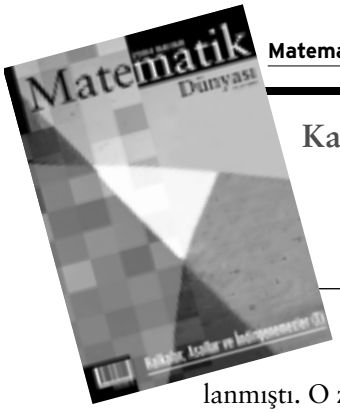


Kapak Konusu: Halkalar, Asallar ve İndirgenemezler (1)

"Modülo n" Sayılar

Bir önceki yazıda, belli bir tamsayı, sözgelimi 7 sıfırlanmıştı. O zaman, –14, –7, 0, 7, 14, 21 gibi 7'ye bölünen tüm tamsayılar birbirine "eşit" kabul edilmiş oldu. Her ne kadar eşitlik yerine ≡ yazılmışsa da, bu yazılım, değişikliği yapılanın özünü değiştirmez: Öyle ya da böyle, geçen yazıda, eşit olmayan sayılar eşit olarak algılanmış oldu.

7'yi sıfırlamanın sonucu olarak, –13, –6, 1, 8, 15, 22 sayıları da birbirine "eşit" olmuşlardı.

7, 0'a eşit olmadığından, 7'yi 0 olarak yazmanın, tam yazılmasa da 7'yi 0'a eşit olarak algılamanın pek matematiksel olduğu, dolayısıyla bu dergiye yakıştığı söylenemez. Okurun bir önceki yazıya nasıl dayandığını anlamak güç! Bu yazıda, geçen yazıda yapılanlara matematiksel bir kılıf uydurup yazarın günahını hafifletmeye çalışacağız.

7'ye bölünen tamsayılar kümesini 7Z olarak yazalım. 7'ye bölündüğünde kalanın 1 olduğu tamsayılar kümesi de 7Z + 1 olsun:

$7\mathbb{Z} + 1 := \{ ..., -20, -13, -6, 1, 8, 15, 22, ...\}$.

Genel olarak, $i = 0, 1, 2, 3, 4, 5, 6$ ise, $7\mathbb{Z} + i$ kümesi, 7'ye bölündüğünde kalanı i olan tamsayılar kümesi olsun:

$7\mathbb{Z} := \{ ..., -21, -14, -7, 0, 7, 14, 21, ...\}$
$7\mathbb{Z} + 1 := \{ ..., -20, -13, -6, 1, 8, 15, 22, ...\}$
$7\mathbb{Z} + 2 := \{ ..., -19, -12, -5, 2, 9, 16, 23, ...\}$
$7\mathbb{Z} + 3 := \{ ..., -18, -11, -4, 3, 10, 17, 24, ...\}$
$7\mathbb{Z} + 4 := \{ ..., -17, -10, -3, 4, 11, 18, 25, ...\}$
$7\mathbb{Z} + 5 := \{ ..., -16, -9, -2, 5, 12, 19, 26, ...\}$
$7\mathbb{Z} + 6 := \{ ..., -15, -8, -1, 6, 13, 20, 27, ...\}$

Böylece tamsayılar kümesini yedi (sayıyla 7) ayrık altkümeye ayırdık. Her altkümede, bir önceki yazıda haksız yere eşitlenen sayılar var. 7Z altkümesinde 0'a eşitlenen sayılar, 7Z + 5 altkümesinde 5'e eşitlenen sayılar...

İşbu yazıda, geçen yazının eşitlenen sayıları aynı altkümenin elemanları olarak görülecek. Bu da eşitlemenin, ama bu sefer çaktırmadan eşitlemenin tahsilli yöntemidir.

Görüldüğü gibi, $i = 0, 1, 2, 3, 4, 5, 6$ ise, $7\mathbb{Z} + i$ altkümesi, 7Z altkümesine i eklenerek elde edilen sayılar kümesidir, aynen $7\mathbb{Z} + i$ yazılımının da söylemek istediği gibi...

Şimdi daha da ileri gidip, i **herhangi** bir tamsayıysa, $7\mathbb{Z} + i$ altkümesini, 7Z altkümesindeki elemanlara i ekleyerek elde edilen sayılar kümesi olarak tanımlayalım. O zaman, örneğin,

$$7\mathbb{Z} + (-6) = 7\mathbb{Z} + 1 = 7\mathbb{Z} + 8 = 7\mathbb{Z} + 15$$

olur.

Bu $7\mathbb{Z} + i$ altkümelerinden tam yedi tane vardır, ne fazla ne eksik. Bu altkümelerin birçoğu birbirine eşittir.

Şimdi şunu farkedelim. i ve j herhangi iki tamsayı olsunlar. $7\mathbb{Z} + i$ altkümesinden herhangi bir eleman alalım. $7\mathbb{Z} + j$ altkümesinden de herhangi bir eleman alalım. Bu iki elemanı toplayalım. Elde ettiğimiz sayı her zaman, ama her zaman, $7\mathbb{Z} + i + j$ altkümesinde olacaktır. Şimdi o iki elemanı çarpalım. Bu sefer elde ettiğimiz sayı hep $7\mathbb{Z} + ij$ altkümesinde olacaktır. Bunlar, geçen yazıda, sırasıyla Olgu 4 ve 5'te kanıtlanmıştı.

Tamsayıların (ya da gerçel sayıların) altkümelerini şu yöntemle toplayıp çarpabiliriz: Eğer A ve B iki sayı kümesiyse, $A + B$, $A - B$ ve AB sayı kümeleri,

$$A + B = \{a + b : a \in A, b \in B\}$$
$$A - B = \{a - b : a \in A, b \in B\}$$
$$AB = \{ab : a \in A, b \in B\}$$

olarak tanımlansınlar. O zaman, bizi ilgilendiren özel durumda,

$$(7\mathbb{Z} + i) + (7\mathbb{Z} + j) = 7\mathbb{Z} + (i + j)$$
$$(7\mathbb{Z} + i) - (7\mathbb{Z} + j) = 7\mathbb{Z} + (i - j)$$
$$(7\mathbb{Z} + i)(7\mathbb{Z} + j) = 7\mathbb{Z} + ij.$$

olur.

Birdenbire,

$\{7\mathbb{Z}, 7\mathbb{Z} + 1, 7\mathbb{Z} + 2, 7\mathbb{Z} + 3, 7\mathbb{Z} + 4, 7\mathbb{Z} + 5, 7\mathbb{Z} + 6\}$ kümesinde toplama, çıkarma ve çarpma yapmaya başladık! Bu kümeye bir ad verelim. Adı Z/7Z olsun. Demek ki,

$$\mathbb{Z}/7\mathbb{Z} = \{7\mathbb{Z}, 7\mathbb{Z} + 1, ..., 7\mathbb{Z} + 5, 7\mathbb{Z} + 6\}.$$

Dikkat edilirse, Z/7Z kümesinin yedi öğesi de Z'nin altkümeleri ve o yedi altkümenin herhangi birinin herhangi iki öğesi bir önceki yazıda eşitlenen sayılar... Bir başka deyişle, bir önceki yazıda eşitlenen sayıları bu yazıda tek bir altkümede topladık.

Yukarda söylenenler salt 7 için değil, genel olarak herhangi bir $n \neq 0$ tamsayısı için de geçerlidir. Bulduklarımızı bir teoremde özetleyelim.

Teorem 1. *$n \neq 0$ ve i tamsayıları için,*

$$n\mathbb{Z} + i = \{nz + i : z \in \mathbb{Z}\}$$

ve

$$\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z} + i : i \in \mathbb{Z}\}$$

olarak tanımlansın. O zaman $\mathbb{Z}/n\mathbb{Z}$ kümesinin tam n tane öğesi vardır:

$$\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}, n\mathbb{Z} + 1, ..., n\mathbb{Z} + (n-1)\}.$$

Eğer n'yi sabit tutup, $n\mathbb{Z} + i$ yerine $\overline{i}$ yazacak olursak, o zaman,

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

olur ve her $i, j \in \mathbb{Z}$ için,

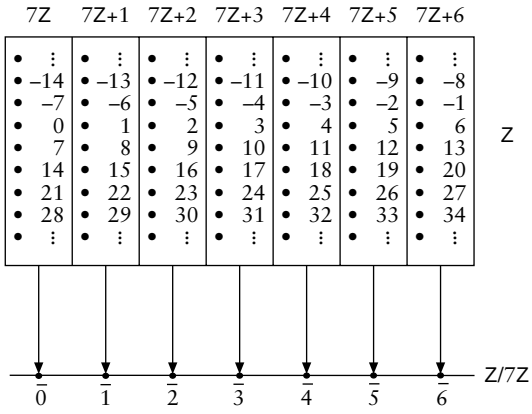
a. $\overline{i} + \overline{j} = \overline{i + j}$,

b. $\overline{i} - \overline{j} = \overline{i - j}$,

c. $\overline{i}\ \overline{j} = \overline{ij}$

eşitlikleri geçerlidir.

Aşağıda $\mathbb{Z}$ ve $\mathbb{Z}/7\mathbb{Z}$'nin birer resmini bulacaksınız. O resim $\mathbb{Z}$'yle $\mathbb{Z}/7\mathbb{Z}$ arasındaki ilişkiyi resmetmek için resmedilmiştir.



$\mathbb{Z}/n\mathbb{Z}$'de, $\overline{i} = \overline{j}$ ancak ve ancak n, $i - j$ sayısını bölüyorsa.

$n = 2, 3, 4, 5$ için $\mathbb{Z}/n\mathbb{Z}$'nin toplama ve çarpım tablolarını aşağıdaki karede bulacaksınız. (Çarpım tablosunda yazması çok zahmetli olan $\overline{i}$ yerine deneyimli matematikçiler gibi i yazdık). Görüldüğü üzere, $\mathbb{Z}/4\mathbb{Z}$'de, $\overline{0}$ olmayan elemanların çarpımı $\overline{0}$ olabiliyor: $\overline{2} \times \overline{2} = \overline{0}$. Böyle bir anomali, genel olarak, ancak eğer n asal değilse olabilir. Bunu daha sonra kanıtlayacağız.

$\overline{-i}$ yerine çoğunlukla $-\overline{i}$ yazacağız.

Her ne kadar $\mathbb{Z}/n\mathbb{Z}$'nin elemanları $\mathbb{Z}$'nin birer altkümesiyse de, bu elemanları toplanıp çarpılan bir tür sayı olarak görmekte sonsuz yarar vardır.

$\mathbb{Z}/7\mathbb{Z}$'de $\overline{95}$ diye bir eleman vardır, açık açık görünmüyorsa da... Nitekim, $\mathbb{Z}/7\mathbb{Z}$'de $\overline{95} = \overline{4}$'tür.

$\overline{95}$ sayısı kimileyin "95 modülo n" diye okunur. $\mathbb{Z}/n\mathbb{Z}$ kümesine de kimileyin "$\mathbb{Z}$ modülo n" ya da "$\mathbb{Z}$ bölü $n\mathbb{Z}$ halkası" denir.

$7\mathbb{Z} + \overline{95}$ yazılımında 7 açık açık görünüyor da, $\overline{95}$ yazılımında 7 görünmüyor. Bu yüzden $\overline{95}$ yazılımı karışıklığa neden olabilir ve tehlikelere maruz kalabiliriz. Eğer $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}/m\mathbb{Z}$, $\mathbb{Z}/p\mathbb{Z}$ gibi değişik kümeler kullanacaksak, bu kümelerin elemanları için, $\bar{a}$, $\tilde{a}$, $\hat{a}$ gibi değişik yazılımlar da kullanılabilir.

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

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	0

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

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

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

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

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

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Yukardaki teoremin a, b ve c özelliklerinden dolayı $\mathbb{Z}$'nin bazı cebirsel özellikleri $\mathbb{Z}/n\mathbb{Z}$'ye yansır.

Teorem 2. *$n > 1$ bir tamsayı olsun. O zaman, $(\mathbb{Z}/n\mathbb{Z}, +, \times, \overline{0}, \overline{1})$ yapısının aşağıdaki özellikleri vardır.* (Burada $\times$ çarpma anlamına geliyor.)

T1 [Birleşme Özelliği]. *Her $x, y, z \in \mathbb{Z}/n\mathbb{Z}$ için,*

$$x + (y + z) = (x + y) + z.$$

T2 [Etkisiz Öğe]. *Her $x \in \mathbb{Z}/n\mathbb{Z}$ için,*

$$\overline{0} + x = x + \overline{0} = x.$$

T3 [Ters Öğenin Varlığı]. *Her $x \in \mathbb{Z}/n\mathbb{Z}$ için,*

$$x + y = y + x = \overline{0}$$

eşitliklerini sağlayan bir $y \in \mathbb{Z}/n\mathbb{Z}$ vardır. Nitekim $y = \overline{0} - x = -x$ elemanı bu denklemleri sağlar.

T4 [Değişme Özelliği]. *Her x ve $y \in \mathbb{Z}/n\mathbb{Z}$ için,*

$$x + y = y + x.$$

Ç1 [Birleşme Özelliği]. *Her $x, y, z \in \mathbb{Z}/n\mathbb{Z}$ için,*

$$x(yz) = (xy)z.$$

Ç2 [Birim Öğe]. *Her $x \in \mathbb{Z}/n\mathbb{Z}$ için,*

$$\overline{1}\ x = x\ \overline{1} = x.$$

Ç3 [Değişme Özelliği]. *Her x ve $y \in \mathbb{Z}/n\mathbb{Z}$ için,*

$$xy = yx.$$

Ç4. $\overline{1} \neq \overline{0}$.

D [Dağılma Özelliği]. *Her $x, y, z \in R$ için,*

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

Herbirinin kanıtı kolay olan ve doğrudan birinci teoremden çıkan bu özellikleri okura bırakıyoruz.

Bu sayının kapak konusu yukardaki özellikleri sağlayan matematiksel yapılarıdır. Tamsayılar kü-

mesi Z'yi de içeren bu yapılar soyut cebirin, dolayısıyla matematiğin de temel taşlarındandır.

Z/nZ yapılarını biraz inceleyelim. Mehmet Kıral'ın Euler φ Fonksiyonları yazısında konuyu biraz daha eşeceğiz.

Teorem 3. *$a \in \mathbb{Z}$ olsun.* Z/nZ'de $\bar{a}\,\bar{x} = \bar{1}$ *denkleminin çözülmesi için yeter ve gerek koşul a ile n'nin aralarında asal olmasıdır. Ayrıca bu durumda denklemin* Z/nZ*'de tek bir çözümü vardır.*

Kanıt: Z/nZ'de $\bar{a}\,\bar{x} = \bar{1}$ denklemini çözmek demek $ax - 1$ sayısı n'ye bölünecek şekilde bir x tamsayısı bulmak demektir. Bu son dediğimiz de $ax - 1 = ny$ denklemini sağlayan x ve y tamsayılarını bulmak demektir. Bu durumda a'yla n'nin ortak bölenleri, $ax - ny$'nin yani 1'in de ortak bölenidir. Demek ki bu durumda a'yla n birbirine asaldır. Şimdi tersini kanıtlamamız gerekiyor: a'yla n birbirine asal iki tamsayıysa, $ax - ny = 1$ denklemini çözen x ve y tamsayıları var mı? Evet vardır. Bilinen bu sonuç yandaki gri karede kanıtlanmıştır.

Şimdi $\bar{x}$ ve $\bar{y}$ denklemin iki çözümü olsun. O zaman, $\bar{x} = \bar{x}\,\bar{1} = \bar{x}\,(\bar{a}\,\bar{y}) = \bar{y}\,(\bar{a}\,\bar{x}) = \bar{y}\,\bar{1} = \bar{y}$. □

Sonuç 4. *Her $\bar{0} \neq \bar{a} \in$* Z/nZ *için $\bar{a}\,\bar{x} = \bar{1}$ denkleminin* Z/nZ*'de çözülmesi için yeter ve gerek koşul n'nin asal olmasıdır.*

Kanıt: Eğer her $\bar{0} \neq \bar{a} \in$ Z/nZ için $\bar{a}\,\bar{x} = \bar{1}$ denklemini Z/nZ'de çözebiliyorsak, yukardaki teoreme göre n'den küçük her pozitif a doğal sayısının n'ye asal olması lazım, yani n'nin asal olması lazım.

Koşulun yeterli olduğu da belli. Ayrıntıları okura bırakıyoruz. □

Sonuç 5. *$\bar{a}, \bar{b} \in$* Z/nZ *ve a, n'ye asal olsun. $\bar{a}\,\bar{b} = \bar{0}$ ise $\bar{b} = \bar{0}$'dır.*

Kanıt: $\bar{x}$, Sonuç 4'teki gibi olsun. O zaman, $\bar{b} = \bar{1}\,\bar{b} = (\bar{x}\,\bar{a})\,\bar{b} = \bar{x}\,(\bar{a}\,\bar{b}) = \bar{x}\,\bar{0} = \bar{0}$. □

Alıştırmalar

Not: Aşağıdaki alıştırmaların bazıları yukardaki yazı kadar kolay olmayabilir.

1. Z/6Z'de $x^2 = x$ denklemini çözün.

2. Eğer n asalsa, Z/nZ'te $x^2 = x$ denklemini sağlayan sadece iki eleman olduğunu gösterin.

3. "n'nin asal olması için gerek ve yeter koşul Z/nZ'de $xy = 0$ eşitliğini sağlayan $x \neq 0$ ve $y \neq 0$ elemanlarının olmamasıdır" önermesini kanıtlayın.

4. Z/nZ'de x, $X^2 = X$ denkleminin bir çözümüyse $1 - x$'in de aynı denklemin çözümü olduğunu gösterin.

5. Eğer $x \in$ Z/nZ ve $k \in \mathbb{N}$ ise x^k, x'in kendisiyle k defa çarpılması sonucu elde edilen eleman olsun. Eğer n asalsa, her $x, y \in$ Z/nZ için,

$$(x + y)^n = x^n + y^n$$

eşitliğini kanıtlayın.

6. p bir asal olsun. Z/p^nZ kümesinin Teorem 3'teki koşulu sağlayan eleman sayısını hesaplayın.

7. $x \in$ Z/nZ olsun. $xy = \bar{1}$ denklemini sağlayan bir y varsa, o zaman belli bir $k \in \mathbb{N}$ için, $x^k = \bar{1}$, hatta $x^{\varphi(x)} = \bar{1}$ (bknz. sayfa 36) eşitliğini kanıtlayın.

8. Eğer n asal değilse, Z/nZ'te $x^2 = x$ denklemini sağlayan ikiden fazla eleman olduğunu gösterin. ♠

Teorem. *Eğer a ve b birbirine asal iki tamsayıysa (yani ortak bölenleri sadece 1 ve –1 ise) o zaman $ax + by = 1$ eşitliğini sağlayan x ve y tamsayıları vardır.*

Kanıt: Önce a ve b'nin doğal sayı olduklarını varsayalım. Teoremi $\max(a, b)$ üzerinden tümevarımla kanıtlayacağız. Simetriden dolayı $a \leq b$ eşitsizliğini varsayabiliriz. Eğer $a = 0$ ise o zaman $b = 1$ olmak zorunda ve $x = 0$, $y = 1$ denklemin çözümüdür. Bundan böyle $a > 0$ olsun. a ve b'nin ortak bölenleri a ve $b - a$'nın da ortak bölenleridir. Dolayısıyla a ve $b - a$ da birbirine asaldır. $\max(a, b - a) < b = \max(a, b)$ olduğundan, tümevarım varsayımına göre $ax_1 + (b - a)y_1 = 1$ denklemini sağlayan x_1 ve y_1 tamsayıları vardır. Şimdi, $a(x_1 - y_1) + by_1 = 1$ ve $x = x_1 - y_1$ ve $y = y_1$ denklemin çözümüdür.

Eğer a ve b birer tamsayıysa, yukarda $|a|x + |b|y = 1$ denklemini çözebildiğimizi gördük. Şimdi, a ve b'nin pozitif ya da negatif olmalarına göre $\pm x$ ve $\pm y$, $ax + by = 1$ denkleminin bir çözümüdür. □

Kanıtın Bir Sonucu: *Eğer a ve b tamsayılarının en büyük ortak böleni d ise, o zaman $ax + by = d$ eşitliğini sağlayan x ve y tamsayıları vardır.*

Kanıt: Aynen yukardaki kanıt gibi. Okura bırakılmıştır. □