$z^n + z^{n-1} + \ldots + z + 1$ POLİNOMUNUN İLGİNÇ BİR ÖZELLİĞİ

Sofia Ostrovska
Ege Üniversitesi, Matematik Bölümü, 35100-İZMİR

Bu yazımızda, başlıkta geçen ve "siklotomik polinom" diye adlandırılan polinomlar hakkında ilginç bir teoremin ispatını vereceğiz. Oldukça basit ve güzel olan bu teorem aynı zamanda az bilinmektedir. Çünkü olasılık teorisinin çok özel bir dalında bulunur ([1]). Bu dala "rasgele değişkenlerin ve vektörlerin parçalanması" denir.

Problemin içeriği şöyledir: $P_n(z) = 1 + z + \ldots + z^n$, bir *siklotomik* polinom olsun. Hangi n 'ler için, $P_n(z)$ polinomu, $Q(z)$ ve $R(Z)$ sabitten farklı, katsayıları negatif olmayan polinomlar olmak üzere, $P_n(z) = Q(z)R(z)$ şeklinde gösterilebilir?

Fransız matematikçi *Mark Krasner* ve Rus matematikçi *Dmitriy Raikov*, 1937 yılında birbirlerinden habersiz, bu problemin çözümünü bulmuşlardır. Gerek ve yeter koşul $(n+1)$ sayısının bir bileşik sayı olmasıdır (yani, asal sayı olmamasıdır).

Bu yazıda **Krasner-Raikov Teoreminin** tam kanıtını vereceğiz.

Önce siklotomik polinomların bazı özelliklerini inceleyelim:

Özellik 1.

$$P_n(z) = \frac{1 - z^{n+1}}{1 - z}.$$

Kanıt. $P_n(z)(1-z)$ çarpımını hesaplarsak, $(1 + z + \ldots + z^n)(1 - z) = 1 - z^{n+1}$ elde edilir.

Özellik 2. $P_n(z)$ siklotomik polinomunun kökleri

$$\zeta_1 = e^{i\frac{2\pi}{n+1}}, \zeta_2 = e^{i\frac{4\pi}{n+1}}, \ldots, \zeta_n = e^{i\frac{2\pi n}{n+1}} \text{ 'dir.}$$

Kanıt. $1 - z^{n+1}$ polinomunun köklerinin 1 'in $(n+1)$. dereceden tüm kökleri olduğu iyi bilinmektedir. Demek ki, $z^{n+1} - 1 = (z-1)(z-\zeta_1)\ldots(z-\zeta_n)$ 'dir. Özellik 1 'den $P_n(z) = (z-\zeta_1)\ldots(z-\zeta_n)$ elde edilir. Böylece $P_n(z)$ polinomunun tüm kökleri $\zeta_1, \ldots, \zeta_n$ 'dir.

Bundan dolayı, $P_n(z)$ siklotomik polinomunun tüm kökleri, 1 'in 1 'den farklı $(n+1)$. dereceden kökleri olur.

Özellik 3. Eğer ζ, $P_n(z)$ siklotomik polinomunun kökü ise, $\frac{1}{\zeta}$ de $P_n(z)$ 'nin kökü olur.

Kanıt. Eğer $P_n(\zeta) = 0$ ise, $P_n(\frac{1}{\zeta}) = 1 + \frac{1}{\zeta} + \ldots + \frac{1}{\zeta^n} = \frac{P_n(\zeta)}{\zeta^n} = 0$ eşitliğini kolayca görürüz.

Son özellik bütün *simetrik polinomlar* için geçerlidir.

Tanım. $f(z) = a_0 + a_1 z + \ldots + a_n z^n$ $(a_n \neq 0)$, bir polinom olsun. Eğer her $j = 0, \ldots, n$ için $a_{n-j} = a_j$ ise, $f(z)$ 'ye *simetrik* bir polinom denir.

Örneğin, $f(z)=1+5z+z^2$, $f(z)=4+3z+3z^2+4z^3$ ve $f(z)=1+\binom{n}{1}z+\binom{n}{2}z^2+\ldots+\binom{n}{n-1}z^{n-1}+z^n$ simetrik polinomlardır.

Simetrik polinomlara ait bazı önermelere bakalım:

Önerme 1. $f(z)$ simetrik bir polinom olsun. Eğer ζ bu polinomun kökü ise, $\frac{1}{\zeta}$ de $f(z)$ 'nin kökü olur.

Kanıt. Eğer $f(z)$ simetrik bir polinom ise, $f(\frac{1}{z})=\frac{f(z)}{z^n}$ olur. Buradan $f(\zeta)=0$ ise, $f(\frac{1}{\zeta})=0$ olduğu kolayca elde edilir.

Önerme 2. Simetrik polinomların çarpımı da simetrik polinomdur.

Kanıt.

$$f(z)=a_0+a_1z+\ldots+a_{l-1}z^{l-1}+a_lz^l \quad (a_l\neq 0),$$

$$g(z)=b_0+b_1z+\ldots+b_{m-1}z^{m-1}+b_mz^m \quad (b_m\neq 0),$$

simetrik polinomlar olsun, yani $a_j=a_{l-j}$ $(j=0,1,\ldots,l)$ $b_k=b_{m-k}(k=0,1,\ldots,m)$.

$l\leq m$ olduğunu kabul edelim.

$$f(z)g(z)=(a_0+a_1z+\ldots+a_{l-1}z^{l-1}+a_lz^l)(b_0+b_1z+\ldots+b_{m-1}z^{m-1}+b_mz^m)$$

çarpımına bakalım ve z^i, z^{l+m-i} 'nin katsayılarını bulalım.

Önce $0\leq i\leq l$ olsun. z^i 'nin katsayısı $a_ib_0+\ldots+a_0b_i$ 'dir ve z^{l+m-i} 'nin katsayısı $a_{l-i}b_m+\ldots+a_lb_{m-i}=a_ib_0+\ldots+a_0b_i$ 'dir. Buna göre $0\leq i\leq l$ için z^i ve z^{l+m-i} 'nin katsayıları eşittir.

Aynı şekilde $l+1\leq i\leq m$ için önermeyi kanıtlayabiliriz.

Önerme 3. $f(z)$ bir polinom ve $f(1)\neq 0$ olsun. $f(z)$ polinomunun her ζ karmaşık kökü için $\frac{1}{\zeta}$ da $f(z)$ 'nin aynı katlı kökü olsun. Bu durumda $f(z)$ simetrik bir polinomdur.

Kanıt. Verilen şartlar altında $f(z)$ polinomu

$$f(z)=(z+1)^{r_0}(z-\zeta_1)^{r_1}(z-\frac{1}{\zeta_1})^{r_1}\ldots(z-\zeta_k)^{r_k}(z-\frac{1}{\zeta_k})^{r_k}$$

şeklinde yazılabilir, burada $r_0\geq 0, r_1,\ldots,r_k>0$ tamsayıları köklerin katlarıdır. Böylece $f(z)=(z+1)^{r_0}p_1^{r_1}(z)\ldots p_k^{r_k}(z)$, burada

$$p_j(z)=(z-\zeta_j)\left(z-\frac{1}{\zeta_j}\right)=z^2-\left(\zeta_j+\frac{1}{\zeta_j}\right)z+1 \quad (j=1,\ldots,k)$$

'dır. $(z+1)$ ve tüm $p_j(z)$ $(j=1,\ldots,k)$ 'lerin simetrik polinomlar oldukları kolayca görülür. Önerme 2 'ye göre $f(z)$, simetrik polinomların çarpımı olarak, kendisi de simetriktir.

Şimdi siklotomik polinomunun çarpanlarının bulunması problemine dönelim ve aşağıdaki temel teoremi inceleyelim:

Teorem 1 (Krasner-Raikov Teoremi). Bir $P_n(z) = 1 + z + \ldots + z^n$ siklotomik polinomunun,

$$Q(z) = 1 + a_1 z + \ldots + a_l z^l,$$

$$R(z) = 1 + b_1 z + \ldots + b_m z^m$$

ve $a_i \geq 0$, $b_j \geq 0$, $a_l b_m \neq 0$ olmak üzere $P_n(z) = Q(z)R(z)$ şeklinde gösterilebileceğini varsayalım.

O zaman a_i, b_j katsayılarının her biri ya 0 ya da 1 'e eşittir.

Kanıt. ζ, $P_n(z)$ polinomunun bir kökü olsun. O halde ζ, $Q(z)$ veya $R(z)$ polinomunun köküdür. Örneğin, $Q(\zeta) = 0$ dır. O zaman $Q(\overline{\zeta}) = 0$ olur çünkü $Q(z)$ polinomunun tüm katsayıları gerçeldir. Siklotomik polinomların 2.özelliğinden, ζ 'nın, 1 'in 1 'den farklı kökü olduğunu biliyoruz. Böylece $\overline{\zeta} = \frac{1}{\zeta}$ 'dır ve Önerme 3, $Q(z)$ 'nin simetrik bir polinom olduğunu gösteriyor. Aynı şekilde $R(z)$ 'nin de simetrik bir polinom olduğunu gösterebiliriz. Buradan $a_l = b_m = 1$ elde edilir. $Q(z)$ ve $R(z)$ polinomlarının derecelerinin eşit olmayacağına dikkat edelim. Gerçekten, eğer $l = m$ ise, z^l 'nin katsayısı $b_l + a_1 b_{l-1} + \ldots + a_l = 2 + \ldots \geq 2$ olur, fakat bu mümkün değildir. Genelliği bozmadan $l < m$ olduğunu kabul edebiliriz. $P_n(z)$ ve $Q(z)R(z)$ 'deki z^j teriminin katsayılarını karşılaştıralım:

$$1 = a_j + a_{j-1} b_1 + \ldots + a_1 b_{j-1} + b_j, \quad 1 \leq j \leq l-1, \tag{0.1}$$

$$1 = 1 + a_{l-1} b_1 + \ldots + a_1 b_{l-1} + b_l, \tag{0.2}$$

$$1 = b_j + a_1 b_{j-1} + \ldots + a_{l-1} b_{j-l+1} + b_{j-l}, \quad l+1 \leq j \leq m-1 \tag{0.3}$$

elde edilir.

Formül (0.2) 'ye göre $a_{l-1} b_1 + \ldots + a_1 b_{l-1} + b_l = 0$ 'dır. Öte yandan, tüm terimler negatif olmadığından $a_{l-1} b_1 = a_{l-2} b_2 = \ldots = a_1 b_{l-1} = b_l = 0$ veya

$$a_1 b_1 = a_2 b_2 = \ldots = a_{l-1} b_{l-1} = b_l = 0 \quad \text{'dır.} \tag{0.4}$$

(Burada $a_i = a_{l-i}$ eşitliklerini kullanıyoruz.)

Formül (0.1) 'de $j = 1$ alalım. Formül (0.4) 'ü kullanarak aşağıdaki denklemler elde edilir: $a_1 + b_1 = 1$, $a_1 b_1 = 0$. Böylece a_1 ve b_1 'in biri 0 diğeri 1 'dir.

Kanıta tümevarımla devam edeceğiz.

$j = 1$ için önermenin doğruluğunu kanıtladık.

$j \leq k < l-1$ için doğru olsun. Yani $a_1, \ldots, a_k$, $b_1, \ldots, b_k$ ya 0 ya da 1 'e eşittir. Formül (0.1) 'e göre $a_{k+1} + b_{k+1}$ bir tamsayıdır ve $0 \leq a_{k+1} + b_{k+1} \leq 1$ 'dir. Formül (0.4) 'ten ise $a_{k+1} . b_{k+1} = 0$ 'dır. Sonuçta, a_{k+1} ve b_{k+1} ya 0 ya da 1 'e eşittir. Böylece tümevarım tamamlanır.

$a_1, \ldots, a_{l-1}$, $b_1, \ldots, b_{l-1}$ katsayılarının ya 0 ya da 1 'e eşit oldukları kanıtlandı.

$a_l = 1$, $b_l = 0$ olduğu için $b_{l+1}, \ldots, b_{m-1}$ katsayılarına bakmamız gerekmektedir.

$j = l+1$ için Formül (0.3) 'e göre

$$1 = b_{l+1} + a_1 b_l + \ldots + a_{l-1} b_2 + b_1 ,$$

dolayısıyla b_{l+1} bir tamsayıdır ve $0 \leq b_{l+1} \leq 1$. Onun için b_{l+1} ya 0 ya da 1 'dir. Tekrar tümevarım kullanarak b_j 'nin $(1 \leq j \leq m)$, ya 0 ya da 1 'e eşit olduğu elde edilir.

Teorem 2. $P_n(z)$ siklotomik polinomunun, sabitten farklı, katsayıları negatif olmayan polinomların çarpımı olması için gerek ve yeter koşul $(n+1)$ 'in asal sayı olmamasıdır.

Kanıt. (1) $(n+1)$ 'in asal sayı olmadığını kabul edelim. O zaman $n+1 = lm$ olur ($l, m \neq 1$ pozitif tamsayılardır). Şimdi

$$P_n(z) = \frac{1-z^{lm}}{1-z^l}\,\frac{1-z^l}{1-z}$$

yazılabilir. $Q(z) = \frac{1-z^{lm}}{1-z^l} = 1 + z^l + z^{2l} + \ldots + z^{l(m-1)}$ ve $R(z) = \frac{1-z^l}{1-z} = 1 + z + \ldots + z^{l-1}$ teoremin koşullarını sağlayan polinomlardır.

(2) $n+1$ bir asal sayı olsun.

$P_n(z) = \tilde{Q}(z)\tilde{R}(z)$, $\tilde{Q}(z)$ ve $\tilde{R}(z)$, sabitten farklı, katsayıları negatif olmayan polinomlar olsun. O zaman $\tilde{Q}(0)\tilde{R}(0) = P_n(0) = 1$ ve

$$P_n(z) = \frac{\tilde{Q}(z)\tilde{R}(z)}{\tilde{Q}(0)\tilde{R}(0)} \tag{0.5}$$

yazabiliriz.

$$Q(z) = \frac{\tilde{Q}(z)}{\tilde{Q}(0)}, \quad R(z) = \frac{\tilde{R}(z)}{\tilde{R}(0)}$$

alalım.

Bu polinomlar sabitten farklı polinomlar olup

$$Q(z) = 1 + a_1 z + \ldots + a_l z^l,$$

$$R(z) = 1 + b_1 z + \ldots + b_m z^m$$

şeklindedir. Burada $a_i \geq 0$ $(i = 1, \ldots, l)$, $b_j \geq 0$ $(j = 1, \ldots, m)$ $a_l b_m \neq 0$ 'dır. Ayrıca formül (5) 'e göre $P_n(z) = Q(z)R(z)$ 'dir. Teorem 1 'i kullanarak a_i ve b_j 'nin ya 0 ya da 1 'e eşit olduğunu görürüz. Onun için $Q(1)$ ve $R(1)$, 1 'den büyük pozitif tamsayılar olur.

$$n + 1 = P_n(1) = Q(1)R(1)$$

eşitliğinden çelişki elde ederiz, çünkü $n+1$ bir asal sayıdır.

KAYNAKÇA

[1] Linnik Ju.V., Ostrovskii I.V., *Decomposition of Random Variables and Vectors*, Amer. Math. Soc., Providence, R.I., 1977.