2016 International Symposium on Nonlinear Theory and Its Applications,
NOLTA2016, Yugawara, Japan, November 27th-30th, 2016

The period of Chebyshev polynomial sequences modulo a prime power p^k

Daisaburo Yoshioka† and Kento Kawano‡

†Department of Computer and Information Sciences, Sojo University
4–22–1 Nishi-ku, Ikeda, Kumamoto 860-0082, Japan
‡Graduate School of Engineering, Sojo University
4–22–1 Nishi-ku, Ikeda, Kumamoto 860-0082, Japan

Abstract—A public-key cryptosystem based on Chebyshev polynomials has been recently proposed. In this paper, we give conditions on the degree of Chebyshev polynomials to be permutation polynomials modulo a prime power. We also derive the period of sequences generated by Chebyshev polynomials modulo a prime power.

1. Introduction

A polynomial over a finite ring is called a *permutation polynomial* if the mapping defined by the polynomial is one-to-one. Permutation polynomials have been used in cryptography, coding, and pseudorandom number generation. Rivest has shown a necessary and sufficient condition on coefficients of polynomials to be a permutation polynomial over a ring of integers modulo a power of two [1]. Umeno proved that Chebyshev polynomials of odd degree become permutation polynomials over the ring [2].

Taking advantage of the commutative property of Chebyshev polynomials in real field, a public key cryptosystem based on Chebyshev polynomials was firstly proposed [3], but soon broken [4]. In order to resist such attack, the definition of Chebyshev polynomials was expanded from real field to finite fields or finite rings [2], [5]. To analyze the security of the cryptosystem, several properties of sequences generated by iterating Chebyshev polynomials over a finite set (called *Chebyshev polynomial sequences in the following discussions*) have been investigated [6]–[10]. Indeed, it turns out that the cryptosystem employing Chebyshev polynomials over the integer ring of powers of two, even if efficient and practical, is unfortunately not secure [10]. The weakness of this algorithm is that Chebyshev polynomial sequences over the ring have *regular* periodicities. Therefore, it is important to clarify periodic properties of Chebyshev polynomials sequences for applications of cryptography and sequence design. However, the periodicities of Chebyshev polynomials modulo powers of odd prime have not been investigated so far, which is this paper's concern.

This paper firstly gives a necessary and sufficient condition on degree of Chebyshev polynomials to be a permutation polynomial over the ring of integers of powers of prime. We also derive a periodicity of Chebyshev polynomial sequences over the ring.

2. Chebyshev polynomial sequences modulo p^k

In this section, after we briefly give the definition and introduce some properties of Chebyshev polynomials, our new results will be presented.

2.1. Chebyshev polynomials modulo p^k

The Chebyshev polynomials of the first kind of degree n are defined by the recurrence relation

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

where $T_0(x) = 1$ and $T_1(x) = x$. The first few Chebyshev polynomials are $T_2(x) = 2x^2 - 1$, $T_3(x) = 4x^3 - 3x$, $T_4(x) = 8x^4 - 8x^2 + 1$.

One of the most important properties of Chebyshev polynomials is the semi-group property, that is, the composition of Chebyshev polynomials is also Chebyshev polynomials. In particular,

$$T_n(T_m(x)) = T_m(T_n(x)) = T_{mn}(x). \tag{2}$$

The commutative property allows us the construction of public-key cryptosystems. Up to linear transformations, the monomial x^n that appears in the Diffie-Hellman key agreement protocol and the Chebyshev polynomials are the only classes of polynomials that satisfy the commutative property. Thus, the cryptosystems employing Chebyshev polynomials have been proposed by replacing x^n with $T_n(x)$ [2],[3].

Let $\mathbb{Z}$ be the set of all integers and p be a prime number. For a positive integer $k \geq 1$, we consider Chebyshev polynomials over the residue ring of integers $R = \mathbb{Z}/p^k\mathbb{Z}$. Namely,

$$y = T_n(x) \bmod p^k. \tag{3}$$

A polynomial $f(x)$ with integer coefficients is said to be a *permutation polynomial* over a finite ring R if the mapping $R \to R$ defined by f is one-to-one. Many cryptographic algorithms use permutation polynomials such as RSA and RC6 block ciphers. Umeno has proven that for any odd n, T_n is a permutation polynomial over the integer ring $R = \mathbb{Z}/2^k\mathbb{Z}$. Here we consider the case of $R = \mathbb{Z}/p^k\mathbb{Z}$, where p is any odd prime.

We introduce the Dickson polynomial $D_n(x,a)$ of degree n which is defined by

$$D_n(x,a) = \sum_{m=0}^{\lfloor n/2 \rfloor} \frac{n}{n-m} \, {}_{n-m}C_m (-a)^m x^{n-2m}, \tag{4}$$

where $\lfloor \cdot \rfloor$ denotes greatest integer function. The first few Dickson polynomials are $D_0(x,a) = 2$, $D_1(x,a) = x$, $D_2(x,a) = x^2 - 2a$, $D_3(x,a) = x^3 - 3xa$, and so on. $D_n(x,a)$ over the ring $R = \mathbb{Z}/p^k\mathbb{Z}$ is a permutation polynomial if and only if the degree n is relatively prime to both p and $p^2 - 1$, where a is a unit over the ring R [11].

Dickson polynomials $D_n(x,a)$ are related to Chebyshev polynomials $T_n(x)$:

$$D_n(2x,1) = 2T_n(x). \tag{5}$$

Lemma 1 *Assume a and p are relatively prime. If $af(x)$ is a permutation polynomial over $R = \mathbb{Z}/p^k\mathbb{Z}$, then $f(x)$ is also a permutation polynomial over R.*

Proof: Suppose that $f(x)$ is not a permutation polynomial over R, then there are some integers x and y such that $f(x) \equiv f(y) \bmod p^k$, which implies $af(x) \equiv af(y) \bmod p^k$. This contradicts the fact that $af(x)$ is a permutation polynomial over R. □

Since $2x$ is a permutation polynomial over R, $D_n(2x,1)$ is also a permutation polynomial over R. Together with Lemma 1, we obtain the following result.

Theorem 1 *Let p be an odd prime and $k > 1$ be an positive integer. A Chebyshev polynomial $T_n(x)$ is a permutation polynomial modulo p^k, if and only if $(n,p) = (n,p^2-1) = 1$, where (a,b) denotes the greatest common divisor of two integers a and b.*

For example, when $p = 3$, $T_n(x)$ is a permutation polynomial modulo 3^k for any odd n which is not multiples of three. Thus, we always assume that n is an integer such that $(n,p) = (n,p^2-1) = 1$ hereafter.

The i-th iterate of $T_n(x)$ is denoted by

$$T_n^i(x) = T_n(T_n^{i-1}(x)) \bmod p^k. \tag{6}$$

We can generate an integer periodic sequence by iterating (6) from an initial value x. The period N is defined as the least positive integer such that

$$T_n^N(x) \equiv x \bmod p^k. \tag{7}$$

We now present examples. We can compute the sequence $\{T_n^i(x) \bmod p^k\}_{i=0}^{N-1}$ until the period N is discovered. For example, when $p = 5$, $n = 7$, $k = 4$, and $x = 4$, the sequence is

$$4, 569, 129, 444, 254, 319, 379, 194, 504, 69$$

the period of which is 10.

Since determining the period is a fundamental problem for engineering applications such as cryptography and pseudorandom numbers, it is important to know the period instead of calculating x, $T_n(x) \bmod p^k$, $T_n^2(x) \bmod p^k, \cdots$ until $T_n^N(x) \equiv x \bmod p^k$, which requires at most p^k times calculations of $T_n(X) \bmod p^k$. We study this in the following section.

2.2. The period of Chebyshev polynomial sequences modulo p^k

When $R = \mathbb{Z}/2^k\mathbb{Z}$, we have already shown an interesting property of Chebyshev polynomial sequences: the period of $\{T_n^i(x) \bmod 2^k\}_{i=0}^{N-1}$ is twice as long as that of $\{T_n^i(x) \bmod 2^{k-1}\}_{i=0}^{N-1}$ [9]. Therefore, it is expected that the period of $\{T_n^i(x) \bmod p^k\}_{i=0}^{N-1}$ is p times as long as that of $\{T_n^i(x) \bmod p^{k-1}\}_{i=0}^{N-1}$ for any odd prime p. However, this is not always true unlike the case of even prime, which is shown by numerical examples. The periods N of $T_n(x) \bmod p^k$ for $x = 2,3,4,5,6$ are shown in Tables 1, 2, and 3, where $\langle p,n \rangle = \langle 3,5 \rangle$, $\langle 5,7 \rangle$ and $\langle 7,5 \rangle$, respectively. For example, such periodic property does not hold when $x = 3,6$ and $k = 2$ in the case of $\langle p,n \rangle = \langle 3,5 \rangle$. Meanwhile, it can be seen from these Tables that the period of sequences modulo p^k is p times as long as that in the operation of modulo p^{k-1} when $k \geq 4$. In this section, we seek conditions for such periodic properties of Chebyshev polynomial sequences modulo p^k.

Assume X and $w \geq 1$ satisfy the relation

$$\begin{aligned} T_n(X) &\equiv X \bmod p^w, \\ T_n(X) &\not\equiv X \bmod p^{w+1}. \end{aligned} \tag{8}$$

According to (8), there exits an integer $b \in \{1, 2, \cdots, p-1\}$ such that

$$T_n(X) = X + b \cdot p^w. \tag{9}$$

Let $\mathcal{G}$ be a finite field with characteristic p. The order of an element m in the group $\mathcal{G}$, denoted as $\mathrm{ord}(m)$, is the least positive number such that $m^{\mathrm{ord}(m)} \equiv 1 \bmod p$. These lemmas will be used in the following discussion.

Lemma 2 *Let p be a prime number. For any integer $x \neq 0, 1$,*

$$1 + x + x^2 + \cdots + x^{\mathrm{ord}(x)-1} \bmod p \equiv 0 \tag{10}$$

Proof: Since $x^{\mathrm{ord}(x)} - 1 = (x-1)(x^{\mathrm{ord}(x)-1} + x^{\mathrm{ord}(x)-2} + \cdots + x + 1) \equiv 0 \bmod p$ and $x - 1 \not\equiv 0 \bmod p$, (10) holds. □

Lemma 3 *Let p be a prime number. For any integer $x \neq 0$,*

$$1 + x + x^2 + \cdots + x^{p-1} \bmod p \equiv \begin{cases} 1, & x \neq 1 \\ 0, & x = 1. \end{cases} \tag{11}$$

Table 1: The list of periods N for several values of x and k, where $p = 3$ and $n = 5$.

	$x = 2$	$x = 3$	$x = 4$	$x = 5$	$x = 6$
$k = 1$	1	1	1	1	1
$k = 2$	1	2	1	1	2
$k = 3$	3	6	1	1	6
$k = 4$	9	18	3	3	18
$k = 5$	27	54	9	9	54

Proof: Using $x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \cdots + x + 1)$ together with Fermat's little theorem, $x^p \equiv x \bmod p$, it is easy to see that the equation (11) holds. □

Let $T_n'(x)$ be the derivative of $T_n(x)$ with respect to x. Then, we have the following lemma.

Lemma 4 *For any x, $T_n'(x) \not\equiv 0 \bmod p$.*

Proof: We just recall the result of [12]. If there is an integer x such that $f'(x) \equiv 0 \bmod p$, the number of solution of $f(x) \equiv 0 \bmod p^k$ is none, where $f(x)$ is any integral polynomial. Since $T_n(x) \bmod p^k$ is a permutation polynomial, there is an integer such that $T_n(x) = 0 \bmod p^k$. Thus, the assertion is verified. □

Firstly, we show the following lemma, which means that the period of $T_n(X) \bmod p^{w+1}$ is related to the value of $T_n'(X) \bmod p$.

Lemma 5 *Assume X and $w \geq 1$ satisfy the relation of (8) Let $\ell = \mathrm{ord}(T_n'(X))$ for $T_n'(X) \not\equiv 1 \bmod p$ and $\ell = p$, otherwise. Then, $T_n^{\ell}(X) \equiv X \bmod p^{w+1}$.*

Proof: Substituting (9) into $T_n(x) = a_1x + a_3x^3 + \cdots + a_nx^n$ gives

$$\begin{aligned} T_n^2(X) &= a_1(X + b\cdot p^w) + a_3(X + b\cdot p^w)^3 + \cdots \\ &\quad + a_n(X + b\cdot p^w)^n \\ &\equiv T_n(X) + b\cdot p^w \cdot T_n'(X) \bmod p^{w+1} \\ &\equiv X + b\cdot p^w(T_n'(X) + 1) \bmod p^{w+1}. \end{aligned} \tag{12}$$

Repeating the above, it holds that

$$T_n^i(X) \equiv X + b\cdot p^w \sum_{m=0}^{i-1} T_n'(X)^m \bmod p^{w+1}. \tag{13}$$

where integer $i \geq 1$. By virtue of Lemmas 2 and 3, the assertion is verified. □

Let us define G as $G(x) = T_n^i(x) = T_{n^i}(x)$ for a positive integer $i > 1$. From the semi-group property of Chebyshev polynomials, G is also a Chebyshev polynomial of odd degree. The *chain rule* is a formula for computing the derivative of the composition of two functions f and g, that is, $(f(g(x)))' = f'(g(x)) \cdot g'(x)$.

Lemma 6 *Assume X and $w \geq 1$ satisfy the relation of (8). Let $G = T_n^i$. For $i \geq 1$,*

$$G'(X) \equiv (T_n'(X))^i \bmod p. \tag{14}$$

Table 2: The list of periods N for several values of x and k, where $p = 5$ and $n = 7$.

	$x = 2$	$x = 3$	$x = 4$	$x = 5$	$x = 6$
$k = 1$	1	1	1	1	1
$k = 2$	4	4	2	4	2
$k = 3$	4	4	2	4	2
$k = 4$	20	20	10	20	10
$k = 5$	100	100	50	100	50

Table 3: The list of periods N for several values of x and k, where $p = 7$ and $n = 5$.

	$x = 2$	$x = 3$	$x = 4$	$x = 5$	$x = 6$
$k = 1$	2	1	1	2	1
$k = 2$	6	3	3	2	3
$k = 3$	42	21	21	6	21
$k = 4$	294	147	147	42	147
$k = 5$	2058	1029	1029	294	1029

Proof: Using mathematical induction together with $T_n(X) \equiv X \bmod p$ leads to (14). □

When $w \geq 2$, (13) also holds in the operation of modulo p^{w+2}. Thus, we have the following lemma.

Lemma 7 *Assume X and $w \geq 2$ satisfy the relation of (8). If $T_n'(X) \equiv 1 \bmod p$, then $T_n^p(X) \equiv X \bmod p^{w+1}$ and $T_n^p(X) \not\equiv X \bmod p^{w+2}$.*

Next, we show a condition of X for which the period of sequence $\{T_n^i(X) \bmod p^k\}_{i=0}^{N-1}$ becomes p times longer as k increases.

Lemma 8 *Let m be a positive integer. Assume X and $w \geq 2$ satisfy the relation of (8). If $T_n'(X) \equiv 1 \bmod p$, then*

$$\begin{aligned} T_n^{p^m}(X) &\equiv X \bmod p^{w+m}, \\ T_n^{p^m}(X) &\not\equiv X \bmod p^{w+m+1}. \end{aligned} \tag{15}$$

Proof: We prove the above lemma by mathematical induction. It is shown by Lemma 7 that the case of $m = 1$ is satisfied. Suppose that (15) is true when $m = s$. From the semi-group property of T_n, $G = T_n^{p^s} = T_{np^s}$ is also a Chebyshev polynomial. Using (14), $G'(X) \equiv 1 \bmod p$. Therefore, by Lemma 7, we have $G^p(X) \equiv X \bmod p^{w+s+1}$ and $G^p(X) \not\equiv X \bmod p^{w+s+2}$, which means (15) is also true with $m = s + 1$ since $G^p = T^{p^{s+1}}$. From the above discussions, (15) is satisfied for arbitrary $m \geq 1$, which completes the proof. □

As a direct consequence of the above lemma, the period of Chebyshev polynomial sequences modulo p^k is derived as $N = p^{k-w}$ under the assumption that the condition of (8) is satisfied.

Example 1 *When $p = 3$, $n = 5$ and $X = 2$, we obtain $w = 2$ since $T_5(2) \equiv 2 \bmod 3^2$ and $T_5(2) \not\equiv 2 \bmod 3^3$. Since $T_n'(2) \equiv 1 \bmod 3$, the period N of the sequence $\{T_5(2) \bmod 3^k\}$ is derived as $N = 3^{k-2}$ for $k \geq 2$.*

Finally, we have the following theorem.

Theorem 2 *Assume X and w satisfy the relation of (8). Let $\ell = ord(T'_n(X))$ for $T'_n(X) \not\equiv 1 \bmod p$ and $\ell = p$, otherwise. Then, there is an integer w_2 such that $T^\ell_n(X) \equiv X \bmod p^{w_2}$ and $T^\ell_n(X) \not\equiv X \bmod p^{w_2+1}$. Furthermore, the period of Chebyshev polynomial sequences $\{T^i_n(X) \bmod p^k\}_{i=0}^{N-1}$ is derived as $N = \ell \cdot p^{k-w_2}$ for $k \geq w_2$.*

When $T_n(X) \not\equiv X \bmod p$, there is a least positive integer s such that $T^s_n(X) \equiv X \bmod p$. Let $G = T_{n^s}$, then there is an integer w_2 such that $G^\ell(X) \equiv X \bmod p^{w_2}$ and $G^\ell(X) \not\equiv X \bmod p^{w_2+1}$, where $\ell = \mathrm{ord}(G'(X))$ for $G'(X) \not\equiv 1 \bmod p$, and $\ell = 1$, otherwise. For $k \geq w_2$, the period of Chebyshev polynomial sequences $\{T^i_n(X) \bmod p^k\}_{i=0}^{N-1}$ is derived as $N = s \cdot \ell \cdot p^{k-w_2}$.

Proof: First, we consider the case for X with $w \geq 1$. Assume $T^\ell_n(X) \equiv X \bmod p^{w+1}$. Let $G = T_{n^\ell}(x)$, then, there is an integer $w_2 \geq 2$ such that $G(X) \equiv X \bmod p^{w_2}$ and $G(X) \not\equiv X \bmod p^{w_2+1}$. Since ℓ is the order of $T'_n(X) \bmod p$, $G'(X) = (T'_n(X))^\ell \equiv 1 \bmod p$. Together with Lemma 8, $G^{k-w_2}(X) \equiv X \bmod p^k$, which implies that the period of Chebyshev polynomial sequence $\{T^i_n(X) \bmod p^k\}_{i=0}^{N-1}$ must be $N = \ell \cdot p^{k-w_2}$.

For the case that $T_n(X) \not\equiv X \bmod p$, $G(X) \equiv X \bmod p$. By the same argument as the above, the period of sequence $X, G(X) \bmod p^k, \cdots$ is derived as $\ell \cdot p^{k-w_2}$. Thus, we obtain $N = s \cdot \ell \cdot p^{k-w_2}$ for $k \geq w_2$. □

Using Theorem 2, forming a sequence as $X, T_n(X) \bmod p^k, \cdots T^{N-1}_n(X) \bmod p^k$ is not needed to investigate the period. We just try to find the value of w_2 from $w_2 = 1$ to k and the order of derivatives $T'_n(X)$ or $G'(X)$ modulo p. After finding w_2, the period of sequence $\{T^i_n(X) \bmod p^k\}_{i=0}^{N-1}$ is derived for any $k \geq w_2$.

Example 2 *When $p = 5$, $n = 7$ and $X = 2$, we obtain $w = 1$. Since $T'_7(2) \equiv 2 \bmod 5$ and $2^4 \equiv 1 \bmod 5$, $\ell = 4$. Since $T^4_n(2) \equiv 2 \bmod 5^3$ and $T^4_n(2) \not\equiv 2 \bmod 5^4$, the period N is derived as $N = 4 \cdot 5^{k-3}$ for $k \geq 3$.*

Example 3 *When $p = 7$, $n = 5$, and $X = 2$, $T_n(X) \not\equiv X \bmod p$. Define $G = T_{n^2}$, then $G(2) \equiv 2 \bmod 7$ and $G(2) \not\equiv 2 \bmod 7^2$ and $G'(2) \equiv 4 \bmod 7$. Since $4^3 \bmod 7 = 1$, $\ell = 3$ and $G^3(2) \equiv 2 \bmod 7^2$ and $G^3(2) \equiv 2 \not\equiv 7^3$, Therefore, the period N of sequence $\{T^i_n(2) \bmod 7^k\}_{i=0}^{N-1}$ is derived as $N = 2 \cdot 3 \cdot 7^{k-2}$ for $k \geq 2$.*

One can also see that the numerical results in Tables 1, 2, and 3 are consistent with our theoretical results.

3. Conclusion

In this paper, we showed that Chebyshev polynomials become permutation polynomials over the residue rings of integers of powers of odd prime. We also derive the periodic property of Chebyshev polynomial sequences over the ring under some conditions. The result is useful for finding the period of Chebyshev polynomial sequences.

The detailed analysis of the relation of the period, degree, and initial value of Chebyshev polynomials over powers of odd prime is much more complicated. This topic is challenging and needed further research.

References

[1] R. L. Rivest, "Permutation polynomials modulo 2^w," *Finite fields and their applications,* pp.287–292, 2001.

[2] K. Umeno, "Key exchange by Chebyshev polynomials modulo 2^w," *Proc. of INA-CISC*, pp.95–97, 2005.

[3] L. Kocarev and Z. Tasev, "Public-key encryption based on Chebyshev maps," *Proc. of 2003 IEEE int'l Symp. Circuits and Systems*, vol.3, pp.28–31, 2003.

[4] P. Bergamo, P. D'Arco, A. De Santis and L. Kocarev, "Security of public-key cryptosystems based on Chebyshev polynomials," *IEEE Trans. Circuits and systems-I*, vol.52, no.7, pp.1382–1393, 2005.

[5] L. Kocarev, J. Makraduli and P. Amato, "Public-key encryption based on Chebyshev polynomials," *Circuits Systems and Signal Processing*, vol.24, no.5, pp.497–517, 2005.

[6] M. Ishii, "Periodicity of Chebyshev polynomials over the residue ring of $\mathbb{Z}/2^r\mathbb{Z}$ and an electronic signature," *Trans. of The Japan Society for Industrial and Applied Mathematics*, vol.18, no.2, pp.257–265, 2008. (in Japanese)

[7] M. Ishii, "Applications for cryptography of the structure of the group of reduced residue classes of residue ring of $\mathbb{Z}/2^w\mathbb{Z}$," *Trans. of The Japan Society for Industrial and Applied Mathematics*, vol.19, no.1, pp.57–71, 2009. (in Japanese)

[8] X. Liao, F. Chen and K. Wong, "On the security of public-key algorithms based on Chebyshev polynomials over the finite field Z_N,"*IEEE Trans. Computers*, vol.59, no.10, pp.1392–1401, 2010.

[9] D. Yoshioka and Y. Dainobu, "On some properties of Chebyshev polynomial sequences modulo 2^k," *Nonlinear Theory and Its Applications, IEICE*, vol.6, no.3, pp.443–452, 2015.

[10] D. Yoshioka and K. Kawano,"Periodic properties of Chebyshev polynomial sequences over the residue ring $\mathbb{Z}/2^k\mathbb{Z}$," *IEEE Trans. Circuits and Systems II*, 2016. (in press)

[11] P. S. Bremser, "Value sets of Dickson polynomials over Galois Ring," *Journal of Number Theory,* vol.38, pp.240–250, 1991.

[12] R. Lidl and H. Niederreiter, *Finite Fields,* Addison-Wesley, 1983.