BÖLÜM 6

SAYILAR TEORİSİ

6.1 Tamsayılar

Tamsayılar kümesi $\{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$ sayılarından oluşur ve Z sembolü ile gösterilir.

6.1.1 Bölünebilirlik:

a ve b verilen tamsayılar olsun. Eğer $b = a \cdot d$ eşitliğini sağlayan bir d sayısı varsa a b'yi böler(b, a tarafından bölünür ya da a, b nin bir çarpanı) denir ve $a|b$ şeklinde gösterilir.

Her $b > 1$ tamsayısı en azından iki pozitif bölene sahiptir; bunlar 1 ve b dir.

Örnek 6.1.1 *1.* $-5|15$, *çünkü* $15 = 5 \cdot 3$.

2. $256|0$, *çünkü* $0 = 256 \cdot 0$.

3. $16|48$, *çünkü* $48 = 16 \cdot 3$.

6.1.2 Bölünebilirlik Özellikleri

Bütün $a, b, c \in Z$ için, aşağıdakiler doğrudur.

1. $a|a$.
2. Eğer $a|b$ ve $b|c$ ise $a|c$.
3. Eğer $a|b$ ve $a|c$ ise bütün $x, y \in Z$ için $a|bx + cy$ ifadesi doğrudur.
4. Eğer $a|b$ ve $b|a$ ise $a = \pm b$.

6.1.3 Tamsayılar için Bölüm Algoritması:

Eğer a ve b, $b \geq 1$ olmak koşulu ile, tamsayılar ise a'nın b'ye bölümü q tamsayısı gibi bir bölüm ve r tamsayısı gibi bir kalan verir.

$$a = qb + r,\ 0 \leq r < b.$$

Üstelik q ve r tektir. Bu bölümün kalanı $a \, mod \, b$ olarak gösterilir.

Örnek 6.1.2 *Eğer* $a = 73$, $b = 17$ *ise* $q = 4$ *ve* $r = 5$ *tir. Böylece* $73 \, mod \, 17 \equiv 5$ *tir.*

6.1.4 En Büyük Ortak Bölen (Greatest Common Divisor)

a ve b her ikisi birlikte 0 olmamak koşulu ile iki tamsayı olsun. a ve b nin en büyük ortak böleni, a ve b yi bölen en büyük d tamsayısıdır. a ve b nin en büyük ortak böleni $gcd(a, b)$ ya da kısaca (a, b) ile gösterilir.

Örnek 6.1.3 *1.* $gcd(7, 11) = 1$, *çünkü* $7 = 7 \cdot 1$, $11 = 11 \cdot 1$

2. $gcd(48, 40) = 8$, *çünkü* $48 = 2^4 \cdot 3$, $40 = 2^3 \cdot 5$

6.1.5 En Küçük Ortak Kat (Least common Multiple)

a ve b her ikisi birlikte 0 olmamak koşulu ile iki tamsayı olsun. a ve b nin en küçük ortak katı a ve b nin her ikisinin de böldüğü en küçük tamsayıdır ve $lcm(a, b)$ ile gösterilir.

Örnek 6.1.4 $lcm(8, 12) = 24$ *çünkü* $8 = 2^3$ *ve* $12 = 2^2 \cdot 3$ *tür.*

Teorem 6.1.5 *a ve b her ikiside birlikte* 0 *olmayacak şekilde tamsayılar olsun.* $gcd(a, b) = ax + by$ *eşitliğini sağlayan* x *ve* y *tamsayılar her zaman vardır.*

6.1.6 Asal Sayı

1 den büyük, 1 ve kendisinden başka böleni olmayan tamsayılara asal sayı denir.Asal olmayan sayılara da *bölünebilir sayı* denir.

Örnek 6.1.6 $2, 3, 5, 7, 11, 13, 17, 19, 23, \cdots$ *sayıları bazı asal sayılara örnektir.*

NOT: Asal sayılarla ilgili bazı özellikler:

- Eğer p sayısı asal sayı ve $p|ab$ ise $p|a$'yi veya $p|b$'yi böler.
- Sonsuz sayıda asal sayı vardır.

6.1.7 Aralarında Asal Sayı

a ve b iki tamsayısı $gcd(a, b) = 1$ koşulunu sağlıyorsa bu sayılara *aralarında asal* denir. $gcd(12, 5) = 1$ olduğu için 2 ve 5 sayıları aralarında asaldır.

6.1.8 Aritmetiğin Esas Teoremi

$n \geq 2$ olan her tamsayı asal sayıların çarpımları şeklinde tek olarak yazılır. Yani,

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$$

sayısında p_k lar farklı asal sayıları e_k lar da pozitif tamsayıları göstermektedir.

Örnek 6.1.7 $4200 = 2^3 \cdot 3 \cdot 5^2 \cdot 7$.

6.1.9 Öklid Algoritması(Euclidean Algorithm)

a ve b şeklinde olan iki tamsayının en büyük ortak bölenini aritmetiğin esas teoreminde bahsedildiği gibi çarpanlarına ayırarak ve ortak carpanların en büyüğünü alarak bulabiliriz. Eğer a ve b büyük sayılarsa bunların asal çarpanlarını bulmak zor olur; bunun sonucunda da en büyük ortak böleni bulmak da zorlaşır. Sayılar teorisinin önemli bir araştırma alanı da büyük tamsayıları daha çabuk çarpanlarına ayırma üzerine araştırmadır. Eğer a ve b nin asal çarpanları bilinmiyorsa, $gcd(a, b)$ yi bulmak için çabuk bir yol vardır. O da Öklid algoritmasıdır.

Öklid Algoritması şöyle çalışır.

- $a > b$ olmak üzere, a, b 'ye bölünür. Bölüm q_1, kalan r_1 olsun

$$a = b \cdot q_1 + r_1$$

- İkinci bölme işlemi gerçekleştirilir. b, r_1 'e bölünür ve bölüm q_2, kalan ise r_2 olur.

$$b = q_2 \cdot r_1 + r_2$$

- Üçüncü olarak r_1, r_2 'ye bölünür ve bölüm q_3, kalan ise r_3 olur.

$$r_1 = q_3 \cdot r_2 + r_3$$

$\vdots$

- Son olarak r_{n-1}, r_n 'e bölünür ve bölüm q_{n+1}, kalan ise $r_{n+1} = 0$ olur.

$$r_{n-1} = q_{n+1} \cdot r_n + r_{n+1}$$

- $r_{n+1} = 0$ olduğu için r_n değeri a ve b tamsayılarının en büyük ortak böleni olur. Yani $gcd(a, b) = r_n$ dir.

Bu algoritmadaki işlemler sonsuza kadar gitmez, çünkü 0 ile a tamsayısı arasında sonlu sayıda tamsayı vardır.

Örnek 6.1.8 • *$gcd(24, 138)$ 'in sonucu kaçtır? $gcd(24, 138) = ax + by$ ifadesinde x ve y sayıları kaç olur?*

$$\begin{aligned} 138 &= 5 \cdot 24 + 18 \\ 24 &= 1 \cdot 18 + 6 \quad \textit{ise} \quad gcd(24, 138) = 6 \textit{ dır.} \\ 18 &= 3 \cdot 6 + 0 \end{aligned}$$

x ve y aşağıdaki şekilde bulunur. $gcd(24, 138) = 6$

$$\begin{aligned} 6 &= 24 - 1 \cdot 18 &&= 24 - 1 \cdot (138 - 5 \cdot 24) \\ &= 24 - 1 \cdot 138 + 5 \cdot 24 &&= 6 \cdot 24 - 1 \cdot 138 \end{aligned}$$

Yani,

$6 = 6 \cdot 24 + (-1) \cdot 138$. *Buradan* $x = 6$ *ve* $y = -1$ *bulunur.*

- $gcd(1547, 560)$ *'in sonucu kaçtır?* $gcd(1547, 560) = ax+by$ *ifadesinde* x *ve* y *sayıları kaç olur?*

$$\begin{aligned} 1547 &= 2 \cdot 560 + 427 \\ 560 &= 1 \cdot 427 + 133 \quad \textit{ise} \quad gcd(1547, 560) = 7 \textit{ dir.} \\ 427 &= 3 \cdot 133 + 28 \\ 133 &= 4 \cdot 28 + 21 \\ 28 &= 1 \cdot 21 + 7 \\ 21 &= 3 \cdot 7 + 0 \end{aligned}$$

x ve y aşağıdaki şekilde bulunur. $gcd(1547, 560) = 7$

$$\begin{aligned} 7 &= 28 - 1 \cdot 21 \\ &= 28 - 1 \cdot (133 - 4 \cdot 28) &&= 28 - 1 \cdot 133 + 4 \cdot 28 \\ &= 5 \cdot 28 - 1 \cdot 133 &&= 5 \cdot (427 - 3 \cdot 133) - 1 \cdot 133 \\ &= 5 \cdot 427 - 15 \cdot 133 - 1 \cdot 133 &&= 5 \cdot 427 - 16 \cdot 133 \\ &= 5 \cdot 427 - 16 \cdot (560 - 1 \cdot 427) &&= 5 \cdot 427 - 16 \cdot 560 + 16 \cdot 427 \\ &= 21 \cdot 427 - 16 \cdot 560 &&= 21 \cdot (1547 - 2 \cdot 560) - 16 \cdot 560 \\ &= 21 \cdot 1547 - 42 \cdot 560 - 16 \cdot 560 &&= 21 \cdot 1547 - 58 \cdot 560 \end{aligned}$$

Yani,

$7 = 21 \cdot 1547 + (-58) \cdot y$. *Buradan* $x = 21$ *ve* $y = -58$ *bulunur.*

6.2 Asal Sayılar

Tanım 6.2.1 1 *den büyük olan,* 1 *ve kendisinden başka böleni olmayan sayılara asal sayı denir.*

Soru: Verilen bir tamsayının asal sayı olup olmadığı nasıl anlaşılır?

6.2.1 Eratosthenes Kalburu(The Sieve of Eratosthenes)

Verilen bir tamsayının asal sayı olup olmadığı Eratosthenes Kalburu metodu ile bulunabilir. Verilen tamsayı kendisinden önce gelen her pozitif tamsayıyla bölünür. Eğer hiç bir sayıya bölünemiyor ise bu sayıya asal sayı denir.

Metod:

$a > 1$ bir tamsayı olsun.Bu sayı eğer bölünebilir bir sayı ise $1 < b < a\,, 1 < c < a$ olmak üzere $a = b \cdot c$ şeklinde yazılabilir.Bütünlüğü bozmadan $b \leq c$ olduğu farzedilsin. O zaman,

$$b^2 \leq b \cdot c = a \Rightarrow b \leq \sqrt{a}$$

Aritmetiğin esas teoremini kullanarak b yi bölen ve $p \leq b \leq \sqrt{a}$ koşulunu sağlayan bir p sayısı bulunur. Öyle ki bu p sayısı b yi böldüğü ve b de a yı böldüğü için p a yı da bölmüş

olur.

Örnek 6.2.2

- $a = 173$. *a asal mıdır?* $13 < \sqrt{173} < 14$. 173 *sayısını bölebilecek asal sayılar* $2, 3, 5, 7, 9, 11, 13$ *olabilir. Bu sayıların* 173 *ü bölüp bölmediği kontrol edilir. Hiç birisi* 173 *sayısını bölmediği için sayı asal sayıdır.*

- 701 *ve*1009 *sayıları asal mıdır?* $26 < 701 < 27$. 701 *sayısını bölebilecek asal sayılar* $2, 3, 5, 7, 9, 11, 13, 17, 19, 23$ *olabilir. Bu sayıların* 173 *ü bölüp bölmediği kontrol edilir. Hiç birisi* 701 *sayısını bölmediği için sayı asal sayıdır.*

  $31 < 1009 < 32$. 1009 *sayısını bölebilecek asal sayılar* $2, 3, 5, 7, 9, 11, 13, 17, 19, 23, 29, 31$ *olabilir. Bu sayıların* 1009 *ü bölüp bölmediği kontrol edilir. Hiç birisi* 1009 *sayısını bölmediği için sayı asal sayıdır.*

6.3 Eratosthenes Metodu (Method of Eratosthenes)

Bu metod, verilen bir tamsayının altında kalan bütün asal sayıları bulmak için kullanılır. Öncelikle 2 den n ye kadar olan tamsayılar sırasıyla yazılır ve $\sqrt{n}$ den küçük ve eşit olan asalların çarpanları $(2p, 3p, \cdots)$ elimine edilir. Listede geri kalan sayılar asal sayıları gösterir.

Örnek 6.3.1 49 *u aşmayan bütün asalları bulunuz.*

	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	48	49	

$\sqrt{49} = 7$. *Böylelikle cevap:*$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47$ *asal sayılarıdır.*

6.4 Denklik Teorisi(Theory of Congruence (Modularity))

Tanım 6.4.1 *n sabit pozitif bir tamsayı olsun. Eğer $n|a-b$ ya da bir k tamsayısı için $a-b=nk$ eşitliği sağlanırsa, a b ye mod n e göre denktir denir ve $a \equiv b$ mod n ile gösterilir.*

Örnek 6.4.2

- $1 \equiv 5$ *mod* 4, *çünkü* $1-5=-4$ *ve* $4|-4$.
- $-2 \equiv 9$ *mod* 11, *çünkü* $-2-9=-11$ *ve* $11|-11$.

6.4.1 Teoremler:

1. $a \equiv b \bmod n \Leftrightarrow a = bk + n$ esitliğini sağlayan bir k vardır.
2. Her tamsayı mod n ye göre $0, 1, 2, \cdots, n-1$ sayılarından sadece birine denktir.
3. $a \equiv b \bmod n \Leftrightarrow a$ ve b, n ile bölündüğünde aynı kalanı verir.
4. $a \equiv a \bmod n$

5. $a \equiv b \bmod n \Rightarrow b \equiv a \bmod n$

6. $a \equiv b \bmod n$ ve $b \equiv c \bmod n \Rightarrow a \equiv c \bmod n$

7. $a \equiv b \bmod n$ ve $c \equiv d \bmod n \Rightarrow a + c \equiv b + d \bmod n$

8. $a \equiv b \bmod n \Rightarrow a^k \equiv b^k \bmod n$

6.4.2 Aritmetik Tersi

$a \neq 0$ herhangi bir tamsayı olmak üzere,eğer $a \cdot a^* \equiv 1 \bmod n$ denkliğini sağlayan bir a^* tamsayısı var ise bu a^* sayısına a nın mod n ye göre aritmetik tersi denir.

Teorem 6.4.3 *Eğer* $gcd(a, n) = 1 \Rightarrow a$ *nın aritmetik tersi vardır.*

Örnek 6.4.4 $gcd(4, 9) = 1$ *çünkü Öklid algoritmasına göre,* $9 = 4 \cdot 2 + 1$ *böylece* $1 = 4 \cdot 2 - 1 \cdot 9$ *bulunur.*

$1 = 4 \cdot 2 + (-1) \cdot 9 \Rightarrow 4 \cdot 2 \equiv 1 \ mod\ 9$

Neticede 4 *ün mod* 9 *a göre tersi* 2 *dir.*

NOT: $a \cdot b \equiv 1 \bmod m$ eşitliğinin sağlanması $gcd(a, m) = 1$ olmasıyla mümkündür.

Teorem 6.4.5 *(Fermat's Little Theorem) Eğer* p *asal bir sayı ise ve* $gcd(a, p) = 1$ *koşulunu sağlıyor ise*

$a^{p-1} \equiv 1$ *(mod* p*) denkliği her zaman doğrudur.*

NOT: $a^{p-1} \equiv 1 \pmod{p} \Rightarrow a^p \equiv a \pmod{p}$

Tanım 6.4.6 *Eğer p ve q, $a^p \equiv a \ (mod\ p)$ ile $a^q \equiv a \ (mod\ q)$ denkliklerini sağlayan farklı asal sayılar ise $a^{pq} \equiv a \ (mod\ pq)$ dur.*

Örnek 6.4.7

- $2^{1000000} \equiv \ ?\ (mod\ 7)$

$$p = 7 \qquad\qquad p - 1 = 6$$
$$1000000 = 6 \cdot 166666 + 4 \quad yani \quad 1000000 \equiv 4(mod 6)$$

Böylece

$$2^{1000000} = (2^6)^{166666} \cdot 2^4 \equiv 1 \cdot 2^4 = 16 \equiv 2\, mod 7$$

- $2^{340} \equiv \ ?\ (mod\ 341)$

$$2^{11} = 2 \cdot 2^{10} \equiv 2 \cdot 1 \equiv 2\, mod 31$$
$$2^{31} = 2 \cdot (2^{10})^3 \equiv 2 \cdot 1^3 \equiv 2\, mod 11$$

$$\Rightarrow a = 2,\ p = 11,\ q = 31$$

$$2^{11 \cdot 31} \equiv 2\, mod 341$$
$$2^{341} \equiv 2\, mod 341 \Rightarrow 2^{340} \equiv 1\, mod 341$$

6.5 Euler Fi(ϕ) Fonksiyonu (Euler Phi Function)

Tanım 6.5.1 *$n \geq 1$ bir tamsayı olsun. $\phi(n)$ fonksiyonu, $1 \leq a \leq n$ ve $gcd(a, n) = 1$ koşulunu sağlayan a tamsayılarının sayısını gösterir, yani n ye kadar olan ve n ile*

aralarında asal olan sayıların sayısını verir.

Örnek 6.5.2

$$\Phi(1) = 1$$
$$\Phi(2) = 1 \quad \text{çünkü} \quad gcd(1,2) = 1$$
$$\Phi(3) = 2 \quad \text{çünkü} \quad gcd(1,3) = gcd(2,3) = 1$$
$$\Phi(4) = 2 \quad \text{çünkü} \quad gcd(1,4) = gcd(3,4) = 1$$
$$\Phi(5) = 4 \quad \text{çünkü} \quad gcd(1,5) = gcd(2,5) = gcd(3,5) = gcd(4,5) = 1$$

NOT: $\phi(n) = n - 1 \Leftrightarrow n$ bir asal sayı olursa.

Teorem 6.5.3 *Eğer p asal bir sayı ise ve $k > 0$ ise $\phi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p})$ dir.*

Teorem 6.5.4 *(Euler Teoremi) $n > 1$ ve $gcd(a, n) = 1$ ise $a^{\phi(n)} \equiv 1 \, mod \, n$*

Örnek 6.5.5 $3^{\phi(8)} \equiv 1 \, mod \, 8$ *olduğunu gösterin.*

- $\phi(8) = \phi(2^3) = 2^3 - 2^2 = 4$

  $3^{\phi(8)} = 3^4 = 81 \equiv 1 \bmod 8$