Communications in Mathematics

Karl Dilcher; Larry Ericksen
Reducibility and irreducibility of Stern $(0,1)$-polynomials

*Communications in Mathematics*, Vol. 22 (2014), No. 1, 77--102

Persistent URL: http://dml.cz/dmlcz/143908

VOLUME
22/2014
No. 1

ISSN 1804-1388 (Print)
ISSN 2336-1298 (Online)

# COMMUNICATIONS IN MATHEMATICS



Available online at
http://cm.osu.cz

UNIVERSITAS OSTRAVIENSIS

Communications in Mathematics 22 (2014) 77–102



# Reducibility and irreducibility of Stern $(0,1)$-polynomials[1]

*Karl Dilcher, Larry Ericksen*

**Abstract.** The classical Stern sequence was extended by K. B. Stolarsky and the first author to the Stern polynomials $a(n;x)$ defined by $a(0;x)=0$, $a(1;x)=1$, $a(2n;x)=a(n;x^2)$, and $a(2n+1;x)=x\,a(n;x^2)+a(n+1;x^2)$; these polynomials are Newman polynomials, i.e., they have only 0 and 1 as coefficients. In this paper we prove numerous reducibility and irreducibility properties of these polynomials, and we show that cyclotomic polynomials play an important role as factors. We also prove several related results, such as the fact that $a(n;x)$ can only have simple zeros, and we state a few conjectures.

## 1 Introduction

The *Stern sequence* $\{a(n)\}_{n\geq 0}$ is defined recursively by $a(0)=0$, $a(1)=1$, and for $n\geq 1$ by

$$a(2n)=a(n),\qquad a(2n+1)=a(n)+a(n+1). \tag{1}$$

The sequence starts as $0,1,1,2,1,3,2,3,1,4,3,5,2,5,3,4,1,5,4,7,3,\dots$ See [3] for some historical remarks and for some properties of this sequence. Perhaps the most remarkable properties are that the terms $a(n),a(n+1)$ are always relatively prime, and that each positive reduced rational number occurs once and only once in the sequence $\{a(n)/a(n+1)\}_{n\geq 1}$.

Recently the Stern sequence was extended to two different sequences of polynomials, one by the first author and K. B. Stolarsky [3], and the other independently by Klavžar, Milutinović and Petr [8]. These sequences are quite different from each other, but both have interesting and useful properties. In this paper we will only

*2010 MSC:* Primary: 11B83, Secondary: 11R09

*Key words:* Stern sequence, Stern polynomials, reducibility, irreducibility, cyclotomic polynomials, discriminants, zeros

[1]Presented at the 21st Czech and Slovak International Conference on Number Theory (September 2–6, 2013, Ostravice, Czech Republic)

consider the sequence introduced in [3]; it is defined recursively by $a(0;x) = 0$, $a(1;x) = 1$, and for $n \geq 1$ by

$$a(2n;x) = a(n;x^2)\,, \tag{2}$$

$$a(2n+1;x) = x\,a(n;x^2) + a(n+1;x^2)\,. \tag{3}$$

We call the polynomial $a(n;x)$ the $n$-th *Stern* $(0,1)$*-polynomial*. However, if there is no danger of confusion with the polynomials of Klavžar et al., we will simply refer to them as *Stern polynomials*, as we do in the remainder of this paper. Numerous properties of these polynomials can be found in [3] and [4]; here we only repeat the obvious properties

$$a(n;0) = 1 \quad (n \geq 1), \qquad a(n;1) = a(n) \quad (n \geq 0)\,, \tag{4}$$

where the second identity follows from comparing (2), (3) with (1). Also, for all $m \geq 0$ we have

$$a(2^m;x) = 1\,, \tag{5}$$

and the identities (2), (3) immediately give

$$a(2n+1;x) = x\,a(2n;x) + a(2n+2;x)\,. \tag{6}$$

To obtain an expression for the degree of $a(n;x)$, we let $e(n)$ denote the highest power of 2 dividing $n$. Then for $n \geq 1$,

$$\deg a(n;x) = \frac{n - 2^{e(n)}}{2}\,, \tag{7}$$

and in particular $\deg a(2n+1;x) = n$. Another important property of these Stern polynomials is the fact that they are $(0,1)$-polynomials, also known as *Newman polynomials*, which is not the case for the Stern polynomials of Klavžar et al. Tables of $a(n;x)$ for $1 \leq n \leq 32$ can be found in both [3] and [4], and Table 1 shows the irreducible factors (if any) of these polynomials.

While reducibility and irreducibility properties of the sequence of Klavžar et al. have been studied (see [17] and [20]), only one irreducibility result of limited scope is known for the other sequence.

**Proposition 1 ([3]).** *If $p$ is a prime and 2 is a primitive root modulo $p$, then $a(p;x)$ is an irreducible polynomial over the rationals.*

Table 1 indicates that relatively few Stern polynomials are reducible. However, we are going to show that several infinite classes of these polynomials are in fact reducible. Other infinite classes of polynomials will be proven irreducible. Throughout this paper, reducibility and irreducibility is assumed to be over the rationals.

This paper is structured as follows. In Section 2 we are going to prove reducibility and irreducibility results for certain binomials, trinomials and quadrinomials among the Stern polynomials; part of this will be based on several known irreducibility results. In Section 3 we will prove reducibility and irreducibility for two

| $n$ | $a(n;x)$ | $n$ | $a(n;x)$ |
|---|---|---|---|
| 1 | $1$ | 17 | $(x^4+x^3+x^2+x+1)(x^4-x^3+1)$ |
| 2 | $1$ | 18 | $x^8+x^4+x^2+1$ |
| 3 | $x+1$ | 19 | $x^9+x^8+x^5+x^4+x^3+x+1$ |
| 4 | $1$ | 20 | $(x^2+x+1)(x^2-x+1)(x^4-x^2+1)$ |
| 5 | $x^2+x+1$ | 21 | $x^{10}+x^9+x^8+x^6+x^5+x^2+x+1$ |
| 6 | $x^2+1$ | 22 | $x^{10}+x^8+x^6+x^2+1$ |
| 7 | $x^3+x+1$ | 23 | $x^{11}+x^9+x^8+x^7+x^3+x+1$ |
| 8 | $1$ | 24 | $x^8+1$ |
| 9 | $x^4+x^2+x+1$ | 25 | $(x^2-x+1)(x^{10}+x^9+x^8+x^7-x^5$ $-x^4+2x^2+2x+1)$ |
| 10 | $(x^2+x+1)(x^2-x+1)$ | | |
| 11 | $x^5+x^4+x^3+x+1$ | 26 | $x^{12}+x^{10}+x^4+x^2+1$ |
| 12 | $x^4+1$ | 27 | $x^{13}+x^{12}+x^{11}+x^5+x^4+x^3+x+1$ |
| 13 | $x^6+x^5+x^2+x+1$ | 28 | $x^{12}+x^4+1$ |
| 14 | $x^6+x^2+1$ | 29 | $x^{14}+x^{13}+x^6+x^5+x^2+x+1$ |
| 15 | $x^7+x^3+x+1$ | 30 | $x^{14}+x^6+x^2+1$ |
| 16 | $1$ | 31 | $x^{15}+x^7+x^3+x+1$ |

Table 1: $a(n;x)$ and their factorizations, $1 \le n \le 31$.

special classes of Stern polynomials with increasing numbers of terms. In Section 4 we derive several new identities for the Stern polynomials which will be used later. Section 5 is devoted to results concerning divisibility by $x^2 \pm x+1$, and in Section 6 these results are extended to more general classes of cyclotomic factors. Section 7 deals with the question of the existence of multiple factors and multiple zeros, along with some brief general remarks on the distribution of zeros of Stern polynomials. We conclude this paper with some further remarks and conjectures in Section 8.

## 2 Binomials, trinomials and quadrinomials

In this section we will deal with the smallest Stern polynomials, in the sense of having the least number of terms. By the second part of (4) and the fact that we are dealing with (0,1)-polynomials, the number of terms of $a(n;x)$ is just the number $a(n)$ in the Stern sequence. We can therefore use known results for this sequence. First we note that $a(n)=1$ if and only if $n=2^m$, $m\ge 0$. So by (5) the only monomial that can occur is the constant polynomial 1.

Next we use an observation by Lehmer [9] which essentially says that, given an integer $k\ge 2$, the number of integers $n$ in the interval $2^{k-1}\le n\le 2^k$ for which $a(n)=k$ is $\varphi(k)$, where $\varphi$ denotes Euler's totient function. Furthermore, it is the same number in any subsequent interval between two consecutive powers of 2. This means that there are exactly $\varphi(2)+\varphi(3)+\varphi(4)=5$ classes of binomials, trinomials and quadrinomials. Their smallest elements (by degree) can be found in Table 1, and all others are generated from them by (2). These classes are

$$a(3;x) = x+1\,, \qquad a(3\cdot 2^k;x) = x^{2^k}+1\,; \tag{8}$$

$$a(5;x) = x^2+x+1\,, \qquad a(5\cdot 2^k;x) = x^{2^{k+1}}+x^{2^k}+1\,; \tag{9}$$

$$a(7;x) = x^3+x+1\,, \qquad a(7\cdot 2^k;x) = x^{3\cdot 2^k}+x^{2^k}+1\,; \tag{10}$$

$$a(9;x) = x^4+x^2+x+1\,, \qquad a(9\cdot 2^k;x) = x^{2^{k+2}}+x^{2^{k+1}}+x^{2^k}+1\,; \tag{11}$$

$$a(15;x) = x^7+x^3+x+1\,, \qquad a(15\cdot 2^k;x) = x^{7\cdot 2^k}+x^{3\cdot 2^k}+x^{2^k}+1\,. \tag{12}$$

We deal with these classes in sequence.

**Proposition 2.** *The polynomials $a(3\cdot 2^k;x)$ are irreducible for all $k\geq 0$.*

*Proof.* There are two ways of proving this. First, it is known that $x^{2^k}+1$ is the cyclotomic polynomial $\Phi_{2^{k+1}}(x)$, and as such it is irreducible. Second, it is easy to see that all coefficients of $a(3\cdot 2^k;x+1)$ are even, except for the leading coefficient 1, and that the constant coefficient is 2. This shifted polynomial is therefore 2-Eisenstein for any $k$, and is thus irreducible. □

**Proposition 3.** *We have $x^2+x+1 \mid a(5\cdot 2^k;x)$ for all $k\geq 0$. In other words, $a(5;x)=x^2+x+1$ is the only irreducible polynomial in this class.*

*Proof.* Using the factorization

$$x^4+x^2+1 = (x^2+x+1)(x^2-x+1) \tag{13}$$

with $x$ replaced by $x^{2^k}$, we get

$$a(5\cdot 2^{k+1};x) = \left(x^{2^{k+1}}-x^{2^k}+1\right)a(5\cdot 2^k;x)\,.$$

The result now follows immediately by induction. □

Proposition 3 could also be obtained from a short paper by Tuckerman [19]. The situation for the trinomials in (10) is quite different, as the following result shows.

**Proposition 4.** *The polynomials $a(7\cdot 2^k;x)$ are irreducible for all $k\geq 0$.*

For $k=0$, the polynomial is easily verified to be irreducible; it is also a special case of Theorem 1 in [18]. For the cases $k\geq 1$ we apply Theorem 4 in [18] which we state as a lemma.

**Lemma 1 (Selmer).** *If $f(x)=x^n+ax^m+b$ $(m<n)$ is an irreducible trinomial satisfying one of the two sets of conditions*

$$2^3\nmid a, 2\nmid b, n\neq 2m\,, \qquad \text{or} \qquad a\equiv 1 \text{ or } 2 \pmod 4, 2\mid b\,, \tag{14}$$

*then $f(x^2)$ is also irreducible.*

We now prove the proposition by induction on $k$. The base case $k = 0$ has already been established; assume now that $a(7 \cdot 2^k; x)$ is irreducible for some $k \geq 0$. By (2) we have $a(7 \cdot 2^{k+1}; x) = a(7 \cdot 2^k; x^2)$, and by (10) the first condition in (14) is clearly satisfied. Hence $a(7 \cdot 2^{k+1}; x)$ is also irreducible, and we are done.

**Proposition 5.** *The polynomials $a(9 \cdot 2^k; x)$ and $a(15 \cdot 2^k; x)$ are irreducible for all $k \geq 0$. In other words, all Stern quadrinomials are irreducible.*

This is a fairly easy consequence of a result of Finch and Jones [7] which we quote as another lemma.

**Lemma 2 (Finch and Jones).** *The polynomial $x^a + x^b + x^c + 1$ is reducible if and only if exactly one of the integers $a/2^\nu, b/2^\nu, c/2^\nu$ is even, where $\gcd(a, b, c) = 2^\nu m$ with $m$ odd.*

We apply this lemma to the polynomials in (11) and (12), noting that in both cases we have $\nu = k$. In the first case the three quotients in the lemma are 4, 2, 1, while in the second case they are 7, 3, 1. This proves irreducibility in all cases.

In closing we mention that the irreducibility of $a(15 \cdot 2^k; x)$ could also be obtained from a result of Ljunggren [10, p. 69] (corrected in [13]).

## 3 Stern polynomials with index $2^k \pm 1$

In this section we deal with two further classes of Stern polynomials for which we can obtain some interesting reducibility results. In contrast to the polynomials in the previous section, these have increasing numbers of terms. In [3] it was shown that

$$a(2^k - 1; x) = 1 + x + x^3 + x^7 + \cdots + x^{2^{k-1}-1}, \tag{15}$$

$$a(2^k + 1; x) = 1 + x + x^2 + x^4 + \cdots + x^{2^{k-1}}; \tag{16}$$

both follow quite easily, by induction, from (2), (3) and (5).

### 3.1 The polynomials $a(2^k - 1; x)$

This special case is essentially the same as a sequence of polynomials $P_n(x)$ which was studied by K. Mahler [11]:

$$x \cdot a(2^n - 1; x) = P_n(x) := \sum_{j=0}^{n-1} x^{2^j}. \tag{17}$$

In particular, Mahler studied divisibility of the polynomials $P_n(x)$ by cyclotomic polynomials $\Phi_k(x)$. He used a classical result by L. Fuchs (1863) which gives a complete characterization of the pairs $(n, k)$ for which $\Phi_k(x) \mid P_n(x)$. Using a different approach, in [1] we gave a more explicit version of the result of Mahler and Fuchs. In what follows we give a brief summary of these results, using the notation of Stern polynomials, via (17).

The multiplicative order of 2 modulo an integer $m$, which we denote by $t(m)$ following Mahler and others, plays an important role in most of these results. We recall that $t(m)$ is the smallest positive integer $t$ for which $2^t \equiv 1 \pmod{m}$. The main result in [1] can now be stated as follows.

**Proposition 6.** *Let $p \geq 3$ be a fixed prime. Then for all $m \geq 1$ we have*

$$\Phi_p(x^{2^{t(p)m}-1}) \bigm| a(2^{t(p)pm}-1;x)\,. \tag{18}$$

As an illustration we state the smallest case, $p = 3$. Since $\Phi_3(x) = x^2 + x + 1$ and $t(3) = 2$, we immediately get, for all $m \geq 1$,

$$x^{2^{2m+1}-2} + x^{2^{2m}-1} + 1 \bigm| a(2^{6m}-1;x)\,.$$

Using standard properties of cyclotomic polynomials, we can factor the left-hand side of (18), which gives the following more explicit expression.

**Corollary 1.** *Let $n$ be such that $n = t(p)pm$ for some prime $p \geq 3$ and integer $m \geq 1$. Then $a(2^n-1;x)$ is divisible by all $\Phi_d(x)$ with $d \mid p(2^{t(p)m}-1)$ and $p^{u(p)+1} \mid d$, where $u(p)$ is the highest power of $p$ dividing $2^{t(p)m}-1$.*

This, together with the following result, gives all cyclotomic factors of the polynomials $a(2^n-1;x)$.

**Proposition 7.** *If $\Phi_k(x) \mid a(2^n-1;x)$ for some $n$, then $\Phi_k(x) \mid a(2^{nm}-1;x)$ for all integers $m \geq 1$.*

The fact that these results give all cyclotomic factors of all $a(2^n-1;x)$ was proved in [1], using Mahler's and Fuchs's results. See [1] also for a table of admissible pairs $(n,k)$. To conclude our discussion of the polynomials $a(2^n-1;x)$, we state the following consequence of the above results; see [1], where a more general version is obtained.

**Corollary 2.** *For all $m \geq 1$ we have*

$$\prod_{\substack{3^k \mid 6m\\ k\geq 1}} \Phi_{3^{k+1}}(x) \bigm| a(2^{6m}-1;x)\,.$$

*In particular, Stern polynomials can have arbitrarily many irreducible factors.*

Finally, some further remarks on the polynomials $a(2^n-1;x)$ can be found in Subsection 8.4.

### 3.2 The polynomials $a(2^k+1;x)$

Computations show that these polynomials, as given in (16), are divisible by $1 + x + \cdots + x^k$ when $k = 1, 2, 4, 10, 12, 18, 28, \ldots$ At first sight there seems to be no pattern to this sequence, but we quickly notice that $k+1$ is always a prime. Furthermore, based on our knowledge of Proposition 1, we were able to identify this sequence of primes. When $k = 1$ or 2, the divisibility observation holds trivially since $a(2^1+1;x) = 1+x$ and $a(2^2+1;x) = 1+x+x^2$. For $k \geq 2$ we can prove the following result, where we set $k+1 = p$, an odd prime.

**Proposition 8.** *Let $p \geq 3$ be a prime which has 2 as a primitive root. Then*

$$(1 + x + x^2 + \cdots + x^{p-1}) \mid a(2^{p-1} + 1; x).$$

*In particular, if $p \geq 5$ is such a prime, then $a(2^{p-1} + 1; x)$ is reducible.*

*Proof.* If 2 is a primitive root of $p$, then $2^0, 2^1, \ldots, 2^{p-2}$ is a reordering of $1, 2, \ldots, p-1 \pmod{p}$. Therefore with (16) we have

$$a(2^{p-1} + 1; x) = 1 + \sum_{j=0}^{p-2} x^{2^j} \equiv 1 + \sum_{j=1}^{p-1} x^j \pmod{x^p - 1}.$$

Since $(x^{p-1} + \cdots + x + 1)(x - 1) = x^p - 1$, this shows that $a(2^{p-1} + 1; x)$ is divisible by $x^{p-1} + \cdots + x + 1$. □

Computations indicate that those polynomials $a(2^k \pm 1; x)$ that were not proven reducible in this section seem to be irreducible. In Section 6 we will reformulate Proposition 8 in terms of cyclotomic polynomials and extend it to larger classes of Stern polynomials. See also Subsection 8.4 for another remark on the polynomials $a(2^k + 1; x)$.

## 4 Identities for Stern polynomials

Both the (numerical) Stern sequence and the sequence of Stern polynomials have a great deal of internal structure which manifests itself through various identities. In addition to the elementary identities (1)–(6) which all involve just one parameter, the following identities, involving two or three parameters, were obtained in [3] and [4]: For all $k \geq 0$ and $0 \leq j \leq 2^k$ we have

$$a(2^k + j; x) - x^j a(2^k - j; x) = a(j; x) \tag{19}$$

(see [3, Lemma 2.1]), and for $0 \leq k \leq n$ and $0 \leq j \leq 2^k$ we have

$$a(2^n - j; x) - a(2^k - j; x) = x^{2^k - j} a(j; x) a(2^n - 2^k; x) \tag{20}$$

(see [4, Proposition 2.1]). It is the purpose of this section to derive extensions or generalizations of these identities which will be applicable for our purposes. We prove four identities, two of which extend (19) and (20).

**Proposition 9.** *For all integers $k \geq 0$, $0 \leq j \leq 2^k$, and odd $m \geq 1$ we have*

$$a(m2^k + j; x) + x^j a(m2^k - j; x) = \big(a(j; x) + 2x^j a(2^k - j; x)\big)\, a(m2^k; x). \tag{21}$$

*Proof.* We first treat the case $j = 0$ separately; it reduces to

$$a(m2^k; x) + a(m2^k; x) = \big(a(0; x) + 2a(2^k; x)\big)\, a(m2^k; x),$$

which is trivially true by (5) and the fact that $a(0; x) = 0$. Assuming now that $j \geq 1$, we prove (21) by induction on $k$. The base case $k = 0$, $j = 1$ reduces to

$$a(m + 1; x) + xa(m - 1; x) = (a(1; x) + 2xa(0; x))\, a(m; x).$$

We note that the expression in large parentheses on the right is identically 1, and since $m$ is odd, this identity is therefore equivalent to (6).

Now assume that (21) holds for some $k-1$ and all $0 \le j \le 2^{k-1}$. For the induction step we first let $j$ be even, say $j = 2\ell$, with $0 \le \ell \le 2^{k-1}$. Then using the reduction formula (2), the identity (21), with $j = 2\ell$, becomes

$$\begin{aligned} &a(m2^{k-1}+\ell;x^2)+(x^2)^\ell a(m2^{k-1}-\ell;x^2) \\ &\qquad = \left(a(\ell;x^2)+2(x^2)^\ell a(2^{k-1}-\ell;x^2)\right) a(m2^{k-1};x^2)\,. \end{aligned} \tag{22}$$

This identity holds by the induction hypothesis, with $x$ replaced by $x^2$. Second, we let $j$ be odd, say $j = 2\ell+1$. Then the polynomials $a(m2^k+j;x)$, $a(m2^k-j;x)$, $a(j;x)$, $a(2^k-j;x)$ in (21) have odd index; hence we use (6) to rewrite (21) as follows:

$$\begin{aligned} &xa(m2^k+2\ell;x)+a(m2^k+2\ell+2;x) \\ &\qquad + x^{2\ell+1}\left[xa(m2^k-2\ell-2;x)+a(m2^k-2\ell;x)\right] \\ &= [xa(2\ell;x)+a(2\ell+2;x) \\ &\qquad +2x^{2\ell+1}\left(xa(2^k-2\ell-2;x)+a(2^k-2\ell;x)\right)]\, a(m2^k;x). \end{aligned}$$

This holds when both the following identities hold:

$$\begin{aligned} &xa(m2^k+2\ell;x)+x^{2\ell+1}a(m2^k-2\ell;x) \\ &\qquad = \left[xa(2\ell;x)+2x^{2\ell+1}a(2^k-2\ell;x)\right] a(m2^k;x)\,, \end{aligned} \tag{23}$$

$$\begin{aligned} &a(m2^k+2\ell+2;x)+x^{2\ell+2}a(m2^k-2\ell-2;x) \\ &\qquad = \left[a(2\ell+2;x)+2x^{2\ell+2}a(2^k-2\ell-2;x)\right] a(m2^k;x)\,. \end{aligned} \tag{24}$$

To deal with (23), we divide both sides by $x$ and use the reduction formula (2). This gives us (22) which holds by the induction hypothesis. Similarly, we use (2) for all terms in (24), which gives (22) with $\ell$ replaced by $\ell+1$. This is still valid by the induction hypothesis since $j = 2\ell+1 \le 2^k$ implies $2\ell \le 2^k-2$, and thus $\ell \le 2^{k-1}-1$ and $\ell+1 \le 2^{k-1}$, as required. Both (23) and (24) are therefore true, which completes the proof by induction. □

**Proposition 10.** *For all integers $m \ge 1$, $k \ge 0$, and $0 \le j \le 2^k$ we have*

$$a(m2^k-j;x)-a(2^k-j;x)a(m2^k;x) = x^{2^k-j}a(j;x)a((m-1)2^k;x)\,. \tag{25}$$

*Proof.* As in the previous proof we treat the case $j=0$ separately; the identity (25) then reduces to

$$a(m2^k;x)-a(2^k;x)a(m2^k;x) = x^{2^k}a(0;x)a((m-1)2^k;x)\,,$$

and with (5) and $a(0;x)=0$ we see that both sides are identically 0. Now assume that $j \ge 1$; we prove (25) by induction on $k$. The base case $k=0$, $j=1$ is

$$a(m-1;x)-a(0;x)a(m;x) = x^0 a(1;x)a((m-1);x)\,,$$

and we see that both sides are identical. (Note that, in contrast to Proposition 9, we do not require $m$ to be odd).

Next, assume that (25) holds for some $k-1$ and all $0 \le j \le 2^{k-1}$. For the induction step we proceed exactly as in the proof of Proposition 9, distinguishing between the cases $j$ even and $j$ odd. We leave the details to the reader. □

**Remark.** The case $m = 1$ in (25) is trivially true, as both sides are identically 0. When $m = 2^{n-k}$, then (25) implies (20) if we take (5) into account.

We obtain the following consequence from (25) if we replace $j$ by $2^k - j$ and then $m$ by $m+1$.

**Corollary 3.** *For all integers $m \ge 0$, $k \ge 0$, and $0 \le j \le 2^k$ we have*

$$a(m2^k + j; x) - x^j a(2^k - j; x)a(m2^k; x) = a(j; x)a((m+1)2^k; x)\,. \tag{26}$$

We note that (26) with $m = 1$ gives (19), once again taking (5) into account. The final result in this section is of a slightly different nature, but will also be needed later.

**Proposition 11.** *Let $k \ge 0$ be an integer and $m \ge 1$ an odd integer. Then*

$$2a((m+1)2^k; x) - a(m2^k; x) = a(m; -x^{2^k})\,. \tag{27}$$

*Proof.* By (2) we have $a(2n; -x) = a(n; (-x)^2) = a(n; x^2) = a(2n; x)$, and therefore (6) gives

$$a(2n+1; -x) = a(2n+2; x) - x\,a(2n; x) \tag{28}$$

We now iterate the reduction formula (2):

$$\begin{aligned} 2a((m+1)2^k; x) - a(m2^k; x) &= a(m+1; x^{2^k}) + \Big(a(m+1; x^{2^k}) - a(m; x^{2^k})\Big) \\ &= a(m+1; x^{2^k}) - x^{2^k} a(m-1; x^{2^k}) = a(m; -x^{2^k})\,, \end{aligned}$$

where we have first used (6) and then (28), keeping in mind that $m$ is odd. This completes the proof of (27). □

## 5 Divisibility by $x^2 \pm x + 1$

In the next section we will show that each of the "allowable" polynomials $1 + x + x^2 + \cdots + x^{p-1}$ in Proposition 8, as well as their alternating analogues $1 - x + x^2 - \cdots + x^{p-1}$, divide infinite classes of the Stern polynomials $a(n; x)$. Since the largest proportion of reducible Stern polynomials are divisible by $x^2 \pm x + 1$, we will treat this case separately, and in greater detail, including relevant tables. This is also done to illustrate the methods of proof, which rely on a repeated use of the identities from the previous section.

### 5.1 Divisibility by $x^2 + x + 1$

We begin with a general observation. If $a(n;x)$ is reducible for some $n$ then, by (2), $a(2n;x)$ is also reducible. But we can say more: If $x^2+x+1 \mid a(n;x)$, then by the factorization (13) we also have $x^2+x+1 \mid a(2n;x)$. We may therefore restrict our attention to *odd* indices $n$.

We observe by computation that $x^2+x+1$ divides $a(n;x)$ only when $n$ is divisible by 5. We therefore consider $a(5\nu;x)$ with $\nu$ odd. The first few such $\nu$ for which $x^2+x+1 \mid a(5\nu;x)$ are

$$\nu = 1, 7, 9, 15, 17, 21, 31, 33, 55, 57, 63, 65, 71, 73, 107, 111, 113, \ldots$$

We see that most come in pairs $(\nu, \nu+2)$, while a few are "isolated", such as 21 and 107 (leaving aside $\nu = 1$). The first 64 of the pairs are listed in Table 2, and the first 40 isolated $\nu$ are in Table 3.

The following result, along with its corollaries, will explain all entries in Table 2 and many entries in Table 3. It is an easy consequence of identities in Section 4.

**Proposition 12.** *Suppose that $\mu \geq 1$ and $j \geq 1$ are such that both $a(5\mu;x)$ and $a(5j;x)$ are divisible by $x^2+x+1$. If $k$ is such that $j \leq \lfloor 2^k/5 \rfloor$, then $a(5(\mu\cdot 2^k \pm j);x)$ is divisible by $x^2+x+1$.*

*Proof.* We use (25) with $m = 5\mu$ and $j$ replaced by $5j$. Then

$$a(5(\mu\cdot 2^k - j);x) - a(2^k-5j;x)a(5\mu 2^k;x) = x^{2^k-5j}a(5j;x)a((5\mu-1)2^k;x). \quad (29)$$

The right-hand side is divisible by $x^2+x+1$, by hypothesis. Similarly, the second term on the left is also divisible by $x^2+x+1$ since $a(5\mu 2^k;x) = a(5\mu;x^{2^k})$ is, where we have used (13). This proves the "−" part of the statement.

For the "+" part we use (21) with $m$ and $j$ as above. Noting that the right-hand side is always divisible by $x^2+x+1$, we see that $a(5\cdot 2^k+j;x)$ is divisible by this trinomial if and only if $a(5\cdot 2^k - j;x)$ is. Finally, using the fact that (21) and (25) hold for all $j \leq 2^k$, we see that the statement of the proposition holds for $j \leq \lfloor 2^k/5 \rfloor$. □

If we set $\mu = 1$ in Proposition 12, we immediately get the following consequence.

**Corollary 4.** *Let $k \geq 3$ be an integer. If $x^2+x+1$ divides $a(5j;x)$ for some $1 \leq j \leq \lfloor 2^k/5 \rfloor$, then $x^2+x+1$ also divides $a(5(2^k \pm j);x)$. In particular, for all $k \geq 3$, $x^2+x+1$ divides $a(5(2^k \pm 1);x)$.*

Although this result holds for all $j$ in the given range, we will be mainly interested in odd values of $j$. An even $j$ will lead to even parameters $5(2^k \pm j)$, which gives us nothing new; see the remark at the beginning of this section.

Corollary 4 explains a large number of entries in Table 2. For instance, the entries 55, 57 and 71, 73 result from $k = 6$ and $j = 7, 9$. Each new entry, in turn, leads to an infinite class of further integers $j$ for which $a(5j;x)$ is divisible by $x^2+x+1$.

| $\nu$ | $j$ | $\nu$ | $j$ | $\nu$ | $j$ | $\nu$ | $j$ |
|---|---|---|---|---|---|---|---|
| 7, 9 | 1 | 263, 265 | 33 | 583, 585 | 73 | 1039, 1041 | 130 |
| 15, 17 | 2 | 271, 273 | 34 | 671, 673 | 84 | 1055, 1057 | 132 |
| 31, 33 | 4 | 287, 289 | 36 | 855, 857 | 107 | 1079, 1081 | 135 |
| 55, 57 | 7 | 335, 337 | 42 | 879, 881 | 110 | 1087, 1089 | 136 |
| 63, 65 | 8 | 439, 441 | 55 | 887, 889 | 111 | 1095, 1097 | 137 |
| 71, 73 | 9 | 447, 449 | 56 | 895, 897 | 112 | 1135, 1137 | 142 |
| 111, 113 | 14 | 455, 457 | 57 | 903, 905 | 113 | 1143, 1145 | 143 |
| 119, 121 | 15 | 479, 481 | 60 | 911, 913 | 114 | 1151, 1153 | 144 |
| 127, 129 | 16 | 495, 497 | 62 | 951, 953 | 119 | 1159, 1161 | 145 |
| 135, 137 | 17 | 503, 505 | 63 | 959, 961 | 120 | 1167, 1169 | 146 |
| 143, 145 | 18 | 511, 513 | 64 | 967, 969 | 121 | 1191, 1193 | 149 |
| 167, 169 | 21 | 519, 521 | 65 | 991, 993 | 124 | 1335, 1337 | 167 |
| 223, 225 | 28 | 527, 529 | 66 | 1007, 1009 | 126 | 1343, 1345 | 168 |
| 239, 241 | 30 | 543, 545 | 68 | 1015, 1017 | 127 | 1351, 1353 | 169 |
| 247, 249 | 31 | 567, 569 | 71 | 1023, 1025 | 128 | 1511, 1513 | 189 |
| 255, 257 | 32 | 575, 577 | 72 | 1031, 1033 | 129 | 1711, 1713 | 214 |

Table 2: Odd $\nu$ for which $x^2+x+1 \mid a(5\nu;x)$, and $j$ such that $\nu = 8j \pm 1$.

The first paired entries in Table 2 not generated in this way are 167, 169, and then 335, 337; 439, 441; 455, 457; and a total of 16 other pairs in this table. Before explaining these entries, we list in Table 3 the first 40 "isolated" integers $\nu$ for which $a(5\nu;x)$ is divisible by $x^2+x+1$.

A hint towards explaining the remaining pairs of entries in Table 2 is given in the "$j$" columns: The values of $j$ associated with the four pairs of entries mentioned in the previous paragraph are $j = 21, 42, 55$ and $57$, respectively. We note that 21 is the smallest entry in Table 3, and 42 is twice that number, while 55 and 57 are the smallest entries in Table 2 that are not of the form $2^k \pm 1$. This is easily explained by the following consequence of Proposition 12 which is obtained by taking $j = 1$ and $k = 3$.

**Corollary 5.** *Suppose that the integer $\mu \geq 1$ is such that $a(5\mu;x)$ is divisible by $x^2+x+1$. Then $a(5(8\mu \pm 1);x)$ is also divisible by $x^2+x+1$.*

We note in passing that the case where $\mu$ differs by 1 from a power of 2 is already covered by Corollary 4. Also, in contrast to Corollary 4, where we could restrict ourselves to odd values of $j$, in Corollary 5 we must consider all allowable integer parameters $\mu$, even or odd.

For example, starting with the smallest entry in Table 3, the values $\mu = 21, 42, 84$, and $168$ each lead to a pair of entries in Table 2. In general, for each $k \geq 0$, the value $\mu = 21 \cdot 2^k$ gives a new pair of Stern polynomials divisible by $x^2+x+1$. In fact, every entry in Tables 2 and 3 leads to an infinite class of such Stern polynomials.

We now turn to a partial explanation of the entries in Table 3. All the entries for which the second columns are not left blank are immediately explained by

| $\nu$ | $\nu =$ | $\nu$ | $\nu =$ | $\nu$ | $\nu =$ | $\nu$ | $\nu =$ |
|---|---|---|---|---|---|---|---|
| 21 | | 373 | | 1173 | $2^{10}+149$ | 1899 | $2^{11}-149$ |
| 107 | $2^7-21$ | 491 | $2^9-21$ | 1213 | $2^{10}+189$ | 1941 | $2^{11}-107$ |
| 149 | $2^7+21$ | 533 | $2^9+21$ | 1675 | $2^{11}-373$ | 2027 | $2^{11}-21$ |
| 189 | | 693 | | 1699 | $2^{11}-349$ | 2069 | $2^{11}+21$ |
| 235 | $2^8-21$ | 835 | $2^{10}-189$ | 1707 | $2^{11}-341$ | 2155 | $2^{11}+107$ |
| 277 | $2^8+21$ | 875 | $2^{10}-149$ | 1723 | $2^{11}-325$ | 2197 | $2^{11}+149$ |
| 315 | | 917 | $2^{10}-107$ | 1733 | $2^{11}-315$ | 2237 | $2^{11}+189$ |
| 325 | | 1003 | $2^{10}-21$ | 1771 | $2^{11}-277$ | 2283 | $2^{11}+235$ |
| 341 | | 1045 | $2^{10}+21$ | 1813 | $2^{11}-235$ | 2325 | $2^{11}+277$ |
| 349 | | 1131 | $2^{10}+107$ | 1859 | $2^{11}-189$ | 2363 | $2^{11}+315$ |

Table 3: Isolated odd $\nu$ for which $x^2+x+1 \mid a(5\nu;x)$.

Corollary 4. For other cases we need Proposition 12 in its greater generality. For instance, the smallest "isolated" cases not already covered by Corollary 4 occur when $\mu = j = 21$ and $k = 7$. This shows that $a(5\cdot 2667;x)$ and $a(5\cdot 2709;x)$ are both divisible by $x^2+x+1$.

**Remark 1.** We note that in contrast to the "paired" cases (Table 2), where $\nu \equiv \pm 1 \pmod 8$, all "isolated" cases (Table 3) appear to satisfy $\nu \equiv \pm 3 \pmod 8$.

**Remark 2.** Numerous "isolated" cases remain unexplained, beginning with $\nu = 21$ and seven more cases indicated in Table 3 with blank entries, then followed by $\nu = 2749, 2941, 3005, 3029, 3037, 3053, 3133, 3213$. The next block of unexplained cases begins with $\nu = 4947$.

### 5.2 Divisibility by $x^2 - x + 1$

As in the previous subsection we observe that $x^2-x+1$ divides $a(n;x)$ only when $n$ is divisible by 5. We therefore consider again $a(5\nu;x)$. In spite of many similarities to divisibility properties by $x^2+x+1$, there are some substantial differences. In particular, while we have the factorization (13), namely $x^4+x^2+1 = (x^2+x+1)(x^2-x+1)$, the analogous polynomial $x^4-x^2+1$ is irreducible. This means that $x^2-x+1 \mid a(n;x)$ does not imply $x^2-x+1 \mid a(2n;x)$. Therefore, if we want to consider divisibility by $x^2-x+1$, as opposed to just reducibility, we have to consider $a(5\nu;x)$ also for even $\nu$. In this connection we have the following consequence of the factorization (13) quoted above.

**Corollary 6.** *If $x^2+x+1$ divides $a(5\nu;x)$, then $x^2-x+1$ divides $a(5\cdot 2^k\nu;x)$ for all $k \ge 1$.*

We may now restrict our attention to odd $\nu$, and observe that the first few such $\nu$ for which $x^2-x+1 \mid a(5\nu;x)$ are

$$\nu = 5, 27, 37, 59, 69, 79, 81, 85, 93, 123, 133, 173, 219, 229, 251, 261, 283, 293.$$

We see that most of these come in pairs $(\nu, \nu+10)$, while others are once again "isolated", such as $\nu = 5, 85, 93$, and others again come in pairs $(\nu, \nu+2)$, such as

$(79, 81)$. Tables 4, 5 and 6 show the first instances of each of these cases. Much of this is explained by the following result which is analogous to Proposition 12 and also follows immediately from (29).

**Proposition 13.** *Suppose that $\mu \geq 1$ and $j \geq 1$ are such that $x^2+x+1 \mid a(5\mu;x)$ and $x^2-x+1 \mid a(5j;x)$. If $k$ is such that $j \leq \lfloor 2^k/5 \rfloor$, then $a(5(\mu\cdot 2^k \pm j);x)$ is divisible by $x^2-x+1$.*

We begin with the case illustrated by the entries in Table 4. We'll show that this case is directly related to divisibility of $a(5\nu;x)$ by $x^2+x+1$. Indeed, by taking $j=5$ in Proposition 13 and recalling from Table 1 that $x^2-x+1 \mid a(25;x)$, we get the following result.

**Corollary 7.** *If $\mu \geq 1$ is such that $x^2+x+1 \mid a(5\mu;x)$, then $x^2-x+1$ divides $a(5(32\mu \pm 5);x)$.*

| $\nu$ | $j$ | $\nu$ | $j$ | $\nu$ | $j$ | $\nu$ | $j$ |
|---|---|---|---|---|---|---|---|
| 27, 37 | 1 | 571, 581 | 18 | 1755, 1765 | 55 | 2267, 2277 | 71 |
| 59, 69 | 2 | 667, 677 | 21 | 1787, 1797 | 56 | 2299, 2309 | 72 |
| 123, 133 | 4 | 891, 901 | 28 | 1819, 1829 | 57 | 2331, 2341 | 73 |
| 219, 229 | 7 | 955, 965 | 30 | 1915, 1925 | 60 | 2683, 2693 | 84 |
| 251, 261 | 8 | 987, 997 | 31 | 1979, 1989 | 62 | 3419, 3429 | 107 |
| 283, 293 | 9 | 1019, 1029 | 32 | 2011, 2021 | 63 | 3515, 3525 | 110 |
| 443, 453 | 14 | 1051, 1061 | 33 | 2043, 2053 | 64 | 3547, 3557 | 111 |
| 475, 485 | 15 | 1083, 1093 | 34 | 2075, 2085 | 65 | 3579, 3589 | 112 |
| 507, 517 | 16 | 1147, 1157 | 36 | 2107, 2117 | 66 | 3611, 3621 | 113 |
| 539, 549 | 17 | 1339, 1349 | 42 | 2171, 2181 | 68 | 3643, 3653 | 114 |

Table 4: Odd $\nu$ for which $x^2-x+1 \mid a(5\nu;x)$, and $j$ such that $\nu = 32j \pm 5$.

| $\nu$ | $\nu =$ | $\nu$ | $\nu =$ | $\nu$ | $\nu =$ | $\nu$ | $\nu =$ |
|---|---|---|---|---|---|---|---|
| 5 | | 931 | $2^{10}-93$ | 1313 | | 1875 | $2^{11}-173$ |
| 85 | | 939 | $2^{10}-85$ | 1365 | | 1955 | $2^{11}-93$ |
| 93 | | 1109 | $2^{10}+85$ | 1373 | | 1963 | $2^{11}-85$ |
| 173 | | 1117 | $2^{10}+93$ | 1397 | | 2133 | $2^{11}+85$ |
| 419 | $2^9-93$ | 1197 | $2^{10}+173$ | 1449 | | 2141 | $2^{11}+93$ |
| 427 | $2^9-85$ | 1247 | | 1469 | | 2221 | $2^{11}+173$ |
| 597 | $2^9+85$ | 1259 | | 1493 | | 2515 | |
| 605 | $2^9+93$ | 1271 | | 1501 | | 2605 | |
| 757 | | 1289 | | 1517 | | 2733 | |
| 851 | $2^{10}-173$ | 1301 | | 1565 | | 2773 | |

Table 5: Isolated odd $\nu$ for which $x^2-x+1 \mid a(5\nu;x)$.

The "isolated" cases, the first 40 of which are shown in Table 5, are partly explained by Proposition 13. For instance, the entries in the columns ($\nu =$) correspond to $\mu = 1$. The next smallest class of examples occurs when $\mu = 7$ and $k = 9$, in which case $x^2 - x + 1 \mid a(5\nu; x)$ for $\nu = 3491$, 3499, 3669, 3677.

We now turn to the third case, which corresponds to $x^2 - x + 1 \mid a(5\nu; x)$ for pairs $(\nu, \nu + 2)$; see Table 6. This case is fully explained by the following result.

**Proposition 14.** *If $j \ge 1$ is an odd integer such that $x^2 - x + 1 \mid a(5j; x)$, then $x^2 - x + 1$ divides $a(5(16j \pm 1); x)$.*

*Proof.* We subtract (26) from (21) and set $j = 5$, $k = 4$, and replace $m$ by $5j$, which gives

$$x^5 a(5(16j-1); x) - \big(a(5; x) + 2x^5 a(11; x)\big)\, a(80j; x) \\ = -x^5 a(11; x) a(80j; x) - a(5; x) a(80j + 16; x)\,. \tag{30}$$

We are going to use the fact that

$$a(5; x) + 2x^5 a(11; x) \\ = (x^2 - x + 1)(2x^8 + 4x^7 + 4x^6 - 2x^4 + 2x^2 + 2x + 1)\,, \tag{31}$$

which is easy to verify by direct computation. Multiplying the left-hand side of (31) by $a(80j + 16; x)$ and adding the product to both sides of (30), we get

$$x^5 a(5(16j-1); x) + \big(a(5; x) + 2x^5 a(11; x)\big)\, (a(80j + 16; x) - a(80j; x)) \\ = x^5 a(11; x)\, (2a(80j + 16; x) - a(80j; x))\,. \tag{32}$$

Using (27) with $k = 4$ and $m = 5j$, we get

$$2a(80j + 16; x) - a(80j; x) = a(5j; -x^{16})\,. \tag{33}$$

Now, if $x^2 - x + 1 \mid a(5j; x)$, then $x^{32} + x^{16} + 1 \mid a(5j; -x^{16})$, and by iterating the factorization (13) we see that $x^2 - x + 1 \mid x^{32} + x^{16} + 1$. Hence, with (33) we see that $x^2 - x + 1$ divides the right-hand side of (32), and (31) shows that it also divides the second term on the left-hand side of (32). This proves the "$-$" part of the proposition.

To prove the "+" part, we use (21) with $j, k$ and $m$ as above, obtaining

$$a(5(16j+1); x) + x^5 a(5(16j-1); x) = \big(a(5; x) + 2x^5 a(11; x)\big)\, a(80j; x)\,.$$

By (31) the right-hand side of this last identity is divisible by $x^2 - x + 1$, and since the second term on the left is also divisible by $x^2 - x + 1$, then so is the first term. This completes the proof. $\square$

| $\nu$ | $j$ | $\nu$ | $j$ | $\nu$ | $j$ | $\nu$ | $j$ |
|---|---|---|---|---|---|---|---|
| 79, 81 | 5 | 1103, 1105 | 69 | 1487, 1489 | 93 | 3503, 3505 | 219 |
| 431, 433 | 27 | 1263, 1265 | 79 | 1967, 1969 | 123 | 3663, 3665 | 229 |
| 591, 593 | 37 | 1295, 1297 | 81 | 2127, 2129 | 133 | 4015, 4017 | 251 |
| 943, 945 | 59 | 1359, 1361 | 85 | 2767, 2769 | 173 | 4175, 4177 | 261 |

Table 6: Odd $\nu$ for which $x^2 - x + 1 \mid a(5\nu; x)$, and $j$ such that $\nu = 16j \pm 1$.

## 6 Divisibility by certain cyclotomic polynomials

Computations show that numerous Stern polynomials $a(n;x)$ are divisible by $x^4 + x^3 + x^2 + x + 1$ or by $x^4 - x^3 + x^2 - x + 1$, and it appears that this occurs only when $n = 17\nu$ for a positive integer $\nu$. We could prove results very similar to those in Section 5; however, both these cases and divisibility properties by $x^2 \pm x + 1$ are in fact special cases of a much more general result, as we shall see in this section.

Returning to Proposition 8, we note that for an odd prime $p$ we have

$$\Phi_p(x) = 1 + x + x^2 + \cdots + x^{p-1},$$

the $p$-th cyclotomic polynomial. Furthermore, for ease of notation we set

$$m_p := 2^{p-1} + 1.$$

We can then reformulate Proposition 8 as follows: Let $p$ be an odd prime; then

$$\Phi_p(x) \mid a(m_p; x) \quad \text{if 2 is a primitive root of } p. \tag{34}$$

The first twenty such primes $p$ are 3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83, 101, 107, 131, 139, 149, 163, 173, 179; see also [15, A001122]. By a conjecture of Artin we would expect the existence of infinitely many such primes. We will also need the identity

$$\Phi_p(x^2) = \Phi_p(x)\Phi_p(-x), \tag{35}$$

valid for all odd primes; note that $\Phi_p(-x) = \Phi_{2p}(x)$ is also a cyclotomic polynomial. The identity (35) is a generalization of (13), which is the case $p = 3$.

### 6.1 Divisibility by $\Phi_p(x)$

We are now ready to state and prove the first main result of this section; it is a direct generalization of Proposition 12.

**Proposition 15.** *Let $p$ be an odd prime which has 2 as a primitive root, and suppose that $\mu \geq 1$ and $j \geq 1$ are such that both $a(m_p\mu; x)$ and $a(m_p j; x)$ are divisible by $\Phi_p(x)$. If $k$ is such that $j \leq \lfloor 2^k/m_p \rfloor$, then $a(m_p(\mu \cdot 2^k \pm j); x)$ is divisible by $\Phi_p(x)$.*

*Proof.* Following the proof of Proposition 12, we use (25) with $m = m_p\mu$ and replace $j$ with $m_p j$. Then

$$\begin{aligned} a\big(m_p(\mu \cdot 2^k - j); x\big) - a(2^k - m_p j; x)a(m_p\mu 2^k; x) \\ = x^{2^k - m_p j} a(m_p j; x) a\big((m_p\mu - 1)2^k; x\big) . \end{aligned} \tag{36}$$

The right-hand side is divisible by $\Phi_p(x)$, by hypothesis. Also by hypothesis we have

$$\Phi_p(x^{2^k}) \mid a(m_p\mu; x^{2^k}) = a(m_p\mu 2^k; x)\,, \tag{37}$$

where we have once again used (2). By iterating (35) we then see that the terms in (37) are divisible by $\Phi_p(x)$. Altogether, this shows that the first term in (36) is divisible by $\Phi_p(x)$, which proves the "−" part of the statement of the proposition.

For the "+" part we use the identity (21) with $m$ and $j$ as above. It suffices to show that the right-hand side of that identity is divisible by $\Phi_p(x)$. But since the final term in (21) is the same as the right-hand side in (37), this is the case, as we have seen above. The proof is now complete. □

As in the special case $p = 3$ in Section 5, we get the following immediate consequences.

**Corollary 8.** *Let $p$ be an odd prime which has 2 as a primitive root. If $\Phi_p(x)$ divides $a(m_pj; x)$ for some $1 \le j \le \lfloor 2^k/m_p \rfloor$, then also $\Phi_p(x) \mid a(m_p(2^k \pm j); x)$. In particular, if $k \ge p$, then $\Phi_p(x) \mid a(m_p(2^k \pm 1); x)$.*

The first statement of this result follows from Proposition 15 with $\mu = 1$, where we have used (34). The second statement follows from the first by setting $j = 1$ and using (34) again. Also note that the condition $2^k \ge m_p$ holds whenever $k \ge p$.

The next consequence is an extension of Corollary 5 and is simply the case $j = 1$ and $k = p$ in Proposition 15.

**Corollary 9.** *Let $p$ be an odd prime which has 2 as a primitive root. Suppose that $\mu \ge 1$ is such that $a(m_p\mu; x)$ is divisible by $\Phi_p(x)$. Then $a(m_p(2^p\mu \pm 1); x)$ is also divisible by $\Phi_p(x)$.*

### 6.2 Divisibility by $\Phi_p(-x)$

We continue with extending the results in Section 5; we first state an easy consequence of (35) and (2).

**Corollary 10.** *Let $p$ be an odd prime which has 2 as a primitive root. If $\Phi_p(x)$ divides $a(m_p\nu; x)$, then $\Phi_p(-x)$ divides $a(m_p2^k\nu; x)$ for all $k \ge 1$.*

Next we state the relevant generalization of Proposition 13.

**Proposition 16.** *Let $p$ be an odd prime which has 2 as a primitive root and suppose that $\mu \ge 1$ and $j \ge 1$ are such that $\Phi_p(x) \mid a(m_p\mu; x)$ and $\Phi_p(-x) \mid a(m_pj; x)$. If $k$ is such that $j \le \lfloor 2^k/m_p \rfloor$, then $a(m_p(\mu 2^k \pm j); x)$ is divisible by $\Phi_p(-x)$.*

The "−" part of this statement follows immediately from (36), using Corollary 10. The "+" part follows once again from (21) and the "−" part, with $m$ and $j$ as before.

Recall that Corollary 7 follows directly from Proposition 13 due to the fact that $x^2 - x + 1$ divides $a(25; x)$, that is, $\Phi_p(-x) \mid a(m_p^2; x)$ for $p = 3$. In order to generalize Corollary 7, we need this fact to be true more generally, which is indeed the case.

**Proposition 17.** *If $p$ is an odd prime which has 2 as a primitive root, then $\Phi_p(-x)$ divides $a(m_p^2;x)$.*

*Proof.* Using the definition of $m_p$, we note that

$$(2^{p-2}+1)2^p = 2^{2(p-1)} + 2\cdot 2^{p-1} = m_p^2 - 1\,.$$

We now apply the identity (26) with $m = 2^{p-2}+1$, $k=p$ and $j=1$, to obtain

$$a(m_p^2;x) = a((2^{p-3}+1)2^{p+1};x) + x\cdot a(2^p-1;x)a((2^{p-2}+1)2^p;x)\,. \tag{38}$$

We claim that we have the following congruences modulo the polynomial $\Phi_p(-x)$, valid for all primes $p\geq 3$ which have 2 as a primitive root:

$$a((2^{p-3}+1)2^{p+1};x) \equiv -x^2+x \pmod{\Phi_p(-x)}\,, \tag{39}$$

$$a(2^p-1;x) \equiv x^{p-2}-x^{p-3}+\cdots-x^2+x \pmod{\Phi_p(-x)}\,, \tag{40}$$

$$a((2^{p-2}+1)2^p;x) \equiv x \pmod{\Phi_p(-x)}\,. \tag{41}$$

Substituting these congruences into the right-hand side of (38), we immediately get

$$a(m_p^2;x) \equiv x^p - x^{p-1}+\cdots+x^3-x^2+x \pmod{\Phi_p(-x)}\,,$$

and the right-hand side is obviously divisible by $\Phi_p(-x)$. This proves the result, provided we can prove the congruences (39)–(41).

The proofs of these congruences are based on the following two fundamental facts. First, if $p$ has 2 as a primitive root, then $2^0, 2^1, 2^2, \ldots, 2^{p-2}$ is a reordering, modulo $p$, of $1,2,3,\ldots,p-1$. Second, we have

$$x^p \equiv -1 \pmod{\Phi_p(-x)} \tag{42}$$

since $\Phi_p(-x) = (x^p+1)/(x+1)$.

To prove (39), we first note that by Fermat's little theorem we have $2^{p+1} = 4\cdot 2^{p-1} \equiv 4 \pmod p$. This, together with $2^{p+1}\equiv 0 \pmod 2$ gives $2^{p+1}\equiv 4 \pmod{2p}$ by the Chinese Remainder Theorem, and thus

$$x^{2^{p+1}} \equiv x^4 \pmod{\Phi_p(-x)}\,. \tag{43}$$

Now, iterating the identity (2) and using (16), we get

$$a((2^{p-3}+1)2^{p+1};x) = a(2^{p-3}+1;x^{2^{p+1}}) = 1+\sum_{j=0}^{p-4}\left(x^{2^{p+1}}\right)^{2^j} \tag{44}$$

$$\equiv 1+\sum_{j=0}^{p-4}\left(x^4\right)^{2^j} = 1+\sum_{j=0}^{p-4}\left(x^2\right)^{2^{j+1}}$$

$$\equiv 1+(x^2)^2+(x^2)^3+\cdots+(x^2)^{p-1}-(x^2)^{2^{p-2}} \pmod{\Phi_p(-x)}\,,$$

where we have taken into account the fact that $2^{j+1}, j=0,1,\ldots,p-3$, is a reordering of $2,3,\ldots,p-1 \pmod p$, and that the upper limit of summation in the second line of (44) is only $p-4$. Next we note that by Fermat's little theorem we have $2^{p-2} \equiv \frac{p+1}{2} \pmod{p}$, so that

$$(x^2)^{2^{p-2}} \equiv x^{p+1} \pmod{\Phi_p(-x)}. \tag{45}$$

Using this congruence and (42), we get with (44) that

$$a((2^{p-3}+1)2^{p+1};x) \equiv 1+x^4+x^6+\cdots+x^{p-1}-x^3-x^5-\cdots-x^{p-2} \pmod{\Phi_p(-x)}.$$

Finally, subtracting $\Phi_p(-x) = 1-x+x^2-\cdots+x^{p-1}$ from the right-hand side of this last congruence, we get (39).

To prove (40), we use (15) and (42) to obtain

$$\begin{aligned} a(2^p-1;x) &= 1+\frac{1}{x}\sum_{j=0}^{p-2}\left(x^2\right)^{2^j} \\ &\equiv 1+\frac{1}{x}\left(x^2+(x^2)^2+(x^2)^3+\cdots+(x^2)^{p-1}\right) \\ &= 1+x+x^3+\cdots+x^{p-2}+x^p+x^{p+2}+\cdots+x^{p+p-3} \\ &\equiv 1+x+x^3+\cdots+x^{p-2}-1-x^2-\cdots-x^{p-3} \pmod{\Phi_p(-x)}, \end{aligned}$$

but this is just the right-hand side of (40)

Finally, to prove (41), we proceed exactly as in the proof of (39). Again (42) and a version of (43) are used; we leave the details to the reader. This completes the proof of Proposition 17. □

Using this result, we immediately obtain the following consequence of Proposition 16.

**Corollary 11.** *Let $p$ be an odd prime which has 2 as a primitive root. If $\mu \geq 1$ is such that $\Phi_p(x) \mid a(m_p\mu;x)$ then $\Phi_p(-x)$ divides $a(m_p(\mu 2^k \pm m_p);x)$ whenever $k \geq 2p-1$.*

This corollary follows from Proposition 16 by setting $j = m_p$; it is then easy to see with the definition of $m_p$ that the condition $j \leq \lfloor 2^k/m_p \rfloor$ holds whenever $k \geq 2p-1$.

Finally, as far as a generalization of Proposition 14 is concerned, we note that the proof of that result depended in an essential way on the fact that the left-hand side of (31) is divisible by $x^2-x+1$. For this proof to work in general, we require the following extension of (31).

**Lemma 3.** *If $p$ is an odd prime which has 2 as a primitive root, then*

$$\Phi_p(-x) \mid a(m_p;x) + 2x^{m_p} a(2^{2p-2}-m_p;x). \tag{46}$$

*Proof.* We begin by showing that

$$a(m_p;x) = a(2^{p-1}+1;x) \equiv 2x \pmod{\Phi_p(-x)}. \tag{47}$$

Indeed, using (16) and the remarks in the proof of Proposition 17, including (45), we find that

$$\begin{aligned} a(m_p;x) &= 1+x+\sum_{j=0}^{p-3}\left(x^2\right)^{2^j} \\ &\equiv 1+x+x^2+(x^2)^2+(x^2)^3+\cdots+(x^2)^{p-1}-(x^2)^{2^{p-2}} \\ &\equiv 1+x+x^2+x^4+x^6+\cdots+x^{p-1}+x^{p+1}+x^{p+3}+\cdots+x^{p+p-2}-x^{p+1} \\ &\equiv 1+x+x^2+x^4+x^6+\cdots+x^{p-1}-x^3-x^5-\cdots-x^{p-2} \\ &\equiv 2x \pmod{\Phi_p(-x)}\,. \end{aligned}$$

This proves (47). Next we use (25) with $k=p$, $j=m_p$, $m=2^{p-2}$, and note that $2^p-m_p=2^{p-1}-1$. This gives

$$a(2^{2p-2}-m_p;x)=a(2^{p-1}-1;x)+x^{2^{p-1}-1}a(m_p;x)a(2^{2p-2}-2^p;x)\,. \tag{48}$$

We now evaluate, modulo $\Phi_p(-x)$, the various terms in (46) and (48). First, by Fermat's little theorem we have $2^{p-1}+1\equiv 2 \pmod p$ and also $2^{p-1}+1\equiv 1 \pmod 2$, which combines to give $m_p=2^{p-1}+1\equiv p+2 \pmod{2p}$ by the Chinese Remainder Theorem. Consequently, we get $2^{p-1}-1\equiv p \pmod{2p}$. Thus, by (42) we have

$$x^{m_p}\equiv -x^2 \pmod{\Phi_p(-x)},\qquad x^{2^{p-1}-1}\equiv -1 \pmod{\Phi_p(-x)}\,. \tag{49}$$

Next, using (19) with $k=p-1$ and $j=1$, we get

$$x\cdot a(2^{p-1}-1;x)=a(2^{p-1}+1;x)-1\equiv 2x-1 \pmod{\Phi_p(-x)}\,, \tag{50}$$

where we have used (47). Similarly, using (19) with $k=2p-2$ and $j=2^p$, we get with (5) that

$$x^{2^p}a(2^{2p-2}-2^p;x)=a(2^{2p-2}+2^p;x)-1\,. \tag{51}$$

Since $2^p\equiv 2 \pmod p$ and $2^p\equiv 2 \pmod 2$, the Chinese Remainder Theorem gives $2^p\equiv 2 \pmod{2p}$, and by (42) we have

$$x^{2^p}\equiv x^2 \pmod{\Phi_p(-x)}\,.$$

This congruence and (41), together with (51), shows that

$$x^2a(2^{2p-2}-2^p;x)\equiv x-1 \pmod{\Phi_p(-x)}\,. \tag{52}$$

Finally, combining (47) and (48) with (49), (50) and (52), the right-hand side of (46), taken modulo $\Phi_p(-x)$, becomes

$$2x-2[x(2x-1)-2x(x-1)]=0\,,$$

which completes the proof of (46). □

We are now ready to state the desired generalization of Proposition 14.

**Proposition 18.** *Let $p$ be an odd prime which has 2 as a primitive root. If $j \geq 1$ is an odd integer such that $\Phi_p(-x)$ divides $a(m_p j; x)$, then $\Phi_p(-x)$ also divides $a(m_p(2^{2p-2}j \pm 1); x)$.*

The proof of this result is completely analogous to that of Proposition 14, with $m_3 = 5$ replaced by $m_p$ and $k = 4$ replaced by $k = 2p - 2$. The divisibility relation (46) plays the role of the identity (31). We leave all further details to the reader. As an illustration we explicitly state the case $p = 5$.

**Corollary 12.** *If $j \geq 1$ is an odd integer such that $x^4 - x^3 + x^2 - x + 1$ divides $a(17j; x)$, then $x^4 - x^3 + x^2 - x + 1$ divides $a(17(256j \pm 1); x)$.*

# 7 Discriminants and zeros

## 7.1 The discriminant of $a(n; x)$

The various results on cyclotomic factors in this paper give rise to the natural question as to whether a square or a higher power of a cyclotomic polynomial can divide a Stern polynomial. In this subsection we will show that this cannot happen.

**Proposition 19.** *A Stern polynomial $a(n; x)$ cannot be divisible by the square of a nonconstant polynomial.*

By (2) and (4) it suffices to consider odd indices $n$ since a square factor of $a(2n; x)$ would also be one of $a(n; x^2)$, which in turn means that $a(n; x)$ would have a square factor. Proposition 19 is now an immediate consequence of the following result since the discriminant of a polynomial vanishes if and only if the polynomial has a multiple zero. This is clear from the definition of the discriminant: Suppose we are given a polynomial

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 = a_n(x - r_1) \ldots (x - r_n) \tag{53}$$

with nonzero leading coefficient $a_n$ and not necessarily distinct zeros $r_1, \ldots, r_n$. Then the *discriminant* of $f(x)$ can be defined as

$$D_x(f(x)) := a_n^{2n-2} \prod_{i<j} (r_i - r_j)^2 \,; \tag{54}$$

see, e.g., [16, p. 217]. We are now ready to state and prove a result which immediately implies Proposition 19.

**Proposition 20.** *The discriminant $D_x(a(2n + 1; x))$ is always an odd integer, and is therefore nonzero.*

For the proof of this we require a general fact about the discriminant of a polynomial, which we were unable to find in the literature.

**Lemma 4.** *Let $f(x)$ be a polynomial of degree $n \geq 1$ with $f(0) \neq 0$. Then*

$$D_x(f(x)) = D_x\left(x^n f(\tfrac{1}{x})\right). \tag{55}$$

*In other words, the discriminants of a polynomial and of its reciprocal are identical.*

*Proof.* The polynomial $x^n f(1/x)$ can be obtained from $f(x)$ by reversing the order of the coefficients. Also, if $f(x)$ is given as in (53), then the zeros of $x^n f(1/x)$ are obviously $1/r_1, \dots, 1/r_n$. Hence, with (54) we have

$$D_x\left(x^n f(\tfrac{1}{x})\right) = a_0^{2n-2}\prod_{i<j}\left(\frac{1}{r_i}-\frac{1}{r_j}\right)^2 = a_0^{2n-2}\prod_{i<j}\left(\frac{r_j-r_i}{r_ir_j}\right)^2. \tag{56}$$

By counting the number of times each $r_j$ occurs in the first product below, we get

$$\prod_{i<j}\frac{1}{r_ir_j} = \left(\prod_{j=1}^{n}\frac{1}{r_j}\right)^{n-1} = \left(\frac{(-1)^n a_n}{a_0}\right)^{n-1},$$

where the second equality follows from (53). Rewriting this, and squaring, we get

$$a_0^{2n-2}\prod_{i<j}\frac{1}{(r_ir_j)^2} = a_n^{2n-2}.$$

Finally, this last identity, together with (56) and (54), gives the desired identity (55). □

*Proof of Proposition 20.* The discriminant of a polynomial $f$ of degree $n$ and leading coefficient $a_n$ satisfies $D_x(f) = (-1)^{n(n-1)/2}a_n^{-1}R(f,f')$, where $R(f_1,f_2)$ is the resultant of the polynomials $f_1$ and $f_2$, which can be written as a determinant (the determinant of the Sylvester matrix) that involves sums of products of the coefficients of $f_1$ and $f_2$. Therefore, if $f$ is a monic polynomial with integer coefficients, we have the relation

$$D_x(f(x)) \equiv D_x(g(x)) \pmod{n} \quad \text{if} \quad f(x) \equiv g(x) \pmod{n}$$

for any integer $n > 1$. Now, in [3, (6.2)] it was shown that

$$a(2n+1;x) \equiv x^n U_{2n}\left(\tfrac{1}{2\sqrt{x}}\right) \pmod{2},$$

where $U_n(x)$ is the $n$th Chebyshev polynomial of the second kind. This congruence, combined with identity (55), means that we are done if we can show that $D_x(U_{2n}(\sqrt{x}/2))$ is an odd integer. We are going to show more, namely

$$D_x\left(U_{2n}\left(\tfrac{\sqrt{x}}{2}\right)\right) = (2n+1)^{n-1}. \tag{57}$$

To do so, we first note that $U_{2n}(x) = 2^{2n}x^{2n} - \cdots + (-1)^n$ has only even powers of $x$ and coefficients with alternating signs (see, e.g., [16]), and as a consequence we have $U_{2n}(\sqrt{x}/2) = x^n - \cdots + (-1)^n$. This is a monic polynomial, again with alternating coefficients which are integers, a fact that follows easily from standard properties of the $U_n(x)$. We also know that $U_{2n}(x)$ has $2n$ distinct real zeros, say $\pm\rho_j$, $j = 1,\dots,n$; the polynomial $U_{2n}(\sqrt{x}/2)$ then has the $n$ positive real zeros $4\rho_j^2$. Now by (54) we have

$$D_x\left(U_{2n}(x)\right) = \left(2^{2n}\right)^{4n-2}\prod_{i<j}(\rho_i-\rho_j)^2(\rho_i+\rho_j)^2(-\rho_i-\rho_j)^2(-\rho_i+\rho_j)^2\prod_{j=1}^{n}(2\rho_j)^4,$$

which can be seen by ordering the zeros of $U_{2n}(x)$ as $r_1 = -\rho_1, r_2 = \rho_1, \dots, r_{2n-1} = -\rho_n$, $r_{2n} = \rho_n$. Rearranging the factors, we get

$$D_x\left(U_{2n}(x)\right) = 2^{2n(4n-2)}\prod_{i<j}(\rho_i^2-\rho_j^2)^4\prod_{j=1}^{n}(2\rho_j)^4. \tag{58}$$

Now the product $\prod\rho_j^2$ is the product of all zeros of $U_{2n}(x)$, times $(-1)^n$; but the product of all the zeros is $a_0/a_{2n} = (-1)^n2^{-2n}$, by (53). Hence, the powers of 2 will cancel in the second product on the right of (58), and this product will simply be 1. On the other hand, it is known that

$$D_x\left(U_{2n}(x)\right) = 2^{4n^2}(2n+1)^{2n-2};$$

see [16, p. 219]. By combining this with (58) and taking square roots, we obtain

$$\prod_{i<j}(\rho_i^2-\rho_j^2)^2 = 2^{2n-2n^2}(2n+1)^{n-1}. \tag{59}$$

From the definition (54) and our above observation concerning $U_{2n}(\sqrt{x}/2)$, we get

$$D_x\left(U_{2n}(\tfrac{\sqrt{x}}{2})\right) = \prod_{i<j}(4\rho_i^2-4\rho_j^2)^2 = 16^{n(n-1)/2}\prod_{i<j}(\rho_i^2-\rho_j^2)^2.$$

This identity, combined with (59), finally gives (57), and the proof is complete. □

In the special case of the polynomials $a(2^n-1;x)$, the result of Proposition 19 was obtained in [1] in two different ways, distinct from the approach given above.

### 7.2 Zeros of the Stern polynomials

Proposition 19 can also be seen as a result on the zeros of Stern polynomials in that it shows that there can only be simple zeros. Also, since the zeros of cyclotomic polynomials all lie on the unit circle and (at least in the case of $\Phi_p(\pm x)$) have an almost uniform angular distribution, it may be of interest to consider the distribution of all zeros of the Stern polynomials $a(n;x)$. This was in fact done in a recent paper of A. R. Vargas [21]. Among other results, Vargas showed that, given a real number $\rho$ satisfying $0<\rho<1$, the proportion of zeros of $a(n;z)$ that lie on the annulus $1-\rho\le|z|\le1/(1-\rho)$ approaches 1 as $n\to\infty$, and that the zeros are uniformly distributed in a certain sense. For details, see [21, Prop. 2.1]. On the other hand, it was shown in [11] and [1] that we must expect infinite subsequences of Stern polynomials which have zeros bounded away from the unit circle. In particular, this is the case for the sequence of polynomials in (17).

## 8 Conjectures and further remarks

We conclude this paper with a few open problems and conjectures, as well as some related results and remarks.

### 8.1 Stern polynomials with prime index

We begin by considering the question of irreducibility of Stern polynomials with prime index. On the one hand we have Proposition 1 which shows that we do have irreducibility for a certain important class of prime indices, but on the other hand there is the obvious counterexample $a(17;x)$; see Table 1. We have not found any other reducible Stern polynomial with prime index; therefore we propose the following conjecture.

**Conjecture 1.** *Let $q \geq 3$ be a prime, $q \neq 17$. Then $a(q;x)$ is irreducible.*

We verified Conjecture 1 by computation for all primes up to 16 000. This conjecture is also supported by the fact that all Stern polynomials which we found and proved to be reducible have indices that are of the form $2^{t(p)pm} - 1$ (and thus are composite) as in Proposition 6, or have indices which are multiples of $m_p = 2^{p-1} + 1$, as in Section 6. This last case includes the possibility of $m_p$ itself being the index, as in Proposition 8. For this reason the following easy result is relevant.

**Lemma 5.** *The integer $m_p = 2^{p-1} + 1$ is prime for $p = 3$ and $p = 5$, and is composite for all other primes $p$ which have 2 as a primitive root.*

This means that $m_3 = 5$ and $m_5 = 17$ are the only prime indices which occur in Proposition 8, or in any other divisibility result. While we have $x^2+x+1 = a(5;x)$, the next case, namely $x^4 + x^3 + x^2 + x + 1$, is in fact a proper divisor of $a(17;x)$. This explains the exceptionality of $q = m_5 = 17$, and the likelihood of this being the only exception. Note that $p = 3, 5$ and $q = 5, 17$ are among the first three Fermat primes, a fact that plays a role in the following proof.

*Proof of Lemma 5.* A necessary condition for $2^{p-1} + 1$ being prime (and thus a Fermat prime) is that $p - 1 = 2^k$ for some $k \geq 1$; i.e., $p$ itself has to be a Fermat prime. However, the multiplicative order of 2 modulo a Fermat prime $F_k = 2^{2^k} + 1$ is $2^{k+1}$ since $2^{2^k} \equiv -1 \pmod{F_k}$. But $F_k - 1 = 2^{2^k} > 2k + 1$ for $k \geq 2$, so no Fermat prime $F_k$, $k \geq 2$, can have 2 as a primitive root. This leaves $p = F_0 = 3$ and $p = F_1 = 5$ as the only possibilities, and the proof is complete. □

### 8.2 Cyclotomic factors

Our second conjecture is related to the remarks following Conjecture 1.

**Conjecture 2.** *Let $p \geq 3$ be a prime which has 2 as a primitive root. If $\Phi_p(x)$ or $\Phi_p(-x)$ divides $a(n;x)$, then $m_p$ divides $n$.*

Cyclotomic polynomials seem to be even more prevalent than this conjecture may indicate. Indeed, we propose the following.

**Conjecture 3.** *If a Stern polynomial is reducible, then it is divisible by a cyclotomic polynomial $\Phi_k(x)$ for some $k \geq 3$.*

### 8.3 Non-reciprocal parts

Much of the work in this paper has been devoted to exposing small factors of Stern polynomials. These factors all turned out to be cyclotomic (see also Conjecture 3), while the non-cyclotomic cofactors seem to be irreducible.

This observation is related to the following concepts and results. The *non-reciprocal part* of a polynomial $f(x)$ with integer coefficients is essentially $f(x)$ with its irreducible reciprocal factors removed, where a *reciprocal polynomial* $g(x)$ satisfies $g(x) = \pm x^{\deg g} g(1/x)$. In Table 1, for instance, the first factors of $a(17;x)$ and $a(25;x)$ are reciprocal polynomials, while the second factors are the non-reciprocal parts. Also, the polynomials $a(n;x)$ for $n = 3$, 5, 6, 10, 12, 20 and 24 are themselves reciprocal, and their non-reciprocal parts are therefore identically 1. We recall that cyclotomic polynomials are reciprocal as well. For further remarks on these concepts see, e.g., the introduction of [6].

Based on earlier work of Schinzel, a criterion for a polynomial of the form $f(x)x^n + g(x)$, with $f(x), g(x) \in \mathbb{Z}[x]$, to have an irreducible non-reciprocal part was established by Filaseta, Ford and Konyagin [5]. This result was considerably strengthened by Filaseta and Matthews [6] in the special case of $(0,1)$-polynomials. Although this last result fails to be applicable to the Stern polynomials, our observations suggest that the conclusion still holds:

**Conjecture 4.** *All Stern polynomials have a non-reciprocal part that is either irreducible or is identically* 1.

As pointed out in [6], if it is known that a polynomial $f(x)$ has an irreducible non-reciprocal part, then $f(x)$ is itself irreducible if it has no factor in common with its reciprocal $x^{\deg f} f(1/x)$. Thus, assuming Conjecture 4, we were able to verify Conjecture 1 by computation for all $q \le 100\,000$.

### 8.4 Relations with $(-1,0,1)$ polynomials

Related to the above discussion, we observed that in two special cases the non-reciprocal factors seem to have a very specific form in that they have coefficients $-1, 0, 1$. These cases are

(1) $a(2^{t(p)pm} - 1; x)$ for $m \ge 1$ and primes $p \ge 3$; see Proposition 6;

(2) $a(2^{p-1} + 1; x)$ for a prime $p \ge 3$ which has 2 as a primitive root; see Proposition 8.

In the second case we observed, in addition, that the nonzero coefficients are alternating between $\pm 1$. As this lies outside the scope of the present paper, we did not pursue this further.

### 8.5 Another irreducibility criterion

We conclude this section by mentioning an irreducibility criterion of a different nature from those discussed earlier. Building on an interesting irreducibility result of A. Cohn, which had earlier been extended by Brillhart, Filaseta and Odlyzko (1981) and by Filaseta (1988), M. R. Murty [14] proved the following result.

**Proposition 21 (Murty).** *Let $b \geq 2$ and let $p$ be a prime with $b$-adic expansion $p = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0$. Then the polynomial $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ is irreducible.*

Since Stern polynomials are $(0,1)$-polynomials, we immediately get the following consequence.

**Corollary 13.** *If $a(n;b)$ is prime for some integer $b \geq 2$, then $a(n;x)$ is irreducible.*

By (7) we know that in most cases the degree of $a(n;x)$ is $(n-1)/2$, or close to it. Thus, even for $b = 2$ the integers $a(n;b)$ will soon get very large as $n$ grows. Therefore in most cases primality testing will not be competitive in comparison with irreducibility testing algorithms as implemented in computer algebra systems such as Maple or Mathematica.

## Acknowledgement

We thank the referee for several helpful suggestions.

Research was supported in part by the Natural Sciences and Engineering Research Council of Canada.

## References

[1] K. Dilcher, L. Ericksen: The polynomials of Mahler and roots of unity. *Amer. Math. Monthly.* (To appear).

[2] K. Dilcher, L. Ericksen: Identities and restricted quotients in the Stern sequence. (In preparation).

[3] K. Dilcher, K.B. Stolarsky: A polynomial analogue to the Stern sequence. *Int. J. Number Theory* 3 (1) (2007) 85–103.

[4] K. Dilcher, K.B. Stolarsky: Stern polynomials and double-limit continued fractions. *Acta Arith.* 140 (2) (2009) 119–134.

[5] M. Filaseta, K. Ford, S Konyagin: On an irreducibility theorem of A. Schinzel associated with coverings of the integers. *Illinois J. Math.* 44 (3) (2000) 633–643.

[6] M. Filaseta, M. Matthews (Jr.): On the irreducibility of 0,1-polynomials of the form $f(x)x^n + g(x)$. *Colloq. Math.* 99 (1) (2004) 1–5.

[7] C. Finch, L. Jones: On the irreducibility of $\{-1,0,1\}$-quadrinomials. *Integers* 6 (2006). A16, 4 pp.

[8] S. Klavžar, U. Milutinović, C. Petr: Stern polynomials. *Adv. in Appl. Math.* 39 (2007) 86–95.

[9] D.H. Lehmer: On Stern's diatomic series. *Amer. Math. Monthly* 36 (1929) 59–67.

[10] W. Ljunggren: On the irreducibility of certain trinomials and quadrinomials. *Math. Scand.* 8 (1960) 65–70.

[11] K. Mahler: On the zeros of a special sequence of polynomials. *Math. Comp.* 39 (159) (1982) 207–212.

[12] I. Mercer: Newman polynomials, reducibility, and roots on the unit circle. *Integers* 12 (2012) 503–519.

[13] W.H. Mills: The factorization of certain quadrinomials. *Math. Scand.* 57 (1985) 44–50.

[14] M.R. Murty: Prime numbers and irreducible polynomials. *Amer. Math. Monthly* 109 (2002) 452–458.

[15] OEIS Foundation Inc. (2011): The On-Line Encyclopedia of Integer Sequences. http://oeis.org

[16] T.J. Rivlin: *Chebyshev Polynomials*, second edition. Wiley, New York (1990).

[17] A. Schinzel: On the factors of Stern polynomials (remarks on the preceding paper of M. Ulas). *Publ. Math. Debrecen* 79 (1–2) (2011) 83–88.

[18] E.S. Selmer: On the irreducibility of certain trinomials. *Math. Scand.* 4 (1956) 287–302.

[19] B. Tuckerman: Factorization of $x^{2n} + x^n + 1$ using cyclotomic polynomials. *Math. Magazine* 42 (1) (1969) 41–42.

[20] M. Ulas: On certain arithmetic properties of Stern polynomials. *Publ. Math. Debrecen* 79 (1–2) (2011) 55–81.

[21] A.R. Vargas: Zeros and convergent subsequences of Stern polynomials. *J. Math. Anal. Appl.* 398 (2013) 630–637.

[22] E.W. Weisstein: Cyclotomic Polynomial. From MathWorld–A Wolfram Web Resource. http://mathworld.wolfram.com/CyclotomicPolynomial.html

*Authors' addresses:*
Karl Dilcher: Department of Mathematics and Statistics, Dalhousie University, Halifax, Nova Scotia, B3H 4R2, Canada

*E-mail:* dilcher@mathstat.dal.ca

Larry Ericksen: P.O. Box 172, Millville, NJ 08332-0172, USA

*E-mail:* LE22@cornell.edu

*Received:* 28 October, 2013
*Accepted for publication:* 9 May, 2014
*Communicated by:* Olga Rossi