Bölüm 2

Modüler Aritmetik

2.1 Tamsayı Kongrüansları

Tanım 2.1.1 $n \in \mathbb{Z}^+$ olsun. $x, y \in \mathbb{Z}$ için $n|x-y$ ise **x ile y modn e göre kongrüanttır** denir ve $x \equiv y \ (mod\ n)$ ile gösterilir.

Teorem 2.1.2 *mod n bağıntısı, $\mathbb{Z}$ tamsayılar kümesi üzerinde bir denklik bağıntısıdır.*

İspat (i) Yansıma: $\forall x \in \mathbb{Z}$ için $n|x-x=0$ olduğundan $x \equiv x \ (mod\ n)$ dir.
(ii) Simetri: $\forall x, y \in \mathbb{Z}$ için $x \equiv y \ (mod\ n)$ olsun. Bu durumda $n|x-y$ ve $n|-(x-y)=y-x$ olduğundan $y \equiv x \ (mod\ n)$ dir.
(iii) Geçişme: $\forall x, y, z \in \mathbb{Z}$ için $x \equiv y \ (mod\ n)$ ve $y \equiv z \ (mod\ n)$ olsun. Eğer $n|x-y$ ise $x-y=nk_1$ olacak şekilde $k_1 \in \mathbb{Z}$ ve $n|y-z$ ise $y-z=nk_2$ olacak şekilde $k_2 \in \mathbb{Z}$ vardır. Bu durumda $x-z=n(k_1+k_2)$ olacak şekilde $k_1+k_2 \in \mathbb{Z}$ vardır. Böylece $n|x-z$ ve $x \equiv z \ (mod\ n)$ dir. ■

Şimdi *mod n* bağıntısı sonucunda ortaya çıkan denklik sınıflarını belirleyelim. $x \in \mathbb{Z}$ için *mod n* bağıntısına göre denklik sınıfı

$$\begin{aligned}
[x] &= \{y \in \mathbb{Z} : y \equiv x \ (mod\ n)\} \\
&= \{y \in \mathbb{Z} : n|y-x\} \\
&= \{y \in \mathbb{Z} : y-x=nk \ , \ k \in \mathbb{Z}\} \\
&= \{y \in \mathbb{Z} : y=x+nk \ , \ k \in \mathbb{Z}\} \\
&= \{x+nk \ : \ k \in \mathbb{Z}\}
\end{aligned}$$

biçimindedir. Bu sebeple *mod n* bağıntısı sonucunda ortaya çıkan denklik sınıfları:

$$\begin{aligned}
[0] &= \{\dots, -3n, -2n, -n, 0, n, 2n, 3n, \dots\} \\
[1] &= \{\dots, -3n+1, -2n+1, -n+1, 1, n+1, 2n+1, 3n+1, \dots\} \\
&\vdots \\
[n-1] &= \{\dots, -3n-1, -2n-1, -n-1, -1, n-1, 2n-1, 3n-1, \dots\}
\end{aligned}$$

şeklindedir.

Tanım 2.1.3 *mod n* bağıntısı sonucunda ortaya çıkan denklik sınıflarına **kongrüans sınıfları** veya **kalan sınıfları** adı verilir.

$x = y \pmod n$ kongrüansı bir denklem olmamasına rağmen, denklemlerde yapabildiğiniz birçok işlemi kongrüanslar içinde yapabileceğiz. Şimdi bir kongrüansın her iki tarafına aynı sayıyı ekleyip, her iki tarafını aynı sayıyla çarpabileceğinizi gösterelim.

Teorem 2.1.4 *Eğer* $a = b \pmod n$ *ve* $x \in \mathbb{Z}$ *ise*

$$a + x = b + x \pmod n \quad ve \quad ax = bx \pmod n$$

dir.

İspat ✔ $a = b \pmod n \Rightarrow n|a-b \Rightarrow a - b = nk\ ;\ k \in \mathbb{Z} \Rightarrow (a+x) - (b+x) = nk \Rightarrow n|(a+x)-(b+x) \Rightarrow a + x = b + x \pmod n$

✔✔ $a = b \pmod n \Rightarrow n|a-b \Rightarrow a - b = nk\ ;\ k \in \mathbb{Z} \Rightarrow (a-b)x = (nk)x \Rightarrow ax - bx = n(kx) \Rightarrow n|ax-bx \Rightarrow ax = bx \pmod n$

■

Kongrüanslar yukarıdaki özelliklere ek olarak taraf tarafa toplama ve taraf tarafa çarpma özelliklerine de sahiptirler.

Teorem 2.1.5 $a = b \pmod n$ *ve* $c = d \pmod n$ *ise*

$$a + c = b + d \pmod n \quad ve \quad a.c = b.d \pmod n$$

dir.

İspat $a = b \pmod n$ ise bir önceki teorem gereğince $c \in \mathbb{Z}$ için $ac = bc \pmod n$ dir. Benzer şekilde $c = d \pmod n$ olduğunda $b \in \mathbb{Z}$ için $bc = bd \pmod n$ elde edilir. $=$ bağıntısının geçişme özelliğinden $a.c = b.d \pmod n$ bulunur. ■

Uyarı 2.1.6 Şu ana kadar gördüğümüz sayı sistemlerinde kısaltma özelliği sağlanıyor olmasına rağmen kongrüanslar için

$$"ax = ay \pmod n \Rightarrow x = y \pmod n"$$

önermesi her zaman doğru değildir. Örneğin $(4)(6) = (4)(21) \pmod{30}$ olmasına rağmen $6 \neq 21 \pmod{30}$ dir.

Teorem 2.1.7 (Kısaltma Kuralı) *$ax \equiv ay \pmod n$ ve $obeb(a,n) = 1$ ise $x \equiv y \pmod n$ dir.*

İspat $ax \equiv ay \pmod n \Rightarrow n|ax - ay$
$\Rightarrow n|a(x-y)$; $ebob(a,n) = 1$
$\Rightarrow n|x - y$
$\Rightarrow x \equiv y \pmod n$

■

Teorem 2.1.8 *Eğer a ile n aralarında asal ise $ax \equiv b \pmod n$ denkliğinin bir x çözümü vardır. Ayrıca $\mathbb{Z}$ içindeki herhangi iki çözüm mod n e göre kongrüanttır.*

İspat $ebob(a,n) = 1 \Rightarrow 1 = as + nt$ *olacak şekilde* $s,t \in \mathbb{Z}$ *vardır*
$\Rightarrow b = asb + ntb$
$\Rightarrow a(sb) - b = n(-tb)$
$\Rightarrow n|a(sb) - b$
$\Rightarrow a \underbrace{(sb)}_{x} \equiv b \pmod n$

Böylece verilen denkliğin bir $x = sb$ çözümü vardır. Eğer y bu denkliğin başka bir çözümü ise, bu durumda $ax \equiv b \pmod n$ ve $ay \equiv b \pmod n$ olduğundan $ax \equiv ay \pmod n$ elde edilir. Teorem 1.1.7 gereğince $x \equiv y \pmod n$ dir. ■

Örnek 2.1.9 $20x \equiv 14 \pmod{63}$ denkliğini sağlayan x i bulalım:

$63 = 20.3 + 3$
$20 = 3.6 + 2$
$3 = 2.1 + 1$
$2 = 2.1 + 0$

$ebob(20,63) = 1$ olduğundan $1 = 20s + 63t$ olacak biçimde $s,t \in \mathbb{Z}$ vardır. Euclid bölme algoritmasından $1 = 20.(-22) + 63.7$ elde edilir. O halde $14 = (20)(-308) \pmod{63}$ olduğundan $x = -308 \equiv 7 \pmod{63}$ bulunur.

Şimdi aynı kongrüansı başka bir yolla çözmeye çalışalım:

$20x \equiv 14 \pmod{63} \Rightarrow 2.10x \equiv 2.7 \pmod{63}$; $ebob(2,63) = 1$
$\Rightarrow 10x \equiv 7 \pmod{63}$
$\Rightarrow 10x \equiv 70 \pmod{63}$; $ebob(10,63) = 1$
$\Rightarrow x \equiv 7 \pmod{63}$

•

2.2 Kongrüans Sınıfları

Daha önce olduğu gibi *mod n* bağıntısı sonucunda ortaya çıkan denklik sınıflarının kümesini

$$\mathbb{Z}_n = \{[0],[1],\cdots,[n-1]\}$$

ile göstereceğiz.

Teorem 2.2.1 *$n > 1$ olmak üzere $[a], [b] \in \mathbb{Z}_n$ için*

$$[a] \oplus [b] = [a+b] \quad , \quad [a] \odot [b] = [a.b]$$

şeklinde tanımlı işlemler aşağıdaki özelliklere sahiptir:

1. *$\oplus$, $\mathbb{Z}_n$ üzerinde bir işlemdir.*
2. *$\oplus$, $\mathbb{Z}_n$ üzerinde birleşimlidir.*
3. *$\mathbb{Z}_n$ nin $\oplus$ işlemine göre birim elemanı vardır.*
4. *$\mathbb{Z}_n$ de her elemanın $\oplus$ işlemine göre tersi vardır.*
5. *$\oplus$, $\mathbb{Z}_n$ üzerinde değişmelidir.*
6. *$\odot$, $\mathbb{Z}_n$ üzerinde bir işlemdir.*
7. *$\odot$, $\mathbb{Z}_n$ üzerinde birleşimlidir.*
8. *$\mathbb{Z}_n$ nin $\odot$ işlemine göre birim elemanı vardır.*
9. *$\odot$, $\mathbb{Z}_n$ üzerinde değişmelidir.*

İspat $\oplus : \begin{array}{ccc} \mathbb{Z}_n \times \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \\ ([a],[b]) & \longrightarrow & [a] \oplus [b] \end{array}$

$([a],[b]) = ([x],[y])$ olsun.

$$\begin{array}{lllll} [a] = [x] & \Rightarrow & a \in [x] & \Rightarrow & a \equiv x \pmod n \\ [b] = [y] & \Rightarrow & b \in [y] & \Rightarrow & b \equiv y \pmod n \\ \hline & & & & a+b \equiv x+y \pmod n \quad \Rightarrow \quad [a+b] = [x+y] \\ & & & & a.b \equiv x.y \pmod n \quad \Rightarrow \quad [a.b] = [x.y] \end{array}$$

(1) $\oplus$ nın iyi tanımlı olduğunu gösterelim:

$$\oplus([a],[b]) = [a] \oplus [b] = [a+b] = [x+y] = [x] \oplus [y] = \oplus([x],[y])$$

(2) $[a], [b], [c] \in \mathbb{Z}_n$ için

$$\begin{aligned} [a] \oplus ([b] \oplus [c]) &= [a] \oplus ([b+c]) \\ &= [a+(b+c)] \\ &= [(a+b)+c] \\ &= [a+b] \oplus [c] \\ &= ([a] \oplus [b]) \oplus [c] \end{aligned}$$

olduğundan $\oplus$, $\mathbb{Z}_n$ de birleşimlidir.

(3) $[a] \in \mathbb{Z}_n$ için

$$[a] \oplus [0] = [a+0] = [a] \quad ve \quad [0] \oplus [a] = [0+a] = [a]$$

olacak biçimde $[0] \in \mathbb{Z}_n$ olduğundan $[0]$ birim elemandır.

(4) $[a] \in \mathbb{Z}_n$ için

$$[a] \oplus [-a] = [a+(-a)] = [0] \quad ve \quad [-a] \oplus [a] = [(-a)+a] = [0]$$

olacak biçimde $[-a] = [n-a] \in \mathbb{Z}_n$ olduğundan, $[a]$ elemanının $\oplus$ işlemine göre tersi $[n-a]$ dır. (☞[-a]=[n-a] olduğunu gösteriniz.)

(6) $\odot$ nın iyi tanımlı olduğunu gösterelim:

$$\odot([a],[b]) = [a] \odot [b] = [a.b] = [xy] = [x] \odot [y] = \odot([x],[y])$$

Benzer şekilde diğer şıklar da kolaylıkla gösterilebilir. ■

Örnek 2.2.2 $\mathbb{Z}_6 = \{[0],[1],\ldots,[5]\}$ üzerinde tanımlı $\oplus$ ve $\odot$ işlemlerinin tablolarını oluşturalım.

$\oplus$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

$\odot$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

•

Uyarı 2.2.3 Yukarıdaki tablodan da görüleceği gibi $\mathbb{Z}_n$ de her elemanın çarpımsal tersi mevcut olmak zorunda değildir.

Teorem 2.2.4 *$[0] \neq [a] \in \mathbb{Z}_n$ olmak üzere $[a]$ nın çarpımsal tersinin olması için gerek ve yeter koşul $ebob(a,n) = 1$ olmasıdır.*

İspat $[a], [b] \in \mathbb{Z}_n$ ve $[a][b] = 1$ olsun.

$$\begin{aligned}
[a][b]=1 &\Leftrightarrow ab\equiv 1 \ (mod\ n)\\
&\Leftrightarrow n|ab-1\\
&\Leftrightarrow ab-1=nq \quad ;q\in\mathbb{Z}\\
&\Leftrightarrow ab+n(-q)=1\\
&\Leftrightarrow ebob(a,n)=1
\end{aligned}$$

■

Örnek 2.2.5 $[a]\in\mathbb{Z}_{15}$ olmak üzere, Teorem 2.2.4 gereğince $[a]$ nın $\mathbb{Z}_{15}$ içerisinde çarpımsal tersinin olması için gerek ve yeter koşul $ebob(a,15)=1$ olmasıdır. Bu sebeple, $\mathbb{Z}_{15}$ içerisinde çarpımsal tersi mevcut olan elemanlar

$$[1],[2],[4],[7],[8],[11],[13],[14]$$

ve $\mathbb{Z}_{15}$ içerisinde çarpımsal tersi mevcut olmayan elemanlar

$$[3],[5],[6],[9],[10],[12]$$

şeklindedir. •

Örnek 2.2.6 $\mathbb{Z}_{191}$ içerisinde $[13]$ elemanının çarpımsal tersinin mevcut olup olmadığını araştıralım.

$$\begin{aligned}
191&=13.14+9\\
13&=9.1+4\\
9&=4.2+①\\
4&=1.4+0
\end{aligned}$$

$ebob(13,191)=1$ olduğundan $\mathbb{Z}_{191}$ içerisinde $[13]$ nın çarpımsal tersi mevcuttur. Yani; $13x\equiv 1\ (mod 191)$ denkliğinin bir çözümü vardır. Şimdi bu çözümü bulalım. $ebob(13,191)=1$ olduğundan $1=13s+191t$ olacak biçimde $s,t\in\mathbb{Z}$ vardır. Euclid bölme algoritmasını tersten uygularsak;

$$\begin{aligned}
1 &= 9-(4)(2)\\
&= 9-[13-(9)(1)](2)\\
&= (9)(3)-(13)(2)\\
&= [191-(13)(14)](3)-(13)(2)\\
&= (191)(3)+(13)(-44)
\end{aligned}$$

elde edilir. Böylece $13(-44)\equiv 1\ (mod 191)$ olduğundan

$$x=[13]^{-1}=[-44]=[147]$$

bulunur. •

Örnek 2.2.7 $\mathbb{Z}_{26}$ içerisinde

$$\begin{aligned}
[4][x]+[y]&=[22]\\
[19][x]+[y]&=[15]
\end{aligned}$$

denklem sistemini gözönüne alalım. Bu iki denklemi aşağıdaki gibi ifade edebiliriz:

$$\begin{aligned}
4x+y &\equiv 22 \quad (mod 26)\\
19x+y &\equiv 15 \quad (mod 26)
\end{aligned}$$

Bu iki denklikten $15x \equiv 19\ (mod 26)$ elde edilir. Örnek 1.2.5 dekilere benzer işlemler yapılarak $[15]^{-1} = [7]$ bulunur. Bunu son denklikte yerine yazarsak;

$$\begin{aligned} x &\equiv 19.7 \quad (mod 26) \\ &\equiv 3 \quad (mod 26) \end{aligned}$$

elde edilir ve son olarak

$$y = 22 - 4x\ (mod 26) \Rightarrow y \equiv 10\ (mod 26)$$

bulunur. Yani; verilen denklem sisteminin çözümü $[x] = [3], [y] = [10]$ dur. •

Örnek 2.2.8 $x \equiv 0(mod 2), x \equiv 1(mod 3)$, $x \equiv 2(mod 5)$ denklem sisteminin $\mathbb{Z}_{30}$ içerisinde bir çözümü var mıdır? Araştıralım.
$x \equiv 0(mod 2)$, $x \equiv 1(mod 3)$, $x \equiv 2(mod 5)$ olsun. $x = 2k$ olacak şekilde $k \in \mathbb{Z}$ vardır. $x \equiv 1(mod 3)$ denkliğinden $2k \equiv 1(mod 3)$ olup $k = 3t + 2$ olacak şekilde $t \in \mathbb{Z}$ vardır. Bu durumda $x = 6t + 4$ olup $x \equiv 2(mod 5)$ de yerine yazarsak $6t + 4 \equiv 2(mod 5)$ olacaktır. Böylece $t + 4 \equiv 2(mod 5)$ olup $t \equiv 3(mod 5)$ dir. Bu durumda $t = 5m + 3$ dür. Ayrıca $x = 6(5m + 3) + 4 = 30m + 22$ elde edilir. Sonuç olarak $x \equiv 22(mod 30)$ dur. •

Tanım 2.2.9 *Euler φ fonksiyonu, n pozitif tamsayısı için n ye eşit veya n den küçük ve n ile aralarında asal olan pozitif tamsayıların sayısı olarak tanımlanır.*

Örnek 2.2.10 $\varphi(2) = 1, \varphi(4) = 2, \varphi(5) = 4$ dür. •

Teorem 2.2.11 *p asal ve a pozitif tamsayı olmak üzere*

$$\varphi(p^a) = p^a - p^{a-1} = p^a(1 - \frac{1}{p})$$

dir.

Örnek 2.2.12 $\varphi(9) = \varphi(3^2) = 3^2 - 3 = 6$ dır. •

Teorem 2.2.13 (Euler Teoremi) *a ve n tamsayıları için eğer $ebob(a, n) = 1$ ise, $a^{\varphi(n)} \equiv 1\ (mod\ n)$ dir.*

Örnek 2.2.14 33^{100} sayısının 40 a bölümünden kalanı bulalım. Euler teoremi gereğince $33^{16} \equiv 1\ (mod\ 40)$ elde edilir. Böylece

$$33^{100} = 33^{96}.33^4 = (33^{16})^6.1089^2 = 9^2 = 81 = 1\ (mod\ 40)$$

bulunur. •

Fermatın küçük teoremi Euler teoreminin özel bir halidir. Euler teoreminde n yerine p alınmasıyla Fermatın küçük teoremi elde edilir.

Teorem 2.2.15 (Fermatın Küçük Teoremi) *p asal tamsayı ise her $a \in \mathbb{Z}^+$ için $a^p \equiv a \pmod p$ dir. Eğer $(a,p) = 1$ ise, bu durumda $a^{p-1} \equiv 1 \pmod p$ dir.*

Örnek 2.2.16 $5555^{2222}+2222^{5555}$ sayısının 7 ye bölümünden kalanı hesaplayalım. Fermatın küçük teoremi yardımıyla

$$5555^{2222} + 2222^{5555} = 4^{2222} + 3^{5555} = (4^6)^{370}4^2 + (3^6)^{925}3^5 = 4^2 + 3^5 = 2 + 3^5 = 0 \pmod 7$$

elde edilir. •

Teorem 2.2.17 (Wilson Teoremi) *p asal tamsayı ise $(p-1)! \equiv -1 \pmod p$ dir.*

Örnek 2.2.18 $12!$ sayısının 13 e bölümünden kalanı hesaplayalım.

$$1.2.3.4.5.6.7.8.9.10.11.12 \equiv 1.2.3.4.5.6.(-6).(-5).(-4).(-3).(-2).(-1) \equiv -1 \pmod{13}$$

bulunur. Diğer taraftan Wilson Teoremi yardımıyla $(12)! \equiv -1 \pmod{13}$ olduğu kolayca görülür. •

2 . Bölüm Özeti

- $n \in \mathbb{Z}^+$ ve $x, y \in \mathbb{Z}$ olmak üzere

  $$"n|x-y \Leftrightarrow x \equiv y \pmod n"$$

  bağıntısı bir denklik bağıntısıdır. Bu denklik bağıntısının oluşturduğu denklik sınıflarının kümesi $\mathbb{Z}_n$ ile gösterilir.

- $a \equiv b \pmod n$ ve $x \in \mathbb{Z}$ olmak üzere

  $$a + x \equiv b + x \pmod n \quad ve \quad a.x \equiv b.x \pmod n$$

- $a \equiv b \pmod n$ ve $c \equiv d \pmod n$ ise

  $$a + c \equiv b + d \pmod n \quad ve \quad a.c \equiv b.d \pmod n$$

- $ax \equiv ay \pmod n$ ve $ebob(a,n) = 1$ ise $x \equiv y \pmod n$ dir.

- Eğer a ile n aralarında asal ise $ax \equiv b \pmod n$ denkliğinin bir x çözümü vardır. Ayrıca $\mathbb{Z}$ içindeki herhangi iki çözüm $mod\ n$ e göre kongrüanttır.

- $\mathbb{Z}_n$ üzerinde

  $$\begin{array}{rccl} \oplus: & \mathbb{Z}_n \times \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \\ & ([a],[b]) & \longrightarrow & [a] \oplus [b] = [a+b] \end{array}$$

  $$\begin{array}{rccl} \odot: & \mathbb{Z}_n \times \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \\ & ([a],[b]) & \longrightarrow & [a] \odot [b] = [ab] \end{array}$$

  biçiminde tanımlı işlemler aşağıdaki özelliklere sahiptir: