KARMAŞIK SAYILAR VE İKİ TAMKARE TEOREMİ

Oktay K. Pashaev-Engin Büyükaşık
İYTE,Matematik Bölümü, Urla, İZMİR

1. Giriş

Babilli matematikçiler günümüzde Pisagor bağıntısı olarak bilinen

$$x^2 + y^2 = z^2$$

eşitliği ve bunu sağlayan (x, y, z) tamsayı üçlülerini merak etmiş ve bunun üzerinde çalışmışlardır. Bu bağıntıyı sağlayan x, y, z tamsayıları Pisagor üçlüleri olarak adlandırılır.

Hellenistik dönemden beri ilkel Pisagor üçlülerinin (1 dışında ortak çarpanı olmayan) şu yolla elde edillebileceği biliniyordu; p ve q aralarında asal ve ikisi birden tek olmamak üzere $a = p^2 - q^2$, $b = 2p\ q$, $c = p^2 + q^2$. Bu durumda a, b, c'nin bir Pisagor üçlüsü, yani $a^2 + b^2 = c^2$ olduğunu görmek kolaydır. Bunun yanında, iki tamkare toplamının, başka bir iki tamkare toplamı ile çarpımının yine iki tamkare toplamına eşit olduğu yaklaşık 4000 yıl önce Babilliler tarafından biliniyordu.

Örneğin: $2 = 1^2 + 1^2$, $34 = 3^2 + 5^2$

$68 = 2.34 = (1^2 + 1^2)(3^2 + 5^2) = 2^2 + 8^2$

Fibonacci, "Tamkareler Kitabı" adlı eserinde, Diophantus özdeşliği olarak bilinen bu özdeşlikten sözeder.

Bu özdeşlik başka bir ünlü problemde önemli rol oynar. Bu problem, büyük olasılıkla Pisagor üçlülerinin yukarıdaki gösteriminden etkilenilerek oluşturulmuş olan "Herhangi bir pozitif tamsayının iki tamkare toplamı şeklinde yazılıp yazılamıyacağı" problemidir. Bu broblem, geçmişteki bütün ünlü matematikçilerin dikkatini çekmiştir. P. Fermat 1659'da yazdığı bir yazısında, $p = 4n + 1$ şeklindeki her asal sayının iki tamkare toplamı şeklinde olduğunu ispatladığını açıklamıştır. Ancak Fermat'ın bu ispatına ilişkin herhangi bir kayıt bulunamamıştır. Yaklaşık 100 yıl sonra kayda geçen ilk ispatlar 1749'da Euler'e, 1775'de Lagrange, 1776'da Laplace aittir. Gauss'da iki tamkare yazılımının tek olması gerektiğini göstermiştir. Bu problemin en basit ispatı D. Zagier'e aittir ve bu ispatı "$p \equiv 1 (mod 4)$ şeklindeki her asal sayının iki tamkare toplamına eşit olduğunun bir satırlık ispatı" adlı makalesinde tanıtmıştır. Gerçekten de ispat tek satır içerir. Bu ispat aslında Liouville tarafından yapılan bir ispattan etkilenen Heath-Brown'ın ispatının basitlestirilmesidir.

İkinci bölümdeki iki tamkare teoreminin ifadesini vermeden önce birinci bölümde karmaşık sayılar ile iki tamkare özdeşliğinin geometrik yorumunu ele alacağız.

Hamilton tarafından gözlemlendiği gibi karmaşık sayılar; vektörel toplam ve vektörel çarpım yardımıyl R^2 olarak düşünülebilir. Bu yaklaşım "quaternionlar ve dört tamkare" ve " oktanionlar ve sekiz tamkare" özdeşliklerine açılımı elverişli kıldığı için uygundur.

Ünlü dört tamkare özdeşliği ve quaternionlar konusu bir sonraki yazımızda ele alınacaktır.

2. Karmaşık Sayılar

Pisagor teoremine göre; dik kenar uzunlukları x, y ve hipotenüsünün uzunluğu r olan bir dik üçgende

$$x^2 + y^2 = r^2 \tag{1}$$

eşitliği vardır. Şimdi $\mathcal{R} \times \mathcal{R} \equiv \mathcal{R}^2$ düzlemini ele alalım. Bu düzlemdeki her $P(x, y)$ noktası için (1) eşitliğindeki r gerçel sayısı, P noktasının orijine O(0,0) olan uzaklığını gösterir. Her $P(x, y)$ noktası $z = x + iy$ $(i^2 = -1)$ ile eşleştirilirse bu işlemin sonunda $C = \{z = x + iy | x \in \mathcal{R},\ y \in \mathcal{R}\}$ kümesi elde edilir. Elde ettiğimiz C kümesine karmaşık sayılar kümesi denir. z_1, z_2 iki karmaşık sayı olmak üzere; bu iki sayının toplamı(farkı):

$$z_1 \pm z_2 = (x_1 + iy_1) \pm (x_2 + iy_2) = (x_1 \pm x_2) + i(y_1 \pm y_2) \tag{2}$$

olarak tanımlanır. Bu ise koordinatları (x_1, y_1) ve (x_2, y_2) olan iki vektörün toplamı(farkı)dır. Aynı şekilde z_1 ve z_2 karmaşık sayılarının çarpımı

$$z_1 z_2 = (x_1 + iy_1)(x_2 + iy_2) = (x_1x_2 - y_1y_2) + i(x_1y_2 + x_2y_1) \tag{3}$$

dir. Ancak bunun (2) deki gibi vektörel bir işlemin sonucu olarak ifadesi kolay değildir. Sözkonusu ifadeyi oluşturmadan önce, her z karmaşık sayısına $\bar{z}$ ile gösterilen ve z'nin eşleniği olarak adlandırılan $\bar{z} = x + i(-y) = x - iy$ karmaşık sayısını karşılık getirelim. Bu işlem karmaşık sayılar kümesinde $\sigma(z) = \bar{z}$ olarak tanımlanan bir involüt (bkz. Ek) örneğidir (Gerçekten $\sigma^2 = I$ ve $\sigma^2(z) = z$). Bu involütün sabit noktaları ($\sigma(z) = z$) ise $z = \bar{z}$ koşulunu sağlayan sayılardır, yani gerçel sayılardır.
Bir $x \in \mathcal{R}$ modülü ile x sayısının orjine olan uzaklığı kastedilir ve $|x|$ ile gösterilir. Bir $z = x + iy$ karmaşık sayısının modülü ise Pisagor teoremi yardımıyla;

$$|z|^2 = x^2 + y^2 = r^2 \tag{4}$$

olarak tanımlanır. Bu son eşitlik aynı zamanda birbirinin eşleniği olan iki karmaşık sayının çarpımına karşılık gelir, yani

$$z\bar{z} = (x + iy)(x - iy) = x^2 + y^2 = r^2 \tag{5}$$

İki Tamkare Özdeşliği: *(Alexandria'lı Diophantus)*

$$(x_1^2 + y_1^2)(x_2^2 + y_2^2) = (x_1x_2 - y_1y_2)^2 + (x_1y_2 + x_2y_1)^2 \tag{6}$$

Bu özdeşliğin ispatı aşağıdaki eşitliklerden doğrudan elde edilebilir.

$$(x_1x_2 - y_1y_2)^2 = (x_1x_2)^2 + (y_1y_2)^2 - 2x_1x_2y_1y_2$$

$$(x_1y_2 + y_1x_2)^2 = (x_1y_2)^2 + (y_1x_2)^2 + 2x_1x_2y_1y_2$$

Bu özdeşliğe göre z_1 ve z_2 karmaşık sayıları için aşağıdaki förmül elde edilir.

$$|z_1|^2|z_2|^2 = |z_1z_2|^2 \tag{7}$$

Aşağıda;

$$\sigma(z) = z^{-1} = \frac{\bar{z}}{|z|^2} \tag{8}$$

$(z.z^{-1} = 1)$ ile tanımlı dönüşüm de karmaşık sayılarda bir involüt örneğidir.

Problem 1. σ nın bir involüt ve $\sigma^2 = I$ olduğunu gösteriniz.
Problem 2. Bu involütün sabit noktalarını bulunuz.

Şimdi (3) formülü ve bu formülün geometrik anlamına geri dönelim. İlk olarak $u = x + iy$ için,

$$|u|^2 = \bar{u}u = 1 \tag{9}$$

koşulunu sağlayan noktalar kümesini gözönüne alalım. Bu küme yarıçapı $r = 1$ olan $x^2 + y^2 = r^2$ çemberi üzerindeki noktalara karşılık gelir. Ayrıca $\cos^2 t + \sin^2 t = 1$ eşitliğinden yola çıkarak bu çember üzerindeki noktalar, $0 \leq t < 2\pi$ olmak üzere,

$$x = \cos t, \quad y = \sin t \tag{10}$$

şeklinde yazılır ve buradan da

$$u = \cos t + i \sin t \tag{11}$$

elde edilir.
$u_1 = \cos t_1 + i \sin t_1$ ve $u_2 = \cos t_2 + i \sin t_2$ karmaşık sayıları birim çember üzerinde ve argümenti sırasıyla t_1, t_2 olan noktaları temsil eder. Şimdi u_1 ve u_2 birbiri ile çarpılırsa,

$$u_1u_2 = (\cos t_1 + i \sin t_1)(\cos t_2 + i \sin t_2) =$$

$$(\cos t_1 \cos t_2 - \sin t_1 \sin t_2) + i(\cos t_1 \sin t_2 + \cos t_2 \sin t_1) =$$
$$\cos(t_1 + t_2) + i \sin(t_1 + t_2) \tag{12}$$

elde edilir ve görüldüğü gibi $u_1.u_2$ çarpımıda birim çember üzerinde argümenti t_1+t_2 olan bir noktadır. Böylece her $z = x + iy$ karmaşık sayısı modülü $|u| = 1$ olan bir $u \in C$ için,

$$u = \frac{z}{|z|} = \frac{x+iy}{\sqrt{x^2+y^2}} = \frac{x}{\sqrt{x^2+y^2}} + i\frac{y}{\sqrt{x^2+y^2}}$$

şeklinde yazılabilir. Buradan (11) denklemine göre

$$\frac{x}{\sqrt{x^2+y^2}} = \cos t, \quad \frac{y}{\sqrt{x^2+y^2}} = \sin t$$

bulunur. Buradan da herhangi bir $z \in C$ için

$$z = r(\cos t + i \sin t) \tag{13}$$

elde edilir. O halde
$z_1 = r_1(\cos t_1 + i \sin t_1)$, $z_2 = r_2(\cos t_2 + i \sin t_2)$ herhangi iki karmaşık sayı olmak üzere

$$z_1 z_2 = r_1 r_2[\cos(t_1 + t_2) + i \sin(t_1 + t_2)] \tag{14}$$

çarpımı elde edilir. Böylece herhangi iki karmaşık sayının çarpımının geometrik anlamının; modülü $r_1.r_2$ ve argümenti $t_1 + t_2$ olan bir nokta olduğu görülür.

3. Gauss Tamsayıları

$m, n \in \mathcal{Z}$ olmak üzere $z = m+in$ karmaşık sayısını gözönüne alalım. Bu şekildeki tüm z sayılarının kümesine *karmaşık tamsayılar* ya da *Gauss tamsayıları* denir ve $\mathcal{Z}[i] = \{n+im | n, m \in \mathcal{Z}\}$ ile gösterilir. Geometrik olarak Gauss tamsayıları düzlem üzerinde koordinatları tamsayılar olan noktalar kümesini, başka bir değişle tamsayılar kafesini verir. (2) denklemine göre iki Gauss tamsayısının toplamı (farkı) bir Gauss tamsayısıdır. (3) denklemine göre $z_1 = n_1 + im_1$, $z_2 = n_2 + im_2$ için;

$$z_1 z_2 = (n_1 + im_1)(n_2 + im_2) = (n_1 n_2 - m_1 m_2) + i(n_1 m_2 - m_1 n_2) \tag{15}$$

çarpımı bir Gauss tamsayısıdır. Bu son eşitlikten iki tamkare özdeşliğinin Gauss tamsayılarının modülü için sağlandığı görülür yani;

$$(n_1^2 + m_1^2)(n_2^2 + m_2^2) = (n_1 n_2 - m_1 m_2)^2 + (n_1 m_2 + m_1 n_2)^2 \tag{16}$$

C de olduğu gibi $\sigma : z = m + in \to \bar{z} = m - in$ dönüşümü $\mathcal{Z}[i]$ üzerinde de bir involüt'dir. Ancak (8) ile tanımlanan involüt genelde $\mathcal{Z}[i]$'de involüt değildir. Bunun sebebi bölme işleminin Gauss tamsayıları üzerinde tanımlı olmamasıdır. Başka bir açıdan bakılırsa, $z = m + in$ ve $n = kn_1$, $m = km_1$, $k \in \mathcal{Z}$ yada $n \equiv 0(mod\ k)$, $m \equiv 0(mod\ k)$ olacak şekilde bir karmaşık sayı ise $z = m+in = k(m_1 + in_1) = kz_1$, $z_1 \in \mathcal{Z}[i]$ olur. Buradan da

$$|z|^2 = n^2 + m^2 = k^2(n_1^2 + m_2^2) = k^2|z_1|^2 \tag{17}$$

Böylece $z \equiv 0(mod\ k)$ ise $|z|^2 \equiv 0\,(mod\ k)$ olur.

Şimdi $M = \{m^2+n^2 \mid |z|^2 = m^2+n^2,\ z \in \mathcal{Z}[i]\}$ kümesinin elemanlarını belirlemeye çalışalım. Bu küme aslında iki tamsayının kareleri toplamı şeklinde yazılabilen tamsayılar kümesidir. Her tamsayı sonlu sayıda asal sayının çarpımı olarak yazılabildiğinden, sözkonusu problem $p = m^2 + n^2$ şeklinde yazılabilen p asal sayılarını bulmaya indirgenir.

Teorem 1. *(Fibonacci)* p ve q iki tamkare toplamı şeklinde yazılabilen iki asal sayı ise, çarpımları da iki tamkare toplamı şeklinde yazılabilir.

İspat (16) daki iki tamkare özdeşliğinden doğrudan yapılabilir.

Böylece iki tamkare toplamı şeklinde gösterilebilen asal sayıları bulabilirsek iki tamkare toplamı şeklinde yazılabilen bütün tamsayıları belirlemiş oluruz.

Her $p \geq 3$ asal sayısı $k \in$N için $4k+1$ ya da $4k+3$ şeklinde olduğundan bu sayıları dikkate almamız yeterli olur.

Teorem 2. $p = 4k+3$ şeklinde bir asal sayı ise, p iki tamkare toplamı şeklinde yazılamaz.

İspat: n^2+m^2 toplamı ancak n, m sayılarından en az biri tek olduğunda asal olabilir. Gerçekten n, m çift sayıları için, $(2k)^2+(2l)^2 = 4(k^2+l^2)$ olur. Bu durumda n^2+m^2 toplamı için iki olası durum vardır:

$$(2k+1)^2+(2l+1)^2 = 4(k^2+k+l^2+l)+2$$

ya da

$$(2k+1)^2+(2l)^2 = 4(k^2+k+l^2)+1$$

Görüldüğü gibi iki tamkare toplamının 4 ile bölümünden kalan 0,1,2 olabilir.

Teorem 3. $p = 4k+1$ şeklindeki her asal sayı iki tamkare toplamı şeklinde yazılabilir.

İspat:

$$x^2+4yz = p \tag{18}$$

denkleminin doğal sayılardaki bütün x, y, z çözümler kümesini gözönüne alalım ve bu kümeyi M ile gösterelim. İspatı tamamlamak için, $p = 4k+1$ ise (18) denkleminin $y = z$ olacak şekilde bir (x, y, z) çözümünün varlığını göstermek yeterli olur. Ancak $y = z$ olan çözüm M üzerinde tanımlanan;

$$\sigma(x, y, z) = (x, z, y) \tag{19}$$

involütünün (nin bir involüt olduğunu gösteriniz) bir sabit noktasıdır. Bu nedenle (18) denkleminin çözümler kümesi olan M'nin eleman sayısının tek olduğunu göstermek yeterlidir.
Bunu göstermek için D. Zagier başka bir τ involütü tanımlar ve bu invölütün tam bir sabit noktası olduğunu gösterir. Böylece M'nin eleman sayısının tek olduğu gösterilmiş olur. İlk olarak (18) denklemi için aşağıdaki ifadelere bakalım;
a. $x \neq 2y$, aksi halde $p = x^2+4yz = 4(y^2+yz)$ asal bir sayı değil,
b.$x \neq y-z$, aksi halde $p = (y-z)^2+4yz = (y+z)^2$ asal bir sayı değil.
Dahası $y-z < 2y$ dir. Böylece x değerlerini üç aralığa bölebiliriz:

$$(I) \quad x < y-z$$

$$(II) \quad y-z < x < 2y$$

$$(III) \quad 2y < x$$

Şimdi aşağıdaki involütü ele alalım,

$$\tau(x, y, z) = \begin{cases} (x+2z, z, y-x-z), & x \in (I) \\ (2y-x, y, x-y+z), & x \in (II) \\ (x-2y, x-y+z, y), & x \in (III) \end{cases} \tag{20}$$

x^2+4xy denkleminin herhangi bir çözümünün τ involütü ile aynı denklemin bir başka çözümüne dönüştüğünü kontrol etmek kolaydır. Gerçekten (I)'de

$$(x+2z)^2+4z(y-x-z) = x^2+4yz$$

(II) ve (III)'de

$$(x-2y)^2+4y(x-y+z) = x^2+4yz.$$

olduğu görülür.

Şimdi $\tau(x,y,z) = (x',y',z')$ olsun. $x \in (I)$ ise $(x < y-z)$, bu durumda $x' = x+2z > 2z = 2y'$ olur ve (I)'deki bir nokta (III)'deki bir noktaya dönüşmüş olur yani $x' \in (III)$. Benzer şekilde $x \in (III)$ noktasının $x' \in (I)$ noktasına dönüştüğü görülür. Buradan (I) yada (III)'deki bir noktanın; (I)'de $x' = x+2z > x$ ve (III)'de $x' = x-2y < x$ olduğundan sabit bir nokta olamıyacağı görülür. Bunun anlamı sabit nokta yalnız (II) aralığında olabilir ve böyle bir nokta için $z' = x-y+z$ ve buradan $z = z'$ olduğundan $x = y$ olur. Böylece $p = x^2+4yz = x^2+4xz = x(x+4z)$ ve p asal bir sayı olduğundan $x = y = 1$ bulunur. Sonuç olarak $p = 4k+1$ ise $(1,1,k)$ bir sabit noktadır. Gerçekten $x = 1, y = 1$ ve $z = k$ ise, $x' = 2-1 = 1, y' = 1$ ve $z' = 1-1+k = k$ ve $p = 4k+1$ olur.

Şimdi yukarıdaki teoremler yardımıyla elde etmek istediğimiz sonucu yazabiliriz.

Sonuç: *(Fermat)* n tamsayısının iki tamkare toplamı şeklinde yazılabilmesi için gerek ve yeter şart n'nin $4k+3$ şeklindeki bütün asal çarpanlarının üssünün çift olmasıdır.

Örnek: $245 = 5.7.7 = 7^2+14^2$, $42 = 2.3.7 \neq a^2+b^2$

Yukarıdaki sonuçtan da görüldüğü gibi her tamsayıyı iki tamkare ya da Legendre'nin "üç tamkare teoremine" göre üç tamkare toplamı şeklinde yazmak mümkün değil.
Bundan sonraki yazımızda her tamsayıyın dört tamkare toplamı şeklinde bir gösterimi olduğunu ifade eden "Dört Tamkare Teoremi" ni ve bu teoremin, karmaşık sayıların genelleşmesi olan quaternionlarla ilişkisini bulabileceksiniz.

Ek: M herhangi bir küme ve $\sigma : M \to M$ bir dönüşüm olsun. Eğer σ dönüşümü her $m \in M$ için $\sigma(\sigma(m)) = m$ koşulunu sağlarsa σ'ya bir involüt denir. İnvolüt M'nin elemanlarını $(m,\sigma(m))$ gibi çiftlere ayırır. $\sigma(\sigma(m)) = m$ olduğundan m ve $\sigma(m)$ elemanları için sırasıyla simetrik $(m,\sigma(m))$ ve $(\sigma(m),m)$ çiftleri elde edilir. Ancak $\sigma(m) = m$ olduğunda (m,m) elemanı elde edilir. Böyle bir noktaya sabit nokta denir. Böylece M sonlu bir küme ise $(m,\sigma(m))$ noktalar kümesinin eleman sayısının çift yada tek olması, sabit noktalarının çift ya da tek olmasına bağlı olduğu görülür.

KAYNAKLAR:

1. V.V. Prasolov, Story of numbers, polynomials and figures, Moscov, 1997.

2. D. Zagier, A one-sentence proof that every prime $p \equiv 1(mod4)$ is a sum of two squares, American Math Montly, 1990,114

3. D.R. Heath-Brown, Fermat's two squares theorem, Invariant 1984,3-5.

Modern matematiğin kapsadığı o çok geniş alan hakkında bir fikir vermek zordur. Ben matematik denilince çıplak bir düzlük anlamıyorum; matematik, içinde binbir güzelliğin kaynaştığı nefis manzaralı bir vatan köşesi gibidir; önce uzaktan şöyle bir görülür; fakat bu yetmez; bir uçtan, diğer uca onun en ince ayrıntıları, vadileri, ırmakları, kayaları, ormanları ve çiçekleri mutlaka incelenmeye değer.

ARTHUR CAYLEY