Factorization of Chebyshev Polynomials

Mohamed Omar 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
Depart. of Mathematics and Comp. Science
Kent State University
Kent, OH, 44240
pwang@mcs.kent.edu

February 17, 1998

Abstract

The complete factorization of Chebyshev polynomials, of the first and second kind, into irreducible factors over the integers **Z** is described. Conditions are given for determining when a Chebyshev polynomial is divisible by another. And, if non-zero, the remainder is again a Chebyshev polynomial, up to a sign. Algorithms are also specified to find two infinite sets of fields Z_p where a given Chebyshev polynomial factors completely into linear factors and to obtain the factors. The results also lead to the assertion: *An odd integer $n > 0$ is prime if and only if the Chebyshev polynomial of the first kind $T_n(x)$, divided by x, is irreducible over the integers.*

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

1 Introduction

Chebyshev polynomials are of great importance in many areas of mathematics, particularly approximation theory. Numerous articles and books have been written about this topic. Analytical properties of Chebyshev polynomials are well understood, but algebraic properties less so. Reported here are several algebraic properties of Chebyshev polynomials including factorization and irreducibility. By extending a result of H. J. Hsiao [7], we characterize the complete factorization of Chebyshev polynomials into irreducible factors over the integers $\mathbf{Z}$. Conditions for determining when a Chebyshev polynomials is divisible by another are developed. It is also shown that the remainder produced by Euclidean division of two Chebyshev polynomials is again a Chebyshev polynomial, up to a sign. Also studied is the factorization of Chebyshev polynomials over finite fields. Given any Chebyshev polynomial, two infinite sets of primes p can be found such that $\mathbf{Z}_p$ contains all the roots of the polynomial. A procedure for finding the modular roots is also outlined.

2 Chebyshev Polynomials

For easy reference, the definitions and certain basic properties of the Chebyshev polynomials are presented. The properties are needed to prove the 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 [13, 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 [14, pg. 97].

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

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

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 [13] and M. Snyder [14].

3 Integral Factorization

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, 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 [9] 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 $h = (k, 2n+2)$. □
With theorems 1 and 2, one 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. □

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

Proof: If we write

$$T_p(x) = t_p x^p + \cdots t_1 x,$$

then the leading coefficient t_p is

$$t_p = 2^{p-1} \text{ for } p > 0,$$

the trailing coefficient is

$$t_1 = (-1)^{(p-1)/2} p$$

All other coefficients [1] are given by

$$t_{p-(2k+1)} = 0, \qquad k = 0, \ldots, \lfloor (p-1)/2 \rfloor$$

$$t_{p-2k} = (-1)^k \sum_{j=k}^{\lfloor p/2 \rfloor} \binom{p}{2j} \binom{j}{k}, \qquad k = 0, \ldots, \lfloor p/2 \rfloor .$$

The leading coefficient of the polynomial $T_p(x)/x$ is 2^{p-1} and its independent coefficient is $(-1)^{(p-1)/2}p$. It is easy to see, by inspecting the closed formula for the coefficients of T_p, that the remaining coefficients are also divisible by p. The irreducibility follows by the Eisenstein's criterion. □ We are now ready to state the following theorem

[1] See Rivlin [13] for more detailed derivation of the closed formula of the coefficients.

Theorem 3 *Let n be an odd positive integer. Then n is a prime if and only $\frac{T_n(x)}{x}$ 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 criteria. Now suppose that $\frac{T_n(x)}{x}$ is irreducible in **Z**[x]. Corollary 2 states that the number of irreducible factors of $T_n(x)$ equals the number of odd divisors $h <= n$ of n. Since $\frac{T_n(x)}{x}$ is irreducible, it follows that $T_n(x)$ has exactly two irreducible factors:

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

Hence, n is prime. □

4 Division Properties

The division properties of Chebyshev polynomials $T_n(x)$ and $U_n(x)$ are characterized. Criteria to determine when a Chebyshev polynomials is divisible by another are given. We also prove that Chebyshev polynomials are (essentially) closed under division. Specifically, we show that the remainder of dividing two Chebyshev polynomials is, up to a sign, another Chebyshev polynomial.

4.1 Divisors of $T_n(x)$

The following property may be proven by applying the decomposition property (4).

Property 1 *Let $n > 1$ be an integer. If h is any odd divisor of n, then $T_{n/h}(x)$ is a divisor of $T_n(x)$.*

Let $T_m(x)$ and $T_n(x)$ be two Chebyshev polynomials of the first kind. Performing the Euclidean division we obtain integral quotient and remainder polynomials $q(x)$ and $r(x)$ satisfying

$$T_m(x) = q(x)T_n(x) + r(x), \quad \deg(r) < \deg(T_n). \tag{15}$$

The $q(x)$ and $r(x)$ can be determined using the result,

Property 2 *Let $m \geq n$ be two positive integers. The polynomials $q(x)$ and $r(x)$ satisfying the Euclidean division (15) are given by*

$$\begin{aligned} q(x) &= 2\sum_{k=1}^{l}(-1)^k T_{m-(2k-1)n}(x) \\ r(x) &= (-1)^l T_{|m-2ln|}(x), \end{aligned}$$

if there is an integer $l \geq 1$ satisfying $(2l-1)n < m \leq 2ln$, otherwise

$$\begin{aligned} q(x) &= 2\sum_{k=1}^{l-1}(-1)^k T_{m-(2k-1)n}(x) + (-1)^{l-1} \\ r(x) &= 0, \end{aligned}$$

where l satisfies $m = (2l-1)n$.

Proof: Replacing m by $m-n$ in equation (5), and using the extended definition (6), we have

$$T_m(x) = 2\ T_n(x)\ T_{m-n}(x) - T_{m-2n}(x), \quad \text{integers}\ \ m,n. \tag{16}$$

Let l be the only positive integer satisfying $(2l-1)n \leq m \leq 2ln$. Applying the decomposition formula (16) $l-1$ times, we deduce

$$\begin{aligned} T_m(x) &= 2T_n(x)\left\{T_{m-n}(x) - T_{m-3n}(x) + \cdots + (-1)^{l-1}T_{m-(2l-3)n}(x)\right\} \\ &\quad +(-1)^{l-1}T_{m-(2l-2)n}(x). \end{aligned}$$

If $(2l-1)n < m \leq 2ln$, then $\deg(T_n(x)) < \deg(T_{m-(2l-2)n}(x))$ and we can apply property (17) once more, proving the first case. On the other hand, if $m = (2l-1)n$, then $m-(2l-2)n = -n$. It follows that $r(x) = 0$ and the second case is proved. □ From the above property, we see that the remainder of two Chebyshev polynomials of the first kind is either zero or another Chebyshev polynomials of the first kind (up to a sign). We may also deduce from property 2 that if $T_n(x)$ is a divisor of $T_m(x)$ then n is an odd divisor of m. This statement may be seen as the converse of property 1. The following theorem summarizes results of this section.

Theorem 4 *For integers $0 < n \leq m$, $T_n(x)$ is a divisor of $T_m(x)$ if and only if $m = (2l-1)n$ for some integer $l > 1$. Otherwise, the remainder of the Euclidean division of $T_m(x)$ by $T_n(x)$ is given by $r(x) = (-1)^l T_{|m-2nl|}(x)$, where l is the smallest positive integer satisfying $|m-2nl| < n$.*

4.2 Divisors of $U_n(x)$

By applying the decomposition property 10, we obtain

Property 3 *$U_n(x)$ is a divisor of U_m if there exists an integer $l > 0$ such that $m = ln + l - 1$.*

Proof: $U_m(x) = U_{l(n+1)-1}(x) = U_{l-1}(T_n(x))U_n(x)$. □ To determine the Euclidean division of U_m by U_n, we use the extended definition for negative indices of Chebyshev polynomials and applying equation (11) with $m+n-1$ replaced by m and $m-1$ replaced by n.

$$U_m(x) = 2T_{m-n}(x)U_n(x) - U_{2n-m}(x), \quad \text{integers}\ \ m,n. \tag{17}$$

Because $U_{-1}(x) = 0$, the above works for $2n-m = -1$. For $m = n$, the formula still holds and can be written as $U_m(x) = (2T_{m-n}(x) - 1)U_n(x)$. Also notice that $2n - m \leq n$ and if $2n - m \geq -1$ we have the remainder and quotient determined. If, on the other hand, $2n - m \leq -2$, we may apply the extended definition for $U_{2n-m}(x)$. Summarizing, we have

$$U_m(x) = \begin{cases} 2T_{m-n}(x)U_n(x) - U_{2n-m}, & \text{if}\ \ n \leq m \leq 2m+1 \\ 2T_{m-n}(x)U_n(x) + U_{m-2n-2}, & \text{if}\ \ 2n+2 \leq m < 3n+2 \end{cases} \tag{18}$$

If $m \geq 3n+2$, we apply again the formula given by equation (17). In general, we have

Property 4 *Let $m \geq n$ be positive integers. If there is an integer $l \geq 0$ satisfying $(2l+1)n+2l \leq m \leq (2l+2)n+2l+1$, then*

$$U_m(x) = 2U_n(x)\sum_{k=0}^{l} T_{m-(2k+1)n-2k}(x) - U_{2(l+1)n-m-2l}(x),$$

otherwise

$$U_m(x) = 2U_n(x)\sum_{k=0}^{l} T_{m-(2k+1)n-2k}(x) + U_{m-2(l+1)n-2(l+1)}(x),$$

where m satisfies $(2l+2)n+2l+2 \leq m < (2l+3)n+2l+2$,

When $m = (2l+1)n+2l$, the above equation can be rewritten as

$$U_m(x) = U_n(x)\left(2\sum_{k=0}^{l} T_{m-(2k+1)n-2k}(x) - 1\right),$$

and we have, from property 3, zero remainder. If $m = (2l+2)n+2l+1$, we again have zero remainder (because $U_{-1}(x) = 0$). In all other cases, the first term of the equations given in property 4 determines the quotient of the Euclidean division of U_m by U_n, while the second term gives the (nonzero) remainder. Using the extended definition (12), we have proved the following

Theorem 5 *Let $m \leq n$ be two positive integers. $U_m(x)$ is a multiple of $U_n(x)$ if and only if $m = (l+1)n+l$ for some integer $l \geq 0$. Otherwise, the remainder of the Euclidean division of $U_m(x)$ by $U_n(x)$ is given by $r(x) = -U_{2(l+1)n-m-2l}(x)$, where $l \geq 0$ satisfies $(l+1)n+l < m < (l+3)n+l+2$.*

Example: Consider $m = 33$ and $n = 4$. As $30 = 6.4+6 \leq 33 < 7.4+6 = 34$, we use the second formula of property 4, determining that

$$U_{33}(x) = 2U_4(x)(T_{29}(x) + T_{19}(x) + T_9(x)) + U_3(x)$$

5 Modular Factorization

We now consider the factorization of Chebyshev polynomials over finite fields $\mathbf{Z}_p$. Specifically, we show the existence of primes p for which the $T_n(x)$ (or $U_n(x)$) factors into linear factors in $\mathbf{Z}_p$. Let ξ_k be the roots of $T_n(x)$ defined in equation (3), for $k = 1, \ldots, n$, for some some fixed n. Notice that $\xi_k = \cos\frac{2\pi}{4n}(2k-1)$, or

$$\xi_k = \frac{\left(e^{i\frac{2\pi}{4n}}\right)^{2k-1} + \left(e^{-i\frac{2\pi}{4n}}\right)^{2k-1}}{2} = \frac{w^{2k-1} + w^{-2k+1}}{2},$$

where $w = e^{\frac{i2\pi}{4n}}$ is a primitive complex $(4n)^{\mathrm{th}}$ root of unity. Consider the field $\mathbf{Q}(w)$, the rationals adjoined by w. We know by definition that

$$\mathbf{Q}(w) = \left\{(a_0/b_0) + (a_1/b_1)w + \cdots + (a_{s-1}/b_{s-1})w^{s-1} : a_j, b_j \in \mathbf{Z}\right\},$$

where $s = [\mathbf{Q}(w) : \mathbf{Q}]$ is the degree of the extension field $\mathbf{Q}(w)$ over $\mathbf{Q}$. It is well known that $s = \phi(4n)$. As a remark, we observe that Lehmer's result [9] shows that $[\mathbf{Q}(w) : \mathbf{Q}(w + 1/w)] = 2$. Let p be an odd prime. We define

$$\mathbf{Q}_{\overline{p}}(w) = \left\{(a_0/b_0) + (a_1/b_1)w + \cdots + (a_{s-1}/b_{s-1})w^{s-1} : a_j, b_j \in \mathbf{Z},\ p \not| b_j\right\}.$$

It is easy to see that $\mathbf{Q}_{\overline{p}}(w)$ is a ring. Moreover, all the powers of w, including negative ones, belong to $\mathbf{Q}_{\overline{p}}(w)$. Let $GF(q)$ be a finite field of characteristic p with q elements (q is some power of p). Let us assume that $GF(q)$ has a primitive $(4n)^{\mathrm{th}}$ root of unity θ. Defining the natural ring homomorphism

$$\Psi : \ \mathbf{Z} \longrightarrow \mathbf{Z}_p$$

by $\Psi(a) = a \mod p$, we can extend Ψ to the polynomial ring $\mathbf{Q}_{\overline{p}}(w)[x]$ onto $GF(q)[x]$ in the following way.

$$\begin{aligned}\Psi(a/b) &= \Psi(a)/\Psi(b)\\ \Psi(w) &= \theta\\ \Psi(x) &= x\end{aligned}$$

We see now that

$$\begin{aligned}\Psi(T_n(x)) &= \Psi\left(2^{n-1}(x-\xi_1)\cdots(x-\xi_n)\right)\\ &= \Psi\left(2^{n-1}(x - \frac{w+w^{-1}}{2})(x - \frac{w^3+w^{-3}}{2})\cdots(x - \frac{w^{2n-1}+w^{-2n+1}}{2})\right)\\ &= \Psi(2)^{n-1}(x - \frac{\theta+\theta^{-1}}{\Psi(2)})(x - \frac{\theta^3+\theta^{-3}}{\Psi(2)})\cdots(x - \frac{\theta^{2n-1}+\theta^{-2n+1}}{\Psi(2)}).\end{aligned}$$

Since the quantities $\frac{\theta^{2k-1}+\theta^{-2k+1}}{\Psi(2)}$ are well defined in $GF(q)$, we see that $\Psi(T_n(x))$ has all its roots in $GF(q)$. Hence, we can find n linear factors of $T_n(x)$ modulo an odd prime p if either one of the following circumstances occur. (i) The field $\mathbf{Z}_p$ itself has a primitive $(4n)^{\mathrm{th}}$ root of unity. (ii) $GF(q)$, a field with characteristic p, has a primitive $(4n)^{\mathrm{th}}$ root of unity and all the quantities $\theta^{2j-1} - \theta^{-2j+1}$, $j = 1, \ldots, n$, belong to the ground field $\mathbf{Z}_p$.

Lemma 2 *Let n and K be positive integers. If $p = 4nK + 1$ is prime, then $\mathbf{Z}_p$ has a primitive $(4n)^{th}$ root of unity.*

Proof: A well known result states that $\mathbf{Z}_p$ has a primitive $(M)^{\mathrm{th}}$ root of unity if and only if M divides $p - 1$ (see, for example [10]). □

Lemma 3 *Let n and K be positive integers. If $p = 4nK - 1$ is prime, then $GF(p^2)$ has a primitive $(4n)^{th}$ root of unity θ and all the quantities $\theta^{2j-1} - \theta^{-2j+1}$, $j = 1, \ldots, n$, belong to the groung field $\mathbf{Z}_p$.*

Proof: From the fact that $4n$ divides $p^2 - 1$ follows the existence of θ, a primitive $(4n)^{\text{th}}$ root of unity in $GF(p^2)$. Let $f(x) = x^2 + ax + b$ be an irreducible polynomial in $\mathbf{Z}_p[x]$ and let α be a root of $f(x)$. Considering the arithmetic of $GF(p^2) = \mathbf{Z}_p(\alpha)$, we denote $\theta = c + d\alpha$, for some $c, d \in \mathbf{Z}_p$ and compute $\theta^{-1} = \frac{c - da - d\alpha}{c^2 - cda + d^2 b}$. It follows that

$$\theta + \theta^{-1} = c + \frac{c - ad}{c^2 - cda + d^2 b} + \alpha\left(d - \frac{d}{c^2 - cda + d^2 b}\right).$$

To show that $\theta + \theta^{-1} \in \mathbf{Z}_p$ it suffices to show that $c^2 - cda + d^2 b = 1$. By the technical lemma 4 below we observe that $\theta^{p+1} = c^2 - cda + d^2 b$. As $p + 1 = 4nK$ and θ is a primitive $(4n)^{\text{th}}$ root of unity, it follows that $c^2 - cda + d^2 b = 1$. From the identity

$$\theta^j + \theta^{-j} = (\theta + \theta^{-1})(\theta^{j-1} + \theta^{-(j-1)}) - (\theta^{j-2} + \theta^{-(j-2)}),$$

follows that all the other quantities $\theta^{2j-1} + \theta^{-(2j-1)}$ belong to $\mathbf{Z}_p$. □

Lemma 4 *Let p be a prime. Let $\alpha \in GF(p^2)$ be a root of the irreducible polynomial $f(x) = x^2 + ax + b$ over $\mathbf{Z}_p$. For any $c, d \in \mathbf{Z}_p$, we have*

$$(c + d\alpha)^{p+1} = c^2 - cda + d^2 b \in \mathbf{Z}_p.$$

Proof: As the arithmetic is done modulo p, we have

$$\begin{aligned}
(c + d\alpha)^{p+1} &= \sum_{j=0}^{p+1} \binom{p+1}{j} c^j (d\alpha)^{p+1-j} \\
&= c^{p+1} + (p+1)c^p d\alpha + (p+1)c(d\alpha)^p + (d\alpha)^{p+1} \\
&= c^2 + cd\alpha + cd\alpha^p + d^2\alpha^{p+1}.
\end{aligned}$$

The last equality is a consequence of Fermat's Little Theorem. Observing that α^p is the other distinct root of $f(x)$, we see that $-a = \alpha + \alpha^p, b = \alpha^{p+1}$ and the result follows. □

Theorem 6 *Let $n \geq 2$ be an integer. For all the infinitely many positive integers K for which $p = 4nK \pm 1$ is a prime number, $T_n(x)$ has n roots in $\mathbf{Z}_p$.*

Proof: By the results of lemmas 2 and 3 it remains to show that there are infinitely many primes of the form $p = 4nK + 1$ and $p = 4nK - 1$. This follows from Dirichlet's theorem[2] for $(l, m) = (1, 4n)$ and for $(l, m) = (-1, 4n)$, respectively. □

Example: Consider $T_6(x) = 32\,x^6 - 48\,x^4 + 18\,x^2 - 1$. Primes of the form $p = 4nK + 1$,

[2] If l and m are integers with $\gcd(l, m) = 1$, then there are infinitely many prime numbers p satisfying $p \equiv l \pmod{m}$ (see, for example, [2, pp. 122].

include $p = 73$, for $K = 3$ and primes of the form $p = 4nK - 1$ include $p = 23$, for $K = 1$. We have

$$T_6(x) \equiv 32\ (x+30)\,(x+59)\,(x+16)\,(x+14)\,(x+43)\,(x+57)\ \ (\mathrm{mod}\ 73) \tag{19}$$

$$T_6(x) \equiv 9\ (x+19)\,(x+4)\,(x+10)\,(x+9)\,(x+14)\,(x+13)\ \ (\mathrm{mod}\ 23) \tag{20}$$

The modular properties of the polynomials $U_n(x)$ are similar to those of the polynomials $T_n(x)$. Observing that

$$\eta_k = \frac{w^k + w^{-k}}{2}, \quad k = 1, \ldots, n,$$

where $w = e^{\pi k i/(n+1)}$ is a primitive complex $(2n+2)^{\text{th}}$ root of unity, one can show

Theorem 7 *Let $n \geq 2$ be an integer. For all the infinitely many positive integers K for which $p = 2(n+1)K \pm 1$ is a prime number, $U_n(x)$ has n roots in $\mathbf{Z}_p$.*

6 Finding the Modular Roots

We will now outline methods to find the actual roots of a Chebychev polynomial in a given finite fields $\mathbf{Z}_p$ that contains all its zeros. We construct efficient algorithms that take an integer $n > 1$ and a prime $p = 4nK \pm 1$ ($p = 2(n+1)K \pm 1$) and compute all the zeros of $T_n(x)$ ($U_n(x)$) modulo p. Let us consider first the case $p = 4nK + 1$ ($2(n+1)K + 1$) for some $K > 0$. In this case, the field $\mathbf{Z}_p$ has a primitive $(4n)^{\text{th}}$ ($(2n+2)^{\text{th}}$) root of unity θ. It is easy to find θ if we first search for a primitive element $\beta \in \mathbf{Z}_p$. It is well known that β satisfies $\gcd(p-1, \beta) = 1$. Since n and K are known, we may choose β as the first odd prime not diving n or K ($n+1$ or K). Once a primitive element β is chosen, a primitive $(4n)^{\text{th}}$ ($(2n+2)^{\text{th}}$) root of unity θ is obtained by setting

$$\theta = \beta^{(p-1)/4n} \qquad (\theta = \beta^{(p-1)/(2n+2)}).$$

The roots then are readily computed by the relation $\xi_k = \frac{\theta^{2k-1} + \theta^{-2k+1}}{2}$ ($\eta_k = \frac{\theta^k - \theta^{-k}}{2}$). We formalize these ideas in algorithm **PRoots** (Fig. 1). The number of steps required by algorithm 1 is limited by the primes p_j from the set Q that need to be tested, which in turn is bounded by the number of primes smaller than or equal to p. In other words, according to the Prime Number Theorem (see e. g. [2, pp. 120], algorithm `PRoots` has order

$$O(p/\log p).$$

As an example, consider $T_6(x)$ and $p = 73 = 4 \times 6 \times 3 + 1$. Here the first primitive element of $\mathbf{Z}_p$ is $\beta = 5$. The corresponding primitive $(24)^{\text{th}}$ root of unity is $\theta = 5^{72/24} = 5^3 = 52$ (mod 73). The actual zeros appear in the example above. If we take $U_6(x)$ and $p = 29 = 2(6+1)2 + 1$, the first primitive element of $\mathbf{Z}_p$ is $\beta = 3$.

Algorithm PRoots(n, K)

```
INPUT:      Integers, $n, K, Q = \{p_1 = 3, p_2 = 5, p_3 = 7, p_4 = 11, \ldots\}$
OUTPUT:     Roots of $T_n(x) \mod 4nK+1$    [$U_n(x) \mod 2(n+1)K+1$ ]
PRoots-1    $p = 4nK+1$    [$2(n+1)K+1$]
PRoots-2    (Find $\beta$)
            for $j = 1$ to $p-1$ do
            2.1   $\beta = p_j$
            2.2   if ! ($\beta|n$ or $\beta|K$)    [! ($\beta \mid n+1$ or $\beta|K$)]
                      break
PRoots-3    $\theta = \beta^{(p-1)/4n}$ ( $\theta = \beta^{(p-1)/(2n+2)}$ )
PRoots-4    for $k = 1$ to $n$ do
            output $\xi_k = \frac{\theta^{2k-1}+\theta^{-2k+1}}{2}$    [$\eta_k = \frac{\theta^k-\theta^{-k}}{2}$]
```

Figure 1: Algorithm for computing the roots of $T_n(x)$ ($U_n(x)$)

The corresponding primitive $(14)^{\text{th}}$ root of unity is $\theta = 3^{28/14} = 3^2 = 9 \pmod{29}$. The actual zeros of $U_6(x) \pmod{29}$ are $11, 9, 13, 16, 20$ and 18. We now consider the case $p = 4nK - 1$ ($p = 2(n+1)K - 1$), where the extension field $GF(p^2)$ has a primitive $(4n)^{\text{th}}$ ($(2n+2)^{\text{th}}$) root of unity θ, which we wish to find it. The well known *Law of Quadratic Reciprocity* states: if -1 is not a square modulo p then the polynomial x^2+1 is irreducible in $\mathbf{Z}_p$. We may therefore consider $GF(p^2)$ as the Gaussian integers, with arithmetic done modulo p. For p small, it is alright to find a primitive $(4n)^{\text{th}}$ ($(2n+2)^{\text{th}}$) root of unity θ by trial and error, obtaining first a primitive element in $\mathbf{Z}_p \times i\mathbf{Z}_p$. A more efficient search is to use the result of lemma 4. We find solutions $c, d \in \mathbf{Z}_p$ to the equation $c^2 + d^2 = 1$. Compute the order t of the element $\beta = c + id \in \mathbf{Z}_p \times i\mathbf{Z}_p$. Note t always divides $p+1$, by lemma 4. If $4n$ divides t ($2n+2$ divides t), then we take $\theta = \beta^{t/4n}$ ($\theta = \beta^{t/(2n+2)}$) as our primitive $(4n)^{\text{th}}$ ($(2n+2)^{\text{th}}$) root of unity. We repeat the search until $4n$ divides t ($2n+2$ divides t). Since $p+1$ divides p^2-1, we know that there exist elements of order $p+1$ in $\mathbf{Z}_p \times i\mathbf{Z}_p$ and this search will terminate. This efficient algorithm is shown in Figure 2. Searching for modular roots in the given field is clearly time consuming because the cardinality of the finite field is p^2. But there is no known inexpensive algorithms to find a primitive element in the field $\mathbf{Z}_p \times i\mathbf{Z}_p$. A very rough estimate for the running time of the algorithm `MRoots` is $O(p^3)$, which is in the same order of a trial and error procedure. Clearly this worst-case running time is unlikely and a more detailed complexity analysis of the algorithm will be worthwhile. As an example, we take $U_3(x)$ and $p = 23 = 2(3+1)3 - 1$. Solutions (c, d) to $c^2 + d^2 = 1 \pmod{p}$ include $(4,10), (8,11), (9,9), (10,19), (11,15)$. The respective orders of the corresponding elements are $24, 12, 8, 24, 3$ and we may take $\theta = (4+10i)^{24/8} = 14 + 9i$

```
Algorithm MRoots($n, K$)

INPUT:      Integers, $n, K$
OUTPUT:     Roots of $T_n(x) \mod 4nK-1$   $[U_n(x) \mod 2(n+1)K-1\ ]$
MRoots-1    $p = 4nK-1$   $[2(n+1)K-1]$
MRoots-2    for $j = 1$ to $p-1$ do
                for $k = 1$ to $p-1$ do
                    $a = j^2 + k^2 (\mathrm{mod}\ p)$
                    if $a = 1$ then
                    {   $t = \mathrm{order}(\beta = j + k \times i \mod p)$
                        if $(4n(2n+2) \mid t)$ then goto(Step 3)
                    }
                done
            done
MRoots-3    $\theta = \beta^{t/4n}$ ( $\theta = \beta^{t/(2n+2)}$ )
MRoots-4    for $k = 1$ to $n$ do output $\xi_k = \frac{\theta^{2k-1}+\theta^{-2k+1}}{2}$   [ $\eta_k = \frac{\theta^k-\theta^{-k}}{2}$ ]
```

Figure 2: Another Algorithm for Roots of $T_n(x)$ ($U_n(x)$)

as the primitive $(8)^{\mathrm{th}}$ root of unity. The corresponding roots are 14,0, 9.

7 Conclusion

In this paper, several algebraic properties of Chebyshev polynomials of the

first and second kind have been presented. In particular, criteria for determining irreducibility and factorization of Chebyshev polynomials over the Integer **Z** have been developed. Also, Tests for deciding when Chebyshev polynomials is divisible by one another have been presented. Further, it has been shown that the remainder produced by Euclidean division of two Chebyshev polynomials is, up to a sign, another Chebyshev polynomial. In addition, this paper has discussed the problem of factorizing Chebyshev polynomials over finite fields. It has been shown that, given any Chebyshev polynomials, two infinite sets of primes p can be found such that $\mathbf{Z}_p$ contains all the roots of the polynomial. A procedure for computing the modular roots has been also presented.

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

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

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

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

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

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

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

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