BAB III
POLINOMIAL PERMUTASI

Pada bab ini akan dibahas mengenai ciri-ciri dari polinomial permutasi di *ring* $\mathbb{Z}_n$ serta ciri-ciri dari polinomial Chebyshev yang merupakan polinomial permutasi di *ring* $\mathbb{Z}_n$, dimana nilai $n = 2^w$, $w \geq 1$.

3.1 Polinomial Permutasi di *Ring* $\mathbb{Z}_n$

Sebelum pembahasan lebih lanjut mengenai ciri-ciri dari polinomial permutasi di *ring* $\mathbb{Z}_n$, terlebih dahulu akan diberikan suatu definisi mengenai polinomial permutasi.

Definisi 3.1.1

Suatu polinomial $P(x) = a_0 + a_1 x + ... + a_d x^d$, untuk suatu bilangan bulat tertentu *d*, disebut **polinomial permutasi** di *ring* hingga R jika pemetaan $P : R \to R$ bersifat satu-satu.

(Ronald L. Rivest, 1999)

Definisi 3.1.2

Suatu polinomial disebut **polinomial integral** jika koefisien-koefisiennya berupa bilangan bulat.

(Ronald L. Rivest, 1999)

Dengan asumsi bahwa polinomial yang dibahas seterusnya merupakan polinomial integral, maka dimungkinkan pembicaraan tentang suatu polinomial pada $\mathbb{Z}_n$ dengan nilai *n* yang berbeda. Sebagai contoh $P(x) = 3x^2$ merupakan polinomial permutasi di $\mathbb{Z}_2$, karena

$P([0]_2) = 3([0]_2)^2 = [0]_2$, dan

$P([1]_2) = 3([1]_2)^2 = [1]_2$.

Tetapi $P(x) = 3x^2$ bukan merupakan polinomial permutasi di $\mathbb{Z}_4$, karena

$P([0]_4) = 3([0]_4)^2 = [0]_4$, dan

$P([2]_4) = 3([2]_4)^2 = [0]_4$.

Berikut ini akan dibahas ciri-ciri dari polinomial permutasi di $\mathbb{Z}_n$ dengan $n = 2^w$. Pembahasan untuk nilai *w* yang berbeda ini dibagi menjadi dua bagian yaitu untuk $w = 1$ dan $w > 1$.

a. Untuk $w = 1$ atau $n = 2$

Ciri dari polinomial permutasi di $\mathbb{Z}_2$ ditunjukkan oleh lemma berikut.

Lemma 3.1.3

Polinomial integral $P(x) = a_0 + a_1x + ... + a_dx^d$ adalah polinomial permutasi di $\mathbb{Z}_2$ jika dan hanya jika $(a_1 + a_2 + ... + a_d)$ adalah bilangan ganjil.

Bukti :

($\Rightarrow$) Diketahui $P(x)$ adalah polinomial permutasi di $\mathbb{Z}_2$, maka berdasarkan Definisi 3.1.1 pemetaan $P:\mathbb{Z}_2 \to \mathbb{Z}_2$ bersifat satu-satu. Terdapat dua kemungkinan pemetaan $P:\mathbb{Z}_2 \to \mathbb{Z}_2$, yaitu :

1. $P\left([0]_2\right) = [0]_2$ dan $P\left([1]_2\right) = [1]_2$.
2. $P\left([0]_2\right) = [1]_2$ dan $P\left([1]_2\right) = [0]_2$.

- Kemungkinan pertama : $P\left([0]_2\right) = [0]_2$ dan $P\left([1]_2\right) = [1]_2$.

$$P\left([0]_2\right) = a_0 + a_1[0]_2 + a_2\left([0]_2\right)^2 + \ldots + a_d\left([0]_2\right)^d$$

$$[0]_2 = a_0 + (a_1 + a_2 + \ldots + a_d)[0]_2$$

$$[0]_2 = a_0 + [0]_2 . \qquad (3.1)$$

Persamaan (3.1) hanya terpenuhi ketika a_0 bilangan genap. Untuk $(a_1 + a_2 + \ldots + a_d)$ bilangan ganjil ataupun bilangan genap persamaan tersebut selalu terpenuhi. Tetapi $P\left([1]_2\right) = [1]_2$ juga harus terpenuhi. Pandang,

$$P[1]_2 = a_0 + a_1[1]_2 + a_2\left([1]_2\right)^2 + \ldots + a_d\left([1]_2\right)^d$$

$$[1]_2 = a_0 + (a_1 + a_2 + \ldots + a_d)[1]_2 . \qquad (3.2)$$

Untuk a_0 bilangan genap, persamaan (3.2) hanya akan terpenuhi ketika $(a_1 + a_2 + \ldots + a_d)$ bilangan ganjil.

- Kemungkinan kedua : $P\left([0]_2\right) = [1]_2$ dan $P\left([1]_2\right) = [0]_2$.

$$P\left([0]_2\right) = a_0 + a_1[0]_2 + a_2\left([0]_2\right)^2 + \ldots + a_d\left([0]_2\right)^d$$

$$[1]_2 \quad = a_0 + (a_1 + a_2 + \ldots + a_d)[0]_2$$

$$[1]_2 \quad = a_0 + [0]_2 . \qquad (3.3)$$

Persamaan (3.3) hanya terpenuhi ketika a_0 bilangan ganjil tanpa memperhatikan $(a_1 + a_2 + \ldots + a_d)$ bilangan ganjil atau bilangan genap. Akan tetapi karena pemetaan *P* bersifat satu-satu, maka $P\left([1]_2\right) = [0]_2$ juga harus terpenuhi.

Pandang,

$$P\left([1]_2\right) = a_0 + a_1[1]_2 + a_2\left([1]_2\right)^2 + \ldots + a_d\left([1]_2\right)^d$$

$$[0]_2 \quad = a_0 + (a_1 + a_2 + \ldots + a_d)[1]_2 . \qquad (3.4)$$

Untuk a_0 bilangan ganjil, persamaan (3.4) hanya akan terpenuhi ketika $(a_1 + a_2 + \ldots + a_d)$ bilangan ganjil.

Dengan demikian dari kedua kemungkinan tersebut terbukti jika $P(x)$ adalah polinomial permutasi di $\mathbb{Z}_2$ maka $(a_1 + a_2 + \ldots + a_d)$ bilangan ganjil.

($\Leftarrow$) Diketahui $(a_1 + a_2 + \ldots + a_d)$ adalah bilangan ganjil, maka akan ditunjukkan $P(x)$ adalah polinomial permutasi di $\mathbb{Z}_2$.

Untuk menunjukkan $P(x)$ adalah polinomial permutasi di $\mathbb{Z}_2$, perlu diperhatikan pemetaan $P:\mathbb{Z}_2 \to \mathbb{Z}_2$ dengan

$$P\left([0]_2\right) = a_0 + (a_1 + ... + a_d)[0]_2,$$

dan

$$P\left([1]_2\right) = a_0 + (a_1 + ... + a_d)[1]_2 .$$

Untuk kondisi a_0 sembarang, akan ditunjukkan pemetaan P bersifat satu-satu.

Jika a_0 bilangan genap, maka $P\left([0]_2\right) = [0]_2$ dan $P\left([1]_2\right) = [1]_2$.

Tetapi untuk a_0 bilangan ganjil, maka $P\left([0]_2\right) = [1]_2$ dan $P\left([1]_2\right) = [0]_2$.

Jadi apapun kondisi dari a_0 baik bilangan genap maupun bilangan ganjil, maka pemetaan dari P tetap bersifat satu-satu, atau $P(x)$ adalah polinomial permutasi di $\mathbb{Z}_2$.

Dengan demikian Lemma 3.1.3 terbukti. ■

Jadi dapat disimpulkan bahwa ciri-ciri dari polinomial permutasi di $\mathbb{Z}_2$ adalah penjumlahan semua koefisien kecuali a_0 merupakan bilangan ganjil.

Pembahasan selanjutnya adalah untuk nilai $w > 1$.

b. Untuk $n = 2^w$, $w > 1$

Pembahasan ciri-ciri polinomial permutasi di $\mathbb{Z}_n$ untuk nilai $w > 1$ tidak sesederhana pembahasan polinomial permutasi di $\mathbb{Z}_2$.

Lemma berikut memberikan suatu kondisi untuk koefisien a_1 jika polinomial $P(x) = a_0 + a_1x + a_2x^2 + ... + a_dx^d$ merupakan suatu polinomial permutasi di $\mathbb{Z}_n$.

Lemma 3.1.4

Misalkan $P(x) = a_0 + a_1x + a_2x^2 + ... + a_dx^d$ adalah polinomial integral, dan $n = 2m$ dengan m bilangan genap positif. Jika $P(x)$ adalah polinomial permutasi di $\mathbb{Z}_n$, maka a_1 bilangan ganjil.

Bukti :

Diketahui $P(x)$ adalah polinomial permutasi di $\mathbb{Z}_n$, maka akan ditunjukkan a_1 bilangan ganjil dengan cara kontradiksi.

Andaikan a_1 bilangan genap.

Pandang,

$$\begin{aligned} P\left([0]_n\right) &= a_0 + a_1[0]_n + a_2\left([0]_n\right)^2 + ... + a_d\left([0]_n\right)^d \\ &= a_0 + (a_1 + ... + a_d)[0]_n \\ &= a_0 + [0]_n . \end{aligned} \tag{3.5}$$

Kemudian pandang,

$$P\left([m]_n\right) = a_0 + a_1[m]_n + a_2\left([m]_n\right)^2 + \ldots + a_d\left([m]_n\right)^d .$$

Menurut Sifat 2.8 karena $m = \frac{n}{2}$, n bilangan genap, dan a_1 bilangan genap, maka $a_1[m]_n = [0]_n$.

Menurut Sifat 2.7 $\left([m]_n\right)^2 = \left[m^2\right]_n$, dan $\left[m^2\right]_n = [0]_n$ karena n habis membagi m^2, sehingga $\left([m]_n\right)^2 = [0]_n$.

Begitu juga untuk $\left([m]_n\right)^j$, $j > 2$. Karena $\left([m]_n\right)^j$ dapat ditulis sebagai

$$\left([m]_n\right)^j = \left([m]_n\right)^2 \left([m]_n\right)^{j-2},$$

maka

$$\begin{aligned}\left([m]_n\right)^j &= [0]_n \left([m]_n\right)^{j-2} \\ &= [0]_n .\end{aligned}$$

Sehingga,

$$\begin{aligned}P\left([m]_n\right) &= a_0 + a_1[m]_n + a_2\left([m]_n\right)^2 + \ldots + a_d\left([m]_n\right)^d \\ &= a_0 + [0]_n . \qquad (3.6)\end{aligned}$$

Dari persamaan (3.5) dan (3.6) diperoleh $P\left([0]_n\right) = P\left([m]_n\right)$ dengan $[0]_n \neq [m]_n$. Ternyata pemetaan P tidak bersifat satu-satu, atau dengan perkataan lain $P(x)$ bukan polinomial permutasi di $\mathbb{Z}_n$. Hal tersebut kontradiksi dengan yang diketahui bahwa $P(x)$ adalah polinomial permutasi

di $\mathbb{Z}_n$. Jadi pengandaian a_1 bilangan genap adalah salah dan a_1 haruslah bilangan ganjil.

Jadi, Lemma 3.1.4 telah terbukti. ■

Lemma 3.1.4 menunjukkan salah satu ciri dari polinomial permutasi di $\mathbb{Z}_n$, $n = 2^w$, $w > 1$, yaitu jika $P(x) = a_0 + a_1x + a_2x^2 + ... + a_dx^d$ adalah polinomial permutasi di $\mathbb{Z}_n$, maka a_1 bilangan ganjil.

Untuk menunjukkan ciri-ciri lain dari polinomial permutasi di $\mathbb{Z}_n$, diperlukan beberapa lemma berikut ini.

Lemma 3.1.5

Misalkan $P(x) = a_0 + a_1x + a_2x^2 + ... + a_dx^d$ adalah polinomial integral serta $n = 2^w$ dengan $w > 1$ dan $m = 2^{w-1} = \frac{n}{2}$. Jika $P(x)$ adalah polinomial permutasi di $\mathbb{Z}_n$ maka $P(x)$ adalah polinomial permutasi di $\mathbb{Z}_m$.

Bukti :

Diketahui $P(x)$ adalah polinomial permutasi di $\mathbb{Z}_n$, maka akan ditunjukkan $P(x)$ adalah polinomial permutasi di $\mathbb{Z}_m$ dengan cara kontradiksi.

Andaikan $P(x)$ bukan polinomial permutasi di $\mathbb{Z}_m$. Maka terdapat dua nilai berbeda di $\mathbb{Z}_m$, yaitu $[x]_m$ dan $[x']_m$ sedemikian sehingga

$$P([x]_m) = P([x']_m) = [y]_m \text{ untuk suatu } [y]_m \text{ di } \mathbb{Z}_m.$$

Untuk sembarang *x*, berlaku

$$P\left([x+m]_m\right) = P\left([x]_m + [m]_m\right) = P\left([x]_m + [0]_m\right) = P\left([x]_m\right).$$

Maka akan terdapat 4 nilai di $\mathbb{Z}_n$ yang dipetakan oleh $P:\mathbb{Z}_m \to \mathbb{Z}_m$ ke $[y]_m$ yaitu $\{[x]_n, [x+m]_n, [x']_n, [x'+m]_n\}$.

Karena *P*(*x*) adalah polinomial permutasi di $\mathbb{Z}_n$, maka hanya mungkin ada dua nilai berbeda di $\mathbb{Z}_n$ yang dipetakan oleh $P:\mathbb{Z}_m \to \mathbb{Z}_m$ ke nilai yang sama, tetapi ternyata terdapat empat nilai berbeda di $\mathbb{Z}_n$ yang dipetakan oleh $P:\mathbb{Z}_m \to \mathbb{Z}_m$ ke $[y]_m$. Hal tersebut kontradiksi dengan yang diketahui bahwa *P*(*x*) adalah polinomial permutasi di $\mathbb{Z}_n$. Jadi pengandaian bahwa *P*(*x*) bukan polinomial permutasi di $\mathbb{Z}_m$ adalah salah, seharusnya *P*(*x*) adalah polinomial permutasi di $\mathbb{Z}_m$.

Dengan demikian Lemma 3.1.5 terbukti. ■

Lemma 3.1.5 dapat diilustrasikan seperti contoh berikut ini. Jika suatu polinomial di $\mathbb{Z}_{64}$ merupakan polinomial permutasi maka polinomial tersebut juga merupakan polinomial permutasi di $\mathbb{Z}_{32}$. Jika polinomial tersebut merupakan polinomial permutasi di $\mathbb{Z}_{32}$, maka juga merupakan polinomial permutasi di $\mathbb{Z}_{16}$. Begitu seterusnya hingga polinomial tersebut juga merupakan polinomial permutasi di $\mathbb{Z}_2$.

Berikut ini akan ditunjukkan akibat dari Lemma 3.1.5.

Lemma 3.1.6

Misalkan $P(x) = a_0 + a_1x + a_2x^2 + ... + a_dx^d$ adalah polinomial integral serta $n = 2m$, m bilangan genap positif. Jika $P(x)$ adalah polinomial permutasi di $\mathbb{Z}_n$, maka $P\left([x+m]_n\right) = P\left([x]_n\right) + [m]_n$ untuk setiap $[x]_n$.

Bukti :

Diketahui $P(x)$ adalah polinomial permutasi di $\mathbb{Z}_n$, maka berdasarkan Lemma 3.1.5, $P(x)$ juga merupakan polinomial permutasi di $\mathbb{Z}_m$.

Untuk dua nilai berbeda di $\mathbb{Z}_n$, yaitu $[x]_n$ dan $[x+m]_n$, akan menjadi dua nilai yang sama di $\mathbb{Z}_m$.

Sehingga

$$P\left([x+m]_m\right) = P\left([x]_m\right),$$

sedangkan

$$P\left([x+m]_n\right) = P\left([x]_n\right) + [m]_n$$

untuk setiap $[x]_n$, karena $P(x)$ adalah polinomial permutasi di $\mathbb{Z}_n$ dan

$P\left([x]_m\right) + [m]_n = P\left([x]_m\right)$ di $\mathbb{Z}_m$.

Lemma 3.1.6 telah terbukti. ■

Lemma 3.1.7

Misalkan $P(x) = a_0 + a_1x + a_2x^2 + ... + a_dx^d$ adalah polinomial integral, dan $n = 2m$, dengan *m* bilangan genap positif. Untuk $P(x)$ polinomial permutasi di $\mathbb{Z}_m$, maka $P(x)$ adalah polinomial permutasi di $\mathbb{Z}_n$ jika dan hanya jika $(a_3 + a_5 + a_7 + ...)$ adalah bilangan genap.

Bukti :

Diketahui $P(x)$ adalah polinomial permutasi di $\mathbb{Z}_m$, akan ditunjukkan $P(x)$ adalah polinomial permutasi di $\mathbb{Z}_n$ jika dan hanya jika $(a_3 + a_5 + a_7 + ...)$ adalah bilangan genap.

$(\Rightarrow)$ Diketahui $P(x)$ adalah polinomial permutasi di $\mathbb{Z}_n$, maka akan ditunjukkan $(a_3 + a_5 + a_7 + ...)$ adalah bilangan genap.

$P(x)$ adalah polinomial permutasi di $\mathbb{Z}_n$, $n = 2m$, maka dari Lemma 3.1.4 dengan *m* bilangan genap maka a_1 bilangan ganjil.

Pandang

$$P\left([x]_n\right) = a_0 + a_1[x]_n + a_2\left([x]_n\right)^2 + ... + a_d\left([x]_n\right)^d,$$

dan

$$P\left([x+m]_n\right) = a_0 + a_1[x+m]_n + a_2\left([x+m]_n\right)^2 + ... + a_d\left([x+m]_n\right)^d.$$

Akan dilihat nilai dari $a_i\left([x+m]_n\right)^i$, $i \geq 1$, namun sebelumnya akan dibuktikan dengan induksi matematik terhadap *i* bahwa

$$\left([x+m]_n\right)^i = \left([x]_n\right)^i + [im]_n \left([x]_n\right)^{i-1} \text{ untuk } i \geq 1. \quad (3.7)$$

Dimulai dari tahap awal, yaitu untuk i =1,

$$\begin{aligned}[x+m]_n &= [x]_n + [m]_n \left([x]_n\right)^0 \\ &= [x]_n + [m]_n \\ &= [x+m]_n .\end{aligned}$$

Jadi untuk $i = 1$ persamaan (3.7) terpenuhi.

Asumsikan persamaan (3.7) terpenuhi untuk $i = k$, yaitu

$$\left([x+m]_n\right)^k = \left([x]_n\right)^k + [km]_n \left([x]_n\right)^{k-1}.$$

Maka akan ditunjukkan persamaan (3.7) terpenuhi untuk $i = k+1$.

$$\begin{aligned}\left([x+m]_n\right)^{k+1} &= \left([x+m]_n\right)^k [x+m]_n \\ &= \left(\left([x]_n\right)^k + [km]_n \left([x]_n\right)^{k-1}\right)\left([x]_n + [m]_n\right) \\ &= \left([x]_n\right)^{k+1} + [m]_n \left([x]_n\right)^k + [km]_n \left([x]_n\right)^k \\ &\quad + \left[km^2\right]_n \left([x]_n\right)^{k-1} \\ &= \left([x]_n\right)^{k+1} + [k+1]_n [m]_n \left([x]_n\right)^k + [0]_n \\ &= \left([x]_n\right)^{k+1} + \left[(k+1)m\right]_n \left([x]_n\right)^k .\end{aligned}$$

Maka untuk $i = k+1$ persamaan (3.7) juga terpenuhi.

Sehingga terbukti $\left([x+m]_n\right)^i = \left([x]_n\right)^i + [im]_n \left([x]_n\right)^{i-1}$ untuk $i \geq 1$.

Kemudian akan dilihat nilai dari $a_i\left(\left[x+m\right]_n\right)^i$ untuk setiap *i*, dengan membagi menjadi beberapa kasus.

- $i=1$

$$a_1\left[x+m\right]_n = a_1\left(\left[x\right]_n+\left[m\right]_n\right)$$

$$= a_1\left[x\right]_n + a_1\left[m\right]_n$$

karena a_1 bilangan ganjil dan $m=\frac{n}{2}$, maka berdasarkan Sifat 2.8

$$a_1\left[x+m\right]_n = a_1\left[x\right]_n+\left[m\right]_n .$$

- *i* genap, $i=2k$, *k* bilangan bulat positif

$$a_i\left(\left[x+m\right]_n\right)^i = a_i\left(\left(\left[x\right]_n\right)^i+\left[im\right]_n\left(\left[x\right]_n\right)^{i-1}\right)$$

$$= a_i\left(\left[x\right]_n\right)^i + a_i\left[im\right]_n\left(\left[x\right]_n\right)^{i-1}$$

$$= a_i\left(\left[x\right]_n\right)^i + \left[0\right]_n\left(\left[x\right]_n\right)^{i-1}$$

$$= a_i\left(\left[x\right]_n\right)^i .$$

- *i* ganjil, $i=2k+1$, *k* bilangan bulat positif

$$a_i\left(\left[x+m\right]_n\right)^i = a_i\left(\left(\left[x\right]_n\right)^i+\left[im\right]_n\left(\left[x\right]_n\right)^{i-1}\right)$$

$$= a_i\left(\left[x\right]_n\right)^i + a_i\left[im\right]_n\left(\left[x\right]_n\right)^{i-1}$$

$$= a_i\left(\left[x\right]_n\right)^i + a_i\left[(2k+1)m\right]_n\left(\left[x\right]_n\right)^{i-1}$$

$$= a_i\left(\left[x\right]_n\right)^i + a_i\left[(2k)m\right]_n\left(\left[x\right]_n\right)^{i-1} + a_i\left[m\right]_n\left(\left[x\right]_n\right)^{i-1}$$

$$= a_i \left([x]_n \right)^i + [0]_n \left([x]_n \right)^{i-1} + a_i [m]_n \left([x]_n \right)^{i-1}$$

$$= a_i \left([x]_n \right)^i + a_i [m]_n \left([x]_n \right)^{i-1}.$$

Jika a_i bilangan ganjil dan *x* bilangan genap, maka

$$a_i \left([x+m]_n \right)^i = a_i \left([x]_n \right)^i + [0]_n = a_i \left([x]_n \right)^i.$$

Jika a_i bilangan ganjil dan *x* bilangan ganjil, maka

$$a_i \left([x+m]_n \right)^i = a_i \left([x]_n \right)^i + [m]_n.$$

Sehingga dari beberapa kasus di atas, dapat disimpulkan :

- Jika a_i bilangan ganjil dan salah satu berlaku, yaitu $i = 1$ atau $i > 1$ dan *x*, *i* bilangan ganjil, maka $a_i \left([x+m]_n \right)^i = a_i \left([x]_n \right)^i + [m]_n$.
- Selain itu berlaku $a_i \left([x+m]_n \right)^i = a_i \left([x]_n \right)^i$.

Dengan demikian untuk sembarang $[x]_n$ dan $[x+m]_n$ di $\mathbb{Z}_n$ dengan $[x]_n \neq [x+m]_n$ diperoleh :

Untuk *x* bilangan genap dan a_1 bilangan ganjil,

$$P\left([x+m]_n \right) = a_0 + a_1 [x+m]_n + a_2 \left([x+m]_n \right)^2 + \ldots + a_d \left([x+m]_n \right)^d$$

$$= a_0 + a_1 [x]_n + [m]_n + a_2 \left([x]_n \right)^2 + a_3 \left([x]_n \right)^3 + a_4 \left([x]_n \right)^4$$

$$+ \ldots + a_d \left([x]_n \right)^d$$

$$= P\left([x]_n\right) + [m]_n . \tag{3.8}$$

Persamaan (3.8) sesuai dengan Lemma 3.1.6.

Untuk *x* bilangan ganjil,

$$\begin{aligned} P\left([x+m]_n\right) &= a_0 + a_1[x+m]_n + a_2\left([x+m]_n\right)^2 + \ldots + a_d\left([x+m]_n\right)^d \\ &= a_0 + a_1[x]_n + a_1[m]_n + a_2\left([x]_n\right)^2 + a_3\left([x]_n\right)^3 + \\ &\quad a_3[m]_n\left([x]_n\right)^2 + a_4\left([x]_n\right)^4 + \ldots + a_d\left([x]_n\right)^d \\ &= \left(a_0 + a_1[x]_n + a_2\left([x]_n\right)^2 + a_3\left([x]_n\right)^3 + \ldots + a_d\left([x]_n\right)^d\right) \\ &\quad + \left(a_1[m]_n + a_3[m]_n + a_5[m]_n + \ldots\right) \\ &= P\left([x]_n\right) + \left(a_1 + a_3 + a_5 + a_7 + \ldots\right)[m]_n . \end{aligned} \tag{3.9}$$

Berdasarkan Lemma 3.1.6, persamaan (3.9) harus sama dengan

$$P\left([x+m]_n\right) = P\left([x]_n\right) + [m]_n . \tag{3.10}$$

Sehingga dari persamaan (3.9) dan (3.10) diperoleh

$$\left(a_1 + a_3 + a_5 + a_7 + \ldots\right)[m]_n = [m]_n . \tag{3.11}$$

Berdasarkan Sifat 2.8, persamaan (3.11) berlaku untuk $\left(a_1 + a_3 + a_5 + a_7 + \ldots\right)$ bilangan ganjil.

$\left(a_1 + a_3 + a_5 + a_7 + \ldots\right)$ bilangan ganjil dan a_1 bilangan ganjil, maka $\left(a_3 + a_5 + a_7 + \ldots\right)$ adalah bilangan genap.

Dengan demikian terbukti $(a_3 + a_5 + a_7 + ...)$ adalah bilangan genap.

($\Leftarrow$) Diketahui $(a_3 + a_5 + a_7 + ...)$ adalah bilangan genap, maka akan ditunjukkan $P(x)$ adalah polinomial permutasi di $\mathbb{Z}_n$.

Untuk *x* bilangan genap,

$$\begin{aligned} P\left([x+m]_n\right) &= a_0 + a_1[x+m]_n + a_2\left([x+m]_n\right)^2 + ... + a_d\left([x+m]_n\right)^d \\ &= a_0 + a_1[x]_n + a_1[m]_n + a_2\left([x]_n\right)^2 + ... + a_d\left([x]_n\right)^d \\ &= P\left([x]_n\right) + a_1[m]_n . \end{aligned} \tag{3.12}$$

Sedangkan untuk *x* bilangan ganjil,

$$\begin{aligned} P\left([x+m]_n\right) &= a_0 + a_1[x+m]_n + a_2\left([x+m]_n\right)^2 + ... + a_d\left([x+m]_n\right)^d \\ &= a_0 + a_1[x]_n + a_1[m]_n + a_2\left([x]_n\right)^2 + a_3\left([x]_n\right)^3 + \\ &\quad a_3[m]_n\left([x]_n\right)^2 + a_4\left([x]_n\right)^4 + ... + a_d\left([x]_n\right)^d \\ &= \left(a_0 + a_1[x]_n + a_2\left([x]_n\right)^2 + a_3\left([x]_n\right)^3 + ... + a_d\left([x]_n\right)^d\right) \\ &\quad + \left(a_1[m]_n + a_3[m]_n + a_5[m]_n + ...\right) \\ &= P\left([x]_n\right) + (a_1 + a_3 + a_5 + a_7 + ...)[m]_n . \end{aligned} \tag{3.13}$$

Dengan memperhatikan kondisi a_1 dan $(a_3 + a_5 + a_7 + ...)$, terdapat dua kemungkinan untuk nilai $P([x+m]_n)$, yaitu :

1. $P([x+m]_n) = P([x]_n)$
2. $P([x+m]_n) = P([x]_n) + [m]_n$.

Jika $P([x+m]_n) = P([x]_n)$ maka $P(x)$ bukan polinomial permutasi di $\mathbb{Z}_n$. Dengan demikian $P(x)$ dapat gagal menjadi polinomial permutasi di $\mathbb{Z}_n$ saat $P([x+m]_n) = P([x]_n)$.

Berdasarkan Lemma 3.1.4, jika $P(x)$ adalah polinomial permutasi di $\mathbb{Z}_n$, $n = 2m$, dengan m bilangan genap maka a_1 bilangan ganjil. Pernyataan tersebut ekivalen dengan jika a_1 bilangan genap maka $P(x)$ bukan polinomial permutasi di $\mathbb{Z}_n$. Maka dalam pembuktian $P(x)$ adalah polinomial permutasi di $\mathbb{Z}_n$ hanya digunakan untuk kondisi a_1 bilangan ganjil.

Sehingga untuk a_1 bilangan ganjil dan $(a_3 + a_5 + a_7 + ...)$ bilangan genap maka persamaan (3.12) menjadi

$$P([x+m]_n) = P([x]_n) + [m]_n .$$

Sedangkan persamaan (3.13) menjadi

$$P([x+m]_n) = P([x]_n) + [m]_n + [0]_n = P([x]_n) + [m]_n .$$

Dengan demikian $P\left(\left[x+m\right]_n\right)=P\left(\left[x\right]_n\right)$ tidak mungkin terjadi jika diketahui a_1 bilangan ganjil dan $\left(a_3+a_5+a_7+...\right)$ bilangan genap.

Jadi dapat disimpulkan bahwa $P(x)$ adalah polinomial permutasi di $\mathbb{Z}_n$. ■

Teorema berikut ini menjelaskan secara keseluruhan ciri-ciri dari suatu polinomial permutasi di $\mathbb{Z}_n$, $n=2^w$, $w>1$.

Teorema 3.1.8

Misalkan $P(x)=a_0+a_1x+a_2x^2+...+a_dx^d$ adalah polinomial integral. $P(x)$ adalah polinomial permutasi di $\mathbb{Z}_n$ dengan $n=2^w$, $w>1$, jika dan hanya jika a_1 bilangan ganjil, $\left(a_2+a_4+a_6+...\right)$ bilangan genap, dan $\left(a_3+a_5+a_7+...\right)$ bilangan genap.

Bukti :

$\left(\Rightarrow\right)$ Diketahui $P(x)$ adalah polinomial permutasi di $\mathbb{Z}_n$, maka berdasarkan Lemma 3.1.4, a_1 bilangan ganjil.

$P(x)$ adalah polinomial permutasi di $\mathbb{Z}_n$ maka berdasarkan Lemma 3.1.5, $P(x)$ adalah polinomial permutasi di $\mathbb{Z}_m$, $m=2^{w-1}=\frac{n}{2}$. Sehingga berdasarkan Lemma 3.1.7, $\left(a_3+a_5+a_7+...\right)$ bilangan genap.

$P(x)$ adalah polinomial permutasi di $\mathbb{Z}_m$, $m = 2^{w-1} = \frac{n}{2}$, maka $P(x)$ juga merupakan polinomial permutasi di $\mathbb{Z}_2$. Sehingga berdasarkan Lemma 3.1.3, $(a_1 + a_2 + ... + a_d)$ adalah bilangan ganjil.

Sebelumnya diperoleh a_1 bilangan ganjil, $(a_3 + a_5 + a_7 + ...)$ bilangan genap, dan $(a_1 + a_2 + ... + a_d)$ adalah bilangan ganjil maka dari ketiga hal tersebut diperoleh $(a_2 + a_4 + a_6 + ...)$ bilangan genap.

Dengan demikian terbukti jika $P(x)$ adalah polinomial permutasi di $\mathbb{Z}_n$ maka a_1 bilangan ganjil, $(a_2 + a_4 + a_6 + ...)$ bilangan genap, dan $(a_3 + a_5 + a_7 + ...)$ bilangan genap.

$(\Leftarrow)$ Diketahui a_1 bilangan ganjil, $(a_3 + a_5 + a_7 + ...)$ bilangan genap, dan $(a_2 + a_4 + a_6 + ...)$ bilangan genap, maka $(a_1 + a_2 + ... + a_d)$ merupakan bilangan ganjil. Jika $(a_1 + a_2 + ... + a_d)$ bilangan ganjil, maka berdasarkan Lemma 3.1.3, $P(x)$ adalah polinomial permutasi di $\mathbb{Z}_2$. Untuk $P(x)$ polinomial permutasi di $\mathbb{Z}_2$, jika $(a_3 + a_5 + a_7 + ...)$ bilangan genap maka berdasarkan Lemma 3.1.7, $P(x)$ adalah polinomial permutasi di $\mathbb{Z}_4$. Untuk $P(x)$ polinomial permutasi di $\mathbb{Z}_4$, jika $(a_3 + a_5 + a_7 + ...)$ bilangan genap maka berdasarkan Lemma 3.1.7, $P(x)$ juga merupakan polinomial permutasi di

$\mathbb{Z}_8$, begitu seterusnya. Sehingga dapat disimpulkan $P(x)$ adalah polinomial permutasi di $\mathbb{Z}_n$, $n = 2^w$, $w > 1$.

Jadi terbukti jika diketahui a_1 bilangan ganjil, $(a_3 + a_5 + a_7 + ...)$ bilangan genap, dan $(a_2 + a_4 + a_6 + ...)$ bilangan genap, maka $P(x)$ adalah polinomial permutasi di $\mathbb{Z}_n$, dengan $n = 2^w$, $w > 1$.

Dengan demikian Teorema 3.1.8 telah terbukti. ■

Berdasarkan pembahasan di atas terlihat ciri-ciri untuk suatu polinomial $P(x) = a_0 + a_1x + a_2x^2 + ... + a_dx^d$ agar merupakan polinomial permutasi di *ring* $\mathbb{Z}_n$ yang hanya dilihat berdasarkan koefisien $a_1, a_2, a_3, ..., a_d$, dan tidak memperhatikan nilai dari koefisien a_0.

Polinomial $x(a + bx)$ dengan a bilangan ganjil dan b bilangan genap merupakan salah satu contoh polinomial permutasi di $\mathbb{Z}_n$, $n = 2^w$, $w \geq 1$. Contoh lain adalah $x + x^2 + x^4$. Sedangkan polinomial $x^2 + 1$ merupakan salah satu contoh polinomial permutasi hanya di $\mathbb{Z}_2$, bukan merupakan polinomial permutasi di $\mathbb{Z}_n$, $n = 2^w$, $w > 1$.

3.2 Polinomial Chebyshev

Polinomial Chebyshev pertama kali diperkenalkan pada tahun 1853 oleh P.L. Chebyshev. Dalam buku J.C. Mason dan D.C. Handscomb dijelaskan bahwa terdapat empat jenis polinomial Chebyshev. Akan tetapi pada subbab ini hanya dibahas polinomial Chebyshev jenis pertama yang diberikan dalam definisi berikut.

Definisi 3.2.1

Polinomial Chebyshev jenis pertama $T_p(x)$ adalah polinomial dalam x berderajat p, yang memenuhi :

$$T_p(x) = \cos p\theta \text{ dengan } x = \cos\theta, \tag{3.14}$$

untuk $x \in [-1, 1]$.

(J.C. Mason dan D.C. Handscomb, 2003, halaman 14)

Definisi 3.2.2

Untuk $x \in [1, \infty)$, polinomial Chebyshev jenis pertama $T_p(x)$ adalah polinomial dalam x berderajat p, yang memenuhi :

$$T_p(x) = \cosh p\Theta \text{ dengan } x = \cosh\Theta. \tag{3.15}$$

(J.C. Mason dan D.C. Handscomb, 2003, halaman 23-24)

Persamaan (3.14) dapat diuraikan sebagai berikut :

$$T_0(x) = 1,$$

$$T_1(x) = \cos\theta,$$

$$T_2(x) = \cos 2\theta,$$

$$T_3(x) = \cos 3\theta, \text{ dan seterusnya.} \qquad (3.16)$$

Persamaan (3.16) dapat diubah menjadi suatu polinomial dalam x, dengan mengubah bentuk $\cos p\theta$.

$\cos p\theta$ dapat dijabarkan sebagai berikut :

$$\cos(p\theta) = \sum_{k=0}^{\lfloor p/2 \rfloor} \binom{p}{2k} (\cos\theta)^{p-2k} \left((\cos\theta)^2 - 1\right)^k. \qquad (3.17)$$

(*De Moivre's Formula*, n.d)

Dari persamaan (3.17), diperoleh $\cos p\theta$ adalah suatu polinomial dalam $\cos\theta$ berderajat p, yaitu

$$\cos 0\theta = 1,$$

$$\cos 1\theta = \cos\theta,$$

$$\cos 2\theta = (\cos\theta)^2 + \left((\cos\theta)^2 - 1\right) = 2\cos^2\theta - 1,$$

$$\cos 3\theta = (\cos\theta)^3 + 3\cos\theta\left((\cos\theta)^2 - 1\right) = 4\cos^3\theta - 3\cos\theta,$$

dan seterusnya. (3.18)

Sehingga dari persamaan (3.18) dan (3.14), persamaan (3.16) dapat ditulis sebagai :

$$T_0(x) = 1,$$

$$T_1(x) = x,$$

$$T_2(x) = 2x^2 - 1,$$

$$T_3(x) = 4x^3 - 3x, \text{ dan seterusnya.}$$

Dengan substitusi persamaan (3.17) ke persamaan (3.14), polinomial Chebyshev untuk $x \in [-1, 1]$ juga dapat dinyatakan dalam penjumlahan sebagai berikut :

$$T_p(x) = \sum_{s=0}^{\lfloor p/2 \rfloor} (-1)^s \binom{p}{2s} (1-x^2)^s x^{p-2s}, \tag{3.19}$$

Analog dengan polinomial Chebyshev untuk $x \in [-1, 1]$, pembahasan untuk $x \in [1, \infty)$ adalah dengan memandang persamaan (3.15) yang dapat diuraikan sebagai berikut :

$$T_0(x) = 1,$$

$$T_1(x) = \cosh\Theta,$$

$$T_2(x) = \cosh 2\Theta,$$

$$T_3(x) = \cosh 3\Theta, \text{ dan seterusnya.} \tag{3.20}$$

$\cosh p\Theta$ dapat dijabarkan sebagai berikut :

$$\cosh(p\Theta) = \sum_{k=0}^{\lfloor p/2 \rfloor} \binom{p}{2k} (\cosh\Theta)^{p-2k} (\sinh\Theta)^{2k} . \qquad (3.21)$$

(I.S. Gradshteyn & I.M. Ryzhik, 2000, halaman 33)

Karena $(\sinh\Theta)^2 = (\cosh\Theta)^2 - 1$, maka persamaan (3.21) dapat juga dinyatakan sebagai :

$$\cosh(p\Theta) = \sum_{k=0}^{\lfloor p/2 \rfloor} \binom{p}{2k} (\cosh\Theta)^{p-2k} \left((\cosh\Theta)^2 - 1\right)^k . \qquad (3.22)$$

Jika persamaan (3.22) disubstitusi ke persamaan (3.15), maka diperoleh bahwa polinomial Chebyshev untuk $x \in [1, \infty)$ dapat juga dinyatakan dalam penjumlahan sebagai berikut :

$$T_p(x) = \sum_{k=0}^{\lfloor p/2 \rfloor} \binom{p}{2k} x^{p-2k} \left(x^2 - 1\right)^k , \text{ atau}$$

$$T_p(x) = \sum_{k=0}^{\lfloor p/2 \rfloor} (-1)^k \binom{p}{2k} (1-x^2)^k x^{p-2k} . \qquad (3.23)$$

Dengan demikian diperoleh bentuk penjumlahan pada persamaan (3.23) sama seperti bentuk penjumlahan pada persamaan (3.19).

Sehingga untuk sembarang $x \geq 0$, polinomial Chebyshev dapat dinyatakan sebagai :

$$T_p(x) = \sum_{s=0}^{\lfloor p/2 \rfloor} (-1)^s \binom{p}{2s} (1-x^2)^s x^{p-2s} .$$

Kemudian akan diperlihatkan bentuk relasi rekursif dari polinomial Chebyshev untuk $x \in [-1, 1]$ yang berasal dari fungsi trigonometri berikut :

$$\cos p\theta + \cos(p-2)\theta = 2\cos\theta\cos(p-1)\theta. \qquad (3.24)$$

Persamaan (3.24) disubstitusikan ke persamaan (3.14) sehingga diperoleh bentuk relasi rekursif dari polinomial Chebyshev untuk $x \in [-1, 1]$, yaitu :

$$T_p(x) = 2xT_{p-1}(x) - T_{p-2}(x), \qquad p = 2, 3, 4, \ldots$$

dengan nilai awal $T_0(x) = 1$ dan $T_1(x) = x$.

Begitu juga bentuk relasi rekursif dari polinomial Chebyshev untuk $x \in [1, \infty)$, berdasarkan pada fungsi hiperbolik :

$$\cosh p\Theta + \cosh(p-2)\Theta = 2\cosh\Theta\cosh(p-1)\Theta. \qquad (3.25)$$

Jika persamaan (3.25) disubstitusi ke persamaan (3.15) maka akan diperoleh bentuk relasi rekursif sebagai berikut :

$$T_p(x) = 2xT_{p-1}(x) - T_{p-2}(x), \qquad p = 2, 3, 4, \ldots$$

dengan nilai awal $T_0(x) = 1$ dan $T_1(x) = x$.

Sehingga dapat disimpulkan bentuk relasi rekursif tersebut berlaku untuk sembarang $x \geq 0$.

Selanjutnya akan dibahas ciri-ciri dari polinomial Chebyshev yang merupakan polinomial permutasi di $\mathbb{Z}_n$, $n = 2^w$, $w \geq 1$. Pembahasan dibagi

menjadi dua, yaitu ciri-ciri polinomial Chebyshev yang merupakan polinomial permutasi di $\mathbb{Z}_2$ dan ciri-ciri polinomial Chebyshev yang merupakan polinomial permutasi di $\mathbb{Z}_n$, $n = 2^w$, $w > 1$.

Pembahasan untuk ciri-ciri polinomial Chebyshev yang merupakan polinomial permutasi di $\mathbb{Z}_2$, perlu memperhatikan bentuk penjumlahan dari polinomial Chebyshev, yaitu :

$$T_p(x) = \sum_{s=0}^{\lfloor p/2 \rfloor} (-1)^s \binom{p}{2s} (1-x^2)^s x^{p-2s} .$$

Jika p bilangan genap, atau $p = 2k$ untuk suatu bilangan bulat k, maka

$$T_{2k}(x) = \sum_{s=0}^{k} (-1)^s \binom{2k}{2s} (1-x^2)^s x^{2(k-s)}$$

$$= x^{2k} + \left\{ \sum_{s=1}^{k-1} (-1)^s \binom{2k}{2s} (1-x^2)^s x^{2(k-s)} \right\} + (-1)^k (1-x^2)^k .$$

Karena

$$T_{2k}\left([0]_2\right) = [0]_2 + [0]_2 + \left([-1]_2\right)^k = [1]_2 , \text{ dan}$$

$$T_{2k}\left([1]_2\right) = [1]_2 + [0]_2 + [0]_2 = [1]_2 ,$$

maka dapat disimpulkan bahwa polinomial Chebyshev berderajat genap bukan merupakan polinomial permutasi di $\mathbb{Z}_2$.

Sedangkan jika p bilangan ganjil, atau $p = 2k+1$ untuk suatu bilangan bulat k, maka

$$T_{2k+1}(x) = \sum_{s=0}^{k} (-1)^s \binom{2k+1}{2s} (1-x^2)^s x^{2(k-s)+1}$$

$$= x^{2k+1} + \sum_{s=1}^{k} (-1)^s \binom{2k+1}{2s} (1-x^2)^s x^{2(k-s)+1}.$$

Karena

$T_{2k+1}\left([0]_2\right) = [0]_2 + [0]_2 = [0]_2$, dan

$T_{2k+1}\left([1]_2\right) = [1]_2 + [0]_2 = [1]_2$,

maka dapat disimpulkan bahwa polinomial Chebyshev berderajat ganjil merupakan polinomial permutasi di $\mathbb{Z}_2$.

Kemudian akan dibahas ciri-ciri dari polinomial Chebyshev yang merupakan polinomial permutasi di $\mathbb{Z}_n$, $n = 2^w$, $w > 1$. Pembahasan dimulai dengan melihat polinomial Chebyshev derajat satu.

Lemma 3.2.3

Polinomial Chebyshev berderajat satu, $T_1(x) = x$, adalah polinomial permutasi di $\mathbb{Z}_n$.

Bukti :

Karena polinomial Chebyshev berderajat satu, $T_1(x) = x$, merupakan pemetaan satu-satu di $\mathbb{Z}_n$, maka $T_1(x) = x$ merupakan polinomial permutasi di $\mathbb{Z}_n$.

Dengan demikian Lemma 3.2.3 telah terbukti. ■

Selanjutnya akan dibahas polinomial Chebyshev berderajat genap.

Lemma 3.2.4

Polinomial Chebyshev berderajat genap bukan merupakan polinomial permutasi di $\mathbb{Z}_n$.

Bukti :

Diketahui polinomial Chebyshev berderajat genap, $T_p(x)$, p bilangan genap, maka akan ditunjukkan $T_p(x)$ bukan merupakan polinomial permutasi di $\mathbb{Z}_n$. Berdasarkan persamaan (3.19) dan (3.23), polinomial Chebyshev berderajat p, dapat dinyatakan sebagai berikut :

$$T_p(x) = \sum_{s=0}^{\lfloor p/2 \rfloor} (-1)^s \binom{p}{2s} (1-x^2)^s x^{p-2s} \quad ,$$

maka untuk p bilangan genap, $T_p(x)$ tidak memiliki suku polinomial yang berderajat ganjil.

Dengan demikian berdasarkan Teorema 3.1.8, $T_p(x)$ bukan merupakan polinomial permutasi di $\mathbb{Z}_n$.

Lemma 3.2.4 telah terbukti. ■

Jika polinomial Chebyshev berderajat genap ternyata bukan merupakan polinomial permutasi di $\mathbb{Z}_n$, maka pembahasan selanjutnya akan diperlihatkan untuk polinomial Chebyshev berderajat ganjil.

Lemma 3.2.5

Misalkan *p* bilangan ganjil dengan $p > 1$. Jika $T_p(x)$ merupakan polinomial permutasi di $\mathbb{Z}_n$, maka $T_{p+2}(x)$ juga merupakan polinomial permutasi di $\mathbb{Z}_n$.

Bukti :

Misalkan

$$T_p(x) = a_0 + a_1x + \ldots + a_px^p,$$

dan

$$T_{p+2}(x) = b_0 + b_1x + \ldots + b_{p+2}x^{p+2}.$$

Diketahui $T_p(x)$ memiliki bentuk relasi rekursif

$$T_{p+2}(x) = 2xT_{p+1}(x) - T_p(x),$$

atau dapat ditulis sebagai

$$2xT_{p+1}(x) = T_{p+2}(x) + T_p(x).$$

Dengan demikian,

$$T_{p+2}(x)+T_p(x)=\left(b_0+b_1x+...+b_{p+2}x^{p+2}\right)+\left(a_0+a_1x+...+a_px^p\right)$$

$$=\left(b_0+a_0\right)+\left(b_1+a_1\right)x+...+\left(b_p+a_p\right)x^p+b_{p+1}x^{p+1}.$$

Berarti,

$$2xT_{p+1}(x)=\left(b_0+a_0\right)+\left(b_1+a_1\right)x+...+\left(b_p+a_p\right)x^p+b_{p+1}x^{p+1}+b_{p+2}x^{p+2}. \quad (3.26)$$

Persamaan (3.26) memiliki koefisien-koefisien berupa bilangan genap.

Diketahui $T_p(x)$ merupakan polinomial permutasi di $\mathbb{Z}_n$ maka berdasarkan Teorema 3.1.8, a_1 bilangan ganjil, $\left(a_2+a_4+a_6+...+a_{p-1}\right)$ bilangan genap, dan $\left(a_3+a_5+a_7+...+a_p\right)$ bilangan genap.

Sehingga dapat disimpulkan sebagai berikut :

- $\left(b_1+a_1\right)$ merupakan bilangan genap dan a_1 bilangan ganjil, maka b_1 bilangan ganjil.
- $\left(\left(b_2+a_2\right)+\left(b_4+a_4\right)+...+\left(b_{p-1}+a_{p-1}\right)\right)$ bilangan genap dan $\left(a_2+a_4+...+a_{p-1}\right)$ bilangan genap maka $\left(b_2+b_4+...+b_{p-1}\right)$ bilangan genap.

- $\left(\left(b_3 + a_3\right) + \left(b_5 + a_5\right) + ... + \left(b_p + a_p\right)\right)$ bilangan genap dan $\left(a_3 + a_5 + ... + a_p\right)$ bilangan genap maka $\left(b_3 + b_5 + ... + b_p\right)$ bilangan genap.
- Karena $\left(b_2 + b_4 + ... + b_{p-1}\right)$ bilangan genap dan b_{p+1} bilangan genap maka $\left(b_2 + b_4 + ... + b_{p+1}\right)$ bilangan genap.
- Karena $\left(b_3 + b_5 + ... + b_p\right)$ bilangan genap dan b_{p+2} bilangan genap maka $\left(b_3 + b_5 + ... + b_{p+2}\right)$ bilangan genap.

Dengan demikian berdasarkan Teorema 3.1.8, karena b_1 bilangan ganjil, $\left(b_2 + b_4 + ... + b_{p+1}\right)$ bilangan genap, dan $\left(b_3 + b_5 + ... + b_{p+2}\right)$ bilangan genap, maka $T_{p+2}(x) = b_0 + b_1 x + ... + b_{p+2} x^{p+2}$ juga merupakan polinomial permutasi di $\mathbb{Z}_n$.

Jadi Lemma 3.2.5 telah terbukti. ■

Lemma 3.2.6

Jika p bilangan ganjil dengan $p \geq 1$, maka polinomial Chebyshev $T_p(x)$ adalah polinomial permutasi di $\mathbb{Z}_n$.

Bukti :

Diketahui polinomial Chebyshev berderajat ganjil, $T_p(x)$, p bilangan ganjil, maka akan ditunjukkan $T_p(x)$ adalah polinomial permutasi di $\mathbb{Z}_n$.

Untuk $p = 1$, berdasarkan Lemma 3.2.3, $T_1(x)$ adalah polinomial permutasi di $\mathbb{Z}_n$. Untuk $p > 1$, dimana p bilangan ganjil, berdasarkan Lemma 3.2.5 diperoleh $T_p(x)$ adalah polinomial permutasi di $\mathbb{Z}_n$.

Jadi Lemma 3.2.6 telah terbukti. ■

Teorema berikut menunjukkan bahwa polinomial Chebyshev berderajat ganjil merupakan polinomial permutasi di $\mathbb{Z}_n$.

Teorema 3.2.7

Polinomial Chebyshev $T_p(x)$ adalah polinomial permutasi di $\mathbb{Z}_n$, jika dan hanya jika p bilangan ganjil.

Bukti :

$(\Rightarrow)$ Diketahui $T_p(x)$ adalah polinomial permutasi di $\mathbb{Z}_n$, maka akan ditunjukkan p bilangan ganjil dengan cara kontrapositif.

Jika p bilangan genap maka berdasarkan Lemma 3.2.4, $T_p(x)$ bukan merupakan polinomial permutasi di $\mathbb{Z}_n$. Jadi terbukti, jika $T_p(x)$ adalah polinomial permutasi di $\mathbb{Z}_n$ maka p bilangan ganjil.

$(\Leftarrow)$ Diketahui p bilangan ganjil, maka akan ditunjukkan $T_p(x)$ adalah polinomial permutasi di $\mathbb{Z}_n$.

Jika p bilangan ganjil maka berdasarkan Lemma 3.2.6, $T_p(x)$ merupakan polinomial permutasi di $\mathbb{Z}_n$.

Sehingga terbukti polinomial Chebyshev $T_p(x)$ adalah polinomial permutasi di $\mathbb{Z}_n$, jika dan hanya jika p bilangan ganjil.

Teorema 3.2.7 telah terbukti. ■

Dari pembahasan di atas terlihat bahwa hanya polinomial Chebyshev berderajat ganjil yang merupakan polinomial permutasi di $\mathbb{Z}_n$, $n = 2^w$, $w \geq 1$.

Dalam algoritma kesepakatan kunci pada kriptografi, salah satu fungsi yang digunakan adalah monomial x^n, seperti yang diilustrasikan di bawah ini.

Alice ingin mengirimkan pesan rahasia kepada Bob dengan menggunakan algoritma kesepakatan kunci Diffie-Hellman berikut :

1. Alice membuat bilangan positif g dan bilangan prima p sedemikian sehingga $g < p$.
2. Alice menentukan bilangan rahasia m, dengan $0 < m < p$.
3. Alice menghitung $a = g^m \bmod p$.
4. Alice mengirimkan p, g, dan a kepada Bob.

5. Bob menentukan bilangan rahasia *n*, dengan $0 < n < p$.

6. Bob menghitung $b = g^n \bmod p$.

7. Bob mengirimkan *b* ke Alice.

8. Alice menghitung kunci rahasia $k = c$ dengan $c = b^m \bmod p$.

9. Bob menghitung kunci rahasia $k = d$ dengan $d = a^n \bmod p$.

Kunci rahasia *k*, adalah *c* bagi Alice dan *d* bagi Bob, akan tetapi $c = d$ karena

$$\left(g^n\right)^m = g^{nm} = g^{mn} = \left(g^m\right)^n.$$

Algoritma Diffie-Hellman tersebut menggunakan suatu monomial x^n yang memenuhi sifat komutatif terhadap komposisi. Yang menjadi pertanyaan adalah apakah ada suatu polinomial yang memenuhi sifat komutatif terhadap komposisi seperti monomial x^n di atas.

Pembahasan berikut akan menjelaskan bahwa polinomial Chebyshev memenuhi sifat komutatif terhadap komposisi, yaitu :

$$T_m\left(T_n(x)\right) = T_n\left(T_m(x)\right).$$

Untuk $x = [-1, 1]$, persamaan (3.14) dapat juga ditulis sebagai berikut :

$$T_p(x) = \cos\left(p \arccos(x)\right).$$

Sehingga

$$\begin{aligned} T_m\left(T_n(x)\right) &= \cos\left(m \arccos\left(T_n(x)\right)\right) \\ &= \cos\left(m \arccos\left(\cos\left(n \arccos(x)\right)\right)\right) \\ &= \cos\left(mn \arccos\left(x\right)\right) \\ &= \cos\left(nm \arccos\left(x\right)\right) \\ &= \cos\left(n \arccos\left(\cos\left(m \arccos(x)\right)\right)\right) \\ &= \cos\left(n \arccos\left(T_m(x)\right)\right) \\ &= T_n\left(T_m(x)\right). \end{aligned}$$

Sedangkan untuk $x > 1$, persamaan (3.15) dapat ditulis sebagai berikut :

$$T_p(x) = \cosh\left(p \cosh^{-1}(x)\right). \qquad (3.27)$$

Sehingga persamaan (3.27) juga memenuhi

$$T_m\left(T_n(x)\right) = T_n\left(T_m(x)\right).$$

Jadi polinomial Chebyshev memenuhi sifat komutatif terhadap komposisi.

Dengan demikian polinomial Chebyshev dapat menjadi alternatif pada algoritma kesepakatan kunci Diffie-Hellman selain monomial x^n.