Available online at www.sciencedirect.com
SCIENCE DIRECT•

ELSEVIER Computers and Mathematics with Applications 50 (2005) 1231–1240

An International Journal
computers & mathematics
with applications

www.elsevier.com/locate/camwa

Factorization Properties of Chebyshev Polynomials

M. O. RAYES
Southern Methodist University
School of Engineering and Applied Science
Department of Computer Science and Engineering
Dallas, TX 75275, U.S.A.
mrayes@engr.smu.edu

V. TREVISAN
UFRGS-Instituto de Matemática
91509-900 Porto Alegre, RS, Brazil
trevisan@mat.ufrgs.br

P. S. WANG
Department of Computer Science
Kent State University
Kent, OH 44240, U.S.A.
pwang@mcs.kent.edu

(Received June 2004; revised and accepted July 2005)

Abstract—Several factorization properties of Chebyshev are reported here. Studying the euclidean division of two Chebyshev, we observe that the remainder is either zero or (up to a sign) another Chebyshev polynomial. This lead to explicit computation of the greatest common divisor of two Chebyshev. We also obtain conditions for determining when a Chebyshev polynomial is divisible by another. Observing the modular representation over prime fields, we find two infinite sets of fields $\mathbb{Z}_p$ where a given Chebyshev polynomial factors completely into linear factors. We discuss how to obtain the factors. © 2005 Elsevier Ltd. All rights reserved.

Keywords—Chebyshev polynomials, Polynomial factorization, Greatest common divisor, Modular roots, Primitive root.

1. INTRODUCTION

Chebyshev 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 are well understood, but algebraic properties less so. Some examples of algebraic properties of Chebyshev studied may be seen in the references [1–3]. Other examples of algebraic properties for Chebyshev include the work of Hsiao [4], who gave a complete factorization of Chebyshev of the first kind $T_n(x)$, determining which roots should be grouped together to yield

We would like to acknowledge the careful reading of two anonymous referees who caught mistakes and made this paper more readable.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX
doi:10.1016/j.camwa.2005.07.003

irreducible factors with integer coefficients. Extending this result, Rivlin [5] adapts Hsiao's proof for the Chebyshev of the second kind $U_n(x)$.

Reported here are several decomposition properties of Chebyshev including factorization and divisibility. Conditions for determining when a Chebyshev polynomial is divisible by another are developed. It is also shown that the remainder produced by Euclidean division of two Chebyshev is again a Chebyshev polynomial, up to a sign. This fact leads to a direct computation of the greatest common divisor of two Chebyshev. Presented also is the factorization of Chebyshev over finite fields. Given any Chebyshev polynomial of degree n, two infinite sets of primes p are found such that the polynomial can be factored into n linear factors over $\mathbb{Z}_p$. Procedures for finding the modular roots are also discussed.

Let's begin with some basic definitions and properties of Chebyshev.

2. CHEBYSHEV POLYNOMIALS

The Chebyshev 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

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

Alternatively, they may be defined as

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

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

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

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

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

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

are useful. They can be proven using trigonometric identities [5, p. 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 of the second kind are defined by setting $U_0(x) = 1$, $U_1(x) = 2x$, and the recurrence relation,

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

They may also be defined by

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

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,

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

Useful decomposition properties for the U polynomials include the following [6, p. 97],

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

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

To extend the definition of Chebyshev 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 and the reader is encouraged to refer to the excellent books by Rivlin [5] and Snyder [6].

3. DIVISION PROPERTIES

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

3.1. 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 of the first kind. Performing the Euclidean division, we obtain integral quotient and remainder polynomials $q(x)$ and $r(x)$ satisfying

$$T_m(x) = q(x)T_n(x) + r(x), \qquad \deg(r) < \deg(T_n). \tag{13}$$

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

PROPERTY 2. Let $m \geq n$ be two positive integers. The polynomials $q(x)$ and $r(x)$ satisfying the Euclidean division (13) are given by

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

$$r(x) = (-1)^l T_{|m-2ln|}(x),$$

where $l \geq 1$ is the unique integer satisfying $|m - 2ln| < n$, if there is such an l. Otherwise,

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

$$r(x) = 0,$$

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

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

$$T_m(x) = 2T_n(x)T_{m-n}(x) - T_{m-2n}(x), \qquad \text{integers } m, n. \tag{14}$$

Let l be the smallest positive integer satisfying $|m - 2ln| \leq n$. Applying the decomposition formula (14) $l - 1$ times, we deduce

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

If $|m - 2ln| < n$, then $\deg(T_n(x)) < \deg(T_{m-(2l-2)n}(x))$ and so we apply property (14) 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 of the first kind is either zero or another Chebyshev 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 a divisor of m and m/n is odd. This statement may be seen as the converse of Property 1. The following theorem summarizes the results.

THEOREM 1. *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 $l \geq 1$. 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 unique integer satisfying $|m - 2nl| < n$.*

THEOREM 2. *Let m, n be positive integers and $g = \gcd(m, n)$. Let $n = gn_1$ and $m = gm_1$. If n_1 and m_1 are odd, then*

$$\gcd(T_m(x), T_n(x)) = T_{\gcd(m,n)}(x) = T_g(x),$$

otherwise

$$\gcd(T_m(x), T_n(x)) = 1.$$

PROOF. By Theorem 1, all polynomial remainder sequence are Chebyshev, and so the

$$\gcd(T_m(x), T_n(x))$$

is a Chebyshev polynomial. Hence, we need only to consider the common factors $T_h(x)$ of $T_n(x)$ and $T_m(x)$. Let h be a common factor of m and n, say $n = hn_1$ and $m = hm_1$. By Theorem 1, we see that the only common factors of $T_n(x)$ and $T_m(x)$ are those $T_h(x)$ whose cofactors n_1 and m_1 are odd. As $T_g(x)$ is the highest degree polynomial satisfying these conditions, the result is proved. ∎

In particular, we can state the following.

COROLLARY 1. *If m and n are odd, then $\gcd(T_m(x), T_n(x)) = T_{\gcd(m,n)}(x)$.*

COROLLARY 2. *If m or n is a power of two and $m \neq n$, then $\gcd(T_m(x), T_n(x)) = 1$.*

3.2. Divisors of $U_n(x)$

By applying the decomposition property (10), we obtain the following.

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. $U_m(x) = U_{l(n+1)-1}(x) = U_{l-1}(T_{n+1}(x))U_n(x)$. ∎

To determine the Euclidean division of U_m by U_n, we use the extended definition for negative indices of Chebyshev and apply equation (11) with m replaced by $n+1$ and n replaced by $n - m$ and obtain

$$U_m(x) = 2T_{m-n}(x)U_n(x) - U_{2n-m}(x), \qquad \text{integers } m, n. \tag{15}$$

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

$$U_m(x) = \begin{cases} 2T_{m-n}(x)U_n(x) - U_{2n-m}, & \text{if } n \leq m \leq 2n+1, \\ 2T_{m-n}(x)U_n(x) + U_{m-2n-2}, & \text{if } 2n+2 \leq m < 3n+2. \end{cases} \tag{16}$$

If $m \geq 3n + 2$, we apply again the formula given by equation (15). In general, we have the following.

PROPERTY 4. Let $m \geq n$ be two positive integers. Let

$$l = \left\lfloor \frac{m-n}{2n+2} \right\rfloor.$$

Then,

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

When $(m - n)/(2n + 2)$ is an integer, that is, $m = (2l + 1)n + 2l$, 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 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 3. *Let $m \geq n$ 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 $r(x) = -U_{2(l+1)n+2l-m}(x)$, where*

$$l = \left\lfloor \frac{m-n}{2n+2} \right\rfloor.$$

EXAMPLE. Consider $m = 33$ and $n = 4$. We have

$$l = \left\lfloor \frac{m-n}{2n+2} \right\rfloor = 2,$$

determining that

$$U_{33}(x) = 2U_4(x)(T_{29}(x) + T_{19}(x) + T_9(x)) - U_{-5}(x).$$

This sets the remainder as $-U_{-5}(x)$, which is, by equation (12), equal to $U_3(x)$.

THEOREM 4. *Let m and n be two nonnegative integers, $g = \gcd(m + 1, n + 1)$. Then,*

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

PROOF. Using Theorem 3, we see that $U_{g-1}(x)$ divides both $U_m(x)$ and $U_n(x)$. Since Theorem 3 implies that the gcd is a Chebyshev polynomial of the second kind, let us now suppose that $U_h(x)$ is a common factor of $U_m(x)$ and $U_n(x)$. By Theorem 3, h satisfies $m = (h + 1)l_1 + h$ and $n = (h + 1)l_2 + h$, for some integers $l_1 \geq 0$ and $l_2 \geq 0$. These two equations may be rewritten as $m+1 = (h+1)(l_1+1)$ and $n+1 = (h+1)(l_2+1)$. By the definition of $g = \gcd(m+1, n+1)$, we notice that $h + 1 \leq g$, which proves that $U_{g-1}(x)$ is the Chebyshev polynomial of highest degree dividing both $U_m(x)$ and $U_n(x)$. ∎

COROLLARY 3. *If* $m+1$ *or* $n+1$ *is prime and* $n \neq m$, *then* $\gcd(U_n(x), U_m(x)) = 1$.

4. MODULAR FACTORIZATION

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

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

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

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

where $s = [\mathbb{Q}(w) : \mathbb{Q}]$ is the degree of the extension field $\mathbb{Q}(w)$ over $\mathbb{Q}$. It is well known that $s = \phi(4n)$. As a remark, we observe that Lehmer's result [7] shows that $[\mathbb{Q}(w) : \mathbb{Q}(w+1/w)] = 2$. Let p be an odd prime. We define

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

It is easy to see that $\mathbb{Q}_{\overline{p}}(w)$ is a ring. Moreover, all the powers of w, including negative ones, belong to $\mathbb{Q}_{\overline{p}}(w)$. 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 $(4n)^{\text{th}}$ root of unity θ. Defining the natural ring homomorphism,

$$\Psi : \mathbb{Z} \longrightarrow \mathbb{Z}_p,$$

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

$$\Psi(a/b) = \Psi(a)/\Psi(b),$$

$$\Psi(w) = \theta,$$

$$\Psi(x) = x.$$

We see now that

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

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 $\mathbb{Z}_p$ itself has a primitive $(4n)^{\text{th}}$ root of unity.

(ii) $GF(q)$, a field with characteristic p, has a primitive $(4n)^{\text{th}}$ root of unity and all the quantities $\theta^{2j-1} - \theta^{-2j+1}$, $j = 1, \dots, n$, belong to the ground field $\mathbb{Z}_p$.

The first situation is solved by the following.

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

PROOF. A well known result states that $\mathbb{Z}_p$ has a primitive M^{th} root of unity if and only if M divides $p - 1$. ∎

For dealing with the second situation, we need a technical lemma.

LEMMA 2. *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 $\mathbb{Z}_p$. For any $c, d \in \mathbb{Z}_p$, we have*

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

PROOF. As the arithmetic is done modulo p, we have

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

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. ∎

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

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 $\mathbb{Z}_p[x]$ and let α be a root of $f(x)$. Considering the arithmetic of $GF(p^2) = \mathbb{Z}_p(\alpha)$, we denote $\theta = c + d\alpha$, for some $c, d \in \mathbb{Z}_p$ and compute $\theta^{-1} = (c - da - d\alpha)/(c^2 - c\,da + d^2 b)$. It follows that

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

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

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

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

THEOREM 5. *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 $\mathbb{Z}_p$.*

PROOF. By the results of Lemmas 1 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[1] for $(l, m) = (1, 4n)$ and for $(l, m) = (-1, 4n)$, respectively. ∎

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

EXAMPLE. Consider $T_6(x) = 32\,x^6 - 48\,x^4 + 18\,x^2 - 1$. Primes of the form $p = 4nK + 1$, include $p = 73$, for $K = 3$ and primes of the form $p = 4nK - 1$ include $p = 23$, for $K = 1$. We have

$$T_6(x) \equiv 32\ (x+30)\,(x+59)\,(x+16)\,(x+14)\,(x+43)\,(x+57) \pmod{73} \tag{17}$$

$$T_6(x) \equiv 9\ (x+19)\,(x+4)\,(x+10)\,(x+9)\,(x+14)\,(x+13) \pmod{23} \tag{18}$$

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

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

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

THEOREM 6. *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 $\mathbb{Z}_p$.*

5. FINDING THE MODULAR ROOTS

The problem of finding the modular roots of the Chebyshev $T_n(x)$ has been reduced to that of finding a primitive $(4n)^{\text{th}}$ root of unity in $GF(q)$, where either $q = p = 4nK + 1$ or $q = p^2 = (4nK - 1)^2$, where p is some prime number and K is a natural number. We first consider the case, $q = p = 4nK + 1$.

A possible approach is to find a primitive element $\beta \in GF(q)$ and then take $\theta = \beta^{(q-1)/4n}$. The density of primitive elements in $GF(q)$ ensures that a simple search procedure choosing, at random, a small number of elements is an efficient probabilistic procedure. In fact, the expected number of multiplications mod p is $O((\log p)/(\log\log p)^2)$, meaning that the search procedure is $O(((\log p)^4/(\log\log p))^2)$ bit operations [8].

However, the existence of an efficient deterministic search procedure is much harder and has been considered elsewhere. We summarize next the results relevant to this note.

Improving on results of Wang [9], Shoup [10] proved that if the extended Riemann hypothesis (ERH) holds, then the least primitive root mod$p$ is in $O(\log p)^6$. Improving on this, Bach [8] shows that, assuming the ERH, the least primitive root mod$p$ is in $O((\log p)^6/(\log\log p)^3)$. Bach also describes an algorithm to compute a set of size $O((\log p)^4(\log\log p)^{-3})$ which needs to be searched for a primitive element (not necessarily the least). This type of result immediately gives an efficient search procedure for primitive roots modulo p; it shows how to construct a small set of elements of $\mathbb{Z}_p$, one of which generates all the nonzero elements mod p. In fact, this can be done in $O((\log p)^7/(\log\log p)^3)$ bit operations [8].

As an example, consider $T_6(x)$ and $p = 73 = 4 \times 6 \times 3 + 1$. We are looking for the 24th root of unity in $\mathbb{Z}_{73}$. The first primitive element of $\mathbb{Z}_p$ is $\beta = 5$. The corresponding primitive 24th root of unity is $\theta = 5^{72/24} = 5^3 = 52 \pmod{73}$. The actual factorization of $T_6(x) \pmod{73}$ is given above by equation (17).

We consider now the case $p = 4nK - 1$, where the extension field $GF(p^2) = GF(q)$ has a primitive $(4n)^{\text{th}}$ root of unity θ, which we wish to find. Shoup [10] shows that, assuming the ERH, there is a deterministic polynomial time algorithm for primitive roots in $GF(p^2)$, with no restrictions on p.

We consider here an alternative probabilistic procedure for the case where $p = 4nK - 1$. It is well known that -1 is a square modulo p if and only if $p \equiv 1 (\text{mod } 4)$. Hence, for $p = 4nK - 1$, we see that the polynomial $x^2 + 1$ is irreducible in $\mathbb{Z}_p$. Therefore, we may consider $GF(p^2)$ as the Gaussian integers, with arithmetic done modulo p.

The result of Lemma 2 gives us a key for a search procedure. We find solutions $c, d \in \mathbb{Z}_p$ to the equation $c^2 + d^2 = 1$. Compute the order t of the element $\beta = c + id \in \mathbb{Z}_p \bigoplus i\mathbb{Z}_p$. Notice that t always divides $p+1$, by Lemma 2. If $4n$ divides t, then we take $\theta = \beta^{t/4n}$ as our primitive $(4n)^{\text{th}}$ root of unity. We repeat the search until $4n$ divides t . Since $p+1$ divides $p^2 - 1$, we know that

```
Algorithm MRoots($n, K$)
INPUT:      Integers, $n, K$
OUTPUT:     Roots of $T_n(x) \bmod 4nK - 1$
MRoots-1    $p = 4nK - 1$
MRoots-2    Choose randomly $c$ and $d \in GF(p)$
MRoots-3    Compute $a = c^2 + d^2 \bmod p$
MRoots-4    If $a \neq 1$ then GO TO Mroots-2
MRoots-5    Compute the order $t$ of $a \in GF(p^2)$
MRoots-6    If $4n$ divides $t$ then $\theta = (c + id)^{t/4n}$ else go back to MRoots-2
MRoots-7    for $k = 1$ to $n$ do
                output $\xi_k = \dfrac{\theta^{2k-1} + \theta^{-2k+1}}{2} \mod p$
```

Figure 1. A randomized algorithm for roots of $T_n(x)$.

there exist elements of order $p+1$ in $\mathbb{Z}_p \bigoplus i\mathbb{Z}_p$ and this search will terminate. This algorithm is shown in Figure 1.

As the number of primitive elements is $\phi(q-1)$, it follows that average number of trials the algorithm MRoots performs is bounded by $(q-1)/\phi(q-1)$. It has the advantage of testing a prior necessary condition, and such arithmetic is done modulo p, not in $GF(p^2)$.

Similar algorithms may be implemented for finding the linear factors of U_n, the Chebyshev of the second kind. It suffices to replace Step MRoot-1 with $p = 2(n+1)K - 1$ and the condition "if $4n$ divides t" in step MRoots-6 by "if $2n+2$ divides t". Step MRoots-7 also should compute η_k instead of ξ_k.

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 $\theta = (4+10i)^{24/8} = 14 + 9i$ as the primitive 8th root of unity. The corresponding roots are 14, 0, 9.

6. CONCLUSION

In this paper, several algebraic properties of Chebyshev polynomials of the first and second kind have been presented. Also, tests for deciding when a Chebyshev polynomial is divisible by 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, leading to the determination of the greatest common divisor of two Chebyshev.

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 $\mathbb{Z}_p$ contains all the roots of the polynomial. Finally, procedures for computing the modular roots have been discussed.

REFERENCES

1. T. Bang, Congruence properties of Tchebycheff polynomials, *Mathematica Scandinavica* **2**, 327–333, (1954).
2. L. Carlitz, Quadratic residues and Tchebycheff polynomials, *Portugaliae Mathematica* **18** (4), 193–198, (1959).
3. R.A. Rankin, Chebyshev polynomials and the modular group of level p, *Mathematica Scandinavica* **2**, 315–332, (1954).
4. H.J. Hsiao, On factorization of Chebyshev's polynomials of the first kind, *Bulletin of the Institute of Mathematics Academia Sinica* **12** (1), 89–94, (1984).
5. T.J. Rivlin, *The Chebyshev Polynomials—From Approximation Theory to Algebra and Number Theory*, Wiley-Interscience, John Wiley, (1990).
6. M.A. Snyder, *Chebyshev Methods in Numerical Approximation*, Prentice-Hall, New Jersey, (1966).
7. D.H. Lehmer, A note on trigonometric algebraic numbers, *American Mathematical Monthly* **40**, 165–166, (1933).
8. E. Bach, Comments on search procedures for primitive roots, *Mathematics of Computation* **66**, 1719–1729, (1997).

9. Y. Wang, On the least primitive root of a prime, (in Chinese), *Acta Math. Sinica* **9**, 432–441, (1959); On the least primitive root of a prime, (English translation), *Sci. Sinica* **10**, 1–14, (1961).
10. V. Shoup, Searching for primitive roots in finite fields, *Mathematics of Computation* **58**, 369–380, (1992).