Prosiding SPMIPA; pp: 96-101; 2006 ISBN: 979.704.427.0

SUKU BANYAK BIKUADRATIK TAK-TEREDUKSI DENGAN FAKTORISASI MODULO BILANGAN PRIMA

Suryoto
Jurusan Matematika FMIPA Universitas Diponegoro
Jl. Prof. H. Soedarto SH Tembalang, Semarang 50275
e-mail : suryo_undip @ yahoo.com

Abstrak: Suku banyak bikuadratik tak-tereduksi atas himpunan semua bilangan bulat **Z** dapat dijadikan tereduksi melalui faktorisasi modulo bilangan prima. Berawal dari keterduksian atas **Z** dapat diturunkan kriteria ketereduksian modulo suatu bilangan prima. Faktorisasi suku banyak bikuadratik ke dalam suku-suku banyak dengan derajat yang lebih rendah ditentukan oleh kondisi diskriminan suku banyak kuadratik identiknya.

Kata Kunci: suku banyak monik, faktorisasi modulo prima, diskriminan

PENDAHULUAN

Faktorisasi suku banyak merupakan salah satu permasalahan klasik di dalam matematika yang mempunyai sejarah peerkembangan yang cukup panjang dan telah ada sejak 1600 tahun sebelum Masehi. Meski boleh dikatakan sudah cukup tua, ternyata tetap saja menarik untuk mengkaji fenomena-fenomena baru yang muncul berkaitan dengan faktorisasi suku banyak ini.

Dummit dan Foote [1] mengungkapkan bahwa terdapat beberapa contoh suku banyak di **Z**[x], meskipun tak-tereduksi, tetapi dapat dijadikan tereduksi modulo suatu bilangan tertentu. Sebagai contoh suku banyak $x^4 – 10x^2 + 1$ yang tak-tereduksi di **Z**[x], tetapi tereduksi modulo setiap bilangan prima.

Berdasarkan fakta yang telah diungkapkan di atas, pada tulisan ini akan diberikan kondisi-kondisi apakah yang harus dipenuhi oleh suku banyak tak-tereduksi di **Z**[x] ini agar tereduksi modulo suatu bilangan prima.

Pada makalah ini hanya akan dikaji suku banyak kuartik yang mempunyai bentuk yang identik dengan suku banyak kuadratik. Khususnya akan dikaji salah satu keluarga dari suku banyak bikuadratik yang muncul pada Kompetisi Matematika Putnam ke-62 yang telah diselenggarakan pada tahun 2002, empat tahun silam.

PEMBAHASAN

Pandang suku banyak monik $f(x) = x^4 + rx^2 + s$, dengan $r, s \in$ **Z** dan **Z** menyatakan himpunan semua bilangan bulat. Meskipun beberapa penulis menggunakan istilah bikuadratik dan kuartik sebagai satu istilah yang bersinonim, tetapi penulis lebih condong kepada pengertian yang diberikan oleh Kappe dan Waren [3], dimana suku banyak bikuadratik adalah suku banyak kuartik atau suku banyak berderajat empat yang mempunyai bentuk yang identik dengan suku banyak kuadratik.

Kriteria Ketereduksian atas Z

Berikut ini akan diberikan syarat perlu dan cukup suku banyak bikuadratik f(x) di atas tereduksi atas **Z**, seperti diberikan oleh teorema berikut ini.

Teorema 1. Misalkan $r, s \in$ **Z**. Suku banyak bikuadratik-monik $f(x) = x^4 + rx^2 + s$ tereduksi di **Z**[x] jika dan hanya jika terdapat $a, c, e \in$ **Z**, sedemikian hingga berlaku:

$$c + e – a^2 – r = 0 \quad (1)$$

$$a(e – c) = 0 \quad (2)$$

dan
$$ce – s = 0 \quad (3)$$

Dalam hal ini, f(x) = (x2 + ax + c)(x2 – ax + e).

Bukti : ($\Rightarrow$) Misalkan $f(x) = x^4 + rx^2 + s$ tereduksi di **Z**[x], maka setidaknya f(x) mempunyai faktor linier x – m atau faktor kuadratik tak-tereduksi $x^2 + ax + c$ di **Z**[x].

Pandang kemungkinan 1 : Misalkan $m \neq 0$, maka x + m juga merupakan faktor dari f(x). Dengan demikian $x^2 – m^2 = (x – m)(x + m)$ juga merupakan faktor dari f(x) dan

$$f(x) = x^4 + rx^2 + s = (x^2 – m^2)(x^2 + bx + d),$$

dengan $b, d \in$ **Z**.

Sedangkan untuk m = 0, x^2 merupakan salah satu faktor dari f(x) dan

$$f(x) = x^4 + rx^2 + s = x^2(x^2 + r).$$

Dimana untuk kedua nilai m di atas, jelas kondisi (1), (2) dan (3) dipenuhi.
Selanjutnya pandang kemungkinan 2 : f(x) mempunyai faktor kuadratik tak-tereduksi $x^2 + ax + c$ di **Z**[x]. Tulis $f(x) = x^4 + rx^2 + s = (x^2 + ax + c)(x^2 + bx + e)$, dengan b, e $\in$ **Z**. Dengan menyamakan koefisien dari kesamaan dua suku banyak di atas diperoleh b = – a dan

$$f(x) = x^4 + rx^2 + s = (x^2 + ax + c)(x^2 - ax + e)$$

atau $f(x) = x^4 + rx^2 + s = x^4 + (c + e - a^2)x^2 + a(e - c)x + ce$ dan diperoleh :

$$c + e - a^2 - r = 0,\ a(e - c) = 0 \text{ dan } ce - s = 0.$$

($\Leftarrow$) Misalkan kondisi (1), (2) dan (3) dipenuhi, maka

$$(x^2 + ax + c)(x^2 - ax + e) = x^4 + (c + e - a^2)x^2 + a(e - c)x + ce = x^4 + rx^2 + s,$$

yaitu f(x) tereduksi di **Z**[x]. ■

Selanjutnya akan diberikan kriteria ketereduksian yang lain untuk suku banyak bikuadratik-monik $f(x) = x^4 + rx^2 + s$. Untuk itu pandang fungsi kuadrat $f(y) = y^2 + ry + s$, yang diperoleh dari persamaan bikuadratik di atas, dengan mengambil $y = \sqrt{x}$. Berkaitan dengan fungsi kuadrat ini, kita mempunyai $D = r^2 - 4s$, yang dinamakan diskriminan dari fungsi kuadrat f(y).

Dengan memperhatikan kondisi diskriminan dari fungsi kuadrat di atas dan sebagai konsekuensi Teorema 1 dapat diturunkan hasil-hasil berikut ini.

Akibat 1. Misalkan r, s $\in$ **Z** sedemikian hingga $D = r^2 - 4s$ kuadrat sempurna, misalkan $D = k^2$, untuk suatu k $\in$ **Z**, maka $f(x) = x^4 + rx^2 + s$ tereduksi di **Z**[x] dan

$$f(x) = (x^2 + ½(r - k))(x^2 + ½(r + k)).$$

Bukti : Diberikan $f(x) = x^4 + rx^2 + s$, maka $f(\sqrt{x}) = x^2 + rx + s$ dan $D = r^2 - 4s$.

Karena $D = k^2$, untuk suatu k $\in$ **Z**, maka $s = \frac{1}{4}(r^2 - k^2)$ dan diperoleh

$$f(x) = x^4 + rx^2 + \frac{1}{4}(r^2 - k^2) = (x^2 + \frac{1}{2}(r - k))(x^2 + \frac{1}{2}(r + k)).$$

Klaim : $\frac{1}{2}(r \pm k) \in$ **Z**.

Bukti Klaim : Dari $D = r^2 - 4s = k^2$, untuk suatu k $\in$ **Z**, maka $r^2 - k^2 = 4s$ atau
$(r - k)(r + k) = 4s$. Yaitu $(r - k)(r + k)$ genap dan berakibat $(r - k)$ dan $(r + k)$ keduanya harus genap. Sehingga benar bahwa $\frac{1}{2}(r \pm k) \in$ **Z**.

Dengan demikian terbukti bahwa f(x) tereduksi di **Z**[x]. ■

Akibat 2. Misalkan r, s $\in$ **Z** sedemikian hingga $D = r^2 - 4s$ bukan kuadrat sempurna. Maka $f(x) = x^4 + rx^2 + s$ tereduksi di **Z**[x] jika dan hanya jika terdapat bilangan bulat c sedemikian hingga $c^2 = s$ dan $2c - r = a^2$. Dalam hal ini, $f(x) = (x^2 + ax + c)(x^2 - ax + e)$, dengan a suatu bilangan bulat sedemikian hingga $a^2 = 2c - r$.
Bukti : ($\Rightarrow$) Misalkan $f(x) = x^4 + rx^2 + s = (x^2 + ax + c)(x^2 - ax + c)$, dengan a, c $\in$ **Z**, maka

$$f(x) = x^4 + (2c - a^2)x^2 + c^2 \text{ dan diperoleh } 2c - a^2 = r \text{ dan } c^2 = s \text{ atau } 2c - r = a^2 \text{ dan } c^2 = s.$$

($\Leftarrow$) Misalkan $c^2 = s$, dengan c $\in$ **Z** dan $2c - r = a^2$, untuk suatu a $\in$ **Z**, maka $r = 2c - a^2$.
Akibatnya $f(x) = x^4 + rx^2 + s = x^4 + (2c - a^2)x^2 + c^2 = (x^2 + ax + c)(x^2 - ax + c)$, dengan a, c $\in$ **Z**, yaitu f(x) tereduksi di **Z**[x]. ■

Dari Akibat 1 dan 2 dari Teorema 1 di atas, tampak bahwa faktorisasi suku banyak monik bikuadratik $f(x) = x^4 + rx^2 + s$ bergantung kepada kondisi diskriminan $D = r^2 - 4s$ dari suku banyak kuadratik identiknya, yaitu :

1. Jika $D = r^2 - 4s = t^2$, untuk suatu t $\in$ **Z** atau D kuadrat sempurna, maka f(x) teruraikan ke dalam perkalian dua buah suku banyak kuadratik tak lengkap.
2. Jika $D = r^2 - 4s$, bukan kuadrat sempurna, maka f(x) teruraikan ke dalam hasil kali dua buah suku banyak kuadratik biasa.

Contoh 1 :
Suku banyak yang telah diungkapkan pada bagian Pendahuluan, merupakan contoh yang dapat menjelaskan hasil-hasil di atas. Dari suku banyak $f(x) = x^4 - 10x^2 + 1$, kita mempunyai r = –10, s = 1 dan $D = r^2 - 4s = 96$, bukan kuadrat sempurna serta tidak ada bilangan bulat c yang memenuhi $c^2 = 1$ dan 2c + 10 suatu kuadrat sempurna sekaligus. Sehingga menurut Akibat 2, suku banyak $f(x) = x^4 - 10x^2 + 1$ tak-tereduksi di **Z**[x]. ■

Kriteria Ketereduksian Modulo p

Pada bagian sebelumnya, telah diberikan kriteria ketereduksian untuk suku banyak bikuadratik monik $f(x) = x^4 + rx^2 + s$ atas **Z**. Pada bagian ini, akan diberikan syarat perlu dan cukup suku banyak bikuadratik $f(x) = x^4 + rx^2 + s$ tereduksi modulo p, dengan p suatu bilangan prima, yang diadopsi dari Teorema 1, seperti diberikan oleh teorem berikut ini.

Teorema 2. Misalkan p suatu bilangan prima. Maka suku banyak bikuadratik $f(x) = x^4 + rx^2 + s$ di **Z**[x] tereduksi modulo p jika dan hanya jika terdapat a, c, e $\in$ **Z**, yang memenuhi :

$$c + e - a^2 - r \equiv 0 \pmod{p} \tag{4}$$

$$a(e - c) \equiv 0 \pmod{p} \tag{5}$$

$$ce - s \equiv 0 \pmod{p} \tag{6}$$

Dalam hal ini $f(x) \equiv (x^2 + ax + c)(x^2 - ax + e) \pmod{p}$.

Bukti : Sejalan dengan bukti Teorema 1. ■

Pada bagian sebelumnya telah diberikan kriteria ketereduksian suku banyak bikuadratik berturut-turut atas himpunan semua bilangan bulat **Z** dan modulo suatu bilangan prima p. Berikut ini, akan diberikan beberapa kriteria ketereduksian tambahan untuk melengkapi kriteria yang sudah ada. Pembahasan akan dimulai dengan kriteria ketereduksian modulo p, dengan p suatu bilangan prima yang ganjil.

Pandang suku banyak bikuadratik-monik $f(x) = x^4 + rx^2 + s$ di **Z**[x] dan p suatu bilangan prima yang ganjil. Terdapat beberapa kondisi berkaitan dengan suku banyak $f(x) = x^4 + rx^2 + s$, yaitu :

1). Jika $s \equiv 0 \pmod{p}$.
Maka $f(x) = x^4 + rx^2 + s \equiv x^4 + rx^2 \pmod{p} \equiv x^2(x^2 + r) \pmod{p}$.
Sehingga diperoleh a = 0 = c dan e = r.

2). Jika $D = r^2 - 4s \equiv 0 \pmod{p}$.
Maka $r^2 \equiv 4s \pmod{p}$ atau $s \equiv \frac{1}{4} r^2 \pmod{p}$ atau $s \equiv \left(\frac{r}{2}\right)^2 \pmod{p}$.
Dengan demikian $f(x) = x^4 + rx^2 + s \equiv x^4 + rx^2 + \frac{r^2}{4} \pmod{p} \equiv (x^2 + \frac{r}{2})^2 \pmod{p}$ dan diperoleh a = 0 dan $c = e \equiv \frac{r}{2} \pmod{p}$, dimana $\frac{1}{2}$ menyatakan invers dari 2 modulo p.

3). Jika $s \neq 0 \pmod{p}$ dan $D = r^2 - 4s \neq 0 \pmod{p}$.

Berkaitan dengan kondisi 3 ini dan dalam rangka melengkapi kriteria ketereduksian suku banyak bikuadratik f(x) modulo bilangan prima p yang ganjil, akan diberikan terlebih dahulu notasi Legendre $\left(\frac{k}{p}\right)$ dan sifat-sifat pentingnya.

Menurut Rosen [4, p. 332], untuk suatu bilangan bulat k dan bilangan prima p yang ganjil, notasi Legendre $\left(\frac{k}{p}\right)$ didefinisikan oleh :

$$\left(\frac{k}{p}\right) = \begin{cases} 1, \text{ jika p tidak membagi k dan } x^2 \equiv k(\text{mod p}) \text{ dapat diselesaikan} \\ 0, \text{ jika p membagi k} \\ -1, \text{ jika p tidak membagi k dan } x^2 \equiv k(\text{mod p}) \text{ tidak dapat diselesaikan} \end{cases}.$$

Dimana notasi Legendre ini memenuhi sifat-sifat berikut ini :

1). Jika $k \equiv l \pmod{p}$, maka $\left(\frac{k}{p}\right) = \left(\frac{l}{p}\right)$

2). Untuk setiap bilangan bulat k dan l, berlaku :

3). $\left(\frac{kl}{p}\right) = \left(\frac{k}{p}\right)\left(\frac{l}{p}\right)$

4). $\left(\frac{k^2 l}{p}\right) = \left(\frac{l}{p}\right)$, jika p tidak membagi k.

Dari Teorema 2 dan mengingat definisi notasi Legendre beserta sifat-sifat pentingnya, diperoleh hasil, sebagaimana dituangkan dalam teorema berikut ini.

Teorema 3. Misalkan p suatu bilangan prima yang ganjil dan r, s $\in$ **Z**, sedemikian hingga s $\neq$ 0 (mod p) dan D = $r^2 - 4s \neq 0$ (mod p), maka pernyataan-pernyataan berikut ini senantiasa benar :

a. $f(x) = x^4 + rx^2 + s$ teruraikan ke dalam hasil kali dua buah suku banyak monik berlainan berderajat satu dan sebuah suku banyak monik kuadratik tak-tereduksi modulo p jika dan hanya jika

$$\left(\frac{s}{p}\right) = -1 \text{ dan } \left(\frac{D}{p}\right) = 1.$$

b. $f(x) = x^4 + rx^2 + s$ teruraikan ke dalam hasil kali empat buah suku banyak monik berlainan berderajat satu modulo p jika dan hanya jika

$$\left(\frac{s}{p}\right) = 1,\ \left(\frac{D}{p}\right) = 1 \text{ dan } \left(\frac{-r-2t}{p}\right) = 1,$$

dimana t adalah bilangan bulat sedemikian hingga s $\equiv t^2$(mod p).

c. $f(x) = x^4 + rx^2 + s$ teruraikan ke dalam hasil kali dua buah suku banyak monik kuadartik yang berlaianan modulo p jika dan hanya jika

$$\left(\frac{s}{p}\right) = 1,\ \left(\frac{D}{p}\right) = 1 \text{ dan } \left(\frac{-r-2t}{p}\right) = -1,$$

d imana t adalah bilangan bulat sedemikian hingga s $\equiv t^2$ (mod p)

atau $\left(\frac{s}{p}\right) = 1$ dan $\left(\frac{D}{p}\right) = -1$.

d. $f(x) = x^4 + rx^2 + s$ tak-tereduksi modulo p jika dan hanya jika

$$\left(\frac{s}{p}\right) = -1 \text{ dan } \left(\frac{D}{p}\right) = -1.$$

Bukti : Hanya akan dibuktikan bagian (a), karena untuk bukti bagian (b), bagian (c) dan bagian (d) dapat dibuktikan sejalan dengan bukti bagian (a).

($\Rightarrow$) Misalkan $f(x) = x^4 + rx^2 + s \equiv (x-a)(x-b)(x^2+cx+d)$ (mod p), dengan suku banyak $x^2 + cx + d$ tak-tereduksi, maka

$$f(x) = x^4 + (-a-b+c)x^3 + (d+ab-(a+b)c)x^2 + (-(a+b)d+abc)x + abd$$

dan diperoleh :

$$-a-b+c = 0 \quad (1)$$

$$d+ab-(a+b)c = r \quad (2)$$

$$-(a+b)d+abc = 0 \quad (3)$$

$$abd = s \quad (4)$$

Dari persamaan (1) diperoleh c = a + b dan bilamana disubstitusikan ke persamaan (3) diperoleh (a + b)(ab – d) = 0 dan haruslah a + b = 0.

Sebab andaikan ab – d = 0 atau ab = d, maka

$$f(x) \equiv (x-a)(x-b)(x^2+cx+d) \text{(mod p)}$$
$$\equiv (x-a)(x-b)(x^2+(a+b)x+ab) \equiv (x-a)(x-b)(x+a)(x+b),$$

yaitu $x^2 + cx + d = (x+a)(x+b)$ atau $x^2 + cx + d$ tereduksi, bertentangan dengan yang diketahui bahwa suku banyak $x^2 + cx + d$ tak-tereduksi.

Jadi benar bahwa a + b = 0 atau b = – a. Dengan demikian,

$$f(x) \equiv (x-a)(x-b)(x^2+cx+d) \equiv f(x) \equiv (x-a)(x+a)(x^2+d)$$
$$\equiv x^4 + (d-a^2)x^2 - da^2.$$

Sehingga diperoleh $r = d - a^2$, $s = -da^2$ dan $D = r^2 - 4s = (d - a^2)^2 + 4da^2 = (d + a^2)^2$, yaitu $D \equiv x^2 \pmod p$ mempunyai penyelesaian atau $\left(\frac{D}{p}\right) = 1$.

Selanjutnya tinjau $s = -da^2 = abd$. Karena $ab \neq d$ atau $a^2 \neq d$, dengan d bukan kuadrat sempurna, maka s juga bukan kuadrat sempurna, dengan perkataan lain $s \neq t^2 \pmod p$ untuk setiap $t \in \mathbf{Z}$, ini memberikan $\left(\frac{s}{p}\right) = -1$.

($\Leftarrow$) Misalkan $\left(\frac{s}{p}\right) = -1$ dan $\left(\frac{D}{p}\right) = 1$.

Tinjau $f(x) = x^4 + rx^2 + s$, dengan $D = r^2 - 4s$.

Karena $\left(\frac{D}{p}\right) = 1$, maka $D = t^2$, untuk suatu $t \in \mathbf{Z}_p$. Dengan demikian $t^2 = r^2 - 4s$ atau $s = \frac{1}{4}(r^2 - t^2)$ dan $f(x) = x^4 + rx^2 + s = x^4 + rx^2 + \frac{1}{4}(r^2 - t^2) = (x^2 + \frac{1}{2}(r - t))(x^2 + \frac{1}{2}(r + t))$ atau $f(x) = (x^2 - a)(x^2 - b)$, dengan $a = -\frac{1}{2}(r - t)$ dan $b = -\frac{1}{2}(r + t)$, yaitu $f(x) = x^4 + rx^2 + s$ tereduksi.

Andaikan $x^2 - a$ dan $x^2 - b$ keduanya tereduksi, maka terdapat $x_1, x_2 \in \mathbf{Z}_p$ sedemikian hingga $x_1^2 = a$ dan $x_2^2 = b$. Dengan demikian diperoleh $(x_1x_2)^2 = ab = (-\frac{1}{2}(r - t))(-\frac{1}{2}(r + t)) = \frac{1}{4}(r^2 - t^2) = s$, yaitu kongruensi $x^2 \equiv s \pmod p$ mempunyai penyelesaian atau $\left(\frac{s}{p}\right) = 1$. Ini bertentangan dengan yang diketahui bahwa $\left(\frac{s}{p}\right) = -1$.

Jadi haruslah salah satu dari $x^2 - a$ atau $x^2 - b$ tak-tereduksi. Tanpa mengurangi keumuman bukti misalkan $x^2 - b$ tak-tereduksi dan diperoleh

$$f(x) = x^4 + rx^2 + s = (x^2 - a)(x^2 - b) = (x - c)(x - d)(x^2 - b),$$

yaitu $f(x) = x^4 + rx^2 + s$ teruraikan ke dalam hasil kali dua buah suku banyak linier dan sebuah suku banyak kuadratik tak-tereduksi. ■

Sekarang akan diberikan kondisi yang lebih umum bagi kriteria ketereduksian suku banyak bikuadratik $f(x) = x^4 + rx^2 + s$ modulo setiap bilangan prima, seperti diungkapkan dalam teorema berikut ini.

Teorema 4. Misalkan $r, s \in \mathbf{Z}$ sedemikian hingga $D = r^2 - 4s$ bukan kuadrat sempurna. Maka suku banyak $f(x) = x^4 + rx^2 + s$ tereduksi modulo p, untuk setiap bilangan prima p jika dan hanya jika s kuadrat sempurna.
Bukti : Lihat E. Driver, dkk [2, p. 880 – 881]. ■

Dengan mengkombinasikan Teorema 4 dengan Akibat 1 dan 2 dari Teorema 1, diperoleh syarat perlu dan cukup bagi suku banyak bikuadratik-monik $f(x) = x^4 + rx^2 + s$ yang tak-tereduksi di $\mathbf{Z}[x]$, tetapi tereduksi modulo p untuk setiap bilangan prima p. Seperti diberikan oleh teorema berikut ini.

Teorema 5. Misalkan $r, s \in \mathbf{Z}$. Maka suku banyak bikuadratik $f(x) = x^4 + rx^2 + s$ yang tak-tereduksi di $\mathbf{Z}[x]$, tetapi tereduksi modulo p, untuk setiap bilangan prima p jika dan hanya jika hal-hal berikut ini dipenuhi : s kuadrat sempurna, tetapi $D = r^2 - 4s$ dan $\pm 2\sqrt{s} - r$ ketiganya bukan kuadrat sempurna.
Bukti : Terlihat dari bukti Teorema 4 dan bukti Akibat 1 dan Akibat 2. ■

Sebagai fokus dari tulisan ini, sekarang ditinjau keluarga suku banyak bikuadratik yang muncul pada Kompetisi Matematika Putnam ke-62 tahun 2002 [5, Soal A3], yang diberikan oleh :

$$P_m(x) = x^4 - (2m + 4)x^2 + (m - 2)^2, \qquad (m \in \mathbf{Z}).$$

Dari suku banyak bikuadratik ini, kita mempunyai $r = -(2m + 4)$ dan $s = (m - 2)^2$.
Dengan demikian $D = r^2 - 4s = (2m + 4)^2 - 4(m - 2)^2 = 32m$.
Sehingga D merupakan kuadrat sempurna jika dan hanya jika 2m kuadrat sempurna.
Jika 2m suatu kuadrat sempurna, maka $m = 2t^2$, untuk suatu $t \in \mathbf{Z}$ dan menurut Akibat 1 diperoleh :

$$P_m(x) = (x^2 - (2t^2 - 4t + 2))(x^2 - (2t^2 + 4t + 2)).$$

Sebaliknya, misalkan 2m bukan kuadrat sempurna. Maka berdasarkan Akibat 2, $P_m(x)$ tereduksi jika dan hanya jika $\pm$ 2(m – 2) + 2m + 4 suatu kuadrat sempurna dan hal ini benar jika dan hanya jika m kuadrat sempurna. Dalam hal ini, kita mempunyai

$$P_m(x) = (x^2 + 2tx + t^2 - 2)(x^2 - 2tx + t^2 - 2).$$

Dengan demikian diperoleh hasil sebagai berikut :
Suku banyak bikuadratik $P_m(x) = x^4 - (2m + 4)x^2 + (m - 2)^2$, ($m \in \mathbf{Z}$) tak-tereduksi di $\mathbf{Z}[x]$, asalkan m dan 2m keduanya bukan kuadrat sempurna.

Contoh 2 :
Suku banyak $f(x) = x^4 - 10x^2 + 1$, yang telah diberikan pada bagian Pendahuluan tidak lain adalah suku banyak $P_m(x) = x^4 - (2m + 4)x^2 + (m - 2)^2$, dimana m = 3.
Dengan demikian karena m = 3 dan 2m = 6, keduanya bukan kuadrat sempurna, maka berdasarkan hasil di atas, $f(x) = x^4 - 10x^2 + 1$ tak-tereduksi di $\mathbf{Z}[x]$. ■

Contoh 3 :
Pandang kembali suku banyak bikuadratik $f(x) = x^4 - 10x^2 + 1$. Maka kita mempunyai $r = -10$, $s = 1$, $\sqrt{s} = 1$, sehingga $D = r^2 - 4s = 96$, $2\sqrt{s} - r = 12$ dan $-2\sqrt{s} - r = 8$ ketiganya bukan kuadrat sempurna. Dengan demikian menurut Teorema 5 di atas, $f(x) = x^4 - 10x^2 + 1$ yang tidak tereduksi di $\mathbf{Z}[x]$ (berdasarkan Contoh 2), tetapi tereduksi modulo p, untuk setiap bilangan prima p.
Sekarang akan ditinjau untuk p = 5. Akan kita lihat faktorisasi suku banyak bikuadratik-monik $f(x) = x^4 - 10x^2 + 1$ dengan faktorisasi modulo 5. Dari suku banyak f(x) di atas, kita mempunyai $r = -10$, $s = 1$ dan $D = r^2 - 4s = 96$. Karena p = 5, maka $s = 1 \neq 0 \pmod 5$ dan $D = 96 \equiv 1 \neq 0 \pmod 5$, maka diperoleh :

$$\left(\frac{s}{p}\right) = \left(\frac{1}{5}\right) = 1 \text{ (karena residu kuadratik dari 5 adalah 1 dan 4),}$$

$$\left(\frac{D}{p}\right) = \left(\frac{96}{5}\right) = \left(\frac{1}{5}\right) = 1 \text{ dan } \left(\frac{-r-2t}{p}\right) = \left(\frac{8}{5}\right) = \left(\frac{3}{5}\right) = -1,$$

dimana t adalah bilangan bulat sedemikian hingga $s \equiv t^2 \pmod p$ atau $1 \equiv t^2 \pmod 5$, sehingga t = 1.
Dengan demikian menurut Teorema 3 bagian (c), $f(x) = x^4 - 10x^2 + 1$ teruraikan ke dalam hasil kali dua buah suku banyak kuadratik berlainan yang tak-tereduksi modulo 5, yaitu :

$$\begin{aligned} f(x) = x^4 - 10x^2 + 1 &\equiv x^4 + 1 \pmod 5 \equiv (x^2 + 3)(x^2 + 2) \pmod 5 \\ &\equiv (x^2 - 2)(x^2 - 3) \pmod 5. \end{aligned}$$ ■

KESIMPULAN

Dari hasil pembahasan faktorisasi suku banyak bikuadratik tak-tereduksi $f(x) = x^4 + rx^2 + s$ dengan faktorisasi modulo bilangan prima p, dapat disimpulkan bahwa faktorisasi ditentukan oleh dua hal, yaitu kondisi s dan kondisi diskriminan $D = r^2 - 4s$ dari suku banyak kuadratik identiknya, apakah merupakan kuadrat sempurna atau bukan.

DAFTAR PUSTAKA

[1]. Dummit, D. S. and Foote, R. M., *Abstract Algebra*, Prentice-Hall, Englewood Cliffs, New Jersey, 1991.

[2]. Driver, E., Leonard, P. A., and William, K. S., Irredicible Quartic Polynomial with Factorizations Modulo p, *The Mathematical Association of America Monthly 112*, pp. 876 – 889, 2005.

[3]. Kappe, L. C. and Waren, B., An Elementary Test for The Galois Group of a Quartic Polynomial, *The Mathematical Association of America Monthly 96*, pp. 133 – 137, 1989.

[4]. Rosen, K. H., *Elementary Number Theory and Its Applications*, Addison-Wesley, Reading, Massachusetts, 1993.

[5]. 62nd Annual William Lowell Putnam Mathematical Competition, *Math. Magazine*, 75, pp. 72 – 78, 2002.