bulunur.

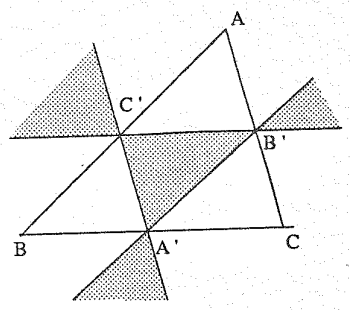
Bunlarda B^2 yi sola geçirerek elde edilen eşitlikler taraf tarafa çarpıldığında ve $AC \equiv B^2 - \Delta$ kullanıldığında kısaltmalardan sonra

$$(2x_0 - 1)(2y_0 - 1)\Delta + (2x_0 + 2y_0 - 1)B^2 = 0$$

$$\Rightarrow (2x_0 - 1)(2y_0 - 1)(2x_0 + 2y_0 - 1) + (2x_0 + 2y_0 - 1)^2(B^2/\Delta) = 0$$

$$\Rightarrow (2x_0 - 1)(2y_0 - 1)(2x_0 + 2y_0 - 1) = -(2x_0 + 2y_0 - 1)(B^2/\Delta) \geq 0$$

elde edilir. Bu eşitsizlik ise ABC nin $A'B'C'$ orta tam üçgeni ile ilgili taralı bölgeyi verir.



Şekil 44

EISENSTEIN KRİTERİ

Mefharet Alpseymen Kocatepe *

Bir polinomu çarpanlarına ayırmak veya çarpanlara ayrılamayacağını göstermek çoğunlukla zordur ve zaman alır. Bir polinomun ne zaman çarpanlara ayrılabileceğini veya ne zaman ayrılamayacağını söyleyen kriterlerin sayısı çok azdır. Bunlardan bir tanesi de ünlü Eisenstein kriteridir.

İsterseniz önce kısaca Eisenstein'dan sözedelim. Ferdinand Gotthold Max Eisenstein 1823-1852 yılları arasında yaşamıştır. Sayılar teorisi, cebir ve eliptik fonksiyonlar üzerinde önemli çalışmalar yapmıştır. Şimdi sözünü edeceğimiz kriteri 1850 yılında bulmuştur.

Şimdi de notasyonu ve terminolojiyi belirleyelim. $\mathbb{Z}[x]$ ile katsayıları $\mathbb{Z}$ kümesinde olan (yani tamsayılar olan) tüm polinomları gösterelim. Aynı şekilde $\mathbb{Q}[x]$ ile katsayıları rasyonel sayılar olan tüm polinomları gösterelim. Eğer $f(x) \in \mathbb{Z}[x]$ polinomu herbirinin derecesi en az 1 olan ve katsayıları tamsayı olan iki polinomun çarpımı şeklinde yazılabiliyorsa $f(x)$ polinomu $\mathbb{Z}[x]$ içinde *indirgenebilir*, aksi halde *indirgenemez* denir. Aynı tanım $\mathbb{Q}[x]$ için de verilebilir. Ayrıca $\mathbb{Z}[x] \subset \mathbb{Q}[x]$ olduğundan $\mathbb{Z}[x]$ in bir elemanının $\mathbb{Q}[x]$ içinde indirgenebilir veya indirgenemez olmasından da söz edilebilir.

Teorem (Eisenstein kriteri). p verilen bir asal sayı,

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

olsun. Eğer $a_n \not\equiv 0 \pmod{p}$,

$$a_{n-1} \equiv \cdots \equiv a_0 \equiv 0 \pmod{p}, \quad a_0 \not\equiv 0 \pmod{p^2}$$

ise, $f(x)$ polinomu $\mathbb{Z}[x]$ içinde indirgenemez.

Not. Bu kriter aslında $f(x)$ in $\mathbb{Q}[x]$ içinde indirgenemeyeceğini söyler. Bunu kanıtlamak da zor değildir.

Kanıt. İddianın doğru olmadığını varsayalım. O zaman $b_i, c_i \in \mathbb{Z}$ olmak üzere

$$f(x) = (b_m x^m + \cdots + b_1 x + b_0)(c_k x^k + \cdots + c_1 x + c_0)$$

şeklinde yazılabilir ($m \geq 1$, $k \geq 1$ ve $n = m + k$.) Katsayılara bakarak $a_0 = b_0 c_0$ olur. $a_0 \equiv 0 \pmod{p}$ ve p asal olduğu için $b_0 \equiv 0 \pmod{p}$ veya $c_0 \equiv 0 \pmod{p}$ olmak zorundadır. $a_0 \not\equiv 0 \pmod{p^2}$ olduğu için de bunların her ikisi birden doğru olamaz. Genelliği bozmadan $c_0 \equiv 0 \pmod{p}$ ve $b_0 \not\equiv 0 \pmod{p}$ olduğunu varsayalım. $a_n = b_m c_k \not\equiv 0 \pmod{p}$ olduğu için $c_k \not\equiv 0 \pmod{p}$ olmak zorundadır ve $c_j \not\equiv 0 \pmod{p}$ özelliğini sağlayan j indislerinin en küçüğünden söz edebiliriz. Bu en küçük indisi

* Bilkent Üniversitesi Matematik Bölümü öğretim üyesi

r ile gösterelim. $c_0 \equiv 0 \pmod{p}$ olduğundan, $1 \leq r$ ve

$$c_{r-1} \equiv \cdots \equiv c_0 \equiv 0 \pmod{p}$$

olur. Bu durumda

$$a_r = b_0 c_r + b_1 c_{r-1} + \cdots + b_r c_0 \equiv b_0 c_r \pmod{p}.$$

$b_0 \not\equiv 0 \pmod{p}$ ve $c_r \not\equiv 0 \pmod{p}$ olduğu için $a_r \not\equiv 0 \pmod{p}$ olmak zorundadır. Hipoteze göre bu koşulu sağlayan tek katsayı a_n olduğundan, $r = n$ bulunur. Buradan da

$$n = m + k > k \geq r = n$$

çelişkisi çıkar.

Örnekler. 1. $f(x) = x^3 + 2x^2 + 4x + 2$. Burada $a_3 = 1$, $a_2 = 2$, $a_1 = 4, a_0 = 2$ dir. $p = 2$ asal sayısına göre

$$a_3 \not\equiv 0 \pmod{p}, \quad a_2 \equiv a_1 \equiv a_0 \equiv 0 \pmod{p},$$

$$a_0 \not\equiv 0 \pmod{p^2}$$

olduğundan Eisenstein kriterini uygulayarak $f(x)$ polinomunun $\mathbb{Z}[x]$ içinde indirgenemeyeceğini buluruz.

2. $f(x) = x^3 + 2x^2 + 2x + 4$. Bu polinomun katsayıları 1,2,2,4 tür. 2,2,4 ü bölen tek asal sayı $p = 2$ dir. Ancak $4 \equiv 0 \pmod{p^2}$ olduğundan bu polinoma Eisenstein kriterini uygulayabilmemiz mümkün değildir. Ama tabii ki bu durum bu polinomun $\mathbb{Z}[x]$ içinde indirgenebileceği anlamına gelmez. Ancak deneyerek

$$\begin{aligned} f(x) &= x^3 + 2x^2 + 2x + 4 \\ &= x^2(x+2) + 2(x+2) \\ &= (x^2+2)(x+2) \end{aligned}$$

bulunduğundan $f(x)$ polinomu $\mathbb{Z}[x]$ içinde indirgenebilir.

3. $f(x) = x^7 - 47$. Burada katsayılar $1, 0, 0, 0, 0, 0, 0, -47$ olduğundan $p = 47$ asal sayısı ile kriterimizi uygulayabilir ve polinomun $\mathbb{Z}[x]$ içinde indirgenemez olduğunu görürüz.

4. $f(x) = x^4 + 15$. Burada da kriterimizi $p = 3$ veya $p = 5$ asal sayısı ile uygulayabiliriz.

5. p bir asal sayı olmak üzere

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

olsun. Polinomun bu şekline Eisenstein kriterinin uygulanamayacağı açıkça görülür. Ancak $f(x) = \dfrac{x^p - 1}{x - 1}$ olduğunu gözleyerek ve $x = y + 1$ tanımlayarak

$$\begin{aligned} f(x) &= \frac{(y+1)^p - 1}{y} \\ &= \frac{1}{y}\left\{\sum_{j=0}^{p} \binom{p}{j} y^{p-j} - 1\right\} \\ &= \sum_{j=0}^{p-1} \binom{p}{j} y^{p-1-j} \\ &= y^{p-1} + py^{p-2} + \frac{p(p-1)}{2} y^{p-3} \\ &\quad + \cdots + p \\ &\overset{\text{tanım}}{=} g(y) \end{aligned}$$

$g(y)$'nin ilki hariç bütün katsayıları p asal sayısı ile bölünebilir. Bunun nedenini görmek için bu katsayıların herbirinin payında p çarpanı olduğunu ve paydasındaki sayıların da p den küçük tamsayıların çarpımı olduğunu ve dolayısıyla p ile sadeleşemeyeceğini gözlemek yeterlidir. $g(y)$ polinomunun Eisenstein kriterinin diğer koşullarını sağladığı açıkça görüldüğünden, $g(y)$ polinomu $\mathbb{Z}[y]$ içinde indirgenemez. Buradan da $f(x)$ in indirgenemediği çıkar. Aksi olsaydı, yani $f(x) = f_1(x) f_2(x)$ şeklinde yazılabilseydi,

$$g(y) = f(x+1) = f_1(x+1) f_2(x+1) = f_1(y) f_2(y)$$

olacağından $g(y)$ indirgenebilecekti.

Bu kriterin bir de genelleştirilmiş bir şekli vardır. Şimdi d ondan söz edelim.

Teorem (Genelleştirilmiş Eisenstein kriteri). $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ olsun. Bir p asal sayısı ve $\ell < n$ için,

$$a_n \not\equiv 0, \; a_\ell \not\equiv 0, \; a_{\ell-1} \equiv \cdots \equiv a_0 \equiv 0 \pmod{p}$$

$$a_0 \not\equiv 0 (\mathrm{mod} p^2)$$

ise $\mathbb{Z}[x]$ içinde, $f(x)$ indirgenemez veya $f(x)$ in derecesi en az ℓ olan ve indirgenemeyen bir çarpanı vardır.

Kanıt. $f(x)$ indirgenebilirse, $m \geq 1$, $k \geq 1$ ve $b_i, c_i \in \mathbb{Z}$ olmak üzere

$$\begin{aligned} f(x) &= \underbrace{(b_m x^m + \cdots + b_1 x + b_0)}_{g_1(x)} \\ &\quad \underbrace{(c_k x^k + \cdots + c_1 x + c_0)}_{f_1(x)} \\ &= g_1(x) f_1(x) \end{aligned}$$

olsun. Önceden olduğu gibi genelliği bozmadan, $b_0 \not\equiv 0 \pmod{p}$ ve $c_0 \equiv 0 \pmod{p}$ olsun.

$$c_1 b_0 + c_0 b_1 = a_1 \equiv 0 \pmod{p}$$

ve

$$b_0 \not\equiv 0 \pmod{p}, \quad c_0 \equiv 0 \pmod{p}$$

olduğundan $c_1 \equiv 0 \pmod{p}$ bulunur. Bu şekilde sırayla $a_2, \ldots, a_{\ell-1}$ i yazarak,

$$c_0 \equiv c_1 \equiv \cdots \equiv c_{\ell-1} \equiv 0 \pmod{p}$$

bulunur. Ayrıca $b_m c_k = a_n \not\equiv 0 \pmod{p}$ olduğundan,

$$c_k \not\equiv 0 \pmod{p}.$$

Böylece $k \leq \ell - 1$ olamayacağı hemen görülür. Demek ki $k \geq \ell$ olmak zorunda.

$k = \ell$ olursa kriterin ilk şekli $f_1(x)$'e uygulanabilir ve $f_1(x)$ in indirgenemez olduğu görülür (derece $f_1(x) = \ell$).

$k > \ell$ ise

$$a_\ell = c_\ell b_0 + c_{\ell-1} b_1 + \cdots \equiv c_\ell b_0 \pmod{p}$$

ve $a_\ell \not\equiv 0 \pmod{p}$ olduğu için $c_\ell \not\equiv 0 \pmod{p}$ bulunur. Bu durumda $f_1(x) = c_k x^k + \cdots + c_1 x + c_0$ olup $k > \ell$ için,

$$c_k \not\equiv 0, \; c_\ell \not\equiv 0, \; c_{\ell-1} \equiv \cdots \equiv c_0 \equiv 0 \pmod{p},$$

$$c_0 \not\equiv 0 \pmod{p^2}$$

sağlandığından, şimdiye kadar $f(x)$ için yaptıklarımızı $f_1(x)$ için yapabiliriz. $f_1(x)$ indirgenemez ise teorem kanıtlanmış olur, indirgenebilirse $f_2(x)$ şekil olarak $f_1(x)$ ve $f(x)$ e benzemek üzere

$$f_1(x) = g_2(x) f_2(x)$$

olarak yazabiliriz ve bu süreci devam ettiririz. Ancak

$$\begin{aligned} \ell &\leq \text{derece} f_i(x) < \text{derece} f_{i-1}(x) \\ &< \cdots < \text{derece} f_1(x) \end{aligned}$$

olduğundan, bu süreç bir yerde bitmek zorundadır. j'nci adımda biterse

$$\begin{aligned} f(x) &= g_1(x) f_1(x) = g_1(x) g_2(x) f_2(x) \\ &= \cdots = g_1(x) g_2(x) \cdots g_j(x) f_j(x) \end{aligned}$$

şeklinde yazılır. Burada $f_j(x)$ indirgenemez ve derecesi de en az ℓ dir.

Örnek. 1993 Uluslararası Matematik Olimpiyatı, birinci sorusunu hatırlayalım. Bu yazımızdaki terminolojiyle ifade edersek bu soruda $n > 1$ iken $f(x) = x^n + 5x^{n-1} + 3$ polinomunun $\mathbb{Z}[x]$ içinde indirgenemeyeceğini göstermemiz isteniyordu. Eisenstein kriterinin ilk şekli bu soruya uygulanamaz, fakat genelleştirilmiş şekli uygulanabilir. $p = 3$ asal sayısı ve $\ell = n - 1$ sayısı için teoremin hipotezi sağlanır. Teoreme göre $f(x)$ indirgenemez veya derecesi en az $n - 1$ olan indirgenemeyen bir $g(x)$ çarpanı vardır. $g(x)$ in derecesi n ise $g(x) = f(x)$ olmak zorundadır. $g(x)$ in derecesi $n - 1$ ise $f(x)$ in aynı zamanda derecesi 1 olan bir çarpanı, yani rasyonel bir kökü vardır. Bu rasyonel kök $\dfrac{\mp 3}{\mp 1} = \mp 3$ olmak zorundadır. Fakat $f(3) \neq 0$ ve $f(-3) \neq 0$ olduğu kolayca görüldüğünden, $f(x)$ in derecesi $n - 1$ olan ve indirgenemeyen çarpanı yoktur. Bu durumda geriye bir tek seçenek kalmaktadır. O da $f(x)$ in indirgenemez olduğudur.