Chebyshev Polynomials and Primality Tests

Mohamed O. Rayes
Texas Instruments Incorporated
Post Office Box 650311, MS 3908
Dallas, Texas 75265 USA
mrayes@ti.com

*Vilmar Trevisan**
UFRGS-Instituto de Matemática
91509-900 Porto Alegre, RS, Brazil
trevisan@mat.ufrgs.br

Paul S. Wang†
Dept. of Mathematics and Comp. Science
Kent State University
Kent, OH, 44240
pwang@mcs.kent.edu

January 18, 1999

Abstract

Algebraic properties of Chebyshev polynomials are presented. The complete factorization of Chebyshev polynomials of the first kind ($T_n(x)$) and second kind ($U_n(x)$) over the integers are linked directly to divisors of n and $n + 1$ respectively. For any odd integer n, it is shown that the polynomial $T_n(x)/x$ is irreducible over the integers iff n is prime. The result leads to a generalization of Fermat's little theorem and an effective test for the compositeness of an integer. Also, factoring of integers is linked directly to the construction of a related Chebyshev polynomial.

1 Introduction

Chebyshev polynomials are important in many areas of mathematics, especially approximation theory. Many articles and books have been written about this topic.

*Partially supported by CAPES, Brazil, under grant BEX 0744/96-4

†Work reported herein has been supported in part by the National Science Foundation under Grant CCR-9721343

Analytical properties of Chebyshev polynomials are well understood, but algebraic properties less so. Reported here are several algebraic properties of Chebyshev polynomials including factorization, irreducibility, and relations between Chebyshev polynomials and integer factoring. By extending a result of H. J. Hsiao [7], we determine the complete factorization of Chebyshev polynomials into irreducible factors over the integers **Z**. We establish a relationship between primality of integers and the irreducibilty of Chebyshev polynomials of the first kind $T_n(x)$. Specifically, we show that an odd integer $n > 1$ is prime if and only if $T_n(x)/x$ is irreducible. Based on this criterion, primality tests have been developed. Also, we connected factorization of integers to Chebyshev polynomials. We show that factoring an odd integer n is equivalent to constructing a Chebyshev polynomial modulo n.

2 Chebyshev Polynomials

For easy reference, let us first state the definitions and basic properties of Chebyshev polynomials needed for our main results. The Chebyshev polynomials of the first kind $T_n(x)$ may be defined by the following recurrence relation. Set $T_0(x) = 1$ and $T_1(x) = x$, then

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

Alternatively, they may be defined as

$$T_n(x) = \cos n(\arccos x), \tag{2}$$

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

$$\xi_k = \cos \frac{(2k-1)}{n}\frac{\pi}{2} \qquad k = 1, \ldots, n. \tag{3}$$

It is easy to see also that the roots ξ_k are symmetric with respect to the line $x = 0$. In other words, if x is a root of $T_n(x)$, then so is $-x$. For factorization purposes, the decomposition properties

$$T_{mn}(x) = T_m(T_n(x)), \quad m, n \geq 0 \tag{4}$$

$$T_m(x)T_n(x) = \frac{1}{2}\left(T_{m+n}(x) + T_{|m-n|}(x)\right), \quad m, n \geq 0 \tag{5}$$

are very useful. They can be proven using trigonometric identities [16, pg. 5]. We can also define $T_{-n}(x)$ as follows:

$$T_{-n}(x) = \cos -n(\arccos x) = \cos n(\arccos x) = T_n(x). \tag{6}$$

The Chebyshev polynomials of the second kind are defined by setting $U_0(x) = 1$, $U_1(x) = 2x$ and the recurrence relation

$$U_n(x) = 2xU_{n-1}(x) - U_{n-2}(x), \qquad n = 2, 3 \ldots. \tag{7}$$

They also may be defined by

$$U_n(x) = \frac{1}{n+1}T'_{n+1}(x) = \frac{\sin\left((n+1)\arccos x\right)}{\sin(\arccos x)}. \tag{8}$$

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

$$\eta_k = \cos\frac{k\pi}{n+1}, \quad k = 1, \ldots, n. \tag{9}$$

Useful decomposition properties for the U polynomials include the following [17, pg. 97].

$$U_{mn-1}(x) = U_{m-1}(T_n(x))U_{n-1}(x), \quad m, n > 0 \tag{10}$$

$$T_n(x)U_{m-1}(x) = \frac{1}{2}\left(U_{m+n-1}(x) + U_{m-n-1}(x)\right), \quad m > n > 0. \tag{11}$$

To extend the definition of Chebyshev polynomials of the second kind for negative n, we notice that for $n > 1$

$$U_{-n}(x) = \frac{1}{-n+1}T'_{-n+1} = -\frac{1}{n-1}T'_{-(n-1)}(x) = -\frac{1}{n-1}T'_{(n-1)}(x) = -U_{n-2}(x). \tag{12}$$

For convenience, we define $U_{-1}(x) = 0$. There are many fascinating properties of the Chebyshev polynomials and the reader is encouraged to look the excellent books by T. Rivlin [16] and M. Snyder [17].

3 Factoring Chebyshev Polynomials over Z

H. J. Hsiao [7] gave a complete factorization of Chebyshev polynomials of the first kind $T_n(x)$, determining which roots should be grouped together to yield irreducible factors with integer coefficients. Here, a similar result for the Chebyshev polynomials of the second kind $U_n(x)$ is derived. With a slight change in notation, Hsiao's result is the following

Theorem 1 (Hsiao) *Let $n > 1$ be an integer. Then*

$$T_n(x) = 2^{n-1}\prod_h D_h(x),$$

where $h \leq n$ runs through all odd positive divisors of n and

$$D_h(x) = \prod_{\substack{k=1 \\ (2k-1,n)=h}}^{n} (x - \xi_k) \tag{13}$$

are irreducible polynomials over the rationals.

Applying the same method used by Hsiao, we prove a similar result for the Chebyshev polynomials of the second kind $U(n,x)$. Consider a fixed integer $n \geq 2$. Let $h \leq n$ be a positive divisor of $2n+2$ and l_h the number of elements in the set

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

It is easy to see that $l_h = \#(S_h) = \phi((2n+2)/h)/2$. Now let

$$E_h(x) = 2^{l_h} \prod_{\substack{k=1 \\ (k,2n+2)=h}}^{n} (x - \eta_k), \tag{14}$$

where η_k are the zeros of $U_n(x)$ defined in equation (9).

Theorem 2 *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: From D. H. Lehmer [11] we know: *If $L > 2$ and $\gcd(k, L) = 1$ then $2\cos\frac{2k\pi}{L}$ is algebraic of degree $\phi(L)/2$.* Setting $k = 1$ and $L = 2n+2$, we obtain that $2\cos\frac{\pi}{(n+1)}$ is algebraic of degree $\phi(2n+2)/2$, or that η_1 is algebraic of degree $\phi(2n+2)/2$. From the proof of Lehmer's result we also see that all η_k with $(k, 2n+2) = 1$ are roots of the same irreducible polynomial. Multiplying this polynomial by 2^{l_1}, where $l_1 = \phi(2n+2)/2$, we obtain that $E_1(x)$ is an integral polynomial irreducible over $\mathbf{Z}$. Let $h > 1$ be a divisor of $2n+2$. Consider all $1 \leq k \leq n$ with $(k, 2n+2) = h$. For each such k there exist an $k/h \leq i \leq \lfloor n/h \rfloor$ such that $(i, (2n+2)/h) = 1$ and conversely. So by the same argument of the previous paragraph, all the η_k, with $(k, 2n+2) = h$ are roots of the same irreducible (rational) polynomial $E'_h(x)$ of degree $l_h = \phi((2n+2)/h)/2$. Multiplying $E'_h(x)$ by 2^{l_h} we obtain the integral polynomial $E_h(x)$. A root η_k of $U_n(x)$ is a root of a unique $E_h(x)$ where $h = (k, 2n+2)$. $\square$
Using theorems 1 and 2, we can group the roots a Chebyshev polynomials to obtain its irreducible factors. **Example:** Suppose $n = 6$. $D_1(x)$ is formed by taking the roots ξ_1, ξ_3, ξ_4, and ξ_6, whereas $D_3(x)$ is obtaining by collecting ξ_2 and ξ_5. Similarly, $E_1(x)$ and $E_2(x)$ are obtained by taking the roots η_1, η_3, η_5 and η_2, η_4, η_6, respectively. Distributing the powers of 2 accordingly, we obtain the integral factorizations:

$$T_6(x) = \left(2\,x^2 - 1\right)\left(16\,x^4 - 16\,x^2 + 1\right)$$

$$U_6(x) = \left(8\,x^3 - 4\,x^2 - 4\,x + 1\right)\left(8\,x^3 + 4\,x^2 - 4\,x - 1\right)$$

Two corollaries follow immediate from theorems 1 and 2.

Corollary 1 *Let n be a positive integer.*

(1) *$D_1(x)$ is the irreducible factor of $T_n(x)$ of largest degree $= \phi(n)$.*

(2) *$E_1(x)$ is the irreducible factor of $U_n(x)$ of largest degree $= \phi(2n+2)/2$.*

Corollary 2 *Let n be a positive integer.*

(1) *The number of irreducible factors of $T_n(x)$ equals the number of odd divisors $h \leq n$ of n.*

(2) *The number of irreducible factors of $U_n(x)$ equals the number of divisors $h \leq n$ of $2n+2$.*

Then, a third corollary can be deduced.

Corollary 3 *Let n be a positive integer.*

(1) *$T_n(x)$ is irreducible if and only if n is a power of two.*

(2) *$U_n(x)$ is reducible for all $n > 1$.*

Proof: The only odd divisor of a power of two is 1. If n is not a power of two, then n has at least two odd divisors. This proves (1). To prove (2) we observe that for any $n > 1$, 1 and 2 are divisors of $2n+2$, so $U_n(x)$ has at least two irreducible factors. □

4 Integer Primality Testing

The task of deciding if a positive integer n is a prime is usually split into two subproblems

1. Test quickly whether n is composite. If n can not be determined composite, then it is probably prime. We refer to such a test as a *nonprimality* or *compositeness test.*

2. Prove n prime, after it passes the compositeness test.

Much research has been done in these two areas. For an excellent introduction see Knuth [9]. For a more in-depth study see [5, 8]. Trial division [5] is a simple and naive method for primality testing. Given a positive integer n, we use the sequence of trial divisors

$$2 = d_0 < d_1 < d_2 ... d_k \leq \sqrt{n}$$

This sequence can simply be $2, 3, 5, 7....$ where we alternately add 2 and 4 after the first three terms. The simple sequence is guaranteed to contain all the prime factors of n. The complexity of the method id $O(\sqrt{n})$. Cohen [5] recommends that trial division not be used except for very small n ($n < 10^8$). A well known compositeness test is based on Fermat's little theorem which states that if n is prime then $a^{n-1} \equiv 1$ *modulo* n for all integers a such that $\gcd(n, a) = 1$. The method can decide if n is composite quickly. However, there exist composite integers k which satisfy $a^k - 1$ *mod* $k = 1$ for all a relatively prime to k. Examples of k are $561 = 3{\cdot}11{\cdot}17$, $1729 = 7{\cdot}13{\cdot}19$, $1105 = 5{\cdot}13{\cdot}17, 2465 = 5{\cdot}17{\cdot}29$, etc. Another compositeness test widely used in practice is due to Rabin and Miller [8]. The test is probabilistic with a probability of failure at most $(\frac{1}{2})^{-t}$ where t is the number of trials. That is, for a randomly chosen odd composite integer n, the expected number of non-witnesses to the compositeness of n is at most $\frac{n}{2}$. The running time of this test is essentially the same as that of the powering algorithm (i.e. computing a^{n-1} *modulo* n) which is $O(\ln n^3)$. Wilson's is a theoretic method to verify that an integer n is prime. The method states that $(n-1)! \equiv 1$ *modulo* n iff n is prime. But, computing $(n-1)!$ *modulo* n is extremely prohibitive. Several other classic deterministic tests for primality are discussed in the literature. These methods require the factorization of $n-1$ (or $n+1$) which is generally a very difficult task in itself. Primality methods in this category include Pocklibton-Lehmer [5] and Lucas-Lehmer [9] tests. Recently, Adleman *et. al.* developed a primality test based on the theory of Elliptic curves. The test was further simplified and improved by Lenstra and Cohen [5]. This algorithm is $O\left(\ln(n)\right)^{C\ln(\ln(\ln(n)))}$ and is almost, but not quite, a polynomial time algorithm.

5 Chebyshev Polynomials and Integer Primality

Investigated here is the relation between the primality of any integer n and the irreducibility of Chebyshev polynomials of the first kind $T_n(x)$. Based on this relation, integer primality criteria are then developed. In this section, without loss of generality, let us consider n an odd integer and denote the Chebyshev polynomial of degree n as $T_n(x) = \sum_{k=0}^{n} t_k x^k$. There exists many closed formulas and recurrence relations for the coefficients t_k of $T_n(x)$. The following formulation is due to Snyder [17, p. 14]. Let

$$T_m^k = (-1)^k 2^{m-1} \left\{ \frac{m+2k}{m+k} \right\} \binom{m+k}{k}, \tag{15}$$

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

$$T_n(x) = \sum_{k=0}^{m} T_{2k+1}^{m-k} x^{2k+1}. \tag{16}$$

Lemma 1 *Let n be an odd prime. The polynomial $T_n(x)/x$ is irreducible.*

Proof: If we write $n = 2m+1$, the coefficient T_{2k+1}^{m-k} of x^{2k+1} in $T_n(x)$ is given by

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

It can be seen, by inspection, that the leading coefficient $T_n^0 = 2^{n-1}$, that the trailing coefficient $T_0^m = (-1)^m n$, and that the remaining coefficients are also divisible by n. The irreducibility of $T_n(x)/x$ follows by the Eisenstein's criterion.

Lemma 2 *theorem Let $p = 2h+1$ be a prime divisor of $n = 2m+1$. Then n does not divide the coefficient T_p^{m-h} of x^p in $T_n(x)$.*

Proof: Further manipulating the closed formula (15) for T_p^{m-h}, we obtain

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

We know p does not divide the binomial coefficient $\binom{p+m-h-1}{p-1}$ because there are $p-1$ consecutive factors in its numerator starting with $m-h+p-1$. Hence n does not divide T_p^{m-h} as stated. □ We are now ready to state the following theorem

Theorem 3 *Let n be an odd positive integer. Then n is a prime if and only if $\frac{T_n(x)}{x}$ is irreducible over the integers.*

Proof: If n is prime, then it is clear from lemma 1 that $\frac{T_n(x)}{x}$ satisfies Eisenstein's irreducibility criterion. Now suppose that $\frac{T_n(x)}{x}$ is irreducible in $\mathbf{Z}$[x]. It follows that $T_n(x)$ has exactly two irreducible factors:

$$T_n(x) = x\,\left(\frac{T_n(x)}{x}\right).$$

Corollary 2 states that the number of irreducible factors of $T_n(x)$ equals the number of odd divisors of n. Hence, n is prime. □ The previous theorem shows the equivalence between primality of an odd integer n and the irreducibility of the Chebyshev polynomial $T_n(x)$ divided by x. This result, as it stands, may not be practical because computing and storing the coefficients of $T_n(x)$ is prohibitive for large n. The following theorem should improve the situation somewhat.

Theorem 4 *An odd integer $n = 2m+1 > 1$ is prime if and only if $T_n(x) \equiv x^n \pmod{n}$.*

Proof: We write $T_n(x) = \sum_{k=0}^{n} t_k x^k$. If n is prime, then as the proof of lemma 1 indicates, $T_n(x)/x$ satisfies Eisentein's irreducibility test and $a_k \equiv 0 \pmod{n}$ for $k = 0, 1, 2, \ldots, n-1$. For $k = n$, we have $t_n = 2^{n-1} \equiv 1 \pmod{n}$, by Fermat's little theorem. Conversely, suppose that n is composite. Let $p = 2h+1$ be a prime dividing n. Lemma 2 shows that $t_p = T_p^{m-h}$ is not divisible by n, which implies that $T_p(x) \not\equiv x^p \pmod{p}$. □ This criterion is apparently more practical than theorem 3, since it requires only constructing a Chebyshev polynomial of degree n modulo n. For this construction, the following divide and conquer technique may be used, which can be deduced from equation (5).

$$T_{2m+1}(x) = 2T_{m+1}(x)T_m(x) - T_1(x). \tag{17}$$

However, it should be noted that the criterion is not an efficient primality test for the cost is dominated by the polynomial multiplication $T_{m+1}(x)T_m(x)$, which is dependent on the number of nonzero coefficients. It happens that, roughly, half of the coefficients of $T_{m+1}(x)$ and $T_m(x)$ are nonzero since there are no cancelation modulo n. By applying Fermat's little theorem and theorem 4, we can state

Theorem 5 *If an odd integer $n > 1$ is prime, then $T_n(a) \equiv a \pmod{n}$ for all integers a.*

To compute $T_n(x)$ at a point a, we may use the recurrence relation defined by

$$T_0(a) = 1 \tag{18}$$

$$T_1(a) = a \tag{19}$$

$$T_k(a) = 2aT_{k-1}(a) - T_{k-2}(a) \quad k = 2, 3, \ldots \tag{20}$$

which has the closed formula

$$T_k(a) = \frac{1}{2}\left[\left(a + \sqrt{a^2 - 1}\right)^k + \left(a - \sqrt{a^2 - 1}\right)^k\right]. \tag{21}$$

Alternatively $T_n(a)$ maybe computed using the relation (17). In any case, this can be done using only $O(\log n)$ operations in $\mathbf{Z}_n$, which is as efficient as the Fermat's theorem based compositeness test. Experiments indicate the $T_n(a)$ *mod* n test easily handles composite numbers such as 561 that cause problems for the Fermat's theorem based test. How efficient is the compositeness test given by theorem 5? For any composite n, how many integers a, on average, need to be tried before obtaining $T_n(a) \not\equiv a \pmod{n}$? In a sense, theorem 5 may be seen as a generalization of Fermat's little theorem. Namely, for n prime, not only $a^n \equiv a \pmod{n}$ but more generally $T_n(a) \equiv a \pmod{n}$. Note also, if the converse of theorem 5 is true, a deterministic primality test with polynomial time complexity may be developed. Following these similarities with Fermat's little theorem, we may call an integer n a *Chebyshev pseudo prime in base* a if n is a composite number such that $T_n(a) = a \pmod{n}$. For example, the smallest Chebyshev pseudo prime in base 2 is $n = 209 = 11{\cdot}19$. There are no pseudo primes in bases 2 and 3 up to $n = 2000$.

Definition 1 *A composite positive integer is a Chebyshev number if $T_n(a) = a$ for all $1 < a < n$.*

Do there exist Chebyshev numbers? If so, how many? How are they distributed? We have not found any Chebyshev number, even though our search was limited to small numbers (up to 4000). Notice that the Lucas sequence $V_n(P,Q) = \alpha^n + \beta^n$ for $n \geq 0$, where α and β are the roots of the polynomial $x^2 - Px + Q$ (see, for example, [15]) satisfy the property:

$$V_k(2a, 1) = 2T_k(a), k \geq 0. \tag{22}$$

Hence all the properties of Lucas sequences, particularly its relation with primality, are also satisfied by the *Chebyshev sequence* $T_k(a)$ defined in (20).

6 Chebyshev Polynomials and Integer Factorization

Let's now consider the relation between integer factorization and Chebyshev polynomials. Essentially, we show that factorization of an odd integer n is equivalent to the construction of the degree-n Chebyshev polynomial modulo n.

Theorem 6 *Let n be an odd integer and $T_n(x) = \sum_{k=0}^{n} t_k x^k$ be the degree-n Chebyshev polynomial. If $\gcd(k, n) = 1$ then $t_k \equiv 0 \pmod{n}$.*

Proof: Consider the Chebyshev polynomial of the second kind $U_{n-1}(x) = \frac{1}{n} T_n'(x)$, $n > 1$. Since U_{n-1} is an integral polynomial, it follows that n divides kt_k, for all $k = 1, \ldots, n$. As n and k are relatively prime, the result follows. □ This result shows that the non-vanishing coefficients of $T_n(x) \pmod{n}$ provide factors of n. Let k be an integer such that $t_k \not\equiv 0 \pmod{n}$. We have, by theorem 6, that $\gcd(k, n)$ is nontrivial. Moreover it is easy to verify that $\gcd(n, t_k)$ is also nontrivial. However, $\gcd(k, n) \neq 1$ does not always imply $t_k \pmod{n}$ is nonzero. For example, in $T_{45}(x)$ the coefficient of x^{15} is zero modulo 45. Lemma 2 however does imply that the coefficient of x^p in $T_n(x) \pmod{n}$ is nonzero for any prime divisor p of n. Thus, there are always enough nonzero coefficients in $T_n(x) \pmod{n}$ to obtain the complete prime factorization of n based on theorem 6.

References

[1] A. V. Aho, J. E. Hopcroft, J. D. Ullman, *The Design and Analysis of Computer Algorithms*. Addison-Wesley, Reading, Massachusetts, 1974.

[2] J. A. Anderson and J. M. Bell, *Number Theory with Applications*, Prentice Hall, 1997.

[3] T. Bang, "Congruence properties of Tchebycheff polynomials", Mathematica Scandinavica 2, 1954, pp. 327-333.

[4] L. Carlitz, "Quadratic residues and Tchebycheff polynomials", Portugaliae Mathematica 18 (4), 1959, pp. 193-198.

[5] H. Cohen, *A Course in Computational Algebraic Number Theory*. Springer-Verlag, Germany, 1995.

[6] K. Geddes, S. Czapor, G. Labahn, *Algorithms For Computer Algebra*. Kluwer Academic, Norwell, Massachusetts, 1993.

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

[8] N. Koblitz. *A Course in Number Theoery and Cryptography*. Springer Verlag, 1994.

[9] D. Knuth, *The Art of Computer Programming*, Vol 2. Addision Wesley, 1998.

[10] C. Lanczos, *Applied Analysis.* Prentice-Hall, N.J. 1956.

[11] D. H. Lehmer, "A note on trigonometric algebraic numbers", American Mathematical Monthly 40, 1933, pp. 165-166.

[12] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and their Applications*, Cambridge university Press, New York, 1994.

[13] J. D. Lipson *Elements of Algebra and Algebraic Computing.* Addison-Wesley, Reading, Massachusetts, 1981.

[14] R. A. Rankin, "Chebyshev polynomials and the modular group of level p", Mathematica Scandinavica 2, 1954, pp. 315-326.

[15] P. Ribenboim, *The Book of Prime Number Records*, Second Edition, Springer-Verlag, 1989.

[16] T. J. Rivlin, *The Chebyshev Polynomials*, Wiley-Interscience, New York, 1974.

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

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