

MODÜLER ARİTMETİK – 2

(MODÜLER ARİTMETİK – MODÜLER ARİTMETİK İŞLEMLERİ VE ÖZELLİKLERİ – DEĞERLENDİRME)

MOD KAVRAMI (DENKLİK)

a ve b tam sayıları arasındaki fark bir m pozitif tam sayısına tam bölünebiliyorsa bu sayılara m modülüne göre denktir denir ve $a \equiv b \pmod{m}$ yazılır.

Yani $m \in \mathbb{Z}^+, m|(a-b) \Leftrightarrow a \equiv b \pmod{m}$ dir

Örnek...1 :

$$18 \equiv 3 \pmod{5}, 18 \equiv 8 \pmod{5}, 18 \equiv -2 \pmod{5}$$

$$18 - 3 = 5 \cdot k \quad k \in \mathbb{Z}$$

$$18 - 8 = 5 \cdot \varphi \quad \varphi \in \mathbb{Z}$$

$$18 - (-2) = 5 \cdot \varphi \quad \varphi \in \mathbb{Z}$$

Örnek...2 :

$x \equiv 3 \pmod{5}$ denkleğini sağlayan x tam sayılarının çözüm kümesini bulalım.

Çözüm :

$x \equiv 3 \pmod{5}$ olduğundan
 $x = 3 + 5 \cdot k \quad (k \in \mathbb{Z})$ yazılabilir.

$k = \dots, -2, -1, 0, 1, 2, 3, \dots$ tam sayıları için

$x = \dots, -7, -2, 3, 8, 13, 18, \dots$ değerlerini alacağı için çözüm kümesi $\{\dots, -7, -2, 3, 8, 13, 18, \dots\}$ dir.

Burada elde ettiğimiz bu küme 5 ile bölündüğünde 3 kalanını veren tüm tam sayıların kümesidir. (Genel kültür olması açısından bu kümeyi $\bar{3}$ ile gösterdiğimiz ve tam olarak şöyle yazdığımızı belirtelim; $\mathbb{Z}/5$ için $\bar{3} = \{\dots, -7, -2, 3, 8, 13, 18, \dots\}$ dir.)

{Bu gösterim matematikte kalan sınıfları kümesi olarak isimlendirilir ve şöyle tanımlanır.

" $m \in \mathbb{Z}^+$ olmak üzere, tam sayıların m' ye bölümünden kalanların kümesi $\mathbb{Z}/m$ şeklinde gösterilir.

$$\mathbb{Z}/m = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \dots, \overline{(m-1)}\}$$

Bu bilgidten dolayı $\mathbb{Z}/4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ ve $\mathbb{Z}/7 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$ dir.

$\mathbb{Z}/4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ kümesinin elemanları olan $\bar{0}, \bar{1}, \bar{2}, \bar{3}$ lerin de birer küme belirttiğine dikkat ediniz.)

Örnek...3 :

$8 \equiv x \pmod{5}$ denkleğini sağlayan en küçük pozitif doğal sayısı ile en büyük negatif tam sayısının çarpımı kaçtır?

$$8 - x = 5 \cdot k \rightarrow x = 8 - 5k$$

-6

$$x_1 = 3$$

$$x_2 = -2$$

$$x_1 \cdot x_2 = -6$$

Örnek...4 :

$24 \equiv 4 \pmod{m}$ denkleğini sağlayan kaç tane m tam sayı değeri vardır? ($m > 1$)

$$24 - 4 = m \cdot k \rightarrow k = \frac{20}{m}$$

5

m 20'nin pozitif böğürüdür. (1 hariç)

$$20 = 2^2 \cdot 5 \rightarrow p.b. = (2+1) \cdot (1+1) = 6$$

$$\rightarrow 6 - 1 = 5 \text{ değeri}$$

Örnek...5 :

$x + 3 \equiv 7 \pmod{9}$ denkleğini sağlayan 50 den küçük kaç tane x doğal sayı değeri vardır?

$$x + 3 - 7 = 9 \cdot k$$

6

$$x = 9k + 4 \rightarrow x = 4, 13, \dots, 49$$

$$0 \quad 1 \quad 5$$

$$6 \text{ değeri}$$

Örnek...6 :

$2x + 3 \equiv 3x + 2 \pmod{5}$ denkleğini sağlayan iki basamaklı en büyük ve en küçük pozitif tam sayıların toplamı kaçtır?

107

$$2x + 3 - (3x + 2) = 5k$$

$$-x + 1 = 5k$$

$$x = -5k + 1$$

$$96 + 11 = 107$$

$$-19 \quad -2$$

$$96 \quad 11$$

Örnek...7 :

$x \equiv 2 \pmod{5}$ ve $x \equiv 2 \pmod{7}$ denkleğini sağlayan üç basamaklı en küçük pozitif tam sayı kaçtır?

107

$$x - 2 = 5k \quad k \in \mathbb{Z}$$

$$x - 2 = 7m \quad m \in \mathbb{Z}$$

$$x - 2 = 5k = 7m \Rightarrow x - 2 = 35 \cdot u \quad u \in \mathbb{Z}$$

$$x_{\min} = 107 \quad (3 \text{ b.})$$

MODÜLER ARİTMETİK – 2

(MODÜLER ARİTMETİK – MODÜLER ARİTMETİK İŞLEMLERİ VE ÖZELLİKLERİ – DEĞERLENDİRME)

Örnek...8 :

$10 - m \equiv 4 \pmod{m}$
denkliğini sağlayan 20 den küçük kaç tam sayı vardır?

$$10 - m - 4 = m \cdot k \quad k \in \mathbb{Z}$$

$$6 - m = m \cdot k$$

$$k = \frac{6-m}{m} = \frac{6}{m} - 1$$

$$m \neq 1 \rightarrow 3 \text{ değer}$$

x	m	Eşitliğinde $x = m \cdot y + k$ ve
-	y	$x - k = m \cdot y$ olduğundan x
k		sayısının m modülüne göre
		denği bulunurken sayı
		modüle bölünüp kalan
		yazılabilir.

Örnek...9 :

$23456 \equiv x \pmod{9}$ denkliğinde x kaç olabilir?
{..., -16, -7, 2, 11, 20, ...}

$$R.T: 2+3+4+5+6 = 20 \rightarrow 2+0 = 2$$

$$x \equiv 2 \pmod{9} \quad x = 2 + 9k \quad k \in \mathbb{Z}$$

$$x = \dots -7, 2, 11, \dots$$

Örnek...10 :

$13826 \equiv x \pmod{11}$ denkliğinde x kaç olabilir?
{..., -23, -12, -1, 10, 21, ...}

$$\begin{array}{r} + - + - + \\ 13826 \\ \hline 6+3+1 \\ \hline 15 \end{array} \quad \begin{array}{r} = \\ 3+2 \\ \hline 5 \end{array}$$

$$15 - 5 = 10$$

$$x \equiv 10 \pmod{11}$$

$$x = 10 + 11k \quad k \in \mathbb{Z}$$

Örnek...11 :

$16895685 \equiv x \pmod{8}$ denkliğinde x kaç olabilir?
{..., -11, -3, 5, 13, 21, ...}

$$\begin{array}{r} 685 \overline{) 16895685} \\ 64 \overline{) 85} \\ \hline 45 \\ \hline 40 \\ \hline 5 \end{array}$$

$$x \equiv 5 \pmod{8}$$

$$x = 5 + 8k \quad k \in \mathbb{Z}$$

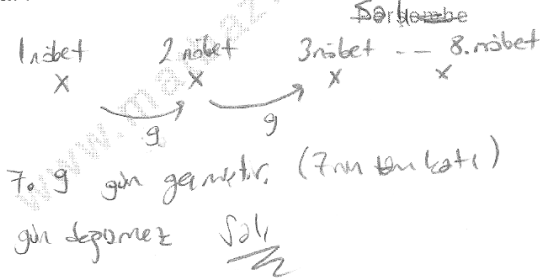
Örnek...12 :

Cumartesi gününden 500 gün sonra hangi gün olur?

$$\begin{array}{r} 500 \overline{) 7} \\ 49 \overline{) 71} \\ \hline 10 \\ \hline 7 \\ \hline 3 \end{array} \rightarrow 3 \text{ gün sonra Cumartesi} + 3 \text{ gün} = \text{Salı}$$

Örnek...13 :

9 günde bir nöbet tutan bir kişi, ilk nöbetini Salı günü tutmuştur. 8. nöbetini hangi gün tutar?



Örnek...14 :

6 gün çalışıp 2 gün tatil yapan bir işçi, işe Salı günü başladığına göre, 11. tatil günü hangi gündür?

Cumartesi

44444478 1516

11. tatil için 5 blok + 6 gün + 1 gün

$5 \cdot 8 + 6 + 1 = 47 \text{ gün (46 gün sonra)}$

$46 \equiv 4 \pmod{7}$

Salı + 4 gün = Cumartesi

Örnek...15 :

5 Ocak 2016'nın Salı günü olduğu bir yılda, 27 Temmuz hangi güne rastlar?

2016 → Subat 29 gündür.

kalan günler

Ocak	Sub	M	N	M	H	T
29	31	30	31	30	27	
26						
↓	↓	↓	↓	↓	↓	↓
5	1	3	2	3	2	6

7'lik kalanlar

$$5+1+3+2+3+2+6 = 22$$

$$3 \text{ hafta} + 1 \text{ gün}$$

$$1 \text{ gün sonra} \rightarrow \text{Salı} + 1 = \text{Çarşamba}$$

MODÜLER ARİTMETİK - 2

(MODÜLER ARİTMETİK - MODÜLER ARİTMETİK İŞLEMLERİ VE ÖZELLİKLERİ - DEĞERLENDİRME)

MOD ÖZELLİKLERİ

k bir tamsayı ,

$$x \equiv y \pmod{m}$$

$$u \equiv v \pmod{m} \text{ iken}$$

$$1) x \pm k \equiv y \pm k \pmod{m}$$

$$2) k.x \equiv k.y \pmod{m}$$

$$3) x \pm u \equiv y \pm v \pmod{m}$$

$$4) x.u \equiv y.v \pmod{m}$$

$$5) x^n \equiv y^n \pmod{m} \quad n \in \mathbb{N}^+$$

$$6) m \in \mathbb{Z}^+, a, b \in \mathbb{Z} \text{ için ebob}(m, a) = 1 \text{ ve}$$

$ax \equiv b \pmod{m}$ denkleminde x'in bir değeri p ise bu denklemin çözüm kümesi $\{p + k.m : k \in \mathbb{Z}\}$ dir. Ayrıca $b \mid (m, a)$ ise çözüm var aksi halde yoktur.

7) m asal ve $(a, p) = 1$ ise $a^m \equiv 1 \pmod{m}$ (burada daha küçük kuvvetlerde de 1 bulunabilir) (Fermat Teoremi)

8) m asal ise $(m-1)! \equiv -1 \pmod{m}$ (Wilson Teoremi)

Örnek...16 :

$2^{27} \equiv x \pmod{9}$ denliğinde x kaç olabilir?

$$\begin{aligned} 2^1 &= 2 \\ 2^2 &= 4 \\ 2^3 &= 8 \\ 2^4 &= 7 \\ 2^5 &= 5 \\ 2^6 &= 1 \end{aligned}$$

$$2^{27} = (2^6)^4 \cdot 2^3$$

$$14 \cdot 8 \equiv 8 \pmod{9}$$

Not Fermat teoremine göre 422 sayı 9'a bölünmez

Örnek...17 :

$1904^{1907} \equiv x \pmod{5}$ denliğinde x kaç olabilir?

$$1904 \equiv 4 \pmod{5}$$

$$1907 \equiv 2 \pmod{5}$$

$$1904^{1907} \equiv 4^{1907} \pmod{5}$$

$$4^1 = 4$$

$$4^2 = 1$$

$$4^{1907} = (4^2)^{953} \cdot 4^1 \equiv 1 \cdot 4 \equiv 4 \pmod{5}$$

Not Fermat teoremine göre $1904^4 \equiv 1 \pmod{5}$ (1904'in daha küçük kuvvetleri bulduk)

Örnek...18 :

$14^x \equiv 5 \pmod{9}$ denliğini x iki basamaklı kaç farklı doğal sayı değeri vardır?

$$14 \equiv 5 \pmod{9} \Rightarrow 5^x \equiv 5 \pmod{9}$$

$$\begin{aligned} 5^1 &\equiv 5 \checkmark \\ 5^2 &\equiv 7 \\ 5^3 &\equiv 8 \\ 5^4 &\equiv 4 \\ 5^5 &\equiv 2 \\ 5^6 &\equiv 1 \end{aligned}$$

$$5^1, 5^6, 5^6 \dots \text{ iktisat kuralı } 5^6 \equiv 1$$

$$5^{1+6k} \equiv 5 \pmod{9}$$

$$1+6k = 13, 19, 25, \dots, 97$$

$$2 \xrightarrow{3} 16$$

Örnek...19 :

$4x \equiv 3 \pmod{5}$ denkleminin çözüm kümesini bulunuz ? $\{2\}$

$$4x - 3 = 5k$$

$$4x = 5k + 3$$

$$\begin{array}{r} \downarrow \quad \downarrow \\ 5 \quad 7 \end{array}$$

$$x = 2 + 5k \Rightarrow 2$$

II. 401

$$4x \equiv 3 \pmod{5}$$

denklemin 4 ile çarpalım

$$4 \cdot (4x \equiv 3) \pmod{5}$$

$$16x \equiv 12$$

$$\downarrow \quad \downarrow$$

$$1 \cdot x \equiv 2 \pmod{5}$$

(Burada 4 sayının mod 5 te çarpımsal tersi 4 tür)

$$4^{-1} \equiv 4 \pmod{5} \quad (4 \cdot 4 \equiv 1 \pmod{5})$$

MODÜLER ARİTMETİK - 2

(MODÜLER ARİTMETİK - MODÜLER ARİTMETİK İŞLEMLERİ VE ÖZELLİKLERİ - DEĞERLENDİRME)

Örnek...20 :

$(-41)^{100}$ sayısının birler basamağı kaçtır?

$$41 \equiv 1 \pmod{10}$$

$$41^{100} \equiv 1^{100} \equiv 1 \pmod{100}$$

Örnek...21 :

$14^{67} + 42^{103} + 16^{314} \equiv x \pmod{5}$ ise x kaçtır?

$$14^{67} \equiv 4^{67} \quad 4^1 = 4 \Rightarrow 4^{67} = (4^2)^{33} \cdot 4^1 \equiv 4 \pmod{5}$$

$$42^{103} \equiv 2^{103} \quad 2^1 = 2 \quad 2^{103} = (2^4)^{25} \cdot 2^3 \equiv 3 \pmod{5}$$

$$16^{314} \equiv 1^{314} \equiv 1 \pmod{5} \Rightarrow 4 + 3 + 1 \equiv 8 \equiv 3 \pmod{5}$$

Örnek...22 :

$3^{200} + 1453^{101}$ sayısının birler basamağı kaçtır?

$$3^1 \equiv 3 \pmod{10} \quad 3^{200} \equiv (3^2)^{100} \equiv (-1)^{100} \equiv 1 \pmod{10}$$

$$3^2 = 9 \equiv -1 \pmod{10}$$

$$1453^{101} \equiv 3^{101}$$

$$3^1 = 3 \quad 3^{101} \equiv (3^2)^{50} \cdot 3^1 \equiv (-1)^{50} \cdot 3^1 \equiv 3 \pmod{10}$$

$$3^2 = 9 \equiv -1 \pmod{10}$$

$$1+3 \equiv 4 \pmod{10}$$

Örnek...23 :

$1^{67} + 2^{67} + 3^{67} + \dots + 12^{67} \equiv x \pmod{13}$ olduğuna göre, x kaç olabilir?

$$1^{67} + 2^{67} + 3^{67} + \dots + 12^{67} \equiv 0 \pmod{13}$$

DEĞERLENDİRME :

1) $49563125 \equiv x \pmod{7}$ ise x kaç olabilir?

$$\begin{array}{cccccccc} 3 & 1 & -2 & -3 & -1 & 2 & 3 & 1 \\ 4 & 9 & 5 & 6 & 3 & 1 & 2 & 5 \end{array} \quad 3$$

$$5+6+2-3-18-10+9+12 \equiv 3 \pmod{7}$$

2) $4x + 3 \equiv 6 \pmod{7}$ denkleğini sağlayan en küçük pozitif x tam sayısı kaçtır?

$$4x + 3 - 6 = 7k \quad k \in \mathbb{Z}$$

$$4x = 7k + 3$$

$$k = \frac{4x-3}{7} \in \mathbb{Z} \quad x=6$$

3) $0! + 1! + 2! + 3! + \dots + 23! \equiv x \pmod{5}$ denkleğinde, x'in değeri kaçtır?

$$\begin{array}{l} 0! \rightarrow 1 \\ 1! \rightarrow 1 > 2 \\ 2! \rightarrow 2 > 8 \\ 3! \rightarrow 6 > 8 \\ + 4! \rightarrow 4 \rightarrow 4 \\ 5! \text{ ve sonrası } 0 \end{array} \quad 14 \equiv 4 \pmod{5}$$

4) x iki basamaklı bir doğal sayıdır.

$$x \equiv 3 \pmod{4}$$

$$x \equiv 3 \pmod{5}$$

olduğuna göre, x'in alabileceği en büyük ve en küçük değerler kaçtır?

83 ve 23

$$x-3 = 4\psi \quad \psi \in \mathbb{Z}$$

$$x-3 = 5\tau \quad \tau \in \mathbb{Z}$$

$$x-3 = 4\psi = 5\tau \Rightarrow x-3 = 20u \quad u \in \mathbb{Z}$$

$$x = 20u + 3$$

$$\begin{array}{l} 1 \\ 23 \text{ (min)} \\ 83 \text{ (max)} \end{array} \quad (2 \text{ basamaklı})$$

MODÜLER ARİTMETİK - 2

(MODÜLER ARİTMETİK - MODÜLER ARİTMETİK İŞLEMLERİ VE ÖZELLİKLERİ - DEĞERLENDİRME)

- 5) İNTEGRALİNTEGRALİNTEGRAL
şeklindeki bir yazılıştaki 976461. harf nedir?

INTEGRAL $\rightarrow$ 8'li tekharf.
 $976461 \equiv 5 \pmod{8}$
 5. harf $\rightarrow$ G

$$\begin{array}{r} 461 \overline{) 8} \\ 40 \\ \hline 61 \\ 56 \\ \hline 5 \end{array}$$

- 6) Bugün günlerden Salı ise 340 gün önce günlerden nedir?

$340 \equiv 4 \pmod{7}$ cuma
 1 gün geriye
 1 hafta geri 3 gün ilerle
 Salı + 3 = Cuma

$$\begin{array}{r} 340 \overline{) 7} \\ 28 \\ \hline 60 \\ 56 \\ \hline 4 \end{array}$$

- 7) KPSS Sınavı 23 Eylül Pazar günü yapılacaktır. Sonuçlar 25 gün sonra sonra duyurulacaksa, bu hangi gün olur?

$25 \equiv 4 \pmod{7}$ perşembe
 Pazar + 4 gün = perşembe

- 8) 1 Aralık'ın Pazar günü olduğu bir yılda, yeni yılın ilk günü hangi güne rastlar?

31 gün sonra günlerden nedir? çarşamba
 $31 \equiv 3 \pmod{7}$
 Pazar + 3 gün = çarşamba

- 9) 5 Ocak 2016'nın Salı günü olduğu bir yılda, 1 Nisan hangi güne rastlar?

Ocak Feb Mar Nisan cuma
 26 29 31 1
 $26 + 29 + 31 + 1$
 $\downarrow \quad \downarrow \quad \downarrow \quad \downarrow$
 5 1 3 1 $\rightarrow$ 3 gün sonra
 Salı + 3 = Cuma

- 10) Daire satın alan bir kişi 140 aylık bir kredi çekmiş ve ilk taksitini Mart ayında yatırmıştır. Bu kişinin taksitleri hangi ayda bitecektir?

$140 \equiv 8 \pmod{12}$ (11 yıl 8 ay) ekim

Mart	Nis	May	Haz	Tem	Ağu	Eyl	Ekim
1	2	3	4	5	6	7	8

 Son kalan 8 ay teker Mart'tan başlayarak sayıldı.

MODÜLER ARİTMETİK - 2

(MODÜLER ARİTMETİK - MODÜLER ARİTMETİK İŞLEMLERİ VE ÖZELLİKLERİ - DEĞERLENDİRME)

- 11) 6 ve 15 günde bir aynı limandan sefere çıkan iki gemi Pazar günü beraber sefere çıkmışlardır. Bundan sonra ikinci defa beraber sefere hangi gün çıkarlar?

perşembe
6 ve 15 → 30 günde birleşir.
x
30 30
60 gün sonra aynı gün çıkar?
 $60 \equiv 4 \pmod{7}$
pazar + 4 = perşembe

- 12) Perşembe günü saat 13:00' ı gösteren bir saat, 2010 saat sonra hangi gün ve saati gösterir?

haftaları, günler bulalım Perşembe; 11:00
2010 | 24
192 | 83 | 7
90 | 7 | 11
72 | 13 | 11
18 | 7 | 6

6 gün 18 saat sonra → 7 gün 6 saat önce
Perşembe + 7 gün - 6 saat : Perşembe 07
13:00

- 13) Beş günde bir nöbet tutan asker, ilk nöbetini salı günü tuttuğuna göre, 25. nöbetini hangi gün tutar?

1. nöbet → 2. nöbet → 3. nöbet → ... → 25. nöbet
Salı 5 5 5
çarşamba
 $24 \cdot 5 = 120$ gün sonra
 $120 \equiv 1 \pmod{7}$
Salı + 1 = Çarşamba

- 14) Herhangi bir yılın Temmuz ayında 5 tane Pazartesi günü vardır. Bunlardan üçünün tarihi tek sayı olduğuna göre, 9 Temmuz hangi gün olabilir?

Pzt Pzt Pzt Pzt pazar, salı
1 8 15 22 29
2 9 salı 16 23 30
3 10 17 24 31
↓
pazar 9 Temmuz
salı

- 15) 6 gün çalışıp 2 gün tatil yapan bir işçi, işe Salı günü başladığına göre, 21. tatil günü hangi gündür?

78 15 perşembe
GGGGGTTT GGGGGTTT - - -
1. TAM BLOK
78 15 16
15 16 24
↓
x
11 blokta 22. tatil gününe ulaşılır.
 $\frac{x-8}{8} + 1 = 11 \rightarrow x = 88$
İsterse 87. gündür
87. gün Salı + 86 gündür.
↓
2 (mod 7)
Salı + 2 = perşembe

- 16) $36! + 51! \equiv x \pmod{37}$ denkleğinde, x değeri kaç olabilir?

$36! + 1 \equiv 0 \pmod{37} \rightarrow \text{Wilson Teoremi}$
 $36! \equiv -1 \equiv 36 \pmod{37}$
 $+ 51! \equiv 0 \pmod{37}$
 $36! + 51! \equiv 36 \pmod{37}$