

Fermat Ne Biliyordu? (2)

Ali Nesin

Bu yazıda geçen yazıda sözünü ettiğim iki teoremi kanıtlayacağız.

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

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

denkleminin tüm çözümleri şöyle elde edilir: Öyle p, q, d sayıları vardır ki,

$$\begin{aligned} x &= 2dpq, \\ y &= d(p^2 - q^2), \\ z &= d(p^2 + q^2) \end{aligned}$$

dir.

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

Bu iki teoremi kanıtlayabilmek için bir önsava gereksiniyoruz:

Önsav. Bir tek sayının karesi 4'e 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 1 kalır.

Teorem 1'in Birinci Kanıtı: Eğer (a, b, c) üçlüsü, (1) eşitliğini sağlayan üç tamsayıya ve d herhangi bir tamsayıya, (ad, bd, cd) tamsayıları da aynı denklemi sağlar. 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 böleni olmayan¹ çözümleri bulmak, tüm çözümleri bulmak için yeterlidir. Bundan böyle, (a, b, c) ortak böleni 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 ve 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 yukardaki önsava göre, $a^2 + b^2$ sayısı dörde bölündüğünde iki kalır, yani $a^2 + b^2$ dörde bölünmez; öte yandan c^2 dörde bölünür.) Demek ki a ve b sayılarından biri çift olmak zorunda. Gerekirse a ve b sayılarının yerlerini değiştirerek, a sayısının çift olduğunu varsayabiliriz. Bundan böyle a 'nın çift olduğunu varsayacağız.

Demek ki b ve c tek sayılar. Dolayısıyla $c-b$ ve $c+b$ çift sayılar. O halde,

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

¹ Daha doğrusu ortak böleni 1 olan!

olarak yazabiliriz. (2) eşitliklerinden,

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

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

eşitlikleri çıktığından, v ve w sayılarının ortak böleni 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

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

eşitliğini buluruz. Demek ki vw bir kare. Öte yandan v ve w sayılarının ortak bölenleri yok. Dolayısıyla 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. \square

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,

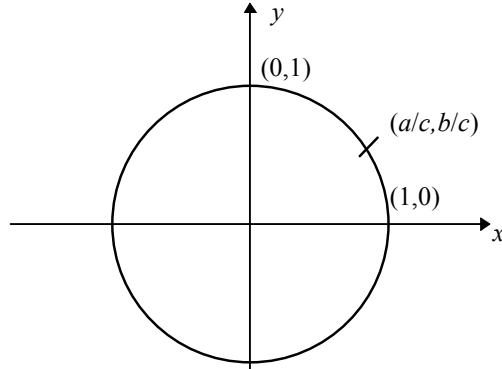
$$y = mx + 1 \quad (6)$$

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

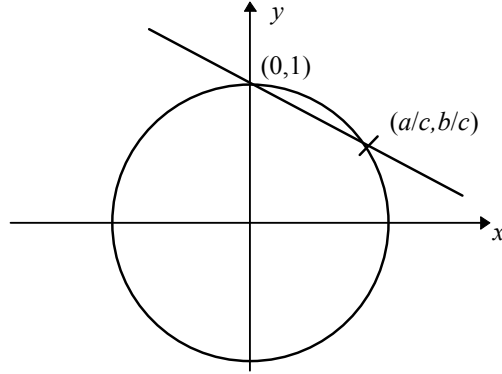
Şimdi a, b, c sayıları, $x^2 + y^2 = z^2$ denklemini sağlayan üç pozitif sayı olsunlar. O zaman a/c ve b/c kesirli sayıları,

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

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



$a > 0$ olduğundan, $(a/c, b/c)$ noktasıyla $(0,1)$ noktası, birim dairenin iki değişik noktalarıdır. 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 tamsayısı için

$$m = \frac{b-c}{a} = p/q \quad (8)$$

yazalım. Ayrıca, r ve s sayılarını

$$r = a/c \text{ ve } s = b/c \quad (9)$$

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

$$r^2 + s^2 = 1 \text{ ve } s = mr + 1. \quad (10)$$

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

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

Sağdaki 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 sadeleştirebiliriz ve

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

yani,

$$r = \frac{-2m}{1 + m^2}$$

buluruz. Bunu ve (10) denklemlerinden ikincisini kullanarak s 'yi de bulabiliriz:

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

Demek ki,

$$r = \frac{-2m}{1 + m^2}$$

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

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

$$a = \frac{-2pq}{p^2 + q^2} c$$

$$b = \frac{p^2 - q^2}{p^2 + q^2} c \quad (11)$$

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 ya da 2'dir². Bu ortak bölenin 1 olduğunu varsayalım (ortak bölenin 2 olduğu şıkkı okura bırakıyoruz.) Demek ki $p^2 + q^2$, c 'yi böler. $c = d(p^2 + q^2)$ eşitliğini sağlayan bir d sayısı bulalım, ve bunu (11) eşitliklerine yerleştirelim. Teorem 1 bir kez daha kanıtlanmıştır. \square

Teorem 2'nin Kanıtı³: *Sonsuz İniş ve Sonsuz Çıkış* adlı yazıda sözünü ettiğimiz sonsuz iniş yöntemini kullanacağız. Teoremin yanlış olduğunu varsayalım, yani

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

eşitliğinin pozitif tamsayılar da bir çözümünün olduğunu varsayalım. Bir çelişki elde edeceğiz. (12)'nin çözümleri arasında z 'nin en küçük olduğu bir çözüm seçelim. Bu çözüme (x, y, z) diyelim. (12) denklemini sadeleştirmeye olanak verdiğinden ve z en küçük olduğundan, x, y ve z sayılarının ortak böleni yoktur. Bundan da x, y, z sayılarından herhangi ikisinin ortak böleninin olmadığı çıkar. Demek ki bu üç sayıdan yalnızca biri çift olabilir ve en az ikisi tektir. 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 yandan z^2 dörde bölünür.) Demek ki ya x ya y çift. Gerekirse x 'le y 'nin yerlerini değiştirerek, x 'in çift olduğunu varsayabiliriz. Şimdi (x^2, y^2, z) sayılarına birinci teoremimizi uygulayabiliriz: ortak bölenleri olmayan öyle a ve b vardır ki,

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

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

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

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:

$$\begin{aligned} y^2 & \stackrel{(14)}{=} a^2 - b^2 = (2a_1)^2 - (2b_1 + 1)^2 \\ & = 4a_1^2 - 4b_1^2 - 4b_1 - 1 \\ & = 4(a_1^2 - b_1^2 - b_1) - 1 \\ & = 4(a_1^2 - b_1^2 - b_1 - 1) + 3 \end{aligned}$$

ve yazının başında kanıtladığımız önsavla çeliştik. İddiamı kanıtladım: a çift olamaz. Demek ki b çifttir. (14) denklemine göre $b^2 + y^2 = a^2$ olduğundan birinci teoremi gene uygulayabiliriz: ortak böleni olmayan öyle c ve d sayıları vardır ki,

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

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

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

dir. Şimdi x^2 'yi hesaplayalım:

$$x^2 \stackrel{(13)}{=} 2ab \stackrel{(16,18)}{=} 4cd(c^2 + d^2).$$

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,

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

² u sayısı hem $p^2 + q^2$ 'yi, hem de $p^2 - q^2$ 'yi bölüyorsa, u bu sayıların toplamını ve farkını da böler. Dolayısıyla u hem $2p^2$ 'yi, hem de $2q^2$ 'yi böler. p ile q 'nün ortak böleni olmadığından, $u = 1$ ya da $u = 2$ 'dir.

³ Bu kanıt Fermat'nındır.

$$c^2 + d^2 = g^2 \quad d = f^2 \quad (20)$$

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 (12) denkleminin bir çözümü. Son olarak, g sayısının, z sayısından küçük olduğunu kanıtlayalım. Bu dilediğimiz çelişkiyi verecek: $z \stackrel{(15)}{=} a^2 + b^2 \stackrel{(16,18)}{=} (c^2 + d^2)^2 + 4c^2d^2 \stackrel{(21)}{=} g^4 + 4c^2d^2 > g^4 \geq g$. İkinci teorem de kanıtlanmıştır. \square