POLİNOMLARIN ASAL BÖLENLERİ (*)

Metehan Aydın
Özel Samanyolu Lisesi

Tamsayı katsayılı polinomlarla tamsayılar arasında belirgin bir ilişki vardır. Bu ilişkiyi kısaca açıklama gerekirse tamsayılarda asallarla, dolayısıyla çarpma işlemiyle ilgili özellikler tamsayı katsayılı polinomlarda indirgenemez polinomlarla ortaya çıkar.

Sözgelimi **Aritmetiğin Temel Teoremi** olarak bilinen bir tamsayının asal sayıların çarpımı olarak tek türlü ifade edilmesi, tamsayı katsayılı polinomlarda farklı bir şekilde yine karşımıza çıkar. Bu benzerliğin oluşmasında polinomun bir fonksiyon olarak sahip olduğu özelliklerin katkısı yoktur. Bu benzerlik tamamiyle cebirseldir.

Yani; $n \geq m$, $a_n \neq 0$, $b_m \neq 0$ olmak üzere

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$$

ve

$$Q(x) = b_m x^m + b_{m-1}x^{m-1} + ... + b_1 x + b_0$$

polinomları yerine

$$A = (..., 0, 0, ..., a_n, a_{n-1}, ..., a_1, a_0)$$

ve

$$B = (..., 0, 0, ..., b_m, b_{m-1}, ..., b_1, b_0)$$

dizilerini düşünerek

$$AB = (..., 0, 0, ..., c_{m+n+1}, c_{m+n}, ..., c_1, c_0)$$

$$c_k = \sum_{i=0}^{k} a_i b_{k-i}$$

şeklinde bir çarpma işlemi ve

$$A + B = (..., 0, 0, ..., 0, a_n + b_n, ..., a_0 + b_0)$$

$n = m$ için ;

$$A + B = (..., 0, 0, ..., a_n, ..., a_m + b_m, ..., a_0 + b_0)$$

$n > m$ için ;

şeklinde bir toplama işlemi tanımlandığında; bu dizilerin oluşturduğu kümenin tüm elemanlarını, cebirsel özelliklerini koruyarak, polinomlar kümesine bire-bir ve örten bir şekilde eşleyebiliriz; yani polinomların çarpma işlemi vasıtasıyla ortaya çıkan özellikleri nedeniyle sayı dizilerinden bir farkı yoktur. Dolayısıyla polinomun bir fonksiyon olarak hangi tamsayı noktasında hangi değerleri alıyor olmasının, polinomların tamsayılarla ilişkilendirilmesi konusunda etkisi yoktur.

Hazırlanan bu projede tamsayı katsayılı polinomların fonksiyon olarak tamsayı noktalarında aldığı değerlerin de, tamsayıların çarpma işlemiyle belirlenen cebirsel özellikleriyle ilişkili olduğu gösterilecek

Projenin hazırlanmasına esin kaynağı olan soru şu şekildedir :

SORU: $P(x)$ tamsayı katsayılı sabit olmayan bir polinom olsun. $P(x)$'in sonsuz sayıda asal böleni bulunduğunu gösteriniz(Bu soru projenin geri kalanında da sık kullanılacağı için (**) ile ifade edilsin)

YANIT: $P(b) = p_1^{\alpha_1}.p_2^{\alpha_2}...p_k^{\alpha_k}$ olsun. Bezout teoreminden,

$$n.p_1^{\alpha_1+1}.p_2^{\alpha_2+1}...p_k^{\alpha_k+1} | P(p_1^{\alpha_1+1}.p_2^{\alpha_2+1}...p_k^{\alpha_k+1}.n + b) - P(b)$$

olduğunu ve dolayısıyla

$$p_1^{\alpha_1+1}.p_2^{\alpha_2+1}...p_k^{\alpha_k+1} | P(p_1^{\alpha_1+1}.p_2^{\alpha_2+1}...p_k^{\alpha_k+1}.n + b) - P(b)$$

olduğunu biliyoruz. Buradan da

$$p_1^{\alpha_1}.p_2^{\alpha_2}...p_k^{\alpha_k} | P(b)$$

ise

$$p_1^{\alpha_1}.p_2^{\alpha_2}...p_k^{\alpha_k} | P(p_1^{\alpha_1+1}.p_2^{\alpha_2+1}...p_k^{\alpha_k+1}.n + b)$$

ve

$$P(p_1^{\alpha_1+1}.p_2^{\alpha_2+1}...p_k^{\alpha_k+1}.n + b) = p_1^{\alpha_1}.p_2^{\alpha_2}...p_k^{\alpha_k}.x_n$$

olarak yazabiliriz.

Ayrıca x_n ; $p_1, p_2, ..., p_k$ dan farklı olarak 0 veya ± 1 ise $p_1^{\alpha_1+1}.p_2^{\alpha_2+1}...p_k^{\alpha_k+1}.n + b$ arttığı için bu durumlarda $P(x)$ polinomu sabit olur. Bu da polinomun verilişiyle çelişir.

Şimdi x_n ; $p_1, p_2, ...p_k$ dan birine eşit olduğunda, örneğin genelliği bozmadan, $x_n = p_1$ olarak alalım. Bu durumda $p_1^{\alpha_1+1} | P(p_1^{\alpha_1+1}.p_2^{\alpha_2+1}...p_k^{\alpha_k+1}.n + b)$ ve $p_1^{\alpha_1+1} | P(b)$ olur. Bu da $P(b)$ yi kabulümüzle çelişir. O halde $P(x)$ in sonsuz tane farklı asal böleni vardır.

SORU : $P(x) = ax^2 + bx + c$ polinomunun her tamsayıdaki değeri bir tamsayının karesine eşitse, her $x \in R$ için, $P(x) = (dx + e)^2$ sağlanacak biçimde d ve e tamsayılarının varlığını kanıtlayınız.

Yukarıdaki sorunun yanıtını [1]'de bulabilirsiniz. Bu sorunun genel şeklinin ifadesi aşağıda verilmiştir.

SORU: $P(x)$ polinomu eğer her tamsayı x değeri için bir tamsayının m. kuvveti oluyorsa; $P(x)$ in bir rasyonel katsayılı polinomun m. kuvveti olduğunu ispat ediniz.

Bu soruda, polinomun tamsayı noktalarında aldığı değerlerin her zaman tamsayının m. kuvveti olabilmesi için gerek ve yeter koşul, her n tamsayısı için, $p \,|P(n)$ ve p asalı için p nin $P(n)$ yi bölen en büyük kuvvetinin m ile bölünüyor olmasıdır. Bu bize, polinomların, bir fonksiyon olarak düşünüldüğünde, asal sayılarla ilşkisini kurmamızı sağlayan ilk soruyu hatırlatır. Şimdi çözümünü başta yaptığımız ilk soruyu kullanarak genel halini çözelim. Öncelikle sorunun yanıtına yardımcı olacak birkaç iddiayı ispatlayalım.

İDDİA 1 : $P(x)$ ve $Q(x)$ aralarında asal tamsayı katsayılı polinomlar olsun. $(P(n), Q(n))$ ni bölmeyen fakat $[P(n), Q(n)]$ i bölen asal sayı bulunacak şekilde sonsuz sayıda n bulunabilir.

İSPAT : $P(x)$ ve $Q(x)$ aralarında asal olduğu için; Euclid Algoritmasından $p(x).P(x) + q(x).Q(x) = m$ olacak şekilde tamsayı katsayılı $p(n)$ ve $q(n)$ polinomları vardır. $(m \in Z - 0)$. Bu ifade de

$(P(n), Q(n))|m$, yani $(P(n), Q(n))$ nin sonlu sayıda asal böleni vardır, fakat (**) dan dolayı $P(n)$ nin $(n = 1, 2, ...)$ sonsuz sayıda asal böleni vardır. O halde $P(n)$ i bölen dolayısıyla $[P(n), Q(n)]$ ni bölen asalların bulunmasını sağlayan sonsuz sayıda n vardır.

İDDİA 2 : $P(x)$ indirgenemeyen, tamsayı katsayılı ve sabit olmayan bir polinom olsun. Bu durumda

$$P(n) \equiv 0 \pmod{p}$$

ve

$$P(n) \not\equiv 0 \pmod{p^2}$$

olacak şekilde bir p asalının bulunmasını olanaklı kılacak sonsuz tane n sayısı bulunabilir.

İSPAT : $P(x)$ ve $P'(x)$ aralarında asal olmalıdır. Çünkü $P(x)$ indirgenemezdir. (**) dan dolayı $P(n)$ yi bölen sonsuz sayıda asal sayı olduğunu ve "İDDİA 1" den dolayı da bunlardan ancak sonlu tanesinin $(P(n), P'(n))$ ni böldüğünü biliyoruz. Yani $P(n) \equiv P(n+p) \equiv 0 \pmod{p}$ ve $P'(n) \not\equiv 0 \pmod{p}$ olacak şekilde sonsuz sayıda p asalı ve bu p asalına bağlı belirlenebilen n tamsayısı vardır. Şimdi

$$P(n+p) - P(n) \equiv p \cdot P'(n) \pmod{p^2}$$

olduğunu gösterelim. Eğer $P(n) = a_m n^m + a_{m-1} n^{m-1} + ... + a_2 n^2 + a_1 n + a_0$ ise

$$P(n+p) - P(n) = a_m((n+p)^m - n^m) + a_{m-1}((n+p)^{m-1} - n^{m-1}) + ... + a_1((n+p) - n)$$

olur. Diğer yandan

$$(n+p)^k - n^k = \binom{k}{k-1} n^{k-1}p + \binom{k}{k-2} n^{k-2}p^2 + ... + \binom{k}{1} np^{k-1} + \binom{k}{0} p^k \equiv p.k.n^{k-1} \pmod{p^2}$$

eşitliğini kullanarak

$$P(n+p) - P(n) = \sum_{k=1}^{m} a_k((n+p)^k - n^k) \equiv \sum_{k=1}^{m} p.k.a_k.n^{k-1} \pmod{p^2}$$

denkliğini elde ederiz.

Öte yandan

$$\sum_{k=1}^{m} a_k.k.n^{k-1} = P'(n)$$

olduğu için

$$P(n+p) - P(n) \equiv p.P'(n) \pmod{p^2}$$

denkliğini ispatlamış oluruz.

O halde $P(n+p)$ ve $P(n)$ aynı anda p^2 ile bölünüyor olamaz; yani p asalı $P(n)$ yi bölecek, $P'(n)$ ni bölmeyecek şekilde seçilirse-böyle sonsuz tane p ve n sayısının bulunabileceğini "İDDİA 1" de gösterdik - ya $P(n)$ ya da $P(n+p)$, p ile bölünür fakat p^2 ile bölünmez.

İDDİA 3 : Tamsayı katsayılı $P(x)$ polinomunu indirgenemez çarpanlarına ayırdığımızı farzedelim. Bu çarpanlardan derecesi en küçük olanın derecesi m olsun. $p^m|P(n)$ ve "p^{m+1}, $P(n)$ yi bölmez" olacak şekilde sonsuz sayıda p asalı ve buna bağlı olarak n bulunabilir.

İSPAT : $P(x) = [R(X)]^m[R_1(x)]^{m_1} \ldots [R_k(x)]^{m_k}$ $(m \leq m_1 \leq \ldots \leq m_k)$ olacak şekilde tamsayı katsayılı $R, R_1, \ldots, R_k$ polinomları vardır. R'lerin tümü indirgenemez olduğundan $(R, R_1R_2...R_k) = 1$ olan ve "İDDİA 1" den dolayı $p|R(n)$ ve "p, $R'.R_1.R_2...R_k(n)$ yi bölmez" olan n ve p asalı vardır. "İDDİA 2" den dolayı $R(n)$ ve $R(n+p)$, p ile bölünür fakat p^2 ile bölünemez. O halde $[R(n)]^m$ ya da $[R(n+p)]^m$, p^m ile bölünür fakat p^{m+1} ile bölünemez.

Şimdi genelleştirilmiş sorumuzun yanıtını verebiliriz.

İSPAT : İddianın aksini farzedelim. $P(x)$ bir polinomun $m.$ kuvveti olmadığından $P(x) = [Q(x)]^m.R(x)$ olacak şekilde tamsayı katsayılı Q ve R polinomları vardır. Burada R indirgenemez polinomların çarpımı şeklinde yazılırsa çarpanların kuvvetleri m den küçüktür. Ancak "İDDİA 3" den dolayı $R(n)$, p ile bölünecek fakat p^m ile bölünmeyecek şekilde sonsuz sayıda p, n ikilisi vardır, böyle bir n için $P(n)$ bir sayının $m.$ kuvveti olamaz. Bu da sorunun verilişiyle çelişir. O halde genelleştirmemizin doğruluğunu ispatlamış olduk.

Şimdi de olimpiyat çalışmalarımız esnasında [2]'de karşılaştığımız şu soruya bakalım.

SORU : Bir aritmetik dizinin aynı asal bölenlere sahip sonsuz uzunlukta bir alt dizisinin varlığını gösteriniz.

YANIT : Söz konusu diziyi; $a, a+d, a+2d, \ldots, a+nd, \ldots$ şeklinde seçelim . Bu durumda

$x_m = (a,d)((\frac{a}{(a,d)})^{m.\phi(\frac{d}{(a,d)})+1})$ dizisi şartı sağlayan bir dizidir. Çünkü

$$(\frac{a}{(a,d)})^{m.\phi(\frac{d}{(a,d)})+1} \equiv \frac{a}{(a,d)} \pmod{\frac{d}{(a,d)}}$$

olduğu için $(a,d)((\frac{a}{(a,d)})^{m.\phi(\frac{d}{(a,d)})+1)}) \equiv a \pmod{d}$ dir. Dolayısıyla; $a, a+d, a+2d, \ldots, a+nd, \ldots$ dizisinin bir alt dizsi olan bu dizinin tüm asal bölenleri de aynıdır.

SORU : $P(x)$ tamsayı katsayılı, sabit olmayan bir polinom olsun. $P(0), P(1), ..., P(n), ...$ dizisinin elemanları sonlu sayıda asal kullanılarak oluşturulamaz. Acaba bu dizinin sonsuz elemanlı bir alt dizisini sonlu sayıda asal kullanarak oluşturmak mümkün müdür? Bu şartı sağlayan $P(x) = (ax+b)^n$ polinomlarının var olduğunu biliyoruz.

KAYNAKLAR:

[1] Karakaş, H.İ ve Aliyev, İ: Sayılar Teorisinde İlginç Olimpiyat Problemleri ve Çözümleri, TÜBİTAK

[2] Sierpinski, A: 250 Problems in Elementary Number Theory

[3] 1998 Uluslararası Bilim Olimpiyatlarına Hazırlık Kış Kampı Notları

(*) Özendirici olacağı inancıyla okuyucularımıza sunduğumuz bu yazı, TÜBİTAK-BAYG tarafından desteklenmiş bir proje olup, 2001 yılı genç araştırmacılar yarışmasında ödüle layık görülmüştür. Biz de, Metehan AYDIN'ı bu başarılı çalışmasından dolayı kutluyoruz. MD