

EISENSTEİN KRİTERİNİN BİR UYGULAMASI

Özgün ÖGE

Özel Selim Pars Lisesi , Florya/İSTANBUL

Giriş :

Bir polinomun asal olup olmadığını belirlemek önemli bir problemdir. Asallığı belirleyen kriterlerden biri de Eisenstein kriteridir. Bu yazıda Eisenstein Asallık kriterinin doğrudan uygulanmadığı 2. ve 3. dereceden polinomlar ele alınmış , $n \in \mathbb{Z}$ olmak üzere $P(x+n)$ ötelemesi yapılmadan bu polinomların asal olduğu gösterilmiştir ve $P(x+n)$ ötelemesi yapılmadan polinomların asallığı için bir yeter koşul verilmiştir.

$\mathbb{Z}[x]$ üzerinde tanımlı $P(x)$ polinomların asal olduğunu belirlemek için, kullanılan Eisenstein Asallık kriterine göre

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \quad (a_i \in \mathbb{Z})$$

ve bir p asal sayısı için ; $p \mid a_i$ ($i = 0, 1, 2, \dots, n-1$) , $p \nmid a_n$, $p^2 \nmid a_0$ ise $P(x)$ asaldır [1].

Örneğin bu kritere göre $P(x) = x^3 - 2$ ($p = 2$) polinomu, $\mathbb{Z}[x]$ üzerinde asaldır. Diğer yandan bu asallık kriteri bazı polinomlar için kullanılamaz. Bu kriter, örneğin, $P(x) = x^2 + x + 1$ polinomu için sonuç vermez. Fakat bir $n \in \mathbb{Z}$ için , $P(x+n)$ asal ise $P(x)$ de asaldır ve uygun bir n için bu kriter $P(x+n)$ 'e uygulanabilir. Bu projede bir $P(x)$ polinomu verildiğinde (uygun n 'i aramadan) $P(x)$ polinomunun asallığı incelenmiştir.

Yöntem :

Şimdi bir $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$ polinomu verilsin. Eğer $P(x) = A(x).B(x)$, burada ($\deg A(x) \geq 1$, $\deg B(x) \geq 1$, $A(x), B(x) \in \mathbb{Z}[x]$), şeklinde bir yazılış mümkün değilse $P(x)$ polinomu $\mathbb{Z}[x]$ üzerinde asaldır denir. Bu çalışmada asal olan bazı polinomları belirleyeceğiz.

Tanım :

Bir $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ ($a_i \in \mathbb{Z}$) polinomunda $(a_n, \dots, a_1, a_0) = 1$ ise $P(x)$ 'e primitif polinom denir. Bu çalışmada ele alacağımız polinomlar primitif polinomlar olacaktır.

1. $P(x) = ax^2 + bx + c$ polinomu

$P(x) = ax^2 + bx + c$, $(a, b, c) = 1$ polinomunu ele alalım. Eisenstein kriterinin bu polinoma uygulanmadığını varsayalım. Uygun bir n için $P(x+n)$ polinomuna Eisenstein kriterinin uygulanıp uygulanmayacağını araştıralım.

$P(x+n) = a(x+n)^2 + b(x+n) + c = ax^2 + (2an+b)x + an^2 + bn + c$ elde edilir. n 'i öyle seçelimki p uygun bir asal sayı olmak üzere ;

$$p \nmid a , p^2 \nmid an^2 + bn + c , p \mid 2an+b , p \mid an^2 + bn + c \quad (1)$$

olsun.

$$\left. \begin{array}{l} p \mid 2an+b \Rightarrow p \mid 4a^2n^2 + 4abn + b^2 \\ p \mid an^2 + bn + c \Rightarrow p \mid 4a^2n^2 + 4abn + 4ac \end{array} \right\} \Rightarrow p \mid b^2 - 4ac \text{ elde edilir.}$$

O halde aranan p , $p \mid b^2 - 4ac$ koşulunu sağlar. Önce şunu görelim: $ax^2 + bx + c$ asal ise $cx^2 + bx + a$ da asaldır ve tersi de doğrudur. Çünkü; $cx^2 + bx + a = (ex+f)(gx+h)$ olsa buradan $ax^2 + bx + c = (fx+e)(hx+g)$ elde edilir.

Şimdi bir p_1 asal sayısı için $p_1 \mid b^2 - 4ac$ ve $p_1^2 \nmid b^2 - 4ac$ olduğunu kabul edelim.

Buna göre $p_1 \mid b^2 - 4ac$ ise $p_1 \nmid a$ kabul edebiliriz. Çünkü $p_1 \mid a$ ise bu durumda $cx^2 + bx + a$ polinomunu alırız ve burada $p_1 \nmid c$ olur. (Çünkü $p_1 \mid c$ olsaydı $p_1 \mid b^2 - 4ac$ ve $p_1 \mid c$ den $p_1 \mid b$ çıkarırdı ve böylece $p_1 \mid a$, $p_1 \mid b$, $p_1 \mid c$ elde edilirdi ki bu $ax^2 + bx + c$ nin primitif oluşu ile çelişirdi.)

Şimdi bu p_1 asal sayısının (1) deki bağıntıları gerçeklediğini gösterelim.

a) $p_1 = 2$ hali: $p_1 = 2$ ise $2 \mid b^2 - 4ac$ den $2 \mid b$ olup $\forall n \in \mathbb{Z}$ için $2 \mid 2an + b$ bulunur.

c tek ise n 'i tek seçerek, c çift ise n 'i çift seçerek $2 \mid an^2 + bn + c$ bulunur.

Şimdi $2^2 \nmid an^2 + bn + c$ olduğunu gösterelim. $2^2 \mid an^2 + bn + c$ olsa $2 \mid 2an + b$ den

$$\left. \begin{array}{l} 2^2 \mid 4a^2n^2 + 4abn + 4ac \\ 2^2 \mid (2an+b)^2 = 4a^2n^2 + 4abn + b^2 \end{array} \right\} \Rightarrow 2^2 \mid b^2 - 4ac \text{ bulunurdu ki bu } p_1 \text{ in seçimi ile çelişir.}$$

b) $p_1 > 2$ olsun. $p_1 \nmid a$ dan $2an+b \equiv 0 \pmod{p_1}$ kongrüansının bir $n = n_0$ çözümü vardır.

$$p_1 \mid (2an_0+b)^2 \Rightarrow p_1 \mid 4a^2n_0^2 + 4abn_0 + b^2$$

$$\Rightarrow p_1 \mid b^2 - 4ac$$

ve buradan

$$p_1 \mid 4a^2n_0^2 + 4an_0b + 4ac \Rightarrow p_1 \mid 4a(an_0^2 + bn_0 + c) \text{ olup } p_1 \nmid 4a \text{ dan } p_1 \mid an_0^2 + bn_0 + c$$

elde edilir.

Şimdide $p_1^2 \nmid an_0^2 + bn_0 + c$ olduğunu gösterelim.

Eğer $p_1^2 \mid an_0^2 + bn_0 + c$ olsa bu ve $p_1^2 \mid (2an_0+b)^2$ den $p_1^2 \mid 4a(an_0^2 + bn_0 + c) - (4a^2n_0^2 + 4an_0b + b^2)$

$\Rightarrow p_1^2 \mid b^2 - 4ac$ elde edilir ki bu p_1 'in seçimi ile çelişir. Böylece şu sonucu buluruz

Sonuç 1.

$P(x) = ax^2 + bx + c$ primitif polinomu verilsin. Eğer bir p asal sayısı için

$p \mid b^2 - 4ac$ ve $p^2 \nmid b^2 - 4ac$ ise $P(x)$ polinomu $\mathbb{Z}[x]$ üzerinde asaldır.

Not : $P(x) = 0$ denkleminin kökleri $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ olduğundan $b^2 - 4ac = -p^2 < 0$ (p asal)

İse $P(x)$ polinomu asaldır. Bu durumda bu polinomun asallığını Eisenstein kriteri ile elde edemeyiz. Buna sebep Eisenstein kriterindeki şartların bir gerek şart olmayışıdır.

1. $P(x) = ax^3 + bx^2 + cx + d$ polinomu

Bu polinomun asallığını direkt olarak Eisenstein kriteri ile test edilmediğini kabul edelim ve $P(x+n)$ polinomunu oluşturalım.

$$P(x+n) = ax^3 + (3an+b)x^2 + (3an^2+2bn+c)x + an^3 + bn^2 + cn + d$$

olup bir p asal sayısı için (ve uygun bir n için)

$$p \mid 3an + b = A, \quad p \mid 3an^2 + 2bn + c = B \quad \text{ve} \quad p \mid an^3 + bn^2 + cn + d = C \quad (2)$$

olduğunu kabul edelim.

$p \mid A$ ve $p \mid B \Rightarrow p \mid nA - B \Rightarrow p \mid bn + c$ ve bunu $p \mid A$ ile kullanarak $p \mid 3a(bn+c) - Ab \Rightarrow p \mid b^2 - 3ac$ elde edilir. Yine ;

$$p \mid 3C, \quad p \mid B \Rightarrow p \mid 3C - Bn \Rightarrow p \mid bn^2 + 2cn + 3d \quad \text{olup} \quad \text{bunu} \quad p \mid B \quad \text{ile} \quad \text{tekrar} \quad \text{kullanarak}$$

$$p \mid 3a(bn^2 + 2cn + 3d) - bB \Rightarrow p \mid (6ac - 2b^2)n + 9ad - bc \quad \text{elde} \quad \text{edilir.}$$

Bunu $p \mid A$ ile tekrar kullanırsak ; $p \mid 27a^2d - 9abc + 2b^3$ bulunur. Yani aranan p asal sayısı

$$p \mid (b^2 - 3ac, 27a^2d - 9abc + 2b^3) \quad (3)$$

koşulunu gerçeğe.

1. hal: (3) bağıntısını sağlayan tek asal sayı 3 olsun. Eğer $3 \mid a$ ise kriter uygulanamaz. $3 \nmid a$ olduğunu kabul edelim. $3 \mid b^2 - 3ac$ den $3 \mid b$ bulunur. Bunu $p \mid B$ de kullanırsak $3 \mid c$ elde edilir. O halde $3 \mid c$ ise kriter uygulanamaz. $3 \mid c$ ise bunu $3 \mid C$ de kullanarak $3 \mid an^3 + d$ bulunur. Burada şu halleri incelemeliyiz.

a) $d \equiv 0 \pmod{3}$ hali

Bu durumda n sayısını $n \equiv 0 \pmod{3}$ olacak şekilde alırsak $3 \mid C$ olur. O halde $9 \nmid d$ ise $P(x)$ asaldır. $9 \mid d$ ise kriter uygulanamaz.

b) $d \equiv 1 \pmod{3}$ hali

Eğer $a \equiv 1 \pmod{3}$ ise n 'i $n \equiv 2 \pmod{3}$ olarak alırsak $3 \mid C$ olur. Eğer $9 \nmid 8a + d$ ise $P(x)$ asaldır. $9 \mid 8a + d$ ise kriter sonuç vermez. $a \equiv 2 \pmod{3}$ durumunda n sayısını $n \equiv 1 \pmod{3}$ olacak şekilde seçersek $3 \mid C$ bulunur. Eğer bu durumda $9 \nmid a + d$ ise $P(x)$ asaldır. $9 \mid a + d$ ise kriter yine uygulanamaz.

c) $d \equiv 2 \pmod{3}$ hali

$a \equiv 1 \pmod{3}$ ise n 'i $n \equiv 1 \pmod{3}$ olarak alırsak $3|C$ olur. Eğer $9|a+d$ ise $(9|c^2$ olacağından) kriter uygulanamaz. $9 \nmid a+d$ ise $(9 \nmid c$ olacağından) $P(x)$ asaldır. Eğer $a \equiv 2 \pmod{3}$ ise n 'i $n \equiv 2 \pmod{3}$ olarak seçersek $3|C$ olur. Eğer $9 \nmid 8a+d$ ise $9 \nmid c^2$ olacağından $P(x)$ asaldır. $9|c$ ise Eisenstein kriteri yine uygulanamaz.

2. hal: (3) bağıntısı $p \neq 3$ için sağlansın. Eğer (3)'ü sağlayan her p asal sayısı için $p|a$ ise kriter uygulanamaz. $p \nmid a$ olsun. n_0 sayısını $3an_0 + b \equiv 0 \pmod{p}$ olacak şekilde seçelim. $((3a, p) = 1$ olduğundan bu mümkündür.)

$$\left. \begin{array}{l} p|3an_0 + b \Rightarrow p|3abn_0 + b^2 \\ p|b^2 - 3ac \end{array} \right\} \Rightarrow p|3abn_0 + 3ac$$

$$\Rightarrow p|3a(bn_0 + c) \Rightarrow p|bn_0 + c$$

bulunur.

Son olarak ;

$$p|bn_0 + c \text{ ve } p|3an_0^2 + bn_0 \text{ dan } p|B$$

elde edilir.

Benzer şekilde $p|A$, $p|B$ ve $p|27a^2d - 9abc + 2b^3$ kullanılarak $p|C$ yani $p|P(n_0)$ elde edilir. Diğer yandan n_0 sayısı $3an_0 + b \equiv 0 \pmod{p}$ 'yi gerçeklersek $3an + b \equiv 0 \pmod{p}$ 'yi gerçekleyen tüm n 'ler $n = kp + n_0$ formundadır. $P(x + n_0)$ yerine $P(x + kp + n_0)$ ötelemesi de yapılsa yine $p|B$ ve $p|C$ bulunur. Bu son öteleme için ne zaman $p^2|C$ olduğunu araştırmalıyız.

$$C \equiv P(n) \equiv 0 \pmod{p^2} \Rightarrow P(kp + n_0) \equiv 0 \pmod{p^2}$$

$$a(kp + n_0)^3 + b(kp + n_0)^2 + c(kp + n_0) + d \equiv 0 \pmod{p^2}$$

Yani; $kp(3an_0^2 + 2bn_0 + c) + P(n_0) \equiv 0 \pmod{p^2}$ ve sonuç olarak

$$kpB + P(n_0) \equiv 0 \pmod{p^2} \text{ olup } B \equiv 0 \pmod{p} \text{ den dolayı } P(n_0) \equiv 0 \pmod{p^2} \text{ elde edilir.}$$

O halde şu teoremi elde ederiz.

Teorem . $P(x) = ax^3 + bx^2 + cx + d$ primitif polinomu verilsin. Bir p asal sayısı için

$$(p, 3a) = 1 \text{ olup } p|(b^2 - 3ac, 27a^2d - 9abc + 2b^3) \text{ ve}$$

$3an_0 + b \equiv 0 \pmod{p}$ olsun. Eğer $P(n_0) \not\equiv 0 \pmod{p^2}$ ise $P(x)$ polinomu $\mathbb{Z}[x]$ üzerinde asaldır.

Uygulama : $P(x) = 2x^3 + 23x^2 + 74x + 54$ polinomunu alalım.

$$b^2 - 3ac = 23^2 - 3 \cdot 2 \cdot 74 = 85$$

$$27a^2d - 9abc + 2b^3 = 27 \cdot 4 \cdot 54 - 9 \cdot 2 \cdot 23 \cdot 74 + 2 \cdot 23^3 = -470 \quad \text{olup,}$$

$p = 5$ alabiliriz.

$$3 \cdot 2n_0 + 23 \equiv 0 \pmod{5} \Rightarrow n_0 \equiv -23 \equiv 2 \pmod{5} \quad \text{olup } n_0 = 2 \text{ için}$$

$$P(2) = 2 \cdot 2^3 + 23 \cdot 2^2 + 74 \cdot 2 + 54 \not\equiv 0 \pmod{5}$$

olduğundan $P(x)$ polinomu $Z[x]$ üzerinde asaldır.

Sonuç ve Tartışma :

$P(x) = ax^3 + bx^2 + cx + d$ ($a, b, c, d \in Z$) polinomu verilsin. Verilen p asal sayısı için $(p, 3a) = 1$ ve $p \mid (b^2 - 3ac, 27a^2d - 9abc + 2b^3)$ olsun. Eğer $3an_0 + b \equiv 0 \pmod{p}$ ve $P(n_0) \not\equiv 0 \pmod{p^2}$ ise $P(x)$ polinomu $Z[x]$ üzerinde asaldır. Bunun için 2. ve 3. dereceden primitif polinomlar, Eisenstein kriteri aracılığıyla asallığı incelenerek konu ile bağlantılı sorulara çözümler getirmede kullanılabilirliği ortaya konmuştur. Hemen hemen tüm elemanter sayılar teorisi kitaplarında Eisenstein kriteri verildikten sonra bazı polinomların asallığı $P(x+n)$ ötelemesi ile gösterilmiş. Fakat hangi "n" için $P(x+n)$ ötelemesinin sonuç vereceği hakkında bir bilgi verilmemiştir. Biz bu çalışmada öteleme yapmadan $P(x)$ polinomlarının asal olması için bir yeter koşul veriyoruz. Burada kullandığımız yöntem daha yüksek dereceli asal polinomlar için uygulanabilir ve polinomların asal olması için bir yeter şart polinomların katsayıları cinsinden verilebilir.

Kaynakça:

Landau, E: Elementary Number Theory, New York, 1958

Matematiksel buluşun itici gücü mantık değil hayal gücüdür.

Augustus de Morgan

Bir matematik problemine dalıp gitmekten daha saf bir zihinsel mutluluk yoktur.

Anonim