Kapak Konusu: Modüler ve p-sel Sayılar

Modüler Sayılar

Tamsayıların dört sütun halinde yazıldığı yandaki çizelgeye bir göz atın. İlk sütunda 4'e tam olarak bölünen sayılar var. Onun sağındaki sütunda 4'e bölündüğünde 1 kalan sayılar var. Onun da sağındaki sütunda 4'e bölündüğünde 2 kalan sayılar ve en sağdaki sütunda 4'e bölündüğünde 3 kalan sayılar var.

	...		
−8	−7	−6	−5
−4	−3	−2	−1
0	1	2	3
4	5	6	7
8	9	10	11
12	**13**	14	15
16	17	18	19
20	21	**22**	23
24	25	26	27
28	29	30	31
32	33	34	**35**
36	37	38	39
40	41	42	43
44	45	46	47
	...		

Sütunlara soldan sağa doğru sıfırıncı, birinci, ikinci, üçüncü diye adlandıralım. 0, 1, 2, 3 sayılarının kendi adlarıyla anılan sütunlarda olduğuna dikkatinizi çekerim: 0, sıfırıncı sütunda, 1, birinci sütunda vs.

Birinci ve ikinci sütunlardan birer sayı alalım, diyelim 13 ve 22. Bu iki sayının toplamı (örnekte 35) hep üçüncü sütunda olacaktır. Birinci sütundan hangi sayıyı alırsak alalım, bu sayının ikinci sütundan herhangi bir sayıyla toplamı – şaşılası şey – hep üçüncü sütunda çıkacaktır. Eğer sayıları çarparsak bu kez çarpım hep ikinci sütunda çıkacaktır. Başka iki sütundan birer sayı alalım. Bu iki sayının da toplamı ve çarpımı hep aynı sütunlarda olacaktır. Sayıların toplamının ya da çarpımının bulunduğu sütun, toplanılan ya da çarpılan sayılardan ziyade, bu sayıların bulundukları sütunlara göre değişiyor.

Böylece, sayıların toplamı ve çarpımı sayesinde, sütunların toplamını ve çarpımını tanımlayabiliriz. Birinci ve ikinci sütunların toplamı üçüncü sütun, çarpımı da ikinci sütun olsun, çünkü sayıların toplamı ve çarpımı bize bu kuralı fısıldıyor. Aynı akıl yürütmeyle iki sütunun farkını da tanımlayabiliriz.

Eğer a bir tamsayıysa, $\overline{a}$, a'nın sütununu simgelesin. 33, 45 ve 1 aynı (birinci) sütunda olduklarından, sütunları aynıdır, yani

$$\overline{1} = \overline{33} = \overline{45}$$

eşitlikleri geçerlidir. Daha genel olarak, aralarındaki fark 4 olan sayılar aynı sütundadırlar:

$$... = \overline{-7} = \overline{-3} = \overline{1} = \overline{5} = \overline{9} = ...$$

Sütunları soldan sağa doğru

$$\overline{0},\ \overline{1},\ \overline{2},\ \overline{3}$$

olarak adlandırdık. Tabii bu sütunlar aynı zamanda (sırasıyla)

$$\overline{8},\ \overline{5},\ \overline{6},\ \overline{7}$$

olarak da ya da bin (ne bini!) değişik şekilde yazılabilirler, ama malum nedenlerden olabildiğince bir önceki yazılımı kullanacağız.

Tanıma göre, $\overline{a}$ ile $\overline{b}$'nin toplamı (yani a'nın bulunduğu sütunla b'nin bulunduğu sütunun toplamı) $a + b$'nin bulunduğu sütundur:

$$\overline{a} + \overline{b} = \overline{a + b} \qquad (1)$$

Çarpım da aynı şekilde tanımlanmıştır:

$$\overline{a} \times \overline{b} = \overline{a \times b} \qquad (2)$$

Bunun gibi, $\overline{a} - \overline{b}$ de,

$$\overline{a} - \overline{b} = \overline{a - b} \qquad (3)$$

olarak tanımlanır.

Bu toplama, çıkarma ve çarpma a ve b'den ziyade, $\overline{a}$ ve $\overline{b}$'ye göre değişir. Yani, $\overline{a}_1 = \overline{a}_2$ ve $\overline{b}_1 = \overline{b}_2$ ise, o zaman,

$$\overline{a}_1 \pm \overline{b}_1 = \overline{a}_2 \pm \overline{b}_2$$

ve

$$\overline{a}_1 \times \overline{b}_1 = \overline{a}_2 \times \overline{b}_2.$$

Zaten sütunları toplamayı, çıkarmayı ve çarpmayı bu sayede tanımlayabildik, bu eşitlikler geçerli olmasaydı böyle bir tanım yapmaya hakkımız olmazdı.

Yukardaki tanımlara göre,

$$\overline{1} + \overline{2} = \overline{3}$$
$$\overline{3} + \overline{2} = \overline{1}$$
$$\overline{3} + \overline{1} = \overline{0}$$
$$\overline{3} - \overline{1} = \overline{2}$$
$$\overline{1} - \overline{3} = \overline{2}$$
$$\overline{3} \times \overline{2} = \overline{2}$$
$$\overline{1} \times \overline{0} = \overline{0}$$
$$\overline{2} \times \overline{2} = \overline{0}$$
$$\overline{33} + \overline{23} = \overline{1} + \overline{3} = \overline{0}$$
$$\overline{33} \times \overline{23} = \overline{1} \times \overline{3} = \overline{3}.$$

Aslında burada yaptığımız şu: Diyelim $\overline{33}$ ile $\overline{23}$'ü çarpmak istiyoruz. O zaman 33'le 23'ü çar-

pıp bu çarpımın bulunduğu sütunu yazarız. Ama 33'le 23'ün çarpımını bulmak kolay olmadığından, 33'ün ve 23'ün sütunlarından çarpması çok daha kolay olan sayıları seçeriz, yukarda 1'i ve 3'ü seçtik.

Negatif sayıların sütunlarını da toplayıp çarpabileceğimizi unutmayalım. Örneğin,

$$\overline{-7} \times \overline{-6} = \overline{1} \times \overline{2} = \overline{2},$$

ya da

$$\overline{-7} \times \overline{-6} = \overline{42} = \overline{2}.$$

Sütunlar kümesi $\mathbb{Z}/4\mathbb{Z}$ olarak tanımlanır:

$$\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}.$$

Bu küme üzerine tanımladığımız toplama ve çarpma işlemlerini aşağıdaki tabloda gösterdik:

+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

×	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$\mathbb{Z}/4\mathbb{Z}$ kümesinin elemanlarının ne olduklarını da unutmayalım:

$$\overline{0} = \{ ..., -8, -4, 0, 4, 8, 12, ...\},$$
$$\overline{1} = \{ ..., -7, -3, 1, 5, 9, 13, ...\},$$
$$\overline{2} = \{ ..., -6, -2, 2, 6, 10, 14, ...\},$$
$$\overline{3} = \{ ..., -5, -1, 3, 7, 11, 15, ...\}.$$

Görüldüğü gibi, $\mathbb{Z}/4\mathbb{Z}$'nin elemanlarının herbiri $\mathbb{Z}$'nin bir altkümesi; genel kabul gören yerleşik kanının tersine $\mathbb{Z}/4\mathbb{Z}$'nin elemanları 0, 1, 2, 3, sayıları değil, $\mathbb{Z}$'nin $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$ ile simgelenen altkümeleridir. Bu altkümeler (sütunlar yani) şöyle de gösterilebilir:

$$\overline{0} = 4\mathbb{Z},$$
$$\overline{1} = 4\mathbb{Z} + 1,$$
$$\overline{2} = 4\mathbb{Z} + 2,$$
$$\overline{3} = 4\mathbb{Z} + 3.$$

Burada, $4\mathbb{Z}$, yazılımın da belirtmek istediği gibi, 4'ün katları olan, yani 4'e bölünen sayılar kümesi demek. $4\mathbb{Z} + 1$ ise, 4'ün katlarına 1 eklendiğinde elde edilen, yani 4'e bölündüğünde 1 kalan sayılar kümesi demek.

Kolayca görüleceği üzere,

$$\overline{0} = 4\mathbb{Z} = 4\mathbb{Z} + 4 = 4\mathbb{Z} + 8 = 4\mathbb{Z} - 4 = \overline{4},$$
$$\overline{1} = 4\mathbb{Z} + 1 = 4\mathbb{Z} + 5 = 4\mathbb{Z} - 3 = \overline{5},$$
$$\overline{2} = 4\mathbb{Z} + 2 = 4\mathbb{Z} + 6 = 4\mathbb{Z} - 2 = \overline{6},$$
$$\overline{3} = 4\mathbb{Z} + 3 = 4\mathbb{Z} + 7 = 4\mathbb{Z} - 1 = \overline{7},$$

Yukarda 4 için yaptıklarımızı herhangi bir pozitif n doğal sayısı için de yapabiliriz. O zaman $\mathbb{Z}/n\mathbb{Z}$ kümesini elde ederiz:

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}.$$

Bu kez $\overline{0}$, $n\mathbb{Z}$ ile simgelenen n'nin katları, yani n'ye bölünen sayılar kümesidir. İşte $\mathbb{Z}/n\mathbb{Z}$ kümesinin elemanları:

$$n\mathbb{Z} = \overline{0} = \{0, \pm n, \pm 2n, \pm 3n, ...\}$$
$$n\mathbb{Z} + 1 = \overline{1} = \{1, \pm n + 1, \pm 2n + 1, \pm 3n + 1, ...\}$$
$$n\mathbb{Z} + 2 = \overline{2} = \{2, \pm n + 2, \pm 2n + 2, \pm 3n + 2, ...\}$$
$$...$$
$$n\mathbb{Z} + n - 1 = \overline{n-1} = \overline{-1}$$
$$= \{n - 1, \pm n + n - 1, \pm 2n + n - 1, ...\}$$

Bu $n\mathbb{Z} + a$ ya da $\overline{a}$ kümelerine ***modülo n*** ya da ***modüler sayılar*** denir. Bunlar bildiğimiz anlamda sayı değiller elbet. Ama aşağıda göreceğimiz üzere, aynen sayılar gibi toplanıp çıkarılıp çarpılırlar.

Modülo n sayıları da aynen $n = 4$ örneğinde olduğu gibi,

$$\overline{a} \pm \overline{b} = \overline{a + b} \qquad (1)$$
$$\overline{a} \times \overline{b} = \overline{a \times b} \qquad (2)$$

kurallarıyla toplayıp çıkarıp çarparız.

Genellikle $\overline{a} \times \overline{b}$ yerine $\overline{a}\,\overline{b}$ yazılır.

(1) ve (2) tanımları sayesinde $\mathbb{Z}$'deki toplama ve çarpmanın birçok özelliği $\mathbb{Z}/n\mathbb{Z}$'ye yansır. Örneğin, $\mathbb{Z}/n\mathbb{Z}$'de de, aynen $\mathbb{Z}$'deki gibi,

$$x(y + z) = xy + xz$$

eşitliği geçerlidir. Bunu kanıtlayalım. $x, y, z \in \mathbb{Z}/n\mathbb{Z}$ olsun. O zaman, $a, b, c \in \mathbb{Z}$ için,

$$x = \overline{a},\ y = \overline{b},\ z = \overline{c}$$

dir. (1) ve (2)'den dolayı:

$$x(y + z) = \overline{a}(\overline{b} + \overline{c}) = \overline{a}\overline{(b + c)} = \overline{a(b + c)}$$
$$= \overline{ab + ac} = \overline{ab} + \overline{ac} = \overline{a}\,\overline{b} + \overline{a}\,\overline{c}$$
$$= xy + xz.$$

Okur, bu kanıttan hareketle, her $x, y, z \in \mathbb{Z}/n\mathbb{Z}$ ve her $a \in \mathbb{Z}$ için,

$$x + (y + z) = (x + y) + z$$
$$x + y = y + x$$
$$x + \overline{0} = \overline{0} + x = x$$
$$\overline{a} + \overline{(-a)} = \overline{0}$$
$$x(yz) = (xy)z$$
$$xy = yx$$
$$\overline{1}x = x\overline{1} = x$$
$$\overline{0}x = x\overline{0} = \overline{0}$$
$$x(y + z) = xy + xz$$

eşitliklerini kolaylıkla kanıtlayabilir.

Üçüncü ve yedinci eşitliklerden dolayı, $\overline{0}$'a $\mathbb{Z}/n\mathbb{Z}$'nin toplama için, $\overline{1}$'e de çarpma için **etkisiz** elemanları denir. Bunlara sırasıyla $\mathbb{Z}/n\mathbb{Z}$'nin **sıfır** ve **birim elemanı** adları da verilir. Dördüncü özellikten dolayı, $\overline{-a}$ elemanını çoğu zaman $-\overline{a}$ olarak yazarız.

Yukardaki dokuz özelliği sağlayan bir "yapı"ya **değişmeli halka** denir. Demek ki

$$(\mathbb{Z}/n\mathbb{Z}, +, \times, \overline{0}, \overline{1})$$

bir değişmeli halkadır. Matematiğin bu önemli yapılarından son üç sayıdır söz ediyoruz. Ama gözünüz korkmasın, bu yazıda soyut halka kavramını kullanmayacağız. Üstelik, değişmeli bir halka, elinden geldiğince tamsayılara benzemek isteyen son derece doğal bir yapıdır. Kolaylık olsun diye, değişmeli halka yerine kısaca halka deyimini kullanıyoruz.

Her ne kadar $a \in \mathbb{Z}$ sayısı modülo 4 ve 5 aynı şekilde, $\bar{a}$ ile gösterilmişse de, bu elemanlar eşit değildirler. Örneğin $a = 0$ ise, $\mathbb{Z}/4\mathbb{Z}$'de $\bar{0} = 4\mathbb{Z}$, ama $\mathbb{Z}/5\mathbb{Z}$'de $\bar{0} = 5\mathbb{Z}$. Dolayısıyla $\bar{a}$ yazılımını kullanırken dikkatli olunmalıdır, eğer herhangi bir karışıklığa neden olma olasılığı varsa, $\bar{a}$ yerine $n\mathbb{Z} + a$ ya da (a mod n) yazılımı yeğlenmelidir.

Yukardaki tartışmadan da anlaşılacağı üzere, eğer $n \neq m$ ise, $\mathbb{Z}/n\mathbb{Z} \cap \mathbb{Z}/m\mathbb{Z} = \varnothing$'dir. Ama daha sonra göreceğiz ki, eğer m, n'yi bölüyorsa, o zaman $\mathbb{Z}/m\mathbb{Z}$'yi $\mathbb{Z}/n\mathbb{Z}$'nin bir altkümesi (üstelik güzel bir altkümesi) olarak görmenin bir yolu vardır.

Bir somut örnek daha verelim:

$$\mathbb{Z}/5\mathbb{Z} = \{5\mathbb{Z}, 5\mathbb{Z}+1, 5\mathbb{Z}+2, 5\mathbb{Z}+3, 5\mathbb{Z}+4\} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\},$$

ve

$$\begin{aligned}
5\mathbb{Z} &= \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\}\\
5\mathbb{Z}+1 &= \{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots\}\\
5\mathbb{Z}+2 &= \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\}\\
5\mathbb{Z}+3 &= \{\ldots, -12, -7, -2, 3, 8, 13, 18, \ldots\}\\
5\mathbb{Z}+4 &= \{\ldots, -11, -6, -1, 4, 9, 14, 19, \ldots\}.
\end{aligned}$$

İşte $\mathbb{Z}/5\mathbb{Z}$'nin toplama ve çarpım tabloları:

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

×	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

$\mathbb{Z}/4\mathbb{Z}$'nin toplama tablosuyla $\mathbb{Z}/5\mathbb{Z}$'nin toplama tabloları arasında büyük bir ayrım yok, ama çarpım tabloları arasında çok önemli bir ayrım var. $\mathbb{Z}/4\mathbb{Z}$'de $\bar{2} \times \bar{2} = \bar{0}$ ama $\mathbb{Z}/5\mathbb{Z}$'de $\bar{0}$ olmayan elemanların çarpımı sıfır olamıyor. Bu çok önemli bir ayrımdır. Sıfır olmayan elemanların çarpımının sıfır olmadığı halkalara **tamlık bölgesi** denir. Örneğin, $\mathbb{Z}/6\mathbb{Z}$ bir tamlık bölgesi değildir, çünkü sıfır olmayan $\bar{2}$ ve $\bar{3}$ elemanlarının çarpımı bu halkada sıfırdır. Kolayca kanıtlanacağı üzere, $\mathbb{Z}/n\mathbb{Z}$'nin bir tamlık bölgesi olması için gerek ve yeter koşul n'nin bir asal olmasıdır.

Geçen sayılarda da kanıtladığımız üzere, eğer p bir asalsa, $\mathbb{Z}/p\mathbb{Z}$ halkasında, 0'a eşit olmayan her b elemanı için $by = 1$ eşitliğini sağlayan bir y vardır. [MD-2004-II, sayfa 11, Önsav 7'de $a = p$ alın.)

En son tanım olarak, $\mathbb{Z}$'nin bir elemanıyla $\mathbb{Z}/n\mathbb{Z}$'nin bir elemanını çarpabileceğimize dikkatinizi çekerim. Nitekim, eğer $m \in \mathbb{Z}$ ve $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ ise, $m\bar{a}$ çarpımını $\mathbb{Z}/n\mathbb{Z}$'nin $\overline{ma}$ elemanı olarak tanımlayalım:

$$m\bar{a} = \overline{ma}.$$

Elbette $2\bar{a} = \bar{a} + \bar{a}$, $3\bar{a} = \bar{a} + \bar{a} + \bar{a}$ vs. Doğallık, her yerde olduğu gibi burada da kendini gösteriyor.

Her $m, m_1, m_2 \in \mathbb{Z}$ ve her $x, y \in \mathbb{Z}/n\mathbb{Z}$ için, aşağıdaki eşitliklerin geçerli olduğunu kanıtlamak çok kolay:

$$\begin{aligned}
&m(x+y) = mx + my\\
&(m_1 + m_2)x = m_1x + m_2x\\
&m(xy) = (mx)y = x(my)\\
&m_1(m_2x) = (m_1m_2)x\\
&m\bar{1} = \bar{m}\\
&nx = \bar{0}\\
&(-1)x = -x.
\end{aligned}$$

Bir sonraki yazıda birkaç n için $\mathbb{Z}/n\mathbb{Z}$ halkasını inceleyeceğiz. Önce $n = 4$ ile başlayacağız incelememize. Yazılımda kolaylık olması için, alışageldiği üzere $\mathbb{Z}/4\mathbb{Z}$ halkasının $\bar{0}$, $\bar{1}$, $\bar{2}$, $\bar{3}$ elemanları yerine 0, 1, 2, 3 yazacağız ama lütfen bunların tamsayı olduklarını sanmayın. Tamsayılarda, $2 + 2 = 0$ eşitliği herkesin bildiği üzere yanlıştır. $\mathbb{Z}/4\mathbb{Z}$ halkasında, yanlış olan $2 + 2 = 0$ eşitliği yerine, durumu kurtarmak için,

$$2 + 2 \equiv 0 \bmod 4$$

yazılır çoğu zaman. Bunun gibi, gene $\mathbb{Z}/4\mathbb{Z}$ halkasında

$$5 \equiv 1 \equiv 9 \equiv -3 \bmod 4$$

gibi "**denklik**"ler yazılır. Bu denkliklerin anlamı bellidir: 5, 1, 9 ve –3 sayılarının aynı sütunda (birincisinde) olduklarını söyler. Genel tanım ve olgular şöyle:

$$a \equiv b \bmod n$$

ancak ve ancak

$$n,\ a - b\text{'yi bölüyorsa,}$$

ancak ve ancak

$$n\mathbb{Z} + a = n\mathbb{Z} + b \text{ ise}$$

ancak ve ancak

$$\mathbb{Z}/n\mathbb{Z}\text{'de } \bar{a} = \bar{b} \text{ ise.}$$

Sonraki yazılarda $\mathbb{Z}/n\mathbb{Z}$'ye çok daha ayrıntılı bir biçimde eğileceğiz. ♦