Algebra and Discrete Mathematics
Number 2. **(2008).** pp. 65 – 82

RESEARCH ARTICLE

Characterization of Chebyshev Numbers

David Pokrass Jacobs, Mohamed O. Rayes and Vilmar Trevisan

Communicated by I. P. Shestakov

Abstract. Let $T_n(x)$ be the degree-n Chebyshev polynomial of the first kind. It is known [1, 13] that $T_p(x) \equiv x^p \bmod p$, when p is an odd prime, and therefore, $T_p(a) \equiv a \bmod p$ for all a. Our main result is the characterization of composite numbers n satisfying the condition $T_n(a) \equiv a \bmod n$, for any integer a. We call these pseudoprimes *Chebyshev numbers*, and show that n is a Chebyshev number if and only if n is odd, squarefree, and for each of its prime divisors p, $n \equiv \pm 1 \bmod p-1$ and $n \equiv \pm 1 \bmod p+1$. Like Carmichael numbers, they must be the product of at least three primes. Our computations show there is one Chebyshev number less than 10^{10}, although it is reasonable to expect there are infinitely many. Our proofs are based on factorization and resultant properties of Chebyshev polynomials.

1. Introduction

Chebyshev polynomials have been used in many areas of mathematics, and their analytic properties are particularly useful in numerical analysis and approximation theory. Recently, there has been a renewed interest in their algebraic properties. Results on factorization and divisibility of Chebyshev polynomials appear in [5, 11, 13, 14]. Congruence and number theoretic properties of Chebyshev polynomials can be found in [1, 10, 12, 13, 14].

Research partially supported by CNPq - Grants 478290/04-7 and 43991/2005-0; and FAPERGS - Grant 05/2024.1

2000 Mathematics Subject Classification: *11A07, 11Y35.*

Key words and phrases: *Chebyshev polynomials, polynomial factorization, resultant, pseudoprimes, Carmichael numbers.*

The *Chebyshev polynomials of the first kind*, denoted $T_n(x)$ throughout this paper, can be defined by the following recurrence relation. Set $T_0(x) = 1$ and $T_1(x) = x$. Then

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x), \qquad n = 2, 3, \ldots$$

Alternatively, they may be defined as

$$T_n(x) = \cos(n \arccos x),$$

where $0 \leq \arccos x \leq \pi$. The roots of $T_n(x)$ are real, distinct, lie within the interval $[-1, 1]$, and are given by the closed formula

$$\xi_k = \cos \frac{(2k-1)}{n} \frac{\pi}{2} \qquad k = 1, \ldots, n.$$

For polynomials $f(x), g(x) \in \mathbb{Z}[x]$, we write $f(x) \equiv g(x) \bmod p$ to mean that corresponding coefficients of $f(x)$ and $g(x)$ are congruent modulo p. Our starting point is the following theorem.

Theorem 1. *If p is an odd prime, then $T_p(x) \equiv x^p \bmod p$.*

This congruence was published in 1954 by Bang [1], and also appears in [13, p. 232], where it is referred to as Fermat's Theorem for the Chebyshev Polynomials. In the next section we show in Theorem 4 that for odd numbers $p > 1$, primality is equivalent to $T_p(x) \equiv x^p \bmod p$. Note that by applying Fermat's Little Theorem, one obtains:

Corollary 1. *For odd primes p, $T_p(a) \equiv a \bmod p$ for all integers a.*

There is some evidence that these results were discovered in the early 1900's by I. Schur. The 1973 volume [14, p. 425] of previously unpublished work of Schur contains the equation $T_p(x) \equiv x \bmod p$, and according to a footnote, was found in a manuscript written between 1905 and 1918.

The main focus of this paper concerns composite numbers n that satisfy the condition of Corollary 1. We say a composite number n is a *Chebyshev number*, or is *Chebyshev*, if for all integers a

$$T_n(a) \equiv a \bmod n.$$

In this paper we characterize Chebyshev numbers. We will prove

Theorem 2. *A Chebyshev number is odd, square free and the product of at least three primes.*

Our main result is

Theorem 3. *An odd square free integer n is a Chebyshev number if and only if for each prime divisor p of n,*

$$n \equiv \pm 1 \bmod p-1 \text{ and } n \equiv \pm 1 \bmod p+1.$$

It is easy to see that the condition on each prime is equivalent to the conjunction of the following four conditions:

$$(p-1) \mid (n+1) \quad \text{and} \quad (p+1) \mid (n+1) \tag{1}$$
$$(p-1) \mid (n-1) \quad \text{and} \quad (p+1) \mid (n-1) \tag{2}$$
$$(p-1) \mid (n-1) \quad \text{and} \quad (p+1) \mid (n+1) \tag{3}$$
$$(p-1) \mid (n+1) \quad \text{and} \quad (p+1) \mid (n-1) \tag{4}$$

A Chebyshev number is a kind of *pseudoprime*, that is, a composite which behaves in some way like a prime. The paper [3] contains an overview of many kinds of pseudoprimes.

Carmichael numbers may be defined as composites n for which $a^n \equiv a \bmod n$ for every integer a. There is an obvious parallel between Chebyshev numbers and Carmichael numbers, as each can be defined with a polynomial equation. Theorem 3 is analogous to the Korselt criterion which states that a composite number n is a Carmichael number if and only if it is squarefree and for each prime p dividing n, we have $n \equiv 1 \bmod p-1$. The result of Theorem 2 also holds for Carmichael numbers. We will see that the sets of Carmichael numbers and Chebyshev numbers intersect, but neither set contains the other.

In the following section, we obtain the converse of Theorem 1. The remainder of the paper is devoted to characterizing Chebyshev numbers. In Section 3, we derive some factorization properties of Chebyshev polynomials. In Section 4 we derive some resultant properties of Chebyshev polynomials in order to obtain the proofs of our main results. This is done is section 5, where Lemmas 20–22 prove Theorem 2 and Lemmas 23–25 prove Theorem 3.

2. Fermat's Theorem for Chebyshev Polynomials

In this section we give a new and elementary proof of Theorem 1, as well as its converse. Let $n = 2m+1$ be an odd integer, and let $T_n(x)$ be the Chebyshev polynomial of degree n. There exist many closed formulas and recurrence relations for the coefficients of $T_n(x)$. The following formulation is due to Snyder [15, p.14]. For $i > 0$ and $j \geq 0$ define

$$t_i^j = (-1)^j 2^{i-1} \left\{ \frac{i+2j}{i+j} \right\} \binom{i+j}{j}. \tag{5}$$

Then, for $n = 2m + 1$, we have

$$T_n(x) = \sum_{k=0}^{m} t_{2k+1}^{m-k} x^{2k+1}. \tag{6}$$

Lemma 1. *Let $p = 2l + 1$ be a prime divisor of $n = 2m + 1$. Then $p \nmid \binom{p+m-l-1}{p-1}$.*

Proof. Since $n-p = 2(m-l)$, p divides $m-l$ and so $p+m-l \equiv 0 \bmod p$. However, the numerator of the binomial coefficient is a product of $p-1$ descending consecutive numbers. The first of these is $p + m - l - 1 \equiv -1 \bmod p$. Hence the remaining factors are not divisible by p either. □

Lemma 2. *Let $p = 2l+1$ be an odd prime divisor of n. Then n does not divide the coefficient t_p^{m-l} of x^p in $T_n(x)$.*

Proof. >From the closed formula (5) for t_p^{m-l}, we obtain

$$\begin{aligned} t_p^{m-l} &= (-1)^{m-l} 2^{p-1} \left\{ \frac{p + 2(m-l)}{p+m-l} \right\} \binom{p+m-l}{m-l} \\ &= (-1)^{m-l} 2^{p-1} \left\{ \frac{p + (n-p)}{p+m-l} \right\} \binom{p+m-l}{p} \\ &= (-1)^{m-l} 2^{p-1} \left\{ \frac{n(p+m-l)}{(p+m-l)p} \right\} \binom{p+m-l-1}{p-1} \\ &= 2^{p-1}(-1)^{m-l} \left\{ \frac{n}{p} \right\} \binom{p+m-l-1}{p-1}. \end{aligned}$$

To complete the proof, let p^k be the largest power of p dividing n. By Lemma 1, $p \nmid \binom{p+m-l-1}{p-1}$. Since p^k does not divide $\frac{n}{p}$, we see that p^k and (hence n) does not divide t_p^{m-l}. □

Theorem 4. *An odd integer $p > 1$ is prime if and only if $T_p(x) \equiv x^p \bmod p$.*

Proof. First let $n = p = 2m+1$ be a prime number. Then the coefficients of x^{2k+1} in $T_p(x)$ are given by

$$t_{2k+1}^{m-k} = (-1)^{m-k} 2^{2k} \left\{ \frac{2m+1}{m+k+1} \right\} \binom{m+k+1}{m-k}.$$

By setting $k = m$ we first see that the leading coefficient is $t_p^0 = 2^{p-1}$. Next, assume $k < m$. Then note that the numerator of $\left\{ \frac{2m+1}{m+k+1} \right\}$ is p, and the denominator is greater than one and less than p. Since p is prime, the

denominator must divide the other factors in the expression, and so the entire expression is divisible by p. This leads to the congruence $T_n(x) \equiv 2^{p-1}x^p \equiv x^p \bmod p$, by Fermat's Little Theorem. Conversely, suppose that n is composite. Let $p = 2l+1$ be a prime dividing n. Lemma 2 shows that t_p^{m-l} is not divisible by n, which implies that $T_n(x) \not\equiv x^n \bmod n$. □

3. Factorization Properties of Chebyshev polynomials

The main purpose of this section is to determine $\gcd(T_m(x)-x, T_n(x)-x)$ which is done in Lemma 8. It will be necessary to make use of *Chebyshev polynomials of the second kind*, denoted $U_n(x)$ throughout the remainder of this paper, which are defined by $U_0(x) = 1$, $U_1(x) = 2x$ and the recurrence relation

$$U_n(x) = 2xU_{n-1}(x) - U_{n-2}(x).$$

They can also be defined by

$$U_n(x) = \frac{1}{n+1}T'_{n+1}(x) = \frac{\sin\left((n+1)\arccos x\right)}{\sin(\arccos x)}. \tag{7}$$

It is easy to see that $U_n(x)$ is an integral polynomial of degree n. Its roots are all real, distinct, symmetric with respect to the line $x = 0$, and are given by the expression

$$\eta_k = \cos\frac{k\pi}{n+1}, \quad k = 1, \ldots, n. \tag{8}$$

We will need a result that gives the factorization of the $U_n(x)$, into irreducible integral factors. Consider a fixed integer $n \geq 2$. Let $h \leq n$ be a positive divisor of $2n+2$, and define

$$S_h = \{k : \gcd(k, 2n+2) = h, 1 \leq k \leq n\}.$$

It can be shown that $l_h = \mid S_h \mid = \frac{\phi(\frac{2n+2}{h})}{2}$, where ϕ is the Euler totient. For, $k \in S_h$ if and only if $\gcd(k, 2n+2) = h$ and $1 \leq k \leq n$. This is equivalent to writing $k = jh$ where $1 \leq j < \frac{n+1}{h}$. It can be shown that for any m, the set $\{j : 1 \leq j < m, \gcd(j, 2m) = 1\}$ has cardinality $\frac{\phi(2m)}{2}$,

Now let

$$E_h(x) = 2^{l_h} \prod_{\substack{1 \leq k \leq n \\ (k, 2n+2) = h}} (x - \eta_k), \tag{9}$$

where η_k are the zeros of $U_n(x)$ defined in equation (8).

Lemma 3. *For any integer $n \geq 2$, $U_n(x)$ has the factorization*

$$U_n(x) = \prod_h E_h(x),$$

where $h \leq n$ runs through all positive divisors of $2n+2$. The E_h are irreducible over the integers.

Proof. With a slight change in notation, this equation appears in [13, Eq. 5.29]. □

It is worth noting that Rivlin attributes his inspiration to a remark made by Schur [14, p. 423]. It is also worth noting that this factorization is similar to one given by Hsiao [5], for factoring Chebyshev polynomials of the first kind into rational irreducible factors.

Lemma 4. *Let $n \leq m$ be two positive integers and let $E_1(x)$ be the irreducible factor of $U_n(x)$ as defined by equation (9). If $E_1(x)$ divides $U_m(x)$, then $U_n(x)$ divides $U_m(x)$.*

Proof. If $E_1(x)$ divides $U_m(x)$, then the root $\cos\frac{\pi}{n+1}$ of $E_1(x)$ is also a root of $U_m(x)$, i.e. $\cos\frac{\pi}{n+1} = \cos\frac{r\pi}{m+1}$, for some $r < m$. Hence $r = \frac{m+1}{n+1}$ or $\frac{1}{n+1} = \frac{r}{m+1}$. Consequently, every root $\cos\frac{k\pi}{n+1}$ of $U_n(x)$ equals $\cos\frac{kr\pi}{m+1}$, a root of $U_m(x)$. Since roots of U_n are simple, it follows that $U_n | U_m$. □

We now devise a decomposition of the polynomial $T_n(x) - x$ whose factors are Chebyshev polynomials of the second kind.

Lemma 5. *For any odd integer $n \geq 3$, the factorization in $\mathbb{Z}[x]$ holds:*

$$T_n(x) - x = -2(1-x^2)U_{\frac{n-1}{2}}(x)U_{\frac{n-3}{2}}(x) \tag{10}$$

Proof. By setting $x = \cos(\theta)$, and then using the trigonometric definition of $T_n(x)$, some well-known trigonometric identities, and (7), we get:

$$\begin{aligned} T_n(x) - x &= \cos(n\theta) - \cos(\theta) \\ &= -2\sin\left(\frac{(n+1)\theta}{2}\right)\sin\left(\frac{(n-1)\theta}{2}\right) \\ &= -2\left(1-\cos^2(\theta)\right)\frac{\sin\left(\frac{(n+1)\theta}{2}\right)}{\sin(\theta)}\frac{\sin\left(\frac{(n-1)\theta}{2}\right)}{\sin(\theta)} \\ &= -2\left(1-x^2\right)U_{\frac{n-1}{2}}(x)\,U_{\frac{n-3}{2}}(x) \end{aligned}$$

□

Lemma 6. *For any two nonnegative integers m and n,*

$$\gcd(U_m(x), U_n(x)) = U_{g-1}(x),$$

where $g = \gcd(m+1, n+1)$.

Proof. This identity appears as Theorem 4 in [11], and as Eq. 5.33 in [13]. □

Lemma 7. *For any nonnegative integer n, $\gcd(U_n(x), U_{n+1}(x)) = 1$.*

Proof. This follows from Lemma 6. □

Lemma 8. *Let $m \geq n \geq 3$ be odd integers. Then*

$$\gcd(T_m(x) - x, T_n(x) - x) = -2(1-x^2)h_1(x)h_2(x)h_3(x)h_4(x), \quad (11)$$

where

$$\begin{aligned} h_1 &= \gcd(U_{\frac{m-1}{2}}, U_{\frac{n-1}{2}}), \\ h_2 &= \gcd(U_{\frac{m-1}{2}}, U_{\frac{n-3}{2}}), \\ h_3 &= \gcd(U_{\frac{m-3}{2}}, U_{\frac{n-1}{2}}), \\ h_4 &= \gcd(U_{\frac{m-3}{2}}, U_{\frac{n-3}{2}}). \end{aligned}$$

Proof. Letting $m_1 = \frac{m-1}{2}$ and $n_1 = \frac{n-1}{2}$, Lemma 5 gives

$$T_m(x) - x = -2(1-x^2)U_{m_1}(x)U_{m_1-1}(x) \text{ and} \quad (12)$$

$$T_n(x) - x = -2(1-x^2)U_{n_1}(x)U_{n_1-1}(x). \quad (13)$$

We first show that the right side of (11) divides both $T_m(x) - x$ and $T_n(x) - x$. By (12) and (13) we may show that $h_1h_2h_3h_4$ divides both $U_{m_1}(x)U_{m_1-1}(x)$ and $U_{n_1}(x)U_{n_1-1}(x)$. By Lemma 7, the pair (U_{n_1}, U_{n_1-1}) is relatively prime, as is the pair (U_{m_1}, U_{m_1-1}). This implies that the h_i, $i = 1, \ldots, 4$ are pairwise relatively prime. Now, as h_1 and h_2 are relatively prime and both divide U_{m_1}, it follows that $h_1h_2 | U_{m_1}$. Similarly $h_3h_4 | U_{m_1-1}$, implying that $h_1h_2h_3h_4 | U_{m_1}U_{m_1-1}$. A similar argument shows that $h_1h_2h_3h_4$ also divides $U_{n_1}U_{n_1-1}$.

Finally, we show any common factor $q(x)$ of $T_m(x) - x$ and $T_n(x) - x$ must also divide the right side of (11). We may assume that q does not contain the factors of $2(1-x^2)$, so that $q | U_{m_1}U_{m_1-1}$ and $q | U_{n_1}U_{n_1-1}$. In order to show that $q | h_1h_2h_3h_4$, we write the unique factorization $q(x) = q_1(x)^{\alpha_1} \cdots q_r(x)^{\alpha_r}$ into irreducible factors and show that $q_i^{\alpha_i} | h_1h_2h_2h_4$, for $i = 1, \ldots, r$. Since $q_i^{\alpha_i} | U_{m_1}U_{m_1-1}$ and $\gcd(U_{m_1}, U_{m_1-1}) = 1$, it follows that $q_i^{\alpha_i} | U_{m_1}$ or $q_i^{\alpha_i} | U_{m_1-1}$. Similarly $q_i^{\alpha_i} | U_{n_1}$ or $q_i^{\alpha_i} | U_{n_1-1}$. Taking into account all four possibilities, we see that either $q_i^{\alpha_i} | h_1$ or $q_i^{\alpha_i} | h_2$ or $q_i^{\alpha_i} | h_3$ or $q_i^{\alpha_i} | h_4$, implying that $q_i^{\alpha_i} | h_1h_2h_2h_4$. □

4. Resultant Properties of Chebyshev Polynomials

In this section, we obtain information about the resultant of the polynomials $\frac{T_m(x)-x}{h(x)}$ and $\frac{T_n(x)-x}{h(x)}$), where $h(x) = \gcd(T_m(x) - x, T_n(x) - x)$. Although the resultant of two polynomials can be defined over more general rings, we assume in this section that all polynomials belong to $\mathbb{Z}[x]$. The resultant of two polynomials

$$\begin{aligned} f(x) &= a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0 \\ g(x) &= b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0 \end{aligned} \tag{14}$$

is defined to be the determinant

$$\operatorname{res}(f,g) = \begin{vmatrix} a_m & a_{m-1} & \cdots & a_0 & & & & \\ & a_m & a_{m-1} & \cdots & a_0 & & & \\ & & & \vdots & & & & \\ & & & a_m & a_{m-1} & \cdots & & a_0 \\ b_n & b_{n-1} & \cdots & b_0 & & & & \\ & b_n & b_{n-1} & \cdots & b_0 & & & \\ & & & & \vdots & & & \\ & & & & b_n & b_{n-1} & \cdots & b_0 \end{vmatrix}$$

in which there are n rows of f coefficients and m rows of g coefficients. For nonzero $a, b \in \mathbb{Z}$, $\operatorname{res}(a, b)$ is defined to be one. Many properties of resultants are well known, (e.g. [16]) however for purposes of this paper we will use the following.

Lemma 9. *Let $f(x), g(x) \in \mathbb{Z}[x]$, as given in (14). Then*

(a) $res(f, g) = 0$ if and only if f and g have a common divisor in $\mathbb{Z}[x]$ of positive degree;

(b) for any q and r, if $f(x) = q(x)g(x)+r(x)$, then $res(g, f) = b_n^{m-\delta} res(g, r)$, where $\delta = \deg r$;

(c) $res(f, g) = (-1)^{mn} res(g, f)$;

(d) for any polynomial h, $res(f, gh) = res(f, g)res(f, h)$;

(e) $res(f, 1) = 1$.

Proof. Property (a) is the most fundamental property of resultants and its proof may be found, for example, in [7], p. 231. Property (b) is proven as Lemma 4.1 of [2]. Note that r can have any degree, and is not necessarily the remainder obtained in Euclidean division. Properties (c) and (d) are well-known, and Property (e) follows easily from the definition. □

Lemma 10. *Let $m \geq n$ be positive integers. If U_m is not a multiple of U_n, then the remainder $R(x)$ of the Euclidean division of U_m by U_n, is given by*

$$R(x) = -U_r$$

where

$$r = 2n\Big(\Big\lfloor \frac{m-n}{2n+2} \Big\rfloor + 1\Big) + 2\Big\lfloor \frac{m-n}{2n+2} \Big\rfloor - m$$

Proof. See Theorem 3 of [11]. □

We will say a number k is a *signed power of 2* if $|k|$ is a power of 2.

Lemma 11. *For any integers m and n, res$(\frac{U_m}{h}, \frac{U_n}{h})$ is a signed power of 2, where $h = \gcd(U_m, U_n)$.*

Proof. By Lemma 9(c) we may assume that $m \geq n \geq 0$. The proof is by induction on $n = \min\{m, n\}$. If $n = 0$, then $U_n = h = 1$ and $\text{res}(U_m/h, U_n/h) = \text{res}(U_m, 1) = 1 = 2^0$. Now suppose that $\text{res}(\frac{U_p}{h_{p,q}}, \frac{U_q}{h_{p,q}})$ is a signed power of two, where $h_{p,q}$ denotes $\gcd(U_p, U_q)$, whenever $\min\{p, q\} < n$. Then consider the Euclidean division of U_m by U_n. If the remainder is zero, then $h = U_n$ and $\text{res}(\frac{U_m}{h}, \frac{U_n}{h}) = 1$. Otherwise, by Lemma 10, the remainder is of the form $-U_r$, so that

$$U_m = qU_n - U_r,$$

and by the Euclidean division property, $h = \gcd(U_m, U_n) = \gcd(U_n, U_r)$. We now have

$$\frac{U_m}{h} = q\frac{U_n}{h} + \frac{-U_r}{h},$$

By Lemma 9(b), it follows that

$$\text{res}(\frac{U_n}{h}, \frac{U_m}{h}) = b' \text{ res}(\frac{U_n}{h}, \frac{-U_r}{h})$$

where b' is a power of the leading coefficient of $\frac{U_n}{h}$. But by Lemma 6, h is also a Chebyshev polynomial of the second kind. Since the leading coefficient of any Chebyshev polynomial is a power of two, b' must be a power of two. By the induction assumption, $\text{res}(\frac{U_n}{h}, \frac{U_r}{h})$ is a signed power of two, and the induction is complete. □

Lemma 12. *For any odd integers m and n, res$(\frac{T_m(x)-x}{h(x)}, \frac{T_n(x)-x}{h(x)})$ is a signed power of 2, where $h(x) = \gcd(T_m(x) - x, T_n(x) - x)$.*

Proof. We may assume $m \geq n \geq 0$. By Lemma 8

$$h(x) = -2(1-x^2)h_1(x)h_2(x)h_3(x)h_4(x),$$

where $h_1 = \gcd(U_{\frac{m-1}{2}}, U_{\frac{n-1}{2}})$, $h_2 = \gcd(U_{\frac{m-1}{2}}, U_{\frac{n-3}{2}})$, $h_3 = \gcd(U_{\frac{m-3}{2}}, U_{\frac{n-1}{2}})$ and $h_4 = \gcd(U_{\frac{m-3}{2}}, U_{\frac{n-3}{2}})$. Using the multiplicative property in Lemma 9(d), the fact that the h_i are pairwise relatively prime, and defining n_1 and m_1 as in Lemma 8, we see that

$$\begin{aligned}
& \operatorname{res}(\frac{T_m(x)-x}{h(x)}, \frac{T_n(x)-x}{h(x)}) \\
= \ & \operatorname{res}(\frac{U_{m_1}U_{m_1-1}}{h_1h_2h_3h_4}, \frac{U_{n_1}U_{n_1-1}}{h_1h_2h_3h_4}) \\
= \ & \operatorname{res}(\frac{U_{m_1}U_{m_1-1}}{h_1h_2h_3h_4}, \frac{U_{n_1}}{h_1h_3}) \cdot \operatorname{res}(\frac{U_{m_1}U_{m_1-1}}{h_1h_2h_3h_4}, \frac{U_{n_1-1}}{h_2h_4}) \\
= \ & \operatorname{res}(\frac{U_{m_1}}{h_1h_2}, \frac{U_{n_1}}{h_1h_3}) \cdot \operatorname{res}(\frac{U_{m_1}}{h_1h_2}, \frac{U_{n_1-1}}{h_2h_4}) \cdot \operatorname{res}(\frac{U_{m_1-1}}{h_3h_4}, \frac{U_{n_1}}{h_1h_3}) \cdot \operatorname{res}(\frac{U_{m_1-1}}{h_3h_4}, \frac{U_{n_1-1}}{h_2h_4})
\end{aligned}$$

We are going to prove that each of the four resultants on the right side of the last equation is a signed power of 2, so that the lemma is proven. Let us examine $\operatorname{res}(\frac{U_{m_1}}{h_1h_2}, \frac{U_{n_1}}{h_1h_3})$, the other cases being similar. Using the properties of resultants, we write

$$\begin{aligned}
\operatorname{res}(\frac{U_{m_1}}{h_1}, \frac{U_{n_1}}{h_1}) &= \operatorname{res}(\frac{h_2U_{m_1}}{h_1h_2}, \frac{h_3U_{n_1}}{h_1h_3}) \\
&= \operatorname{res}(\frac{h_2U_{m_1}}{h_1h_2}, h_3) \cdot \operatorname{res}(\frac{h_2U_{m_1}}{h_1h_2}, \frac{U_{n_1}}{h_1h_3}) \\
&= \operatorname{res}(h_2, h_3) \cdot \operatorname{res}(\frac{U_{m_1}}{h_1h_2}, h_3) \cdot \operatorname{res}(h_2, \frac{U_{n_1}}{h_1h_3}) \cdot \operatorname{res}(\frac{U_{m_1}}{h_1h_2}, \frac{U_{n_1}}{h_1h_3})
\end{aligned}$$

By Lemma 11, the left side of the above equation is a signed power of two. And because all resultants involved are integers, each factor on the right side must also be a signed power of 2. In particular, the last resultant must be a signed power of two. □

5. Characterizing Chebyshev Numbers

In this section we obtain the proofs Theorem 3 and Theorem 2 which characterize Chebyshev Numbers. Theorem 2 is an immediate consequence of Lemmas 20, 21 and 22. Theorem 3 follows from Lemma 23, Lemma 24 and Lemma 25.

In order to characterize Chebyshev numbers, for a composite number n, we study the number of roots of $T_n(x) - x \bmod n$. Since T_n is

a polynomial, the homomorphism of $\mathbb{Z}[x]$ onto $\mathbb{Z}_n[x]$ shows that for any integers a, l, we have $T_n(a+ln) \equiv T_n(a) \bmod n$, so the polynomial equation $T_n(x) - x \equiv 0 \bmod n$ has n distinct roots in $\mathbb{Z}_n[x]$, if and only if n is a Chebyshev number.

Lemma 13. *For any nonnegative integers n and m, $T_m(T_n(x)) = T_{mn}(x)$.*

Proof. This property is exercise 1.1.6 in [13]. □

.

Lemma 14. *If p is an odd prime divisor of n, then $T_n{}'(x) \equiv 0 \bmod p$.*

Proof. Using Lemma 13 and then Theorem 4 we have

$$T_n(x) = T_p(T_{\frac{n}{p}}(x)) \equiv (T_{\frac{n}{p}}(x))^p \bmod p,$$

implying the desired result. □

.

Lemma 15. *Let $a(x), b(x) \in \mathbb{Z}[x]$, and let p be a prime not dividing the leading coefficients of $a(x)$ and $b(x)$. Let $c(x) = \gcd(a(x), b(x))$, and let $a_p(x)$ and $b_p(x)$ denote, respectively, the images of $a(x)$ and $b(x)$ modulo p. If $p \not| res(\frac{a(x)}{c(x)}, \frac{b(x)}{c(x)})$, then $\gcd(a_p(x), b_p(x)) = c(x) \bmod p$.*

Proof. This is Lemma 4.2.2.b in [17]. □

Lemma 16. *Let n be a composite odd integer, and p a prime divisor of n. Let*

$$\begin{aligned} g_p(x) &= \gcd\left(T_p(x) - x, T_{\frac{n}{p}}(x) - x\right) \in \mathbb{Z}[x] \\ G_p(x) &= \gcd\left((T_p(x) - x) \bmod p, (T_{\frac{n}{p}}(x) - x) \bmod p\right) \in \mathbb{Z}_p[x] \end{aligned}$$

Then $G_p(x) = g_p(x) \bmod p$.

Proof. Since p must be odd, p does not divide the leading coefficients $T_p(x) - x$ and $T_{\frac{n}{p}}(x) - x$, which are powers of two. By Lemma 15, it suffices to prove $p \not| res((T_{n/p}(x) - x)/g_p(x), (T_p(x) - x)/g_p(x)$. Both p and $\frac{n}{p}$ are odd, and so by Lemma 12 the only possible prime factor of this resultant is 2. Since p must be odd, the result follows. □

Lemma 17. *Let n be a composite odd integer, p be a prime divisor of n, and*

$$g_p(x) = \gcd\left(T_p(x) - x, T_{\frac{n}{p}}(x) - x\right) \in \mathbb{Z}[x].$$

Then for $a \in \mathbb{Z}_p$,

$$g_p(a) \equiv 0 \bmod p \text{ if and only if } T_n(a) \equiv a \bmod p.$$

Proof. If $g_p(a) \equiv 0 \bmod p$, it follows that, modulo p, $T_p(a) \equiv a$ and $T_{n/p}(a) \equiv a$. By Lemma 13, $T_n(x) = T_{n/p}(T_p(x))$, so

$$\begin{aligned} T_n(a) &= T_{n/p}(T_p(a)) \\ &\equiv T_{n/p}(a) \bmod p \\ &\equiv a \bmod p. \end{aligned}$$

Conversely, if $T_n(a) \equiv a \bmod p$, then

$$T_n(a) = T_{n/p}(T_p(a)) \equiv a \bmod p \tag{15}$$

Since p is an odd prime, by Corollary 1, it follows that

$$T_p(a) \equiv a \bmod p \tag{16}$$

and so from (15), we have

$$T_n(a) \equiv T_{n/p}(a) \equiv a \bmod p. \tag{17}$$

Together, (16) and (17) imply that $x-a$ divides $G_p(x)$ in $\mathbb{Z}_p[x]$ of $T_p(x) - x \bmod p$ and $T_{n/p}(x) - x \bmod p$. So $G_p(a) \equiv 0 \bmod p$. This completes the proof since, by Lemma 16, $G_p(x) = g_p(x) \bmod p$. □

Lemma 18. *Let $f(x) \in \mathbb{Z}[x]$, and let $N(n)$ denote the number of solutions of $f(x) \equiv 0 \bmod n$. Then $N(n) = \Pi_{i=1}^{r} N(p_i^{e_i})$, where $n = p_1^{e_1} \dots p_r^{e_r}$ is the canonical factorization of n.*

Proof. This is Theorem 2.18 in [8]. □

Lemma 19. *If p is an odd prime, then the roots of $T_n(x) - x \equiv 0 \bmod p$ are simple.*

Proof. Recall that a root a of a polynomial f is repeated if and only if $f'(a) = 0$. Lemma 14, and the fact that p is odd, imply that $(T_n(x)-x)' \equiv -1 \bmod p$. □

Lemma 20. *A Chebyshev number must be odd.*

Proof. Indeed, if $n = 2m$, then $T_n(x) = T_m(T_2(x))$ and, as $T_2(x) = 2x^2 - 1$, we see that $T_2(0) = -1$, implying that $T_n(0) = T_m(-1)$. Now by the fact that $T_m(x) = \cos(m \arccos x)$, we obtain that $T_m(-1)$ is either 1 or -1, depending on the parity of m. In any case, $T_n(0) \not\equiv 0 \bmod n$, implying that n is not a Chebyshev number. □

Lemma 21. *A Chebyshev number n must be square-free.*

Proof. Let us assume that $n = p_1^{e_1} \dots p_r^{e_r}$ is the canonical prime factorization of a Chebyshev number n, which must be odd by Lemma 20. By contradiction, suppose n is not square-free. Then for some i, $e_i > 1$. We will reach a contradiction by showing that $T_n(x) - x \equiv 0 \bmod n$ has less than n roots. By Lemma 18, it suffices to show $T_n(x) - x \equiv 0 \pmod{p_i^{e_i}}$ has less than $p_i^{e_i}$ roots, when $i > 1$. We claim, in fact, that $T_n(x) - x \equiv 0 \pmod{p_i^{e_i}}$ has at most p roots. For if $T_n(x) - x$ has more than p_i linear factors in $Z_{p_i^{e_i}}$, then it has more than p_i linear factors in Z_{p_i}. Therefore it would have a root which is not simple, contradicting Lemma 19. □

Lemma 22. *A Chebyshev number must be the product of at least three primes.*

Proof. Let n be a Chebyshev number. By Lemmas 20 and 21, n is odd and square-free. By contradiction, assume $n = pq$, for odd primes p and q, $p < q$. We will show that there exists an a such that $T_n(a) \not\equiv a \pmod n$. Letting,

$$\begin{aligned} g_p(x) &= \gcd(T_p(x) - x, T_{\frac{n}{p}}(x) - x) = \gcd(T_p(x) - x, T_q(x) - x) \\ g_q(x) &= \gcd(T_q(x) - x, T_{\frac{n}{q}}(x) - x) = \gcd(T_q(x) - x, T_p(x) - x) \end{aligned}$$

we see that $g_p = g_q$. Observing that $\deg(g_q) = \deg(g_p) \leq p$, it follows that there are at most p solutions to $g_p(x) \equiv 0 \bmod p$, and there are at most p solutions to $g_q(x) \equiv 0 \bmod q$. From Lemma 17, there are at most p solutions to $T_n(x) - x \equiv 0 \bmod p$, and at most p solutions to $T_n(x) - x \equiv 0 \bmod q$. By Lemma 18, the number of solutions to $T_n(x) \equiv x \bmod n$ is at most $p^2 < n$. Hence there exists an $a < n$ such that $T_n(a) \not\equiv a \bmod n$. □

Note that Lemma 20, Lemma 21 and Lemma 22 establish Theorem 2. Finally, we prove Theorem 3, which will follow immediately from Lemma 23, Lemma 24 and Lemma 25.

Lemma 23. *For an odd prime factor p of n, conditions (1), (2), (3) and (4) are, respectively, equivalent to conditions*

$$(p-1)|(\frac{n}{p}+1) \quad \textit{and} \quad (p+1)|(\frac{n}{p}-1) \tag{18}$$

$$(p-1)|(\frac{n}{p}-1) \quad \textit{and} \quad (p+1)|(\frac{n}{p}+1) \tag{19}$$

$$(p-1)|(\frac{n}{p}-1) \quad \textit{and} \quad (p+1)|(\frac{n}{p}-1) \tag{20}$$

$$(p-1)|(\frac{n}{p}+1) \quad \textit{and} \quad (p+1)|(\frac{n}{p}+1) \tag{21}$$

Proof. This follows from the an easy computation showing that $p-1|n+1 \Leftrightarrow p-1|\frac{n}{p}+1$, $p-1|n-1 \Leftrightarrow p-1|\frac{n}{p}-1$, $p+1|n+1 \Leftrightarrow p+1|\frac{n}{p}-1$ and that $p+1|n-1 \Leftrightarrow p+1|\frac{n}{p}-1$ □

Lemma 24. *Let n be an odd, square-free number. Also assume that for each prime p dividing n, one of the conditions (18), (19), (20), or (21) holds. Then n is a Chebyshev number.*

Proof. Let $p|n$ and suppose (21) holds. As $(p+1)|(\frac{n}{p}+1)$ and both p and $\frac{n}{p}$ are odd, if follows that $\frac{p+1}{2}|\frac{\frac{n}{p}+1}{2}$ so that $\gcd(\frac{p+1}{2},(\frac{n}{p}+1)/2) = \frac{p+1}{2}$. Lemma 6 tells us that

$$\gcd(U_{\frac{p-1}{2}}, U_{\frac{n/p-1}{2}}) = U_{\frac{p+1}{2}-1} = U_{\frac{p-1}{2}}. \tag{22}$$

Similarly, from the fact that $(p-1)|(\frac{n}{p}+1)$ one reasons that

$$\gcd(U_{\frac{p-3}{2}}, U_{\frac{n/p-1}{2}}) = U_{\frac{p-3}{2}}. \tag{23}$$

From Lemma 5 we see that

$$\begin{aligned} T_p(x) - x &= -2(1-x^2)U_{\frac{p-1}{2}}(x)U_{\frac{p-3}{2}}(x) \\ T_{\frac{n}{p}}(x) - x &= -2(1-x^2)U_{\frac{\frac{n}{p}-1}{2}}(x)U_{\frac{\frac{n}{p}-3}{2}}(x) \end{aligned}$$

Equations (22) and (23) imply that both polynomials $U_{\frac{p-1}{2}}$ and $U_{\frac{p-3}{2}}$ divide $U_{\frac{n/p-1}{2}}$. By Lemma 7, they are relatively prime, so their product divides $U_{\frac{n/p-1}{2}}$. It follows that

$$g_p(x) = \gcd(T_p(x) - x, T_{\frac{n}{p}}(x) - x) = T_p(x) - x. \tag{24}$$

If either of conditions (18), (19), or (20) holds, one can similarly argue that Equation (24) holds. As p is prime, the number of roots of $g_p(x) \equiv 0 \bmod p$ is p, by Corollary 1. By Lemma 17, every root of $g_p(x) \equiv 0 \bmod p$ is a root of $T_n(x) \equiv x \bmod p$, implying that $T_n(x) \equiv x \bmod p$ has exactly p distinct roots. As this happens for each prime p dividing n, and n is square-free, one can use Lemma 18 to obtain n distinct roots of $T_n(x) \equiv x \bmod n$, implying that n is a Chebyshev number. □

Lemma 25. *Let n be a Chebyshev number. Then each prime divisor p must satisfy one of conditions (18), (19), (20), or (21).*

Proof. By Lemma 20 and Lemma 21, n must be odd and square-free. Let p be a prime divisor of n. By Lemma 5 we may write

$$T_p(x) - x = -2(1-x^2)U_{\frac{p-1}{2}}(x)U_{\frac{p-3}{2}}(x) \quad (25)$$

$$T_{\frac{n}{p}}(x) - x = -2(1-x^2)U_{\frac{\frac{n}{p}-1}{2}}(x)U_{\frac{\frac{n}{p}-3}{2}}(x) \quad (26)$$

Now consider the polynomial $g_p(x) = \gcd(T_p(x) - x, T_{n/p}(x) - x)$. As n is a Chebyshev number, the number of roots of $T_n(x) \equiv x \bmod p$ is exactly p and they are all distinct. By Lemma 17 this is the number of solutions to $g_p(x) \equiv 0 \bmod p$, which leads to the degree inequality $p \leq \deg(g_p) \leq \min\{p, \frac{n}{p}\}$, implying that $p < \frac{n}{p}$ and that

$$g_p(x) = \gcd(T_p(x) - x, T_{\frac{n}{p}}(x) - x) = T_p(x) - x.$$

The last equation shows that the polynomial $T_{\frac{n}{p}}(x) - x$ is divisible by $T_p(x) - x$. We will show that this divisibility implies one of the following four cases.

1. Both $U_{\frac{p-1}{2}}(x)$ and $U_{\frac{p-3}{2}}(x)$ divide $U_{\frac{\frac{n}{p}-1}{2}}(x)$ This would imply that

$$\gcd(U_{\frac{p-1}{2}}(x), U_{\frac{\frac{n}{p}-1}{2}}(x)) = U_{\frac{p-1}{2}}(x).$$

   and

$$\gcd(U_{\frac{p-3}{2}}(x), U_{\frac{\frac{n}{p}-1}{2}}(x)) = U_{\frac{p-3}{2}}(x).$$

   By Lemma 6, it follows that $(p+1)|(\frac{n}{p}+1)$ and $(p-1)|(\frac{n}{p}+1)$.

2. Both $U_{\frac{p-1}{2}}(x)$ and $U_{\frac{p-3}{2}}(x)$ divide $U_{\frac{\frac{n}{p}-3}{2}}(x)$. By Lemma 6, $(p+1)|(\frac{n}{p}-1)$ and $(p-1)|(\frac{n}{p}-1))$.

3. The polynomials $U_{\frac{p-3}{2}}(x)$ and $U_{\frac{p-1}{2}}(x)$ divide $U_{\frac{\frac{n}{p}-3}{2}}(x)$, $U_{\frac{\frac{n}{p}-1}{2}}(x)$ respectively. By Lemma 6, $(p-1)|(\frac{n}{p}-1)$ and $(p+1)|(\frac{n}{p}+1)$.

4. The polynomials $U_{\frac{p-3}{2}}(x)$ and $U_{\frac{p-1}{2}}(x)$ divide $U_{\frac{\frac{n}{p}-1}{2}}(x)$, $U_{\frac{\frac{n}{p}-3}{2}}(x)$ respectively. By Lemma 6, $(p-1)|(\frac{n}{p}+1)$ and $(p+1)|(\frac{n}{p}-1)$.

It remains to show that if $T_p(x)-x$ divides $T_{n/p}(x)-x$ then one of the four case above happens. To see this, we look at the partial factorization given by equations (25) and (26) and first note that

$$U_{\frac{p-1}{2}}U_{\frac{p-3}{2}} \mid U_{\frac{\frac{n}{p}-1}{2}}U_{\frac{\frac{n}{p}-3}{2}}.$$

We next take the irreducible factor $E_1(x)$ as defined by equation (9) of $U_{\frac{p-1}{2}}$. Now if $E_1(x)$ divides $U_{\frac{\frac{n}{p}-1}{2}}$ then, by Lemma 4, we have that $U_{\frac{p-1}{2}}$ divides $U_{\frac{\frac{n}{p}-1}{2}}$. If, on the other hand, $E_1(x)$ divides $U_{\frac{\frac{n}{p}-3}{2}}$, then the same reasoning leads to the conclusion that $U_{\frac{p-1}{2}}$ divides $U_{\frac{\frac{n}{p}-3}{2}}$.

Clearly now we can apply the same procedure to the polynomial $U_{\frac{p-3}{2}}$ to conclude that either $U_{\frac{p-3}{2}}$ divides $U_{\frac{\frac{n}{p}-1}{2}}$ or $U_{\frac{p-3}{2}}$ divides $U_{\frac{\frac{n}{p}-3}{2}}$, which leads to the four cases above and the lemma is proved. □

6. Searching for Cheybyshev Numbers

We conducted a computer search and discovered only one Chebyshev number less than 10^{10}, namely

$$7056721 = 7 \cdot 47 \cdot 89 \cdot 241.$$

The search was made by first testing whether $T_n(a) \equiv a \bmod n$, for all $0 \leq a \leq n-1$. We repeated this test using the criteria given by Theorem 3, obtaining the same result. In this Chebyshev number, the prime 47 satisfies condition (4), and the remaining three prime factors satisfy condition (2). This number is not a Carmichael number, and most Carmichael numbers are not Chebyshev numbers.

There is, however, a relation between Chebyshev numbers and some classes of numbers studied by Howe [4]. Fix a positive integer m. Then a composite integer n is a *Carmichael number of order m* if and only if it is squarefree, and for each prime p dividing n, and every integer r with $1 \leq r \leq m$, there is an integer $i \geq 0$ such that $n \equiv p^i \bmod (p^r - 1)$. In the case of $m = 2$, the characterization simplifies to being a squarefree composite n such that for each prime divisor p, either

(*i*) $n \equiv 1 \bmod (p^2 - 1)$ or

(*ii*) $n \equiv p \bmod (p^2 - 1)$.

Since (*i*) implies (2), and (*ii*) implies (3), a corollary to Theorem 3 is

Corollary 2. *The Carmichael numbers of order $m \geq 2$ are Chebyshev numbers.*

Howe constructs many Carmichael numbers of order two. By Corollary 2, these are also Chebyshev numbers. His construction may be modified to produce (non-Carmichael) numbers n satisfying, for all p,

$$n \equiv -1 \bmod (p^2 - 1).$$

Thus n satisfies (1) for every p dividing n. Using Maple, we obtained 275 such numbers, ranging from 30 digits to 85 digits. The smallest of those that we found using this construction was

$$43 \cdot 109 \cdot 199 \cdot 233 \cdot 349 \cdot 449 \cdot 521 \cdot 571 \cdot 701 \cdot 3191 \cdot 5851.$$

7. Concluding Remarks

Chebyshev numbers are an interesting pseudoprime sharing properties that are similar to Carmichael numbers, but yet appear more rare. For example, reportedly there are 1547 Carmichael numbers less than 10^{10} [9]. The paper [4] contains a heuristic argument, based on one by Erdos for the Carmichael numbers, that there should be infinitely many higher order Carmichael numbers. Given that the set of Chebyshev numbers properly contains the set of Carmichael numbers of order two, we should expect the same. The smallest Chebyshev number has four prime factors. A natural question to ask is whether a Chebyshev number can be the product of three primes.

Finally, the use of Chebyshev numbers to devise probabilistic algorithms for primality testing is also a problem worthy of attention. In [6] the authors proposed a first experiment for testing integer primality based on the properties of Chebyshev polynomials.

It is worth noting that there is an alternate proof to some of our theorems using properties of the trace and norm. We prefer this more computational proof as it involves a variety of properties of Chebyshev polynomials, like factorization and resultants, that are interesting by themselves.

References

[1] T. Bang, *Congruence properties of Tchebycheff polynomials*, Mathematica Scandinavica 2, 1954, 327–333.

[2] K. Dilcher and K. B. Stolarsky, *Resultants and discriminants of Chebyshev and related polynomials*, Transactions of the AMS, 357 (Number 3, 2005), 965–981.

[3] J. Grantham, *Frobenius pseudoprimes*, Math. Comp. 70 (2001), 873–891.

[4] E. W. Howe, *Higher order Carmichael numbers*, Math. Comp. 69 (2000), 1711–1719.

[5] H. J. Hsiao, *On factorization of Chebyshev's polynomials of the first kind*, Bulletin of the Institute of Mathematics, Academia Sinica 12 (1), 1984, 89–94.

[6] D.P. Jacobs, V. Trevisan, M.O. Rayes,"Randomized Compositeness Testing with Chebyshev Polynomials", International Journal of Pure and Applied Mathematics, to appear.

[7] B. Mishra, *Algorithmic Algebra*, Springer-Verlag, New York, 1993.

[8] I. Niven and H.S. Zuckerman, *An Introduction to the Theory of Numbers*, 4th ed., John Wiley & Sons, New York, 1980.

[9] R.G.E. Pinch, *The Carmichael numbers up to* 10^{15}, Math. Comp. 61 (1993) 381–391.

[10] R. A. Rankin, *Chebyshev polynomials and the modular group of level p*, Mathematica Scandinavica 2, 1954, 315–326.

[11] M. O. Rayes, V. Trevisan and P. S. Wang, *Factorization Properties of Chebyshev Polynomials*, Computers and Mathematics with Applications 50, 2005, 1231–1240.

[12] M. O. Rayes and V. Trevisan *Primality from Factorization Properties of Chebyshev Polynomials*, JP Journal of Algebra, Number Theory and Applications 6(3), 2006, 503-514.

[13] T. J. Rivlin, *The Chebyshev Polynomials - From Approximation Theory to Algebra and Number Theory*, Second Edition, Pure and Applied Mathematics, Jonh Wiley & Sons, New York, 1990.

[14] I. Schur, *Gesammelte Abhandlungen, Band III*. Herausgegeben von Alfred Brauer und Hans Rohrbach, Springer-Verlag, 1973.

[15] M. A. Snyder, *Chebyshev Methods in Numerical Approximation*, Prentice-Hall, N.J. 1966.

[16] B. L. van der Waerden, *Modern Algebra*, Vol. 1, Ungar, New York, 1949.

[17] F. Winkler, *Polynomial Algorithms in Computer Algebra*, Springer-Verlag, 1996.

CONTACT INFORMATION

David Pokrass Jacobs School of Computing, Clemson University, Clemson, SC 29634–0974, USA
E-Mail: dpj@cs.clemson.edu

Mohamed O. Rayes Dept. of Comp. Sci. and Eng., Southern Methodist University, Dallas, TX 75275–0122 USA
E-Mail: mrayes@engr.smu.edu

Vilmar Trevisan Instituto de Matemática, UFRGS, 91509–900 Porto Alegre, Brazil
E-Mail: trevisan@mat.ufrgs.br

Received by the editors: 09.06.2008
and in final form 09.06.2008.