+1)} - \mu^{-pk}}{\mu^p - 1} = \left(\frac{\sum_{j=0}^{p-1} \mu^{(k+1)(p-1)-(2k+1)j}}{\mu^{p-1} + \mu^{p-2} + \cdots + 1}\right)\left(\frac{\mu^{k+1} - \mu^{-k}}{\mu - 1}\right), \tag{75}$$

where the first factor on the right-hand side above is just $R_k(j)$. Thus the denominator of the expression for $R_k(j)$ in (75) is $\sum_{j=0}^{p-1} \mu^j$, which is independent of k, while the numerator is a linear combination of kth powers of the characteristic roots $\mu^{(p-1)}, \mu^{(p-3)}, \ldots, \mu^{-(p-3)}, \mu^{-(p-1)}$, giving a total of p distinct roots. When p is even, the roots come in $p/2$ pairs, namely $\mu^{\pm(2i-1)}$ for $i = 1, \ldots, p/2$, which gives the characteristic polynomial

$$F(\lambda) = \prod_{i=1}^{p/2} (\lambda^2 - \mathcal{T}_{2i-1}(j)\lambda + 1),$$

so that, in particular, for $p = 2$ the recurrence satisfied by $R_k(j)$ is (42), while for p odd there are the pairs $\mu^{\pm 2i}$ for $i = 1, \ldots, (p-1)/2$ together with the root 1, which yields (73). □

Theorem 38. *Let $(a_n)_{n\geq 1}$ be the sequence specified by Definition 1. If $n = \mathcal{T}_2(j)$ for some $j \geq 3$, then $a_n = -1$. Furthermore, if $n = \mathcal{T}_p(j)$ for some $j \geq 3$ with p an odd prime, then either $s_{(p-1)/2}(n)$ is not prime and $a_n = -1$, or $s_{(p-1)/2}(n)$ is the only prime in the sequence $(\, s_k(n)\,)_{k\geq 0}$ and $a_n = (p-1)/2$.*

Proof. First of all, consider the factorization (70) when $p = 2$, with prefactor $r_k(j)$ as in Theorem 11, given by (74). When $j = 2$ this is not interesting, because it gives $r_k(j) = 1$ for all j. However, note the property (mentioned in passing in the proof of Proposition 25), that for real $n > 2$, the sequence $(\, \mathcal{T}_k(n)\,)_{k\geq 0}$ is strictly increasing with the index. Hence, for all $k > 0$, $\mathcal{T}_{2k+1}(\sqrt{j+2}) > \sqrt{j+2} = \mathcal{T}_1(\sqrt{j+2})$. Thus for all $j \geq 3$ and $k \geq 1$, both factors $r_k(j)$, $s_k(j)$ are greater than 1, so $s_k(T_2(j))$ can never be prime, and $a_n = -1$.

Now for any odd prime p, note that, a priori, the prefactor $R_k(j)$ in (70) is a positive rational number, and the formula (72) gives

$$s_k(\mathcal{T}_p(j)) = \frac{s_k(j)\, s_{(p-1)/2}(\mathcal{T}_{2k+1}(j))}{s_{(p-1)/2}(j)}. \tag{76}$$

However, according to Lemma 27, $s_{(p-1)/2}(j) | s_k(j)$ whenever $k \equiv (p-1)/2 \pmod p$. On the other hand, for all values of $k \not\equiv (p-1)/2 \pmod p$, Lemma 28 gives $\gcd(s_k(j), s_{(p-1)/2}(j)) = 1$. Therefore $s_{(p-1)/2}(j)$ divides $s_{(p-1)/2}(\mathcal{T}_{2k+1}(j))$ and $R_k(j) \in \mathbb{Z}$. Thus, for all k, the terms $s_k(\mathcal{T}_p(j))$ can be written as a product of two integers, that is

$$s_k(\mathcal{T}_p(j)) = \begin{cases} \hat{R}_k(j)\, s_{(p-1)/2}(\mathcal{T}_{2k+1}(j)), & \text{if } k \equiv (p-1)/2 \pmod p; \\ R_k(j)\, s_k(j), & \text{otherwise,} \end{cases} \tag{77}$$

where $R_k(j)$ is given by (72) as above, and

$$\hat{R}_k(j) = \frac{s_k(j)}{s_{(p-1)/2}(j)} = s_i(\mathcal{T}_p(j)) \quad \text{for } k = (p-1)/2 + ip, \tag{78}$$

with the latter formula being obtained from (66). In the first case of (77) above, for $k = (p-1)/2$ the prefactor is $\hat{R}_{(p-1)/2}(j) = 1$, while $\hat{R}_k(j) > 1$ for all $k = (p-1)/2 + ip$, $i \geq 1$, by Lemma 25, and the other factor is $s_{(p-1)/2}(\mathcal{T}_{2k+1}(j)) > 1$ for all these values of k. In the second case, for $k > 0$, we can use (59) together with (26) to write

$$\begin{aligned} s_{(p-1)/2}(\mathcal{T}_{2k+1}(j)) &= \tfrac{1}{2}\mathcal{T}_0 + \textstyle\sum_{i=1}^{(p-1)/2} \mathcal{T}_i(\mathcal{T}_{2k+1}(j)) \\ &= \tfrac{1}{2}\mathcal{T}_0 + \textstyle\sum_{i=1}^{(p-1)/2} \mathcal{T}_{(2k+1)i}(j) \\ &> \tfrac{1}{2}\mathcal{T}_0 + \textstyle\sum_{i=1}^{(p-1)/2} \mathcal{T}_i(j) = s_{(p-1)/2}(j), \end{aligned}$$

so $s_{(p-1)/2}(\mathcal{T}_{2k+1}(j))/s_{(p-1)/2}(j) > 1$. Hence both factors $R_k(j)$, $s_k(j)$ are greater than 1 in the second case of (77). Thus the only term that can be prime is $s_{(p-1)/2}(\mathcal{T}_p(j))$, and the result is proved. □

Remark 39. For any odd $p = 2i + 1$, the identity (76) can be rewritten in the symmetric form

$$s_i(j)\, s_k(\mathcal{T}_{2i+1}(j)) = s_k(j)\, s_i(\mathcal{T}_{2k+1}(j)). \tag{79}$$

Remark 40. Similarly to the remark after Lemma 29, the formula (77) also corresponds to factorizations of the corresponding polynomials in $\mathbb{Z}[j]$, according to whether $k \equiv (p-1)/2 \pmod{p}$ or not.

It is clear from the factorizations (77) that in the second case, $s_k(\mathcal{T}_p(j)) \equiv 0 \pmod{s_k(j)}$ whenever k is not congruent to $(p-1)/2 \mod p$. It turns out that an explicit expression for $s_k(\mathcal{T}_p(j)) \mod s_k(j)$ can be given in the first case as well. Before doing so, it is convenient to define some more polynomials, which are shifted versions of the airfoil polynomials.

Definition 41. Polynomials $\mathcal{P}_k(z)$ are defined as elements of $\mathbb{Z}[z]$ by

$$\mathcal{P}_k(z) = s_k(2 - z),$$

or equivalently by

$$\mathcal{P}_k(4\sin^2\theta) = \frac{\sin\Big((2k+1)\theta\Big)}{\sin\theta}. \tag{80}$$

They satisfy the linear recurrence

$$\mathcal{P}_{k+1}(z) + (z-2)\mathcal{P}_k(z) + \mathcal{P}_{k-1}(z) = 0, \tag{81}$$

and for $k \geq 0$ their expansion in powers of z takes the form

$$\mathcal{P}_k(z) = 2k + 1 - c_k^{(1)}\, z + c_k^{(2)}\, z^2 + \cdots + (2k+1)(-z)^{k-1} + (-z)^k. \tag{82}$$

with

$$c_k^{(1)} = \frac{k(k+1)(2k+1)}{3!}, \qquad c_k^{(2)} = \frac{k(k-1)(k+1)(2k^2+5k+2)}{5!}.$$

Theorem 42. *For all odd integers p,*

$$s_k(\mathcal{T}_p(j)) = s_i(\mathcal{T}_p(j))\,\mathcal{P}_{(p-1)/2}\Big((2-j)\,s_k(j)^2\Big) \quad \text{for} \quad k = (p-1)/2 + ip, \tag{83}$$

and in particular,

$$s_k(\mathcal{T}_p(j)) \equiv p\,s_i(\mathcal{T}_p(j)) \pmod{(j-2)\,s_k(j)^2}$$

holds in that case.

Proof. Upon setting $p = 2q+1$, by using (78) together with the first formula in (77), we have

$$\begin{aligned} s_k(\mathcal{T}_p(j))/s_i(\mathcal{T}_p(j)) &= \sin\Big((2q+1)(2k+1)\phi/2\Big)\Big/\sin\Big((2k+1)\phi/2\Big) \\ &= \mathcal{P}_q(z), \qquad \text{where} \qquad z = 4\sin^2\Big((2k+1)\phi/2\Big), \end{aligned}$$

and (with the same notation as in the proof of Theorem 37) we also have $j = 2\cos\phi$. Comparing the expressions for z and j gives $z = 4\sin^2(\phi/2)\,s_k(j)^2 = (2-j)\,s_k(j)^2$, which yields the identity (83) in terms of the shifted airfoil polynomial $\mathcal{P}_{(p-1)/2}$. The terms displayed in the expansion (82) are easily obtained from the recurrence (81), or by substituting $n = 2-z$ in (58), and the leading term gives the reduction of (83) mod $s_k(j)^2$. ◻

We now turn to the sequences $(\,r_k(n)\,)$ for $n > 0$, which are associated with negative values of n via (14). It turns out that these sequences also admit factorizations for certain Chebyshev values of n. The case of $n = \mathcal{T}_p(j)$ for odd index p can be inferred immediately from Theorem 37 together with (14), since $\mathcal{T}_p$ is an odd function of its argument in that case. However, the even case $n = \mathcal{T}_2(j)$ does not translate directly to the sequences $(\,r_k(n)\,)$, and requires a separate treatment. That there should be a significant difference for values of even Chebyshev polynomials is also apparent from comparison of the fact that $a_7 = a_{14} = a_{23} = a_{34} = -1$ in (12), but $\tilde{a}_1 = \tilde{a}_2 = \tilde{a}_{34} = -1$ in (18), while $\tilde{a}_7$, $\tilde{a}_{14}$ and $\tilde{a}_{23}$ are all positive.

The following analogue of Theorem 11 for the sequences $(\,r_k(n)\,)$ only provides a factorization of the terms for a particular subset of the values $n = \mathcal{T}_2(j)$.

Theorem 43. *When $n = \mathcal{T}_2(j) = j^2 - 2$ with $j = 2(\ell^2 - 1)$ for integer $\ell \geq 2$, the terms of the sequence $(\,r_k(n)\,)$ admit the factorization*

$$r_k(j^2 - 2) = f_k^+(j)\,f_k^-(j), \tag{84}$$

where

$$f_k^{\pm}(j) = \frac{\ell r_k(j) \pm \delta_k}{\ell \pm 1} \in \mathbb{Z}, \qquad \delta_k = (-1)^{\lfloor \frac{k+1}{2} \rfloor}. \tag{85}$$

Proof. Since $\delta_k^2 = 1$ and $r_k(j) = (j+2)^{-1/2}\left(\alpha^{(2k+1)/2} + \alpha^{-(2k+1)/2}\right)$, using $\alpha^{1/2} + \alpha^{-1/2} = \sqrt{j+2}$ as in (44), it follows that

$$\begin{aligned} f_k^+(j)\,f_k^-(j) &= (\ell^2 r_k(j)^2 - 1)/(\ell^2 - 1) = j^{-1}\Big((j+2) r_k(j)^2 - 2\Big) \\ &= \Big(\left(\alpha^{(2k+1)/2} + \alpha^{-(2k+1)/2}\right)^2 - 2\Big)/(\alpha + \alpha^{-1}), \end{aligned}$$

which coincides with the formula (37) for $r_k(n)$ with $n = j^2-2 = 4\ell^4-8\ell^2+2$ in this case. To see that each factor $f_k^{\pm}(j)$ is an integer for all k, note that $(\mathrm{S}^2-j\mathrm{S}+1)r_k(j) = 0$, and checking the sequence of signs $+1,-1,-1,+1$ for $k = 0,1,2,3$ shows that $(\mathrm{S}^2 - j\mathrm{S} + 1)\delta_k = j\delta_{k-1}$. Hence the factors in (41) each satisfy an inhomogeneous linear recurrence of second order, that is

$$f_{k+2}^{\pm}(j) - j\, f_{k+1}^{\pm}(j) + f_k^{\pm}(j) = 2(\pm\ell - 1)\delta_{k-1}. \tag{86}$$

From (85) it can be seen that

$$f_{-1}^{\pm}(j) = f_0^{\pm}(j) = 1$$

provide integer initial values for (86) in each case, so these two sequences consist entirely of integers. □

Example 44. For $\ell = 2$, the above result gives $j = \mathcal{T}_2(2\sqrt{2}) = 6$ and $n = \mathcal{T}_2(6) = 34$, with the sequence $(\, r_k(34)\,) = (\, f_k^+(6)\, f_k^-(6)\,)$ beginning

$$1, 33, 1121, 38081, 1293633, \ldots, \tag{87}$$

where the factors are

$$(\, f_k^+(6)\,):\ 1, 3, 19, 113, 657, \ldots, \qquad (\, f_k^-(6)\,):\ 1, 11, 59, 337, 1969, \ldots, \tag{88}$$

and these satisfy the inhomogeneous recurrences

$$\begin{array}{rcl} f_{k+2}^+(6) - 6\, f_{k+1}^+(6) + f_k^+(6) & = & 2(-1)^{\lfloor \frac{k}{2} \rfloor}, \\ f_{k+2}^-(6) - 6\, f_{k+1}^-(6) + f_k^-(6) & = & 6(-1)^{\lfloor \frac{k}{2} \rfloor + 1}. \end{array}$$

For the case where $n = \mathcal{T}_p(j)$ for p odd, the formula (72) can be applied, together with (14), to yield the factorization

$$r_k(\mathcal{T}_p(j)) = \tilde{R}_k(j)\, r_k(j), \tag{89}$$

where

$$\tilde{R}_k(j) = R_k(-j) = \frac{r_{(p-1)/2}(\mathcal{T}_{2k+1}(j))}{r_{(p-1)/2}(j)} \tag{90}$$

satisfies the same recurrence (73) as $R_k(j)$.

Example 45. When $n = \mathcal{T}_3(3) = 18$, the sequence $(\, r_k(18)\,)$ begins

$$1, 17, 305, 5473, 98209, 1762289, 31622993, 567451585, \ldots, \tag{91}$$

so that $\tilde{a}_{18} = 1$ since $r_1(18) = 17$ is prime. By adapting Theorem 37, the terms can be factored as

$$r_k(18) = \tilde{R}_k(3)\, r_k(3),$$

where the sequence $(\, r_k(3)\,)$ begins with

$$1, 2, 5, 13, 34, 89, 233, 610, \ldots, \tag{92}$$

and $(\, \tilde{R}_k(3)\,)$ is a sequence of rational numbers, starting with

$$1, \frac{17}{2}, 61, 421, \frac{5777}{2}, 19801, 135721, \frac{1860497}{2}, \ldots,$$

which satisfies the third order recurrence

$$\tilde{R}_{k+3}(3) - 8\left(\tilde{R}_{k+2}(3) - \tilde{R}_{k+1}(3)\right) - \tilde{R}_k(3) = 0.$$

The prefactors $\tilde{R}_k(3)$ are integers whenever $k \equiv 0$ or $2 \pmod 3$, so $r_k(3)$ divides $r_k(18)$ for all such k, while the terms of the trisection $(\, r_{3k+1}(18)\,)$ are all divisible by $r_1(18)$, which is the only prime in the sequence $(\, r_k(18)\,)_{k\geq 0}$.

Having described the situation for even Chebyshev values, and given the above example of an odd Chebyshev value, the analogue of Theorem 38 for $(\, r_k(n)\,)$ can now be stated.

Theorem 46. *Let $(\tilde{a}_n)_{n\geq 1}$ be the sequence specified by Definition 2. If $n = \mathcal{T}_2(j)$ where $j = 2(\ell^2 - 1)$ for some $\ell \geq 2$, then $\tilde{a}_n = -1$. Furthermore, if $n = \mathcal{T}_p(j)$ for some $j \geq 3$ with p an odd prime, then either $r_{(p-1)/2}(n)$ is not prime and $\tilde{a}_n = -1$, or $r_{(p-1)/2}(n)$ is the only prime in the sequence $(\, r_k(n)\,)_{k\geq 0}$ and $\tilde{a}_n = (p-1)/2$.*

Proof. For the case $n = \mathcal{T}_2(j)$, $j = 2(\ell^2 - 1)$ with $\ell \geq 2$, note that each factor in (84) is an integer, and $r_0(\mathcal{T}_2(j)) = f_0^{\pm}(j) = 1$. Now as noted in the proof of Lemma 25, for fixed argument the sequence of Chebyshev polynomials of the first kind is strictly increasing with the index $k \geq 0$, so from (74) it follows that $(\, r_k(j)\,)_{k\geq 0}$ is strictly increasing. Thus, from their explicit expressions in (85), both sequences $(\, f_k^{\pm}(j)\,)$ are strictly increasing as well. Hence, for these values of j, $r_k(\mathcal{T}_2(j))$ is composite for $k \geq 1$. Hence there are no primes in the sequence $(\, r_k(n)\,)_{k\geq 0}$ for any of these even Chebyshev values of n.

When $n = \mathcal{T}_p(j)$, $j \geq 2$ with p an odd prime, there is the factorization (89), with $\tilde{R}_k(j) \in \mathbb{Q}$ given by (90). Just as for the sequences $(\, s_k(n)\,)$, it is necessary to consider whether $k \equiv (p-1)/2 \pmod p$ or not. One can show that the analogue of Lemma 27 holds for the sequences $(\, r_k(n)\,)$, $n \geq 3$, so that when $k \equiv (p-1)/2 \pmod p$ the denominator of $\tilde{R}_k(j)$ divides $s_k(j)$; or, by using (14) together with (66), one can write the explicit factorization

$$r_k(\mathcal{T}_p(j)) = r_i(\mathcal{T}_p(j))\, r_{(p-1)/2}(\mathcal{T}_{2k+1}(j)) \qquad \text{for} \quad k = (p-1)/2 + ip, \tag{93}$$

where both integer factors above are greater than 1 for $i > 0$. On the other hand, for the case $k \not\equiv (p-1)/2 \pmod p$, one can show that the analogue of Lemma 28 also holds for the sequences $(\, r_k(n)\,)$, so in that case the denominator in (90) must divide the numerator; hence

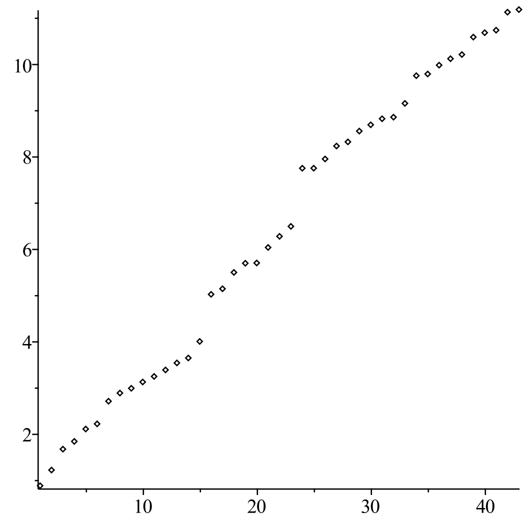

Figure 1: Plot of $\log \log s_{k_N}(n)$ against N for the first 43 primes in the sequence for $n = 3$.

$\tilde{R}_k(j) \in \mathbb{Z}$ and both factors in (89) are integers. Then, similarly to the proof of Lemma 25, setting $\sqrt{j+2} = 2\cosh\tau$ for real $j \geq 2$ in (74) gives

$$r_k(j) = \frac{\cosh((2k+1)\tau)}{\cosh\tau} \implies \frac{\mathrm{d}}{\mathrm{d}\tau} r_k(j) = \frac{2k\sinh((2k+1)\tau)}{\cosh\tau} + \frac{\sinh(2k\tau)}{\cosh^2\tau} > 0$$

for $k > 0$, $\tau > 0$, implying that $r_k(j)$ is a strictly increasing function of j for $j \geq 2$. Hence $\tilde{R}_k(j) > 1$ for $j > 2$, so when $0 < k \not\equiv (p-1)/2 \pmod{p}$, both integer factors in (89) are greater than 1. Thus $r_{(p-1)/2}(\mathcal{T}_p(j))$ is the only term that can be prime. $\square$

6 Appearance of primes for non-Chebyshev values

Theorem 38 says that for the values $n = \mathcal{T}_p(j)$ with prime p and integer $j \geq 3$, the sequence $(\, s_k(n)\,)_{k\geq 0}$ contains at most one prime term, and this can only occur if p is an odd prime, in which case $s_{(p-1)/2}(\mathcal{T}_p(j))$ is the only term that may be prime. It seems likely that these cases are exceptional, and for non-Chebyshev values of n one would expect infinitely many prime terms, in line with general heuristic arguments for linear recurrence sequences [9].

Conjecture 47. Let $n > 1$ be a positive integer. The sequence $(\, s_k(n)\,)_{k\geq 0}$ contains infinitely many primes if and only if $n \neq \mathcal{T}_p(j)$ for some prime p and some integer $j \geq 3$.

In order to consider the distribution of primes in the sequence $(\, s_k(n)\,)$, it is helpful to introduce some notation. Define a subsequence $(k_N)_{N\geq 1}$ of the positive integers by requiring that

$$s_{k_N}(n) = N\text{th prime term in } (\, s_k(n)\,)_{k\geq 0},$$

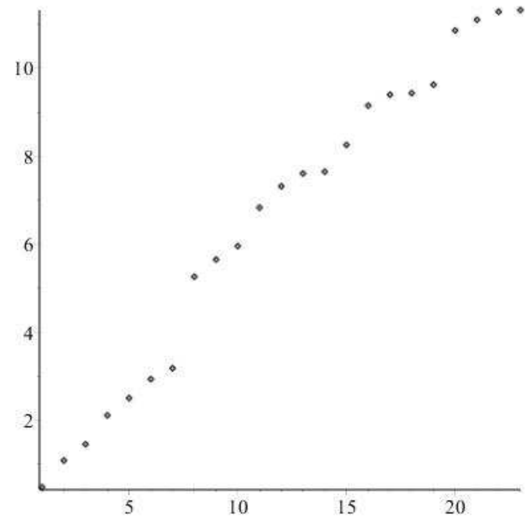

Figure 2: Plot of $\log\log s_{k_N}(n)$ against N for the first 23 primes in the sequence for $n = 4$.

and, for fixed n, let

$$\mathcal{S}_k(n) = \{ \text{prime}\, q \mid q < 4k+1 \} \cup \{ \text{prime}\, q \mid q|\Pi_{k-1}(n) \},$$

where $\Pi_{k-1}(n)$ is the product in (69).

Conjecture 48. If $n \geq 3$ and $n \neq \mathcal{T}_p(j)$ for some prime p and some integer $j \geq 3$, then, as $N \to \infty$,

$$\log\log s_{k_N}(n) \sim C\, N, \qquad \textit{with} \quad C = e^{-\gamma} \log \sqrt{\lambda}, \tag{94}$$

where $\lambda = \frac{n+\sqrt{n^2-4}}{2}$, and γ is the Euler–Mascheroni constant.

The above assertion is analogous to a conjecture of Wagstaff regarding Mersenne primes [31]. If M_N is the Nth prime of the form $2^k - 1$, then the heuristic arguments of Wagstaff suggest that

$$\log\log M_N \sim C'\, N, \qquad \text{with} \quad C' = e^{-\gamma} \log 2.$$

A very clear exposition of the statistical properties of Mersenne primes, with many plots, can be found on Caldwell's website [4].[4] When n is a non-Chebyshev value, a heuristic derivation of the corresponding asymptotics of primes in the sequences $(\, s_k(n)\,)$ can be obtained in a similar way, as we now describe.

By Lemma 26, if $s_k(n)$ is prime then $2k+1$ is prime, and by Lemma 28, $s_k(n)$ is then coprime to $s_j(n)$ for all $1 \leq j \leq k-1$, and for large enough k it is also coprime to the discriminant $n^2 - 4$, hence it is coprime to $\Pi_{k-1}(n)$. On the other hand, by Corollary 35, if $p = 2k+1$ is prime then $s_k(n)$ is coprime to all primes $q < 4k+1$: such primes are either

[4] More specifically, see the page https://primes.utm.edu/notes/faq/NextMersenne.html

primitive divisors of lower terms $s_j(n)$ with $j < k$, or they do not appear as divisors of the sequence at all. Thus no prime $q \in \mathcal{S}_k(n)$ can be a factor of $s_k(n)$ when $2k+1$ is prime. Then from the prime number theorem, for k large,

$$\mathrm{Prob}(2k+1\,\mathrm{prime}) \sim 2/\log(2k+1);$$

and, given that $2k+1$ is prime, the probability that $s_k(n)$ is prime is estimated by dividing by the probability that $s_k(n)$ is indivisible by primes q that either divide lower terms in the sequence, or are forbidden from being divisors of $s_k(n)$ due to Corollary 35, to yield

$$\begin{aligned}\mathrm{Prob}(s_k(n)\,\mathrm{prime}|2k+1\,\mathrm{prime}) &\sim \tfrac{1}{\log s_k(n)} \prod_{q\in\mathcal{S}_k(n)} \left(1-\tfrac{1}{q}\right)^{-1} \\ &\sim \tfrac{1}{k\log\lambda} \prod_{q\in\mathcal{S}_k(n)} \left(1-\tfrac{1}{q}\right)^{-1},\end{aligned}$$

where the latter expression comes from the asymptotics in Proposition 25. By multiplying these two probabilities together, and using the limit

$$\lim_{k\to\infty} \log k \prod_{\substack{q\,\mathrm{prime}\\ q\leq k}} \left(1-\frac{1}{q}\right) = e^{-\gamma},$$

which is one of Mertens' theorems (see section 22.8 in [14]), gives

$$\lim_{k\to\infty} \log(2k+1) \prod_{\substack{q\,\mathrm{prime}\\ q<4k+1}} \left(1-\frac{1}{q}\right) \prod_{\substack{\mathrm{prime}\,q\in\mathcal{S}_k(n)\\ q\geq 4k+1}} \left(1-\frac{1}{q}\right) = e^{-\gamma}$$

which produces the estimate

$$|\{\text{prime terms } s_k(n) \text{ for } 0<k\leq x\}| \sim \frac{1}{e^{-\gamma}\,\log\sqrt{\lambda}} \sum_{k\leq x} \frac{1}{k} \sim C^{-1}\log x,$$

so if $s_{k_N}(n)$ is the Nth prime term in the sequence then the formula (94) follows from taking

$$x = k_N \sim \frac{\log s_{k_N}(n)}{\log\lambda}.$$

Numerical evidence for small values of n suggests that the log log plot of the prime terms in the sequence $(\,s_k(n)\,)$ is approximately linear (see e.g., Figure 1 for the case $n=3$), and gives some support for the proposed value of C. Moreover, it is expected that the appearance of prime terms should behave like a Poisson process, in complete analogy with Wagstaff's observations on the sequence of Mersenne primes [31]. The first appendix below contains a list of the indices k for the first probable primes that appear in the sequences $(\,s_k(n)\,)$ for

$n = 3, 4, 5, 6$, and as well as including the log log plots, in each of these cases a linear best fit value of C is found, with the ratio

$$\rho(n) = \frac{C}{\log \sqrt{\lambda}}$$

being compared with the value

$$e^{-\gamma} \approx 0.561459$$

coming from Mertens' theorem.

An analogous behaviour should be observed in the sequences $(\, r_k(n)\,)$ for positive n.

Conjecture 49. Let $n > 2$ be a positive integer. The sequence $(\, r_k(n)\,)_{k\geq 0}$ contains infinitely many primes if and only if $n \neq \mathcal{T}_p(j)$ for some prime p, where the integer $j \geq 3$ takes one of values specified in Theorem 46.

The first few prime terms in the sequence $(\, r_k(3)\,)_{k\geq 0}$ are plotted in Figure 5; for more details see the first appendix.

7 Conclusions

It seems highly likely that Theorem 38 identifies all those values of $n \geq 3$ such that the sequence $(\, s_k(n)\,)_{k\geq 0}$ contains at most one prime, and Theorem 46 does the same for $(\, r_k(n)\,)_{k\geq 0}$. The sequences corresponding to all other values of n should have infinitely many prime terms, but proving this should be at least as difficult as proving that there are infinitely many Mersenne primes. For Lehmer numbers, the most sophisticated results currently available concern primitive divisors [1, 30].

The statistics of prime appearances for non-Chebyshev values of n suggests a close analogy with Mersenne primes. For Mersenne primes, the Lucas-Lehmer test is extremely efficient [3]. The ideas from [24, 25] can be adapted to yield a necessary condition for primality of $q = s_k(n)$, which can be tested efficiently, but to provide sufficient conditions requires the use of a Lucas test or one of its generalizations [2, 22], for which the formulae (63) and (64) are useful, since they provide partial factorizations of $q \pm 1$. In future we would like to consider some of the large primes that appear in these sequences, extending the approach that was applied to the case $n = 6$ in [19].

8 Acknowledgements

ANWH is supported by EPSRC fellowship EP/M004333/1. Some results in sections 3,4 and 5 of this paper were also obtained independently by Bradley Klee, who provided useful suggestions for an early draft, and has developed a graphical calculator application to verify the factorizations in Theorem 37 for particular values of p [17]. We are grateful to David Harvey, Robert Israel, Don Reble, John Roberts, Igor Shparlinski and Neil Sloane for helpful

comments. We are also extremely indebted to Hans Havermann, whose extensive numerical computations originally inspired many of the results described here.

Appendix A: Sequences of prime appearances

In order to study the appearance of prime terms when n is a non-Chebyshev value, for some particular small values of n we calculated the possible prime terms $q = s_{(p-1)/2}(n)$ when $p = 3, 5, 7, 11, \ldots$ is an odd prime, and then tested them for primality using the Maple `isprime` command. This uses a probabilistic test, which excludes certain composite values of q, while remaining q are only pseudoprimes. For all but the largest values of the index $k = (p-1)/2$, we also checked the computations with Mathematica's `PrimeQ`$[q]$ command, as well as performing a Lucas-Lehmer style test for pseudoprimes of our own, and verified that the answer was the same,

For $n = 3$, the list of the first 43 values k for which $s_k(3)$ appear to be prime is OEIS sequence A117522, beginning

$$2, 3, 5, 6, 8, 9, 15, 18, 20, 23, 26, 30, 35, 39, 56, 156, 176, 251, 306, 308, 431, 548, 680, 2393, 2396, 2925, 3870, 4233, 5345, 6125, 6981, 7224, 9734, 17724, 18389, 22253, 25584, 28001, 40835, 44924, 47411, 70028, 74045.$$

The (probable) primes $s_k(3)$ corresponding to these values of k are listed in sequence A285992. The log log plot of these terms is given in Figure 1. The slope of the best fit line for these points is

$$C = 0.2553739565.$$

For $n = 4$, the list of the first 23 values k for which $s_k(4)$ appear to be prime is

$$1, 2, 3, 6, 9, 14, 18, 146, 216, 293, 704, 1143, 1530, 1593, 2924, 7163, 9176, 9489, 11531, 39543, 50423, 60720, 62868,$$

which are listed in OEIS sequence A299100, while the corresponding values $s_k(4)$ are given in A299107. The log log plot of these terms is given in Figure 2. The best fit line for this set of points has slope

$$C = 0.5196737962.$$

For $n = 5$, the list of the first 24 values k for which $s_k(5)$ appear to be prime is

$$2, 3, 5, 6, 8, 9, 15, 18, 23, 53, 114, 194, 564, 575, 585, 2594, 3143, 4578, 4970, 9261, 11508, 13298, 30018, 54993,$$

as listed in OEIS sequence A299101, with the corresponding values of $s_k(5)$ listed as sequence A299109. The log log plot of these terms is given in Figure 3. The best fit line for this set of points has slope

$$C = 0.4568584420.$$

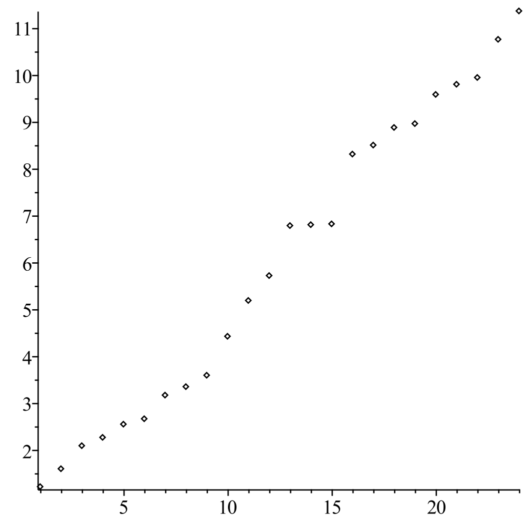

Figure 3: Plot of $\log \log s_{k_N}(n)$ against N for the first 24 primes in the sequence for $n = 5$.

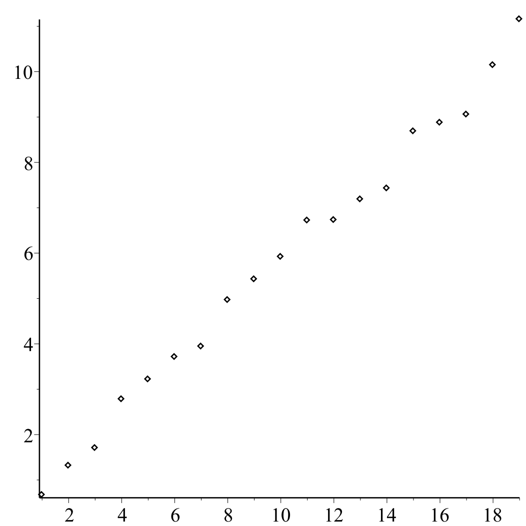

Figure 4: Plot of $\log \log s_{k_N}(n)$ against N for the first 19 primes in the sequence for $n = 6$.

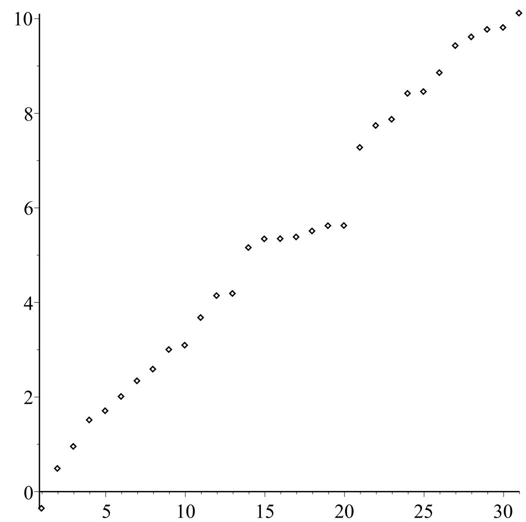

Figure 5: Plot of $\log\log r_{k_N}(n)$ against N for the first 31 primes in the sequence for $n = 3$.

For $n = 6$, the list of the first 25 values k for which $s_k(6)$ appear to be prime is

$$1, 2, 3, 9, 14, 23, 29, 81, 128, 210, 468, 473, 746, 950, 3344, 4043, 4839, 14376, \\ 39521, 64563, 72984, 82899, 84338, 85206, 86121,$$

as given in OEIS sequence A113501, with the corresponding values of $s_k(6)$ given in sequence A088165 (the prime NSW numbers [19]). In our initial submission of this paper, we obtained the first 19 of these values independently, before we were aware of sequence A113501, and made the log log plot of these terms is as in Figure 4. The best fit line for these points has slope

$$C = 0.5434911190.$$

Subsequently we found the web page [20], where the last six indices above are listed separately, together with their date of discovery by Weisstein. However, on that page it is stated unequivocally that all of the corresponding numbers $s_k(6)$ are prime, whereas presumably the largest of these values were obtained using Mathematica's probabilistic primality test, so the most that can be claimed is that they are pseudoprimes.

Assuming that the heuristic arguments given in section 6 above are correct, and that the small number of points plotted really gives an accurate picture of the behaviour for large N, the predicted values for the ratio $\rho(n) = C/\log\sqrt{\lambda}$ in each case are

$$\rho(3) \approx 0.530689,\ \rho(4) \approx 0.789203,\ \rho(5) \approx 0.583174,\ \rho(6) \approx 0.616641.$$

Apart from the case $n = 4$, all of these values are reasonably close to the number $e^{-\gamma} \approx 0.561459$ obtained from Mertens' theorem. The value for $n = 4$ seems anomalous: there are fewer prime terms than predicted in this case. However, it may be unreasonable to expect close agreement with the predicted value, given the rather small number of data points plotted in each case.

One can also consider the prime terms in the sequences $(r_k(n))$, $n \geq 3$, corresponding to negative values of n in $s_k(n)$. The list of the first 31 values k for which $r_k(3)$ appear to be prime is

$$1, 2, 3, 5, 6, 8, 11, 14, 21, 23, 41, 65, 68, 179, 215, 216, 224, 254, 284, 285, 1485, \\ 2361, 2693, 4655, 4838, 7215, 12780, 15378, 17999, 18755, 25416.$$

Figure 5 is the log log plot of these terms. Note that $(r_k(3))$ is a bisection of the Fibonacci sequence, for which the prime terms are listed as OEIS sequence A005478. The slope of the best fit line for these points is

$$C = 0.3409264905.$$

Dividing this value by $\log \sqrt{\lambda} = \log\big((1+\sqrt{5})/2\big)$ gives

$$\rho(-3) \approx 0.708475,$$

which is rather large compared with the value of $e^{-\gamma}$ expected from Mertens' theorem, suggesting that the number of primes in this sequence is initially somewhat lower than would be expected from the heuristic argument in section 6.

Appendix B: Related sequences from the OEIS

Here we briefly mention some other sequences in the OEIS which are related to the considerations in this paper.

Sequence A294099 contains the array of values $s_k(n)$ for $n \geq 1$, $k \geq 0$, while A299045 is the array of $s_k(-n)$ for the same range of n and k.

Sequence A002327 consists of primes of the form $n^2 - n - 1$, and after sending $n \to -n$ this corresponds to prime values of the polynomial $s_2(n) = n^2 + n - 1$, for which the relevant values of n are given by sequence A045546.

Sequence A000032 begins

$$2, 1, 3, 4, 7, 11, 18, 29, 47, \ldots,$$

and consists of the Lucas numbers denoted $\ell_k^+(1, -1)$ in section 2, which satisfy the Fibonacci recurrence $\ell_{k+2}^+(1,-1) = \ell_{k+1}^+(1,-1) + \ell_k^+(1,-1)$. This coincides with an interlacing of two sequences, namely

$$\mathcal{T}_0(3), s_0(3), \mathcal{T}_1(3), s_1(3), \mathcal{T}_2(3), s_2(3), \mathcal{T}_3(3), \ldots,$$

so its two distinct bisections are $(\mathcal{T}_k(3))$ and $(s_k(3))$, given by A005248 and A002878 respectively. Similarly, the Fibonacci sequence A000045 itself coincides with the interlacing

$$\mathcal{U}_{-1}(3), r_0(3), \mathcal{U}_0(3), r_1(3), \mathcal{U}_1(3), r_2(3), \mathcal{U}_2(3), \ldots$$

obtained from $(\mathcal{U}_k(3))$ and $(r_k(3))$, given by A001906 and A001519 respectively.

There are other values of n for which the OEIS entry for the sequence of terms $s_k(n)$ has not been mentioned so far: $(s_k(4))_{k\geq 0}$ is A001834, $(s_k(5))_{k\geq 0}$ is A030221, $(s_k(7))_{k\geq 0}$ is A033890, $(s_k(8))_{k\geq 0}$ is A057080, and $(s_k(9))_{k\geq 0}$ is A057081.

A008865 is the sequence of values of $\mathcal{T}_2(j)$ for $j = 1, 2, 3, \ldots$; the array of values $\mathcal{T}_k(n)$ for $k \geq 1$, $n \geq 1$ is rendered as sequence A298675. The values $\mathcal{T}_p(n)$ for prime p are listed in sequence A298878, while the values $\mathcal{T}_p(n)$ with p an odd prime which are not also of the form $\mathcal{T}_2(m)$ for some m are given in A299071.

References

[1] Yu. Bilu, G. Hanrot, and P. M. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers, With an appendix by M. Mignotte, *J. Reine Angew. Math.* **539** (2001), 75–122.

[2] J. Brillhart, D. H. Lehmer, and J. L. Selfridge, New primality criteria and factorizations of $2^m \pm 1$, *Math. Comp.* **29** (1975), 620–647.

[3] J. W. Bruce, A really trivial proof of the Lucas-Lehmer primality test, *Amer. Math. Monthly* **100** (1993), 370–371.

[4] C. K. Caldwell, The Prime Pages, http://primes.utm.edu/

[5] R. N. Desmarais and S. R. Bland, *Tables of Properties of Airfoil Polynomials*, NASA Reference Publication **1343**, 1995.

[6] A. Dubickas, A. Novikas, and J. Šiurys, A binary linear recurrence of composite numbers, *J. Number Theory* **130** (2010), 1737–1749.

[7] P. F. Duvall and J. C. Mortick, Decimation of periodic sequences, *SIAM J. Appl. Math.* **21** (1971), 367–372.

[8] H. Dym and H. P. McKean, *Fourier Series and Integrals*, Academic Press, 1972.

[9] G. Everest, A. van der Poorten, I. Shparlinski, and T. Ward, *Recurrence Sequences*, AMS Mathematical Surveys and Monographs, vol. 104, American Mathematical Society, 2003.

[10] G. Everest, S. Stevens, D. Tamsett, and T. Ward, Primes generated by recurrence sequences, *Amer. Math. Monthly* **114** (2007), 417–431.

[11] R. L. Graham, A Fibonacci-like sequence of composite integers, *Math. Mag.* **37** (1964), 322–324.

[12] R. L. Graham, D. E. Knuth and O. Patashnik, *Concrete Mathematics*, 2nd edition, Addison-Wesley, 1994.

[13] J. Griffiths, Identities connecting the Chebyshev polynomials, *Math. Gaz.* **100** (2016), 450–459.

[14] G. H. Hardy and E. M. Wright, *Introduction to the Theory of Numbers*, 4th edition, Oxford University Press, 1975.

[15] H. Havermann, L. E. Jeffery, B. Klee, D. Reble, R. G. Selcoe, and N. J. A. Sloane, Information about A269254, available at `https://oeis.org/A269254/a269254.txt` .

[16] B. Klee, submission to the SeqFan mailing list, October 2017, `http://list.seqfan.eu/pipermail/seqfan/2017-October/018016.html`.

[17] B. Klee, Factoring the even trigonometric polynomials of A269254, `http://demonstrations.wolfram.com/` .

[18] J. C. Mason and D. C. Handscomb, *Chebyshev Polynomials*, Chapman & Hall/CRC, 2002.

[19] M. Newman, D. Shanks, and H. C. Williams, Simple groups of square order and an interesting sequence of primes, *Acta Arith.* **38** (1980), 129–140.

[20] NSW Number, `http://mathworld.wolfram.com/NSWNumber.html` .

[21] F. W. J. Olver, A. B. Olde Daalhuis, D. W. Lozier, B. I. Schneider, R. F. Boisvert, C. W. Clark, B. R. Miller, and B. V. Saunders, eds., NIST Digital Library of Mathematical Functions. Available at `http://dlmf.nist.gov/`, Release 1.0.17 of 2017-12-22.

[22] C. Pomerance, Primality testing: variations on a theme of Lucas, *Congr. Numer.* **201** (2010), 301–312.

[23] M. Rayes, V. Trevisan, and P. Wang, Factorization properties of Chebyshev polynomials, *Comput. Math. Appl.* **50** (2005), 1231–1240.

[24] Ö.J. Rödseth, A note on primality tests for $N = h \cdot 2^n - 1$, *BIT* **34** (1994), 451–454.

[25] A. Rotkiewicz and R. Wasén, Lehmer's numbers, *Acta Arith.* **36** (1980), 203–217.

[26] A. Schinzel, On primitive prime factors of Lehmer numbers I, *Acta Arith.* **8** (1963), 213–223.

[27] N. J. A. Sloane, The Online Encyclopedia of Integer Sequences, `https://oeis.org/` .

[28] L. Somer, Second-order linear recurrences of composite numbers, *Fibonacci Quart.* **44** (2006), 358–361.

[29] C. L. Stewart, On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers, *Proc. Lond. Math. Soc.* **35** (1977), 425–447.

[30] C. L. Stewart, On divisors of Lucas and Lehmer numbers, *Acta Math.* **211** (2013), 291–314.

[31] S. S. Wagstaff, Jr., Divisors of Mersenne numbers, *Math. Comp.* **40** (1983), 385–397.

[32] M. Ward, The arithmetical theory of linear recurring series, *Trans. Amer. Math. Soc.* **35** (1933), 600–628.

[33] N. Zierler and W. H. Mills, Products of linear recurring sequences, *J. Algebra* **27** (1973), 147–157.

2010 *Mathematics Subject Classification*: Primary 11B83; Secondary 11A51.

Keywords: recurrence sequence, Chebyshev polynomial, composite number, Lehmer number.

(Concerned with sequence A000032, A000045, A001519, A001834, A001906, A002315, A002327, A002878, A005248, A005478, A008865, A030221, A033890, A045546, A057080, A057081, A088165, A113501, A117522, A269251, A269252, A269253, A269254, A285992, A294099, A298675, A298677, A298878, A299045, A299071, A299100, A299101, A299107, and A299109.)

Received February 8 2018; revised versions received July 23 2018; July 31 2018; August 2 2018. Published in *Journal of Integer Sequences*, August 23 2018.

Return to Journal of Integer Sequences home page.