

Kapak Konusu: Karelerin Toplamı

Lagrange'ın Dört Kare Teoremi



Her doğal sayı dört tane doğal sayının karesinin toplamı olarak yazılabilir. Örneğin,

$$\begin{aligned} 5 &= 2^2 + 1^2 + 0^2 + 0^2 \\ 8 &= 2^2 + 2^2 + 0^2 + 0^2 \\ 11 &= 3^2 + 1^2 + 1^2 + 0^2 \\ 12 &= 2^2 + 2^2 + 2^2 + 0^2 \\ 14 &= 3^2 + 2^2 + 1^2 + 0^2 \\ 23 &= 3^2 + 3^2 + 2^2 + 1^2 \\ 24 &= 4^2 + 2^2 + 2^2 + 0^2 \\ 35 &= 5^2 + 3^2 + 1^2 + 0^2 \\ 43 &= 5^2 + 3^2 + 3^2 + 0^2 \\ 45 &= 6^2 + 3^2 + 0^2 + 0^2 \\ 48 &= 6^2 + 2^2 + 2^2 + 2^2 \end{aligned}$$

Bu yazının konusu olan ve Bachet Sanısı olarak da bilinen bu sonuç, İtalyan asıllı Fransız matematikçi Lagrange (1736-1813) tarafından kanıtlanmıştır.

Teorem [Lagrange, 1770]. Her doğal sayı dört tamkarenin toplamıdır.



Joseph Louis Lagrange

Bu yazıda bu teoremi kanıtlayacağız. Kanıt Euler'in bulduğu şu tuhaf eşitliği kullanır:

$$\begin{aligned} (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) \\ = (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 \\ + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 \\ + (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 \\ + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2. \end{aligned}$$

Bu eşitlikten, dört karenin toplamı olan sayıların çarpma altında kapalı oldukları çıkar, yani iki tane dört karenin toplamının çarpımı gene dört karenin toplamı olarak yazılabilir. Dolayısıyla her asal sayının dört karenin toplamı olarak yazılabildiğini kanıtlarsak istediğimiz sonuca ulaşırız. 2 sayısı dört karenin toplamı olarak yazılabildiğinden, 2'den büyük asal sayılara yoğunlaşabiliriz. Önce şu önsavı kanıtlayalım:

Önsav 1. Eğer $p > 2$ bir asal sayıysa, mp sayısının dört tamkarenin toplamı olduğu bir $0 < m < p$ sayısı vardır.

Kanıt: Şu $(p + 1)/2$ tane tamsayıya bakalım:

$$0^2, 1^2, \dots, \left(\frac{p-1}{2}\right)^2.$$

Bu sayıları p 'ye bölüp kalanlarını bulalım; diyelim

$$0 \leq r_0, r_1, \dots, r_{(p-1)/2} \leq p - 1$$

kalanlarını bulduk. (Örneğin eğer $p = 11$ ise, o zaman $(p-1)/2 = 5$ olur ve kareler

$$0, 1, 4, 9, 16, 25$$

olur, kalanlar da

$$0, 1, 4, 9, 5, 3.$$

olur.) Bu kalanların birbirinden değişik olmak zorunda, çünkü eğer $0 \leq i < j \leq (p-1)/2$ göstergeçleri için $r_i = r_j$ olsaydı, o zaman p asalı

$$j^2 - i^2 = (j-i)(j+i)$$

sayısını bölmek zorunda kalırdı, ama

$$0 < j - i < (p-1)/2 < p$$

ve

$$0 < j + i \leq p - 1 < p$$

olduğundan bu imkânsızdır.

Şimdi, yararı sonradan anlaşılacak bir şey yapalım: Bu kalanlara 1 ekleyip bulunan sayıyı p 'den çıkaralım, yani

$$s_i = p - (r_i + 1)$$

sayılarına bakalım. Bu s_i sayılarından da tam

$$(p + 1)/2$$

tane vardır ve bunlar da en az 0, en fazla $p - 1$ olabilirler. (Eğer $p = 11$ ise, s_i sayıları şöyledir:

$$10, 9, 6, 1, 5, 7.)$$

Demek ki 0, 1, 2, ..., $p-1$ sayılarının $(p+1)/2$ tanesi r_i 'lere ve $(p+1)/2$ tanesi s_i 'lere eşit. Dolayısıyla

$$r_i = s_j = p - (r_j + 1)$$

eşitliğinin sağlandığı $0 \leq i, j < (p - 1)/2$ sayıları olmak zorundadır. ($p = 11$ örneğimizde,

$$r_1 = s_3 = 1, r_3 = 9$$

ya da

$$r_3 = s_2 = 9, r_2 = 1$$

ya da

$$r_4 = s_4 = 5, r_4 = 5$$

olur.)

Buradan

$$r_i + r_j = p - 1$$

çıkar. x ve y doğal sayıları,

$$i^2 = px + r_i$$

ve

$$j^2 = py + r_j$$

eşitliğini sağlasınlar. Bu iki eşitliği altalta toplarsak,

$$i^2 + j^2 = p(x + y) + r_i + r_j = p(x + y) + p - 1$$

buluruz. Yani eğer $m = x + y + 1$ ise,

$$pm = i^2 + j^2 + 1 = i^2 + j^2 + 1^2 + 0^2$$

olur, yani pm dört karenin toplamı olur. Son olarak,

$$\begin{aligned} pm = i^2 + j^2 + 1 &< 2 \times \left(\frac{p-1}{2}\right)^2 + 1 \\ &< 2 \times \left(\frac{p}{2}\right)^2 + 1 = \frac{p^2}{2} + 1 < p^2 \end{aligned}$$

olduğundan, $m < p$ bulunur. \square

Aslında yukarda biraz daha genel bir sonuç kanıtladık:

Sonuç 2. Eğer $p > 2$ bir asal sayıysa, mp sayısı-
nın üç karenin toplamı olduğu bir $0 < m < p$ sayısı vardır. Üstelik karelerden biri 1 olarak alınabilir.

Şimdi teoremi kanıtlayabiliriz. $p > 2$ bir asal sayı olsun. $0 < m$ sayısı, mp 'nin dört asalin toplamı olarak yazıldığı en küçük doğal sayı olsun.

m 'nin 1'e eşit olduğunu kanıtlamalıyız. Diyelim

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2. \quad (1)$$

Yukardaki önsavdan dolayı m 'nin p 'den küçük olduğunu biliyoruz.

Eğer m çift bir sayıysa, o zaman x_1, x_2, x_3, x_4 sayılarından ya hiçbiri çift değildir ya da sadece ikisi ya da hepsi birden çift sayıdır. Eğer sadece ikisi çiftse bu çift sayılar x_1 ve x_2 olsun. O zaman her üç durumda da aşağıda kareleri alınan sayılar tam sayı olurlar:

$$\begin{aligned} \left(\frac{x_1+x_2}{2}\right)^2 + \left(\frac{x_1-x_2}{2}\right)^2 + \left(\frac{x_3+x_4}{2}\right)^2 + \left(\frac{x_3-x_4}{2}\right)^2 \\ = \frac{x_1^2 + x_2^2 + x_3^2 + x_4^2}{2} = \frac{mp}{2} = \left(\frac{m}{2}\right)p. \end{aligned}$$

Bu da m 'nin en küçüklüğüyle çelişir. Demek ki m çift olamaz.

Eğer $m = 1$ ise, o zaman zaten teorem kanıtlanmış demektir, bundan böyle diyelim $m > 1$, yani $m \geq 3$ varsayımını yapalım.

x_i 'lerin her birini m 'ye bölelim ve bulduğumuz kalanlara r_i diyelim. y_i sayılarını şöyle tanımlayalım:

$$y_i = \begin{cases} r_i & \text{eğer } 0 \leq r_i \leq \frac{m-1}{2} \text{ ise} \\ r_i - m & \text{eğer } \frac{m+1}{2} \leq r_i \leq m-1 \text{ ise} \end{cases}$$

Demek ki

$$-\frac{m-1}{2} \leq y_i \leq \frac{m-1}{2}.$$

Öyle q_i doğal sayıları vardır ki,

$$x_i = q_i m + y_i$$

olur. Son eşitlikten,

$$y_i^2 \equiv x_i^2 \pmod{m}$$

çıkar. Demek ki,

$$\begin{aligned} y_1^2 + y_2^2 + y_3^2 + y_4^2 &\equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \\ &= mp \equiv 0 \pmod{m} \end{aligned}$$

bulunur. Diyelim $n \in \mathbb{N}$ için,

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = mn \quad (2)$$

Eğer $n = 0$ olsaydı, o zaman

$$y_1 = y_2 = y_3 = y_4 = 0$$

olurdu, yani x_1, x_2, x_3, x_4 sayıları m 'ye bölünürdü, yani $x_1^2, x_2^2, x_3^2, x_4^2$ sayıları m^2 'ye bölünürdü, ama o zaman da

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

sayısı m^2 'ye bölünürdü, ki bundan da m 'nin bir asal olan p 'yi böldüğü, yani $p = m < p$ çıkar, çelişki. Demek ki $n > 0$.

Ayrıca,

$$mn = y_1^2 + y_2^2 + y_3^2 + y_4^2 \leq 4 \left(\frac{m-1}{2} \right)^2 < m^2$$

olduğundan $n < m$ olur.

Şimdi (1) ve (2)'yi çarparak ve kanıtın ta en başında verdiğimiz eşitliği kullanarak,

$$\begin{aligned} m^2 np &= (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) \\ &= (x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4)^2 \\ &\quad + (x_1 y_2 - x_2 y_1 + x_3 y_4 - x_4 y_3)^2 \\ &\quad + (x_1 y_3 - x_3 y_1 + x_4 y_2 - x_2 y_4)^2 \\ &\quad + (x_1 y_4 - x_4 y_1 + x_2 y_3 - x_3 y_2)^2 \end{aligned}$$

buluruz. Parantezlerdeki ifadelerin her biri modülo m sıfırdır çünkü her $i = 1, 2, 3, 4$ için

$$x_i \equiv y_i \pmod{m}$$

denkliği ve (1) eşitliği doğrudur. Demek ki öyle

$z_1, z_2, z_3, z_4 \in \mathbb{Z}$ tamsayıları vardır ki

$$x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4 = m z_1$$

$$x_1 y_2 - x_2 y_1 + x_3 y_4 - x_4 y_3 = m z_2$$

$$x_1 y_3 - x_3 y_1 + x_4 y_2 - x_2 y_4 = m z_3$$

$$x_1 y_4 - x_4 y_1 + x_2 y_3 - x_3 y_2 = m z_4$$

olur. Bütün bunları bir araya koyarsak,

$$m^2 np = m^2 z_1^2 + m^2 z_2^2 + m^2 z_3^2 + m^2 z_4^2$$

yani

$$np = z_1^2 + z_2^2 + z_3^2 + z_4^2$$

elde ederiz. z_i yerine $|z_i|$ alarak z_i 'lerin doğal sayılar olduklarını varsayabiliriz. $0 < n < m$ olduğundan bu da m 'nin en küçüklüğüyle çelişir. Lagrange'ın teoremi kanıtlanmıştır.

Notlar:

1. Bir sayıyı dört karenin toplamı olarak yazdıktan sonra, karelerin yerini değiştirerek aynı sayıyı değişik biçimde dört karenin toplamı olarak yazabiliriz elbette. Ama bunları değişik biçimler olarak saymayalım; topladığımız kareleri büyükten küçüğe doğru sıralayalım.

2. Gene de bazı sayılar birçok değişik biçimde dört karenin toplamı olarak yazılabilirler. Örneğin,

$$4 = 2^2 + 0^2 + 0^2 + 0^2 = 1^2 + 1^2 + 1^2 + 1^2$$

ya da

$$12 = 3^2 + 1^2 + 1^2 + 1^2 = 2^2 + 2^2 + 2^2 + 0^2.$$

Dört karenin toplamı olarak tek bir biçimde yazılan sayılar,

$$1, 3, 5, 7, 11, 15, 23$$

tek sayıları ve bir k doğal sayısı için,

$$2 \times 4^k, 6 \times 4^k, 14 \times 4^k,$$

biçiminde yazılan sayılardır.

3. Verilmiş bir n sayısını 4 karenin toplamı olarak ne kadar çabuk yazabiliriz? Michael O. Robin ve Jeffrey Shallit, 1986'da bu işi aşağı yukarı $\log^2 n$ zamanda yapan bir algoritma bulmuşlardır.

4. Yazıda her doğal sayının 4 karenin toplamı olarak yazıldığını gördük, yani her sayı

$$x^2 + y^2 + z^2 + t^2$$

biçiminde yazılıyor. Peki her sayı mesela,

$$x^2 + 2y^2 + 5z^2 + 5t^2$$

biçiminde yazılır mı? Bu özel sorunun yanıtı olumlu. Genel yanıt şöyle: Eğer 1, 2, 3, 5, 6, 7, 10, 14, 15 sayılarını

$$ax^2 + by^2 + cz^2 + dt^2$$

biçiminde yazılabilirse, o zaman her sayı bu biçimde yazılır. Bu muhteşem olduğu kadar şaşırtıcı sonuç John H. Conway ve W. A. Schneeberger tarafından 1993'te kanıtlanmıştır ve *Conway-Schneeberger'in 15 Teoremi* olarak bilinir. Aslında Conway ve W. A. Schneeberger bundan birazcık daha genel bir teorem kanıtlamışlardır. 2000'de Hindistan asıllı Amerikalı ve Kanadalı matematikçi Manjul Bhargava bu teoremin çok daha basit bir kanıtını bulmuştur. ♠

Kaynakça:

Hans Rademacher ve Otto Toeplitz, *The Enjoyment of Math*, Princeton Science Library 1956, yedinci basım 1994.

