# Gauss Tamsayıları ve Cebirsel Tamsayı Halkaları


BÜLENT SARAÇ

*Hacettepe Üniversitesi Matematik Bölümü*
bsarac@hacettepe.edu.tr

Önceki yazımızda antik Yunan matematikçilerinin çalışmalarına kadar uzanan tamsayılardaki çarpanlara ayırma özelliğinin başka halkalarca de sağlandığını gördük. Bu kapsamda, özel olarak, Gauss tamsayıları olarak bilinen karmaşık sayılar kümesinde, tıpkı tamsayılarda olduğu gibi, asal sayılar tanımlanabildiğini ve bu sayede çarpanlara ayırma özelliğini tartışabildiğimizi görmüştük. Bu yazımızda, daha önce söz verdiğimiz gibi, Gauss tamsayılarının bu güçlü özelliği sayesinde elde edebilceğimiz bazı sonuçlara ve bu sonuçların sayı teorisi açısından önemli olan ve "iki kare teoremi" olarak bilinen sonucu. Ayrıca gelecek yazımız için bir tür hazırlık olması bakımından bazı cebirsel tamsayı halkalarına da kısaca değinmek istiyoruz.

## Gauss Tamsayıları ve İki Kare Teoremi

Hatırlayacak olursak, Gauss tamsayıları $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ kümesi, karmaşık sayılar kümesinin bir alt halkasıdır. Burada $i$, hayali birim denilen ve $i^2 = -1$ eşitliğini sağlayan sayıdır. Her halkada olduğu gibi Gauss tamsayıları halkasında da asal sayılar, sıfır veya birimsel (yani tersinir) olmayan ve kendisi ile birimsellerin çarpımı dışında başka bir şekilde çarpanlara ayrılamayan elemanlar olarak tanımlanır. Örneğin $1 + i \in \mathbb{Z}[i]$ elemanı bir asal Gauss tamsayısıdır. Çünkü $1 + i$ sayısını çarpanlara ayırmak istediğimizde, $1 + i = (a + bi)(c + di)$ şeklinde bir çarpanlara ayırma yapabilmemiz için $ac - bd = 1$ ve $ad + bc = 1$ denklemlerinin sağlanmaması gerekir. Bu denklemler ancak $a, b, c, d$ tamsayıları için $a = \pm 1, b = 0, c = \pm 1$, $d = 0$ veya $a = 0, b = \pm 1, c = 0, d = \pm 1$ olduğunda sağlanabilir. Yani $1 + i$ sayısını $\mathbb{Z}[i]$ içinde çarpanlara ayırabilmek için çarpanlardan birinin birimsel olması gerekir. Fakat $2 \in \mathbb{Z}$ sayısı Gauss tamsayıları içinde asal değildir. Çünkü $2 = (1 + i)(1 - i)$ şeklinde bir çarpanlara ayırma mümkündür ve ne $1 + i$ ne de $1 - i$ birimsel değildir. Bu örnekler bize Gauss tamsayıları içinde asal sayıların dağılımının tamsayılar içindeki asal sayıların dağılımından farklı olduğunu gösterir. Ancak Gauss tamsayıları halkasında da tamsayılarda olduğu gibi her elemanın asal çarpanlara tek türlü ayrılabildiğini, yani Gauss tamsayıları halkasının da bir tek türlü çarpanlara ayırma halkası olduğunu biliyoruz.

$\mathbb{Z}[i]$ halkasında bir elemanın çarpanlarının (ya da denk olarak bölenlerinin) hangi tipte olduğunu veya bir Gauss tamsayısının birimsel olup olmadığını anlamak için norm fonksiyonunu adı verilen kullanışlı bir araçtan da yararlanabiliriz. Gauss tamsayıları için norm fonksiyonu $N(a + bi) = a^2 + b^2$ şeklinde tanımlanır. Buna göre her $z \in \mathbb{Z}[i]$ için $N(z) \in \mathbb{N}$ ve $N(z) = 0$ ise $z = 0$ olur. Ayrıca her $z_1, z_2 \in \mathbb{Z}[i]$ için $N(z_1 z_2) = N(z_1)N(z_2)$ eşitliği sağlanır. Norm fonksiyonunun bu çarpımsal özelliği sayesinde ilk olarak bir Gauss tamsayısının birimsel olup olmadığını anlayabiliriz.

**Teorem 1.**
*Her $z \in \mathbb{Z}[i]$ için aşağıdakiler denktir:*

*(1) $z$ birimsel bir elemandır.*
*(2) $N(z) = 1$.*
*(3) $z = \pm 1$ veya $z = \pm i$.*

*Kanıt.* (1) $\Rightarrow$ (2): $z$ birimsel ise, $z$'nin bir tersi vardır, yani $zz^{-1} = 1$. Norm fonksiyonunun çarpımsal özelliğinden dolayı $N(z)N(z^{-1}) = N(1) = 1$ olur. $N(z), N(z^{-1} \geq 0)$ olduğundan, $N(z) = 1$ olur.

(2) $\Rightarrow$ (3): $N(z) = 1$ ise, $z = a + bi$ için $a^2 + b^2 = 1$ olur. Bu durumda $(a, b)$ ikilisi yalnızca $(\pm 1, 0)$ veya $(0, \pm 1)$ olabilir. Dolayısıyla $z = \pm 1$ veya $z = \pm i$ olur.

(3) $\Rightarrow$ (1): $1 \cdot 1 = 1$, $(-1) \cdot (-1) = 1$, $i \cdot (-i) = 1$ ve $(-i) \cdot i = 1$ olduğundan, $z = \pm 1$ veya $z = \pm i$ ise, $z$ birimsel bir elemandır. □

Yukarıdaki örnekte ele aldığımız $1 + i$ sayısının normu $N(1 + i) = 1^2 + 1^2 = 2$'dir. $1 + i = z_1 \cdot z_2$ olacak şekilde $z_1, z_2 \in \mathbb{Z}[i]$ elemanları varsa, $N(1 + i) = N(z_1)N(z_2)$ eşitliğinden $2 = N(z_1)N(z_2)$ olur. Buradan $N(z_1)$ ve $N(z_2)$'nin yalnızca 1 ve 2 değerlerini alabileceğini görürüz. Ancak $N(z) = 1$ ise $z = \pm 1$ veya $z = \pm i$, yani $z$ birimsel bir elemandır. Dolayısıyla $1 + i$ sayısı asal bir Gauss tamsayısıdır.

**Teorem 2.**

*$p$ bir asal tamsayı ise, aşağıdakilerden yalnızca biri doğrudur:*

*(1) $p$ Gauss tamsayıları içinde de asaldır.*
*(2) $p = 2$'dir ve $2 = (1 + i)(1 - i)$ şeklinde çarpanlara ayrılır.*
*(3) $p \equiv 1 \pmod 4$ ve $p = a^2 + b^2$ olacak şekilde $a, b \in \mathbb{Z}$ tamsayıları vardır, yani $p$ **iki kare toplamı** olarak yazılabilir.*

*Kanıt.* $p$ bir asal tamsayı olsun. Kabul edelim ki $p \neq 2$ olsun. Bu durumda $N(p) = p^2$ olur. Eğer $p$ Gauss tamsayıları içinde asal ise, (1) maddesi doğrudur. Aksi halde, $p$ Gauss tamsayıları içinde asal değildir. Bu durumda $p = z_1 z_2$ olacak şekilde $z_1, z_2 \in \mathbb{Z}[i]$ elemanları vardır ve ne $z_1$ ne de $z_2$ birimsel değildir. Dolayısıyla $N(z_1), N(z_2) > 1$ olur. Norm fonksiyonunun çarpımsal özelliğinden dolayı $N(p) = N(z_1)N(z_2)$ eşitliği sağlanır. Yani $p^2 = N(z_1)N(z_2)$ olur. Buradan $N(z_1)$ ve $N(z_2)$'nin yalnızca $p$ değerini alabileceğini görürüz. O halde $N(z_1) = p$ ve $N(z_2) = p$ olur. Şimdi $z_1 = a + bi$ için $N(z_1) = a^2 + b^2 = p$ olur. Bu durumda $p = a^2 + b^2$ olacak şekilde tamsayılar $a, b$ vardır. Şimdi $p$'nin 4 ile bölümünden kalanı inceleyelim. $a$ ve $b$ tamsayılarının her biri ya çift ya da tek olabilir.

- Eğer $a$ ve $b$ ikisi de çift ise, o zaman $a = 2m$ ve $b = 2n$ olacak şekilde $m, n \in \mathbb{Z}$ için yazılabilir. Bu durumda $p = a^2 + b^2 = 4m^2 + 4n^2 = 4(m^2 + n^2)$ olur. Yani $p$ sayısı 4'ün katı olur ki, bu da $p$'nin asal sayı olduğu varsayımıyla çelişir.
- Eğer $a$ ve $b$ ikisi de tek ise, o zaman $a = 2m + 1$ ve $b = 2n + 1$ olacak şekilde $m, n \in \mathbb{Z}$ için yazılabilir. Bu durumda

$$\begin{aligned} p = a^2 + b^2 &= (2m + 1)^2 + (2n + 1)^2 \\ &= 4m^2 + 4m + 1 + 4n^2 + 4n + 1 \\ &= 4(m^2 + m + n^2 + n) + 2 \end{aligned}$$

  olur. Bu da $p$'nin bir tek asal sayı olduğu varsayımıyla çelişir.
- Eğer $a$ tek ve $b$ çift ise, o zaman $a = 2m + 1$ ve $b = 2n$ olacak şekilde $m, n \in \mathbb{Z}$ için yazılabilir. Bu durumda

$$\begin{aligned} p = a^2 + b^2 &= (2m + 1)^2 + (2n)^2 \\ &= 4m^2 + 4m + 1 + 4n^2 \\ &= 4(m^2 + m + n^2) + 1 \end{aligned}$$

  olur. Yani $p$ sayısının 4 ile bölümünden kalan 1 olur.
- Eğer $a$ çift ve $b$ tek ise, o zaman da benzer şekilde $p$ sayısının 4 ile bölümünden kalan 1 olur.

Sonuç olarak, $p$ sayısı asal ve $p \neq 2$ ise, $p \equiv 1 \pmod 4$ olur ve $p = a^2 + b^2$ olacak şekilde $a, b$ tamsayıları vardır. Eğer $p = 2$ ise, o zaman $2 = (1+i)(1-i)$ şeklinde çarpanlara ayrılır. Böylece teoremdeki üç durumdan

en birinin doğru olduğu gösterilmiş olur. Ayrıca bu üç dürümun ayrık olduğu da açıktır. Dolayısıyla teorem ispatlanmış olur. □

Yukarıdaki teorem, tamsayılardaki asal sayıların Gauss tamsayıları içindeki durumunu açıklamaktadır. Özellikle (3) maddesi, asal sayıların iki kare toplamı olarak ifade edilebilmesiyle ilgili önemli bir sonuçtur. Buna göre teoremin (1) maddesine uyan asal tamsayıları merak etmek doğaldır. Bunu aşağıdaki teorem ile açıklayabiliriz.

**Teorem 3.**
*$p$ bir asal tamsayı ise aşağıdakiler denktir:*

*(1) $p$, Gauss tamsayıları içinde asaldır.*
*(2) $p \equiv 3 \pmod 4$.*
*(3) $p$ sayısı iki tamsayının karelerinin toplamı olarak ifade edilemez.*

*Kanıt.* $p$ bir asal tamsayı olsun. Eğer (1) maddesi doğru ise, o zaman $p = 2$ olamaz. Ayrıca, bu durumda, önceki teoremin (3) maddesi de doğru olamaz. Çünkü eğer $p = a^2 + b^2$ olacak şekilde $a, b$ tamsayıları varsa, o zaman $p = (a + bi)(a - bi)$ olacağından $p$, Gauss tamsayıları içinde asal değildir. Öte yandan $p \equiv 0 \pmod 4$ veya $p \equiv 2 \pmod 4$ olamayacağı da açıktır. Dolayısıyla (1) maddesi doğru ise, (2) maddesi doğrudur.

Şimdi (2) $\Rightarrow$ (3) gerektirmesini gösterelim. $p = a^2 + b^2$ olacak şekilde $a, b$ tamsayıları olsun. Teorem 2'nin kanıtında olduğu gibi incelenecek olursa

$$p \equiv \begin{cases} 0 \pmod 4, & \text{eğer } a, b \text{ ikisi de çift ise} \\ 2 \pmod 4, & \text{eğer } a, b \text{ ikisi de tek ise} \\ 1 \pmod 4, & \text{eğer } a \text{ tek, } b \text{ çift veya } a \text{ çift, } b \text{ tek ise} \end{cases}$$

durumları elde edilir. Buradan görülebileceği gibi, $p \equiv 3 \pmod 4$ ise, $p = a^2 + b^2$ olacak şekilde $a, b$ tamsayıları bulunamaz.

(3) maddesi doğru ise Teorem 2'den dolayı (1) maddesi de doğrudur. Böylece teorem kanıtlanmış olur. □

Yukarıdaki iki teorem birlikte ele alındığında, bir asal tamsayının Gauss tamsayıları içinde asal olup olmadığını belirlemek için o asal tamsayının 4 ile bölümünden kalanına bakmamız yeterli olur. Eğer asal tamsayı $4k + 1$ şeklinde ise, o zaman o asal tamsayı Gauss tamsayıları içinde asal değildir ve iki kare toplamı olarak ifade edilebilir. Eğer asal tamsayı $4k + 3$ şeklinde ise, o zaman o asal tamsayı Gauss tamsayıları içinde asaldır ve iki kare toplamı olarak ifade edilemez. Ayrıca 2 sayısı da Gauss tamsayıları içinde asal değildir ve $2 = 1^2 + 1^2$ şeklinde iki kare toplamı olarak ifade edilebilir.

**Teorem 4.**
*Bir asal Gauss tamsayısı aşağıdaki şekillerden birinde ifade edilebilir:*

*(I) $p$ bir asal tamsayı ve $p \equiv 3 \pmod 4$ olmak üzere $\pm p$ ve $\pm ip$.*
*(II) $a, b \in \mathbb{Z}$ ve $a^2 + b^2 = p$ asal sayı olmak üzere $a + bi$.*

*Kanıt.* I. tipten Gauss sayılarının asallığı yukarıdaki teoremlerden açıktır. II. tipten bir Gauss tamsayısının asallığını da norm fonksiyonunun çarpımsallığını kullanarak kolayca görebiliriz.

Şimdi $z = a + ib$ bir asal Gauss tamsayısı olsun. Eğer $b = 0$ ise $z = a$ bir tamsayıdır ve bu tamsayı, birden farklı iki tamsayının çarpımına ayrılırsa Gauss tamsayıları içinde de ayrılır. Dolayısıyla $|a|$ bir asal tamsayıdır. $z = a$ bir asal Gauss tamsayısı olduğundan Teorem 3 gereğince $P \equiv 3 \pmod 4$ olur. Öte yandan, $a = 0$ ise $z = ib$ olur ve benzer şekilde $|b|$ bir asal tamsayıdır ve bu durumda $|b| = p$ için $z = \pm ip$ ve $p \equiv 3 \pmod 4$ olur. Böylece I. tipteki asal Gauss tamsayıları elde edilir.

Şimdi $a \neq 0$ ve $b \neq 0$ olduğunu varsayalım. $N(z)$'nin asal bir tamsayı olduğunu gösterelim. Eğer $N(z)$ asal değil ise, $N(z) = mn$ olacak şekilde $m, n \in \mathbb{N}$ ve $1 < m, n < N(z)$ için yazılabilir. O zaman $a^2 + b^2 = mn$ olur. Kabulden dolayı $a + ib$ asal bir Gauss tamsayısıdır. Ayrıca eğer $a - ib$ iki Gauss tamsayısının çarpımı olarak yazılabilirse, eşleniği olan $a + ib$ de bunların eşleniğinin çarpımı olarak yazılabilir. Dolayısıyla, $a - ib$ de bir asal Gauss tamsayısıdır. Eğer $m$ ve $n$ asal Gauss tmasayıları ise $\mathbb{Z}[i]$ bir tek türlü çarpanlara ayırmma bölgesi olduğundan bu durum bir çelişki olur. O halde $m$ veya $n$'den en az biri asal Gauss tamsayısı değildir. Diyelim ki $m$ asal Gauss tamsayısı değildir. O zaman $m = z_1 z_2$ olacak şekilde $z_1, z_2 \in \mathbb{Z}[i]$ ve ne $z_1$ ne de $z_2$ birimsel değildir. Fakat bu durumda da $(a + ib)(a - ib) = mn = z_1 z_2 n$ eşitliğinin sol tarafı iki asal Gauss tamsayısının çarpımı iken sağ tarafı en az üç asal Gauss tamsayısının çarpımı olur. Bu da $\mathbb{Z}[i]$'nin bir tek türlü çarpanlara ayırma bölgesi olmasıyla çelişir. Böylece $N(z)$ bir asal tamsayıdır. O halde $N(z) = a^2 + b^2 = p$ olacak şekilde bir asal tamsayı $p$ vardır. Böylece II. tipteki asal Gauss tamsayıları elde edilir. □

**Teorem 5.**

*$p$ bir asal tamsayı ve $a, b, c, d$ pozitif tamsayılar olmak üzere*

$$p = a^2 + b^2 = c^2 + d^2$$

*olsun. O zaman ya $a = \pm c$ ve $b = \pm d$ ya da $a = \pm d$ ve $b = \pm c$ olur.*

*Kanıt.* $(a + ib)(a - ib) = (c + id)(c - id)$ eşitliği $N(a \pm ib) = N(c \pm id) = p$ eşitliğini verir. Dolayısıyla Teorem 4 gereğince $a \pm ib$ ve $c \pm id$ asal Gauss tamsayılarıdır. $\mathbb{Z}[i]$ bir tek türlü çarpanlara ayırma bölgesi olduğundan, $a + ib$ sayısı $c \pm id$ sayısının birimsel (yani $\pm 1$ veya $\pm i$) katı olmak zorundadır. Bu durumda $a+ib, \pm(c \pm id), \pm i(c \pm id)$ tipindeki elemanlarından biridir. $a, b, c, d > 0$ kabul edildiğinden, $a+ib = c+id$ veya $a + ib = d + ic$ olur. Buradan istenen sonuç kolayca elde edilir. □

Şimdi sadece asal tamsayıların değil, tüm tamsayılar için iki kare toplamı olarak ifade edilebilme durumunu belirleyeceğiz. Fakat öncesinde aşağıdaki lemmayı kanıtlayalım.

**Önsav 1.**

*İki kare toplamı olan sayıların çarpımı da iki kare toplamı olarak yazılabilir.*

*Kanıt.* $a^2 + b^2$ ve $c^2 + d^2$ iki kare toplamı için

$$\begin{aligned}(a^2 + b^2)(c^2 + d^2) &= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 \\ &= (ac - bd)^2 + (ad + bc)^2\end{aligned}$$

olacağından istenen sonuç elde edilir. □

**Teorem 6. (İki Kare Teoremi)**

*$n \in \mathbb{N}$ için aşağıdakiler denktir:*

*(1) $n = a^2 + b^2$ olacak şekilde $a, b \in \mathbb{Z}$ tamsayıları vardır.*
*(2) $n$'nin asal çarpanlarına ayrılışındaki $p$ asallarından $p \equiv 3 \pmod 4$ olacak şekilde olanların kuvvetleri çifttir.*

*Kanıt.* (1) $\Rightarrow$ (2): $n = a^2 + b^2$ olacak şekilde $a, b \in \mathbb{Z}$ tamsayıları olsun. O zaman $n = (a + ib)(a - ib)$ olur. $\mathbb{Z}[i]$ bir tek türlü çarpanlara ayırma bölgesi olduğundan, $a + ib$ ve $a - ib$ Gauss tamsayıları içinde asal çarpanlara ayrılabilir. Teorem 4 gereğince $a + ib = p_1 \dots p_r z_1 \dots z_s$ ve $a - ib = p_1 \dots p_r \overline{z_1} \dots \overline{z_s}$ olacak şekilde 4 ile bölündüğünde 3 kalanı veren $p_i$ asal tamsayıları ile normu asal olan $z_1, \dots, z_m$ Gauss tamsayıları vardır.

Bu durumda

$$n = (a+ib)(a-ib) = p_1^2 \dots p_r^2 N(z_1) \dots N(z_s)$$

ve her $i = 1, \dots, s$ için $N(z_i)$ bir asal tamsayı ve $N(z_i) \equiv 1 \pmod 4$ olur. Buradan görülebileceği gibi, $n$'nin asal çarpanlarına ayrılışında $p_i$ asal tamsayılarının kuvvetleri çifttir.

(2) $\Rightarrow$ (1): $n \in \mathbb{N}$ için $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ şeklinde asal çarpanlara ayrıldığını varsayalım. Burada her $p_i$ bir asal tamsayı ve her $e_i$ bir pozitif tamsayıdır. Kabulden dolayı her $p_i$ için aşağıdakilerden biri doğrudur:

- $p_i = 2$,
- $p_i \equiv 1 \pmod 4$,
- $p_i \equiv 3 \pmod 4$ ve $e_i$ çift sayıdır.

Teorem 2, Teorem 3 ve Lemma 1 gereğince ilk iki durumda $p_i^{e_i}$ ifadesi iki kare toplamı olarak yazılabilir. $p_i \equiv 3 \pmod 4$ ve $e_i = 2t$ çift tamsayısı ise, $p_i^{e_i} = (p_i^t)^2 + 0^2$ şeklinde iki kare toplamı olarak yazılabilir. Ayrıca iki kare toplamı olan sayıların çarpımı da iki kare toplamı olarak yazılabildiğinden, $n$ de iki kare toplamı olarak yazılabilir. □

**Örnek 1.**

$n = 2450$ sayısının iki kare toplamı olarak yazılıp yazılamayacağını belirleyelim. $2450 = 2^1 \cdot 5^2 \cdot 7^2$ şeklinde asal çarpanlara ayrılır. Burada 2 ve 5 sayıları iki kare toplamı olarak yazılabilir. Ayrıca $7 \equiv 3 \pmod 4$ ancak kuvveti çift olduğundan, Teorem 6 gereğince 2450 sayısı da iki kare toplamı olarak yazılabilir. 2450 sayısının iki kare toplamı şeklindeki yazımlarını bulmak için öncelikle bu sayıyı asal çarpanlarına ayıralım:

$$\begin{aligned} 2450 &= 2 \cdot 5^2 \cdot 7^2 \\ &= (1+i)(1-i) \cdot (1+2i)^2 (1-2i)^2 \cdot 7^2 \end{aligned}$$

Gauss tamsayılarında bu çarpanları çeşitli biçimlerde iki gruba ayırabiliriz öyle ki bir grup diğerinin eşleniğidir. İlk olarak,

$$2450 = [(1+i)(1+2i)^2 \cdot 7] \cdot [(1-i)(1-2i)^2 \cdot 7]$$

şeklinde yazarak, birinci çarpanı hesaplayalım:

$$\begin{aligned} (1+2i)^2 &= 1 + 4i - 4 = -3 + 4i \\ (1+i)(-3+4i) &= -3 + 4i - 3i - 4 = -7 + i \\ (-7+i) \cdot 7 &= -49 + 7i \end{aligned}$$

Buna göre $2450 = |-49 + 7i|^2 = 49^2 + 7^2 = 2401 + 49$ olur.

Alternatif olarak,

$$2450 = [(1+i)(1-2i) \cdot 7^2] \cdot [(1-i)(1+2i) \cdot 7^2]$$

şeklinde yazarsak:

$$\begin{aligned} (1+i)(1-2i) &= 1 - 2i + i + 2 = 3 - i \\ (3-i) \cdot 49 &= 147 - 49i \end{aligned}$$

bulunur. Bu durumda $2450 = 147^2 + 49^2 = 21609 + 2401$ olur.

Bir başka gruplandırmada ise,

$$2450 = [(1+i)(1+2i)(1-2i) \cdot 7] \cdot [(1-i)(1+2i)(1-2i) \cdot 7]$$

yazabiliriz. Burada $(1+2i)(1-2i) = 1 + 4 = 5$ olduğundan:

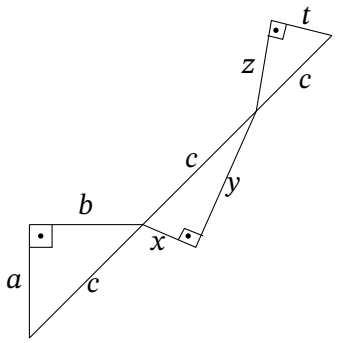
$$(1+i) \cdot 5 \cdot 7 = (5+5i) \cdot 7 = 35 + 35i$$

Bu durumda $2450 = 35^2 + 35^2 = 1225 + 1225$ olur.

Sonuç olarak $2450 = 7^2 + 49^2 = 49^2 + 7^2 = 35^2 + 35^2$ şeklinde farklı biçimlerde iki kare toplamı olarak yazılabilir.

**Örnek 2.**

Aşağıdaki düzlemsel şekilde $a$, $b$, $c$, $x$, $y$, $z$ ve $t$ birbirlerinden farklı birer pozitif tamsayı olmak üzere kenar uzunlukları bu sayılara eşit olan, hipotenüzleri eşit uzunlukta ve aynı doğru üzerinde üç adet dik üçgen gösterilmiştir.




Burada aradığımız, $a$, $b$, $x$, $y$, $z$ ve $t$ sayılarının toplamının en küçük değeridir. Üçgenlerin hipotenüz uzunlukları eşit ve $c$ birim olduğundan Pisagor teoremine göre

$$c^2 = a^2 + b^2 = x^2 + y^2 = z^2 + t^2$$

olur. Dolayısıyla karesi en az üç farklı biçimde iki (pozitif) kare toplamı olarak yazılabilen en küçük $c$ sayısını aramakla başlayabiliriz. Tabii buradaki her yazımda toplam terimlerinin birbirinden farklı olması gerektiğini de unutmamalıyız. Bu ana sorunun çözümü için önce aşağıdaki sorulara yanıt arayarak biraz ısınalım.

*İki pozitif kare toplamı olarak yazılabilen en küçük tamsayı nedir? Toplam terimleri farklı olacaksa bu sayı ne olur?* Bu sorunun yanıtını Teorem 6 gereğince $2 = 1^2 + 1^2$ olarak bulabiliriz. Buradaki toplam terimlerinin aynı olduğuna dikkat edelim. Buna göre toplam terimleri de farklı olup iki pozitif kare toplamı olarak yazılabilen en küçük tamsayı Teorem 4'ün de yardımıyla $5 = 1^2 + 2^2$ olarak bulunur.

*İki pozitif kare toplamı olarak en az iki farklı biçimde yazılabilen en küçük tamsayı nedir?* Bu sorunun yanıtını da Teorem 6 gereğince $50 = 5^2 + 5^2 = 7^2 + 1^2$ olarak bulabiliriz. Buradaki yazımların birinde toplam terimlerinin aynı olduğuna dikkat edelim. Buna göre toplam terimleri de farklı olup iki pozitif kare toplamı olarak en az iki farklı biçimde yazılabilen en küçük tamsayı Teorem 4'ün de yardımıyla $5 \times 13 = 65 = 8^2 + 1^2 = 7^2 + 4^2$ olarak bulunur. Buradaki esas fikir sayının yazımında en az iki asal çarpan bulunmasını sağlamaktır. Bu asalları da 4 modülüne göre 1 kalanı veren asallardan seçmek akıllıca olur; aksi halde diğer asallar, ancak çift kuvvet ile yazılabilmesi ve iki (pozitif) kare toplamı olarak yazılamaması nedeniyle, sayıyı büyütmekten başka bir işe yaramayacaktır. Buna göre $n = pq$ şeklinde bir sayı için $p$ ve $q$ asalları $4k + 1$ şeklinde ise, $p = z_1\overline{z_1}$ ve $q = z_2\overline{z_2}$ olacak şekilde $z_1, z_2 \in \mathbb{Z}[i]$ bulunabilir. Böylece $n = (z_1z_2)(\overline{z_1z_2})$ ve $n = (z_1\overline{z_2})(\overline{z_1}z_2)$ şeklinde iki farklı biçimde yazılabilir. İki durumda da $n = z\overline{z}$ tipinde olacağından $n$ sayısı iki kare toplamı olarak iki farklı şekilde yazılabilir.

Şimdi esas sorumuza geri dönelim. Üç pozitif kare toplamı olarak en az üç farklı biçimde yazılabilen ve tam kare olan en küçük tamsayıyı arıyoruz. Yukarıdaki düşünceleri kullanarak bu sayının $(5)^2$ olması gerektiğini söyleyebiliriz. Nitekim

$$(5 \cdot 13)^2 = (1 + 2i)^2(1 - 2i)^2(2 + 3i)^2(2 - 3i)^2$$

olduğundan bu sayıyı

$$[(1+2i)(2+3i)]^2[(1-2i)(2-3i)]^2 \quad \text{(A)}$$
$$[(1+2i)(2-3i)]^2[(1-2i)(2+3i)]^2 \quad \text{(B)}$$
$$[(1+2i)(1-2i)(2+3i)^2][(2-3i)^2(1-2i)(1+2i)] \quad \text{(C)}$$
$$[(2+3i)(2-3i)(1+2i)^2][(1-2i)^2(2-3i)(2+3i)] \quad \text{(D)}$$

Biçimlerinden biriyle ifade edebiliriz. (A) ifadesinden $65^2 = 33^2 + 56^2$, (B) ifadesinden $65^2 = 16^2 + 63^2$, (C) ifadesinden $65^2 = 25^2 + 60^2$ ve (D) ifadesinden $65^2 = 39^2 + 52^2$ yazımları elde edilir. Üstelik sadece üç değil dört farklı iki kare toplamı bulmuş oluruz. Buradan $c = 65$, $(a,b) = (33,56)$, $(x,y) = (16,63)$, $(z,t) = (25,60)$ olarak alınabilir. Böylece aradığımız toplam en az $33+56+16+63+25+60 = 253$ olur.

## ■ Cebirsel Tamsayı Halkaları: Giriş

Gauss tamsayılarının sahip olduğu benzersiz özellikler – özellikle "Tek Türlü Çarpanlara Ayırma" (Unique Factorization Domain - UFD) ve Öklid Algoritması'nın uygulanabilirliği – bize aritmetiğin güvenli sularında yüzme imkanı vermişti. Ancak cesaret edip matematiğin derin sularına açıldığımızda, bu özelliklerin her zaman elimizin altında olmadığını görürüz. Gelecek yazılarımıza bir köprü olması adına, şimdi tamsayı kavramını biraz genişletelim ve bazı *"iyi huylu"* ve *"kötü huylu"* örneklere göz atalım.

### Cebirsel Tamsayı Nedir?

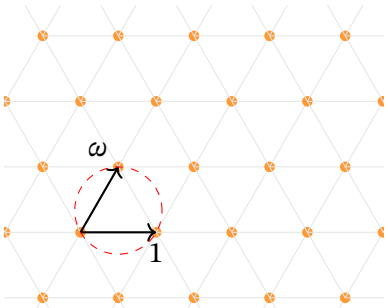
Gauss tamsayılarını tanımlarken katsayıların tamsayı olmasını yeterli görmüştük. Ancak daha genel bir tanım için "monik polinom" kavramına ihtiyacımız vardır. Bir $\alpha$ karmaşık sayısı, katsayıları tamsayı olan ve başkatsayısı 1 olan (monik) bir polinomun kökü ise, $\alpha$'ya bir Cebirsel Tamsayı denir. Örneğin $i$ sayısı $x^2+1=0$ denkleminin kökü olduğundan bir cebirsel tamsayıdır. Benzer şekilde $\sqrt{2}$ sayısı da $x^2-2=0$ denkleminin köküdür ve bir cebirsel tamsayıdır. Peki, rasyonel sayılar kümesindeki $1/2$ sayısı bir cebirsel tamsayı mıdır? $x = 1/2$ için en basit tamsayı katsayılı denklem $2x-1=0$'dır. Ancak bu polinom monik değildir (çünkü başkatsayısı 2'dir). Bunu monik yapmak için 2'ye bölersek $x - 1/2 = 0$ elde ederiz ki bu sefer de katsayıların tümü tamsayı olmaz. Dolayısıyla $1/2$ bir cebirsel sayı olsa da, bir cebirsel tamsayı değildir. Bu ayrım, yapısal olarak tamsayı kavramını genişletirken, bazı önemli özelliklerin korunmasını sağlar.

### İyi Huylu Örnekler: Eisenstein ve Altın Oran

Gauss tamsayılarının yaşadığı evrende yalnız olmadığını göstermek için iki güzel örneğimiz var. Bu halkalar da $\mathbb{Z}[i]$ gibi Tek Türlü Çarpanlara Ayırma Bölgesi (UFD) özelliğine sahiptir.

**1. Eisenstein Tamsayıları ($\mathbb{Z}[\omega]$):** Birimin küp kökü olan $\omega = e^{i2\pi/3} = \frac{-1+i\sqrt{3}}{2}$ sayısını ele alalım. $\omega$, $x^2+x+1=0$ denkleminin köküdür, dolayısıyla bir cebirsel tamsayıdır. $\mathbb{Z}[\omega] = \{a+b\omega \mid a,b \in \mathbb{Z}\}$ kümesi, karmaşık düzlemde kareler yerine eşkenar üçgenlerden oluşan bir kafes (lattice) oluşturur.

$\mathbb{Z}[\omega]$**: Üçgen Kafes**



Gauss tamsayıları için oldukça kullanışlı olan norm fonksiyonu burada $N(a+b\omega) = a^2 - ab + b^2$ şeklinde tanımlanır. Geometrik olarak $\mathbb{Z}[\omega]$, düzlemi $\mathbb{Z}[i]$'den daha sıkı paketler. Herhangi bir karmaşık sayının en yakın kafes noktasına olan uzaklığı $\mathbb{Z}[i]$'de maksimum $1/\sqrt{2} \approx 0.707$ iken, $\mathbb{Z}[\omega]$'da bu mesafe $1/\sqrt{3} \approx 0.577$'dir. Bu "yakınlık", bölme algoritmasının (kalanlı bölme) burada da kusursuz çalışmasını sağlar. Sonuç olarak Eisenstein tamsayıları da bir tek türlü çarpanlara ayırma bölgesidir.

**2. Altın Oran Halkası ($\mathbb{Z}[\phi]$):** $\mathbb{Z}[\sqrt{5}]$ halkasına baktığımızda, burada "eksik" bir şeyler olduğunu görürüz. Çünkü Altın Oran sayısı olan $\phi = \frac{1+\sqrt{5}}{2}$, $x^2 - x - 1 = 0$ monik polinomunun köküdür ve dolayısıyla bir cebirsel tamsayıdır, fakat $\mathbb{Z}[\sqrt{5}]$ içinde değildir.Bu nedenle, $\mathbb{Q}(\sqrt{5})$ cisminin "asıl" tamsayılar halkası $\mathbb{Z}[\phi] = \{a + b\phi \mid a, b \in \mathbb{Z}\}$ kümesidir ve bu halka da bir tek türlü çarpanalra ayırma bölgesidir.

### Kaos: $\mathbb{Z}[\sqrt{-5}]$

Her şeyin $\mathbb{Z}[i]$ veya $\mathbb{Z}[\omega]$ gibi mükemmel işlediği yanılgısına düşmemek gerektiğini, $\mathbb{Z}[\sqrt{-5}] = \{a+b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ halkasının bir tek türlü çarpanlara ayırma bölgesi olmadığına önceki yazımızda değinmiştik. Şimdi bu halkaya biraz daha yakından bakalım.

Norm fonksiyonumuz $N(a + b\sqrt{-5}) = a^2 + 5b^2$ olsun. 6 sayısını iki farklı şekilde çarpanlarına ayıralım:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$$

Çarpanlar daha fazla parçalanabiliyor mu diye bakalım. Bunu normları kontrol ederek yapabiliriz:

- $N(2) = 4$. Eğer $2 = xy$ olsaydı, $N(x)N(y) = 4$ olurdu. $N(x) = 2$ olmalı (aksi halde $x$ birimsel olur). Ancak $a^2 + 5b^2 = 2$ denkleminin tamsayı çözümü yoktur. Demek ki 2, indirgenemez (irreducible) bir elemandır.
- Benzer şekilde $N(3) = 9$ ve normu 3 olan bir eleman olmadığından 3 de indirgenemezdir.
- $N(1 \pm \sqrt{-5}) = 1^2 + 5(1)^2 = 6$. Normu 2 veya 3 olan eleman olmadığı için bunlar da indirgenemezdir.

Elimizde 6 sayısının iki tamamen farklı (birbirinin birimsel katı olmayan) indirgenemez çarpanlara ayrılışı var. Bu durum, $\mathbb{Z}[\sqrt{-5}]$ halkasında Tek Türlü Çarpanlara Ayırma özelliğinin bozulduğunu gösterir. Daha da ilginci, bu halkada "Asal" ve "İndirgenemez" kavramları ayrışır. Tamsayılarda alıştığımız üzere $p$ bir çarpımı bölüyorsa ($p|ab$), çarpanlardan en az birini bölmelidir ($p|a$ veya $p|b$). Buna asallık özelliği denir. Ancak $\mathbb{Z}[\sqrt{-5}]$'te 2 sayısı, $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$ çarpımını böldüğü halde, ne $(1 + \sqrt{-5})$'i ne de $(1 - \sqrt{-5})$'i bölemez. Dolayısıyla 2 sayısı bu halkada indirgenemezdir ama asal değildir. İşte bu aritmetik "kaos", 19. yüzyılda Kummer ve Dedekind gibi matematikçileri "İdeal Sayılar" teorisini geliştirmeye iten temel motivasyon olmuştur. Gelecek yazımızda, bu kaosu çözmek için sayıların kendisi yerine, sayı kümeleri olan "İdealler" ile nasıl çalışacağımızı ve tek türlü çarpanlara ayırma özelliğini idealler dünyasında nasıl geri kazanacağımızı inceleyeceğiz.

## ■ Kaynaklar


[1] Stewart, I. and Tall, D. *Algebraic Number Theory and Fermat's Last Theorem*. 4th ed., CRC Press, 2015.

[2] Dummit, D. S. and Foote, R. M. *Abstract Algebra*. 3rd ed., Wiley, 2004.

[3] Ireland, K. and Rosen, M. *A Classical Introduction to Modern Number Theory*. 2nd ed., Springer, 1990.

[4] Edwards, H. M. *Fermat's Last Theorem: A Genetic Introduction*. Springer, 1977.

[5] Stillwell, J. *Elements of Number Theory*. Springer, 2010.

[6] Conrad, K. *The Gaussian Integers*. (Erişim: Online Ders Notları).