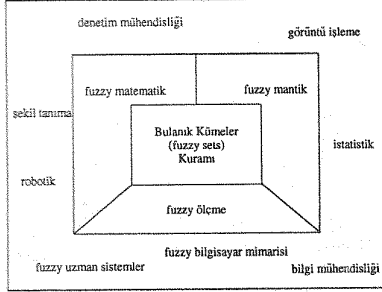


limleri dalındaki uygulamaları şüphesiz ki önümüzdeki yıllarda gündelik hayatımızı daha çok etkileyecek.



Şekilde bulanık kümeler kuramının yaratıldığı uygulamalardan bazıları görülüyor.

Benimle yazışmak için "yasswin.oz.au" internet adresini, ya da "Laboratory of Concurrent Computing Systems, Swinburne University of Technology, P.O. Box 218, Hawthorn, 3122, Avustralya" posta adresini kullanabilirsiniz.

KAYNAKÇA

[Zad65] Lotfi A. Zadeh, *Fuzzy Sets, Information and Control*, 8, 338-353 (1965).

FERMAT NE BİLİYORDU?

Ali Nesin *

350 yıllık bir arayıştan sonra ünlü Fransız matematikçisi Pierre de Fermat'nın (1601-1665) bir kitabının kenarına not olarak kanıtladığını yazdığı, ancak kanıtını hiç bir zaman kâğıda geçirmedığı bir teoremin, geçen yaz Haziran'ın sonuna doğru Andrew Wiles adlı bir matematikçi tarafından kanıtlandığını duymuşsunuzdur. Fermat genellikle kanıtladığı teoremlerin kanıtını yazmazdı. Söz konusu teorem dışında, Fermat'nın kanıtladığını iddia ettiği bütün teoremler (daha doğrusu önermeler) kendisinden sonra gelen matematikçiler tarafından kanıtlanmıştır. Bu yüzden kanıtı daha yeni bulunan söz konusu önerme "Fermat'nın Son Teoremi" diye anılır. İşte önerme:

Fermat'nın Son Teoremi. *Eğer $n \geq 3$ bir tamsayıysa, $x^n + y^n = z^n$ denkleminin pozitif tamsayılarda çözümü yoktur.*

Pierre de Fermat'nın bu teoremi gerçekten kanıtlayıp kanıtlamadığını bilemiyoruz. Büyük bir olasılıkla hiç bir zaman da bilemeyeceğiz. Fermat'nın bir kanıtı sahip olduğunu düşündüğünden pek kuşku duyan yok. Ancak kanıtının yanlış olduğunu düşünen de çok. Gerçekten de, Fermat'nın çağın ünlü matematikçilerine yazdığı mektuplarda bu önermeden

hiç söz etmemesi, kanıtının yanlış olduğunu kendisinin de anlamış olduğu doğrultusunda.

Bu yazının amacı, yukarıdaki teoremle ilgili ve Fermat'nın bildiğinden emin olduğumuz iki teoremin kanıtını vermek.

Önce $x^2 + y^2 = z^2$ denklemini ele alalım. Fermat'nın teoremi bu denklemin çözümünün olmadığını söylemiyor. Nitekim denklemin çözümü var. Örneğin,

$$9144^2 + 14833^2 = 17425^2.$$

Nasıl buldum bu eşitliği? İşte matematiğin gücü ve güzelliği burada. Hesaplamaya gerek kalmadan, bu ve bunun gibi bütün eşitlikleri elde edebiliriz. $x^2 + y^2 = z^2$ denklemini sağlayan daha küçük sayılar da vardır:

$$\begin{aligned} 3^2 + 4^2 &= 5^2 \\ 5^2 + 12^2 &= 13^2 \\ 7^2 + 24^2 &= 25^2 \\ 8^2 + 15^2 &= 17^2. \end{aligned}$$

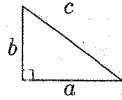
Babilliler bu eşitlikleri biliyorlardı. M.Ö. 1900-1600 yılları arasında kazıldığı anlaşılan bir Babil taş tabletinde bunlar gibi onbeş eşitlik vardır. Babilliler büyük bir olasılıkla

$$(0) \quad (2pq)^2 + (p^2 - q^2)^2 = (p^2 + q^2)^2$$

*Bilkent Üniversitesi Matematik Bölümü öğretim üyesi

eşitliğini de biliyorlardı¹. Bu eşitlikte p ve q yerine iki tamsayı koyarsak, $x^2 + y^2 = z^2$ denklemini sağlayan tamsayılar buluruz. Örneğin, $p = 127$ ve $q = 36$ olarak aldığımızda, yukarıdaki $9144^2 + 14833^2 = 17425^2$ eşitliğini buluruz.

$x^2 + y^2 = z^2$ eşitliğini sağlayan tamsayılara *Pisagor üçlüleri* adı verilir. Çünkü, Pisagor'un ünlü teoremine göre, bir dik üçgenin dik açısını oluşturan iki kenarın karelerinin toplamı, üçüncü kenarın karesine eşittir.



Her Pisagor üçlüsü, üç kenarı da tamsayı uzunluğunda olan bir dik üçgen verir. Bunun tersi de doğrudur: üç kenarı da tamsayı uzunluğunda olan her dik üçgen bir Pisagor üçlüsü verir.

p	q	$x = 2pq$	$y = p^2 - q^2$	$z = p^2 + q^2$	$x^2 + y^2 = z^2$
2	1	4	3	5	$4^2 + 3^2 = 5^2$
3	2	12	5	13	$12^2 + 5^2 = 13^2$
4	1	8	15	17	$8^2 + 15^2 = 17^2$
4	3	24	7	25	$24^2 + 7^2 = 25^2$
5	2	20	21	29	$20^2 + 21^2 = 29^2$
5	4	40	9	41	$40^2 + 9^2 = 41^2$
6	1	12	35	37	$12^2 + 35^2 = 37^2$
6	5	60	11	61	$60^2 + 11^2 = 61^2$

Yukarıda, ortak bölenleri olmayan ve biri çift olan p ve q tamsayılarını aldık yalnızca.

Şimdi $x^4 + y^4 = z^4$ denklemine gelelim. Bu denklemin pozitif tamsayılarda çözümü olmadığını Fermat kanıtlamıştır. Kanıtta, birinci teorem ve Fermat'ın kendi buluşu olan 'sonsuz iniş' adı verilen yöntem kullanmıştır. Aslında Fermat daha genel bir teorem kanıtlamıştır:

Teorem 2. $x^4 + y^4 = z^2$ denkleminin, dolayısıyla $x^4 + y^4 = z^4$ denkleminin de, pozitif tamsayılarda çözümü yoktur.

İkinci teoremin ilginç bir uygulaması vardır. Fermat'ın teoremi salt 4 için değil, dörde bölünen tüm tamsayılar için doğrudur. Örneğin, (a, b, c) tamsayıları, $x^8 + y^8 = z^8$ denkleminin bir çözümü olsaydı, (a^2, b^2, c^2) tamsayıları $x^4 + y^4 = z^4$ denkleminin bir çözümü olurdu. Oysa ikinci teorem bu son

$x^2 + y^2 = z^2$ eşitliğini sağlayan tüm tamsayılar, yani tüm Pisagor üçlüleri bulunabilir mi? Evet. Eski Yunanlı Öklit M.Ö. 300 yılında aşağıdaki teoremi kanıtlamıştır.

Teorem 1. Gerekirse x 'le y 'nin yerlerini değiştirirsek,

$$(1) \quad x^2 + y^2 = z^2$$

denkleminin tüm çözümleri şöyle elde edilir: öyle p, q, d tamsayıları vardır ki

$$x = 2dpq, \quad y = d(p^2 - q^2), \quad z = d(p^2 + q^2)$$

dir.

Birazdan kanıtlayacağımız bu teoremin ışığında, $x^2 + y^2 = z^2$ eşitliğini sağlayan tüm tamsayıları bulabiliriz. Birkaçını bulalım (hep $d = 1$ alacağız).

denklemin çözümünün olmadığını söylüyor. Demek ki $x^8 + y^8 = z^8$ denkleminin de çözümü yoktur. Aynı türden bir akıl yürütme, Fermat'ın teoremini asal n sayıları için kanıtlamanın yeterli olduğunu gösterir. İki büyük ilk asal sayı 3. Fermat, teoremi $n = 3$ için kanıtladığını mektuplarında sık sık yazmıştır, ama her zaman yaptığı gibi, kanıtını açıklamamıştır. Yıllar sonra, İsviçreli matematikçi Euler (1707-1783) $n = 3$ için bir kanıt bulduğunu matematikçi Goldbach'a yazmıştır; kanıtının $n = 4$ şikkının kanıtından çok değişik olduğuna dikkati çekip, yakın gelecekte genel teoremin kanıtlanacağını sanmadığını da eklemiştir. Euler'in 1770 yılında yayımladığı kanıtında açıklamadığı, karanlık kalmış yerler vardı. Bu açıklanmayan yerlerin doğruluğunu büyük bir matematikçi olan Euler'in bilip bilmediği tartışma konusu. Konuyla ilgili okuduğum kitaplardan,

¹ Babil taş tabletindeki eşitliklerden bir tanesi de $4961^2 + 6480^2 = 8161^2$ 'dir! (0) eşitliği bilinmeden bu eşitliğin bulunabilmesi oldukça zor. Bu yüzden Babilliler'in (0) eşitliğinden haberli oldukları sanılıyor.

Euler'in düşüncelerinin doğru olduğu, ancak her nedense her tümcesini açıklamadığı izlenimini edindim. Bu kanıt da 'sonsuz iniş' yöntemini kullanır. 'Sonsuz iniş' yöntemi dışında,

$$\{ a + b\sqrt{-3} : a, b \text{ tamsayılar} \}$$

karmaşık sayılar kümesindeki küpleri bilmek gerekir. Fermat bu kanıtı o çağda bilebilir miydi? Kanıtın Fermat'ın çağının çok ilerisinde olduğu bir gerçek. Ama Fermat da çağının çok ilerisindeydi. Yanıt bilinmiyor.

Yazının kalan bölümünde yukarıdaki iki teoremin kanıtını vereceğiz.

Teorem 1'in Birinci Kanıtı. Eğer (a, b, c) , (1) eşitliğini sağlayan üç tamsayıya ve d herhangi bir tamsayıya, (ad, bd, cd) sayıları da aynı denklemi sağlarlar. Örneğin, $(8, 15, 17)$ bir çözümdür, bu çözümü ikiyle çarpacak olursak $(16, 30, 34)$ çözümünü buluruz. Yani, bir çözümün çarpımlarını alarak yeni çözümler elde edebiliriz. Bunun tersini de yapabiliriz. Eğer (a, b, c) bir çözümse, ve d tamsayısı a, b ve c 'yi bölüyorsa, $(a/d, b/d, c/d)$ tamsayıları da bir çözümdür. Dolayısıyla, ortak bölünen olmayan çözümleri bulmak tüm çözümleri bulmak için yeterlidir. Bundan böyle, (a, b, c) ortak bölünen olmayan bir çözümü simgeleyecek. $a^2 + b^2 = c^2$ olduğundan, a, b, c sayılarından ikisi bir sayıya bölünüyorsa üçüncüsü de aynı sayıya bölünür. Demek ki, a, b, c sayılarından ikisi aynı sayıya bölünemezler. Dolayısıyla bu sayılardan ikisi birden çift olamazlar, yani bu üç sayıdan en az iki tanesi tek sayıdır. Bu sayılardan ikisi tekse üçüncüsü çift olmak zorundadır. Hangi sayı çifttir? c çift olamaz, çünkü c çiftse, a ve b tek sayılardır, dolayısıyla $a^2 + b^2$ dörde bölünmez; öte yandan c^2 dörde bölünür. Demek ki a ve b sayılarından biri çift. Gerekliyorsa a ve b sayılarının yerlerini değiştirerek, a sayısının çift olduğunu varsayabiliriz. Bundan böyle a sayısının çift olduğunu varsayacağız. Demek ki b ve c tek sayılar, ve dolayısıyla $c - b$ ve $c + b$ çift sayılar. O halde

$$(2) \quad a = 2n, \quad c - b = 2v, \quad c + b = 2w$$

olarak yazabiliriz. (2) eşitliklerinden,

$$(3) \quad b = \frac{(c + b) - (c - b)}{2} = \frac{2w - 2v}{2} = w - v$$

$$(4) \quad c = \frac{(c + b) + (c - b)}{2} = \frac{2w + 2v}{2} = w + v$$

eşitlikleri çıktığından, v ve w sayılarının ortak bölüneni yoktur, çünkü hem v 'yi, hem w 'yi bölen bir sayı, b ve c sayılarını da böler. $a^2 + b^2 = c^2$ eşitliğinden, $a^2 = c^2 - b^2 = (c - b)(c + b)$ eşitliği çıkar. Bu eşitlikte, (2)'den yararlanarak, a yerine $2n$, $c - b$ yerine $2v$, $c + b$ yerine $2w$ koyarsak, ve 4'leri sadeleştirirsek

$$(5) \quad n^2 = vw$$

eşitliğini buluruz. Demek ki vw tam bir kare. Öte yandan v ve w sayılarının ortak bölüneni yok. Demek ki v ve w de birer kare olmak zorundalar. $v = q^2$ ve $w = p^2$ olarak yazalım. İşimiz aşağı yukarı bitmiştir: (3) ve (4) eşitlikleri $b = p^2 - q^2$ ve $c = p^2 + q^2$ verir; (5) eşitliği $n = pq$ verir, (2) eşitliği de $a = 2n = 2pq$ verir.

Teorem 1'in İkinci Kanıtı. Bu kanıtta geometrik bir yöntem kullanacağız. Kanıtı başlamadan önce, $(0, 1)$ noktasından geçen ve y eksenine koşut olmayan bir doğrunun denkleminin, bir m sayısı için

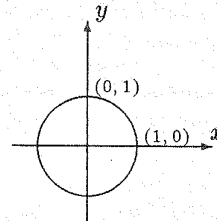
$$(6) \quad y = mx + 1$$

biçiminde yazılabileceğini okura anımsatırım. m sayısına doğrunun eğimi adı verilir.

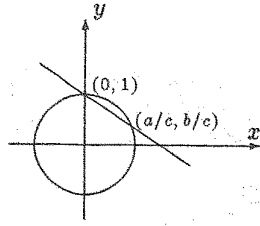
Şimdi a, b, c sayılarını, $x^2 + y^2 = z^2$ denklemini sağlayan üç pozitif tamsayı olsunlar. O zaman a/c ve b/c kesirli sayıları,

$$(7) \quad x^2 + y^2 = 1$$

denklemini sağlarlar. (7) denkleminin gerçel sayılardaki çözümleri, merkezi $(0, 0)$ noktasında olan 1 yarıçaplı çember (*birim çember*) üzerindedir, dolayısıyla $(a/c, b/c)$ noktası da bu çember üzerindedir:



$a > 0$ olduğundan, $(a/c, b/c)$ noktasıyla $(0, 1)$ noktası birim çemberin iki değişik noktasıdır. Bu iki noktadan geçen doğruya bakalım:



Bu doğrunun denklemi

$$y = \frac{b-c}{a}x + 1$$

dir. Yani (6) denklemindeki m sayısı (doğrunun eğimi yani) $\frac{b-c}{a}$ sayısına eşittir, dolayısıyla kesirli bir sayıdır. Ortak böleni olmayan iki p ve q tamsayıları için

$$(8) \quad m = \frac{p}{q}$$

yazalım. Ayrıca,

$$(9) \quad \begin{cases} r = a/c \\ s = b/c \end{cases}$$

yazalım.

(r, s) noktası, yani $(a/c, b/c)$ noktası, hem birim çemberin, hem de $y = mx + 1$ denklemlerinin üstünde. Dolayısıyla (r, s) sayıları (6) ve (7) denklemlerini sağlarlar. Denklemlerimizi yazalım:

$$(10) \quad \begin{cases} r^2 + s^2 = 1 \\ s = mr + 1. \end{cases}$$

İkinci eşitlikten s 'yi biliyoruz: $s = mr + 1$. Bunu birinci eşitliğe yerleştirelim:

$$1 = r^2 + s^2 = r^2 + (mr + 1)^2.$$

Soldaki terimi açalım:

$$1 = (1 + m^2)r^2 + 2mr + 1,$$

yani

$$(1 + m^2)r^2 + 2mr = 0,$$

yani

$$r[(1 + m^2)r + 2m] = 0.$$

Öte yandan $r \neq 0$. Demek ki r 'yi sadeleştirerek,

$$(1 + m^2)r + 2m = 0,$$

² u sayısı hem $p^2 + q^2$ 'yi hem de $p^2 - q^2$ 'yi bölüyorsa, u bu sayıların toplamını ve farkını da, yani $2p^2$ 'yi ve $2q^2$ 'yi böler. Öte yandan p^2 ve q^2 sayılarının ortak böleni yok. Demek ki $u = 1$ ya da $u = 2$.

yani $r = \frac{-2m}{1+m^2}$ buluruz. Bunu ve (10) denklemlerinden ikincisini kullanarak da s 'yi bulabiliriz:

$$s = mr + 1 = \frac{-2m^2}{1+m^2} + 1 = \frac{1-m^2}{1+m^2}.$$

Demek ki

$$\begin{cases} r = \frac{-2m}{1+m^2} \\ s = \frac{1-m^2}{1+m^2} \end{cases}$$

Şimdi (8) ve (9) denklemlerini yukarıdaki denklemlere taşıyıp biraz hesap yapacak olursak,

$$(11) \quad \begin{cases} a = \frac{-2pq}{p^2+q^2}c \\ b = \frac{p^2-q^2}{p^2+q^2}c \end{cases}$$

eşitliklerini elde ederiz. İkinci eşitlikten $p^2 + q^2$ sayısının $(p^2 - q^2)c$ 'yi böldüğü çıkar. Öte yandan $p^2 - q^2$ ile $p^2 + q^2$ sayısının ortak böleni ya 1'dir ya da 2^2 . Ortak bölenin 1 olduğunu varsayalım. (Ortak bölenin 2 olduğu şıkkı okura bırakıyoruz.) Bu varsayımınla $p^2 + q^2$, c 'yi böler.

$$c = d(p^2 + q^2)$$

eşitliğini sağlayan d sayısını bulalım ve bunu (11)'deki eşitliklere yerleştirelim. Teorem 1 bir kez daha kanıtlanmıştır.

Teorem 2'nin Kanıtı. Teoremi kanıtlayabilmek için bir önsava gereksinimiyoruz:

Önsav. Tek bir sayının karesi dörde bölündüğünde 1 kalır.

Önsavın Kanıtı. Tek sayımıza a adını verelim. $a = 2b + 1$ biçiminde yazalım. Şimdi hesaplayalım:

$$a^2 = (2b + 1)^2 = 4b^2 + 4b + 1 = 4(b^2 + b) + 1.$$

Demek ki a^2 dörde bölündüğünde kalan 1'dir. Kanıtımız bitmiştir.

Artık ikinci teoremi kanıtlayabiliriz. 'Son-suz iniş' adı verilen yöntemi kullanacağız. Teoremin yanlış olduğunu varsayalım, yani

$$(12) \quad x^4 + y^4 = z^2$$

eşitliğinin pozitif tamsayılarla bir çözümünün olduğunu varsayalım. Bir çelişki elde edeceğiz. (12)'nin çözümleri arasında z 'nin en küçük olduğu bir çözüm seçelim ve bu çözüme (x, y, z) adını verelim. (12) denklemi sadeleştirmeye

olanak verdiğinden ve z en küçük olduğundan, x, y, z sayılarının ortak böleni yoktur. Bundan da x, y, z sayılarından herhangi iki tanesinin ortak böleninin olmadığı çıkar. Demek ki bu üç sayıdan yalnızca biri çift olabilir, ve en az iki tanesi tek- tir. Sayılardan ikisi tekse, üçüncüsü çift olmak zorunda. z çift olamaz, çünkü z çiftse, x ve y tektir, ve $x^4 + y^4$ dörde bölünmez; öte yan- dan z^2 dörde bölünür. Demek ki ya x ya da y çift. Gerekirse x ile y 'nin yerlerini değiştirerek, x 'in çift olduğunu varsayabiliriz. Şimdi (x^2, y^2, z) sayılarına birinci teoremimizi uygulayabiliriz: or- tak bölenleri olmayan öyle a ve b vardır ki,

$$(13) \quad x^2 = 2ab,$$

$$(14) \quad y^2 = a^2 - b^2,$$

$$(15) \quad z = a^2 + b^2$$

dir. Ayrıca a ve b sayılarından yalnızca biri çifttir. a 'nın çift olamayacağını iddia ediyorum: eğer a çift olsaydı, b tek olurdu. $a = 2a_1$, $b = 2b_1 + 1$ yazalım. Bu eşitlikleri (14)'e yerleştirelim:

$$\begin{aligned} y^2 &\stackrel{(14)}{=} a^2 - b^2 = (4a_1^2) + (2b_1 + 1)^2 \\ &= 4a_1^2 + 4b_1^2 + 4b_1 + 1 \\ &= 4(a_1^2 + b_1^2 + b_1) + 1 \end{aligned}$$

ve yukarıda kanıtladığımız önsavla çeliştik. İddia- mı kanıtladım: a çift olamaz. Demek ki b çifttir. (14) denkleminde göre $b^2 + y^2 = a^2$ olduğundan birinci teoremi gene uygulayabiliriz: ortak böleni olmayan öyle c ve d sayıları vardır ki

$$(16) \quad b = 2cd,$$

$$(17) \quad y = c^2 - d^2,$$

$$(18) \quad a = c^2 + d^2$$

dir. Şimdi x^2 yi hesaplayalım:

$$x^2 \stackrel{(13)}{=} 2ab \stackrel{(16,17)}{=} 4cd(c^2 + d^2).$$

Demek, $4cd(c^2 + d^2)$ tam bir kare. Dolayısıyla $cd(c^2 + d^2)$ de tam bir kare. Öte yandan c , d ve $c^2 + d^2$ sayılarından herhangi ikisinin ortak böleni yok. Bundan da c , d ve $c^2 + d^2$ sayılarının birer tam kare oldukları çıkar. Yani öyle e, f, g sayıları vardır ki,

$$(19) \quad c = e^2,$$

$$(20) \quad d = f^2,$$

$$(21) \quad c^2 + d^2 = g^2$$

dir. Kanıtın sonuna geldik. Hesaplayalım:

$$e^4 + f^4 \stackrel{(19,20)}{=} c^2 + d^2 \stackrel{(21)}{=} g^2.$$

Demek ki (e, f, g) sayıları da (18) denkleminin bir çözümü. Son olarak, g sayısının, z sayısından küçük olduğunu kanıtlayalım. Bu dilediğimiz çelişkiyi verecek:

$$\begin{aligned} z &\stackrel{(15)}{=} a^2 + b^2 \stackrel{(16,18)}{=} (c^2 + d^2)^2 + 4c^2d^2 \\ &\stackrel{(21)}{=} g^4 + 4c^2d^2 > g^4 \geq g. \end{aligned}$$

İkinci teorem de kanıtlanmıştır.

Matematik Dünyası'na yazarak beğendiklerini belirten okurlarımıza teşekkür ederiz. Sevgili Dilek Başol (Kuruçeşme, İzmit) kardeşimizin övgülerini hak etmeye çalışacağız.

Pergel ve cetvel ile bir açının üçe bölünmesi üzerine yazan okurlarımıza bunun yapılamayacağını kanıtının Matematik Dünyası'nda daha önce (cilt 1, sayı 1, sayfa 11-14 ve devamı cilt 1, sayı 2, sayfa 10-15) İsmail Güloğlu tarafından yazıldığını anımsatmak isteriz.

Yazı Kurulu