3. Elemanter Sayılar Teorisinden Hatırlatmalar

Tanım 3.1 $a, b \in Z$, $a \neq 0$, $b = ac$ olacak şekilde $\exists c \in Z$ ise a böler b denir ve $a \mid b$ ile gösterilir.

$p \in Z$ ve $p > 1$ olsun. Eğer p tamsayısının 1 ve p den başka pozitif böleni yoksa p ye asal sayı denir.

Tanım 1 kullanılarak aşağıdaki özellikler kolayca gösterilebilir.

$\forall a, b$ ve $c \in Z$ için

1. $a \mid b$ ve $b \mid c \Longrightarrow a \mid c$

2. $\forall c \in Z$ için $a \mid b \Longrightarrow a \mid bc$

3. $a \mid b$ ve $a \mid c \Longrightarrow \forall x, y \in Z$ için $a \mid bx + cy$

4. $\forall p$ asalı için $p \mid ab \Longrightarrow p \mid a$ veya $p \mid b$

Tanım 3.2 a ve b sıfırdan farklı tamsayılar olsun. Aşağıdaki özellikleri sağlayan bir $d \in Z^+$ varsa bu d tamsayısına a ve b nin en büyük ortak böleni denir ve $ebob(a, b)$ ile gösterilir.

1. $d \mid a$ ve $d \mid b$

2. $\forall c \in Z$ için $c \mid a$ ve $c \mid b \Longrightarrow c \mid d$

Teorem 3.1 (Aritmetiğin Temel Teoremi) $\forall n > 1$ tamsayısı için

$$n = p_1^{n_1} p_2^{n_2} ... p_r^{n_r} \quad \ni \quad p_1 \leqslant p_2 \leqslant ... \leqslant p_r \text{ ve } n_i \in Z^+$$

olacak şekilde $1 \leqslant i \leqslant r$ için p_i asal sayı olmak üzere $\exists p_i \in Z$. Bu yazılış sıra farkıyla tek türlüdür.

Teorem 3.2 $\forall a, b \in Z$ ve $b > 0$ için

$$a = qb + r \text{ ve } 0 \leqslant r \leqslant b \text{ olacak şekilde } \exists!\ q, r \in Z$$

a ve b sıfırdan farklı herhangi iki tamsayı olsunlar. Eğer a ve b tamsayıları asal çarpanlarına ayrılabilirse $ebob(a, b)$ kolayca bulunabilir. Fakat, bir tamsayının asal çarpanlarını bulmak her zaman kolay olmayabilir. Euclid Bölme Algoritması asal çarpanlara ayırmaya gerek duymadan iki sayının en büyük ortak bölenini etkili bir şekilde bulabilir.

Algoritma 3.1 (**Euclid Bölme Algoritması**)

Kabul edelim ki a ve b tamsayılarının her ikisi birden sıfır olmasın. Bu algoritma verilen a ve b tamsayıları için $d := ebob(a, b)$ değerini hesaplar.

1. $x := a$ ve $y := b$
2. Eğer $y = 0$ ise $d := x$ ve Bitir.
3. $r := x \bmod y$
4. $x := y$
5. $y := r$
6. Git Adım 2

Örnek 3.1. $a = 1547$ ve $b = 560$ ise $ebob(a, b) =?$

Çözüm Euclid algoritmasını uygularsak

$$1547 = 2.560 + 427$$

$$560 = 1.427 + 133$$

$$133 = 4.28 + 21$$

$$28 = 1.21 + 7$$

$$21 = 3.7 + 0$$

olduğundan $b = 7, r = 0$ dır. Yani, $ebob(1547, 560) = 7$ dir.

Tanım 3.3 $\forall n \in Z^+$ için Euler ϕ fonksiyonu n sayısından küçük ve n ile arasında asal olan pozitif tamsayıların sayısı olarak tanımlanır. Yani,

$$\phi(n) := \#\{m \mid \ 0 < m < n \quad \ni \ ebob(m, n) = 1\} \text{ dir.}$$

Önerme 3.1 Eğer $ebob(m, n) = 1$ ise $\phi(mn) = \phi(m)\phi(n)$ dir.

Teorem 3.3 p_i ler farklı asallar , $e_i > 0$ ve $1 \leqslant i \leqslant n$ olsun.

$$m := \prod_{i=1}^{n} p_i^{e_i} \Longrightarrow \phi(m) = \prod_{i=1}^{n} (p_i^{e_i} - p_i^{e_i - 1})$$

Tanım 3.4 $\forall a, b$ ve $m \in Z$ için eğer $m \mid a - b$ ise $a \bmod m$ de b ye denktir denir ve $a \equiv b \bmod m$ olarak gösterilir.

Tanımdan '$\equiv$' nin bir denklink bağıntısı olduğu gösterilebilir. Verilen bir m tamsayısı için denklink sınıflarının 0 ve $m - 1$ arasında yalnız ve yalnızca bir temsilcisi vardır. Denklink sınıflarını $Z_m := \left\{\overline{0}, \overline{1}, ..\overline{m-1}\right\}$ ile gösterirsek Z_m aşağıdaki işlemlere göre bir değişmeli halkadır. Eğer m asal sayı ise Z_m bir cisimdir.

$\forall \overline{a}, \overline{b} \in Z_m$ için

$\overline{a} + \overline{b} := \overline{a + b}$

$\overline{a}.\overline{b} := \overline{a.b}$

$-\overline{a} := \overline{-a}$

Tanım 3.5 Eğer $aa^{-1} \equiv 1 \bmod m$ ise $a^{-1} \bmod m$ de a nın tersidir denir ve $a \bmod m$ de terslenebilirdir denir.

Önerme 3.2 Z_m halkasında eğer $ebob(a, m) = 1$ ise $a \in Z_m$ terslenebilirdir. Eğer a terslenebilirse $\exists! b \in Z_m \quad \ni \quad ab \equiv 1 \bmod m$

Teorem 3.4 $d := ebob(a, c)$ olsun.

$$ax \equiv b (\bmod c) \text{ kongrüansının çözümü vardır} \Longleftrightarrow d \mid b$$

Eğer $d \mid b$ ise kongrüansın $\bmod m$ de d tane çözümü vardır. x_0 kongrüansın bir çözümü olmak üzere

$$i = 0, 1, ...d - 1 \text{ için } x_i = x_0 + (\tfrac{c}{d})i$$

ler kongrüansın $\bmod m$ de birbirinden farklı çözümleridir.

Herhangi bir $a \in Z_m$ için $ebob(a, m) = 1$ olsun. Z_m halkasında a elemanının tersi Euclid bölme algoritması kullanarak etkili (hızlı) bir şekilde hesaplanabilir. Euclid algoritması kullanılarak hesaplamalar geriye doğru yapılırsa $1 = au + mv$ olacak şekilde ki u ve v tamsayıları bulunur. Bulduğumuz denklemi $\bmod m$ ye indirgersek $1 \equiv au \bmod m$ kongrüansını elde ederiz. Yani, $u = a^{-1} \bmod m$.

Algoritma 3.2

Bu algoritma Euclid bölme algortimasını kullanarak verilen bir a tamsayısının Modül m de tersinin olup olmadığını belirler ve varsa a nın Modül m de tersini ekrana yazar.

1. $m_0 := m$
2. $a_0 := a$
3. $t_0 := 0$
4. $t := 1$

5. $q := \left\lfloor \frac{m_0}{a_0} \right\rfloor$

6. $r := m_0 - q \times a_0$

7. Eğer $r > 0$ ise

(a) $temp := t_0 - q \times t$

(b) Eğer $temp \geqslant 0$ ise $temp := temp \bmod m$

(c) Eğer $temp < 0$ ise $temp := m - ((-temp) \bmod m)$

(d) $t_0 := t$

(e) $t := temp$

(f) $m_0 := a_0$

(g) $a_0 := r$

(h) $q := \left\lfloor \frac{m_0}{a_0} \right\rfloor$

(i) $r := m_0 - q \times a_0$

(j) Git Adım 7

8. Eğer $a_0 \neq 1$ ise Yaz "a nın Modül m de tersi yok", aksi halde $a^{-1} := t \bmod m$ ve Yaz a^{-1}

9. Bitir.

Örnek 3.2 $a = 23$ sayısının Z_{128} de varsa tersini bulunuz.

Çözüm Euclid algoritmasını uygularsak

$$128 = 5.23 + 13$$

$$23 = 1.13 + 10$$

$$10 = 3.3 + 1$$

$$3 = 3.1 + 0$$

$ebob(23, 128) = 1$dir.Yani, 23 sayısının tersi vardır.

Şimdi, $1 = 28.u + 128v$ olacak şekildeki u ve v tamsayılarını bulabilmek için Euclid algoritmasında hesaplamaları geriye doğru yaparsak (Algoritma 3.2)

$$\begin{aligned} 1 &= 10 - 3.3 \\ &= 10 - 3(13 - 1.10) \\ &= 4.10 - 3.13 \\ &= 4.(23 - 13) - 3.13 \\ \\ &= 4.23 - 7.(128 - 5.23) \\ &= 39.23 - 7.128 \end{aligned}$$

$1 \equiv 39.23 \bmod 128 \Longrightarrow 23^{-1} = 39$

$(G, *)$ sonlu bir grup ve $g \in G$ olsun. $g^m = 1$ olacak şekilde ki en küçük pozitif tamsayıya g nin mertebesi denir. $(Z_p^*, *)$ mertebesi $p - 1$ olan devirli bir gruptur. Yani, mertebesi $p - 1$ olan $\exists \alpha \in Z_p^*$. Z_p^* grubunda mertebesi $p - 1$ olan elemana primitif eleman denir.

Önerme 3.3 p tek asal sayı olsun. Eğer $\forall q \mid p - 1$ asalı için $a^{(p-1)/q} \not\equiv 1 \bmod p$ olacak şekilde bir a tamsayısı varsa a modül p de primitif köktür.

Eğer $p - 1$ in asal çarpanlarına ayrılışını biliyorsak **Önerme 3.3** kullanılarak modül p de primitif kök bulan etkili bir algoritma yazılabilir.

Algoritma 3.3

Bu algoritma verilen $p \geqslant 3$ asalı için modül p de primitif kök bulur. Modül p de bulunacak primitif kökü $primitif$ ile gösterelim.

$p - 1 := q_1^{a_1} q_2^{a_2} ... q_k^{a_k}$

1. $a := 2$ ve $i := 1$

2. Eğer $i > k$ ise $primitif := a$ ve Yaz a , aksi halde Git Adım 3

3. Eğer $a^{(p-1)/q_i} \not\equiv 1 \bmod p$ ise $i := i+1$ ve Git Adım 2, aksi halde $i := i+1, a := a + 1$ ve Git Adım 3.

4. Bitir.

Teorem 3.5 (Fermat) p asal sayı olsun.
$\forall a \in Z$ için $a^p \equiv a \bmod p$ ve eğer $ebob(a, p) = 1$ ise $a^{p-1} \equiv 1 \bmod p$ dir.

İspat Teoremi pozitif tamsayılar için ispatlamak yeterlidir. a sayısı üzerinde tümevarım kullanılarak ispat yapılabilir.

$a = 0$ için $0^p \equiv 0 \bmod p$ olduğundan iddia doğrudur.

$a = 1$ için $1^p \equiv 1 \bmod p$ olduğundan iddia doğrudur.

$a = n$ için iddianın doğru olduğunu kabul edip $a = n+1$ için de doğru olduğunu gösterelim :

Binom teoreminden

$$(n+1)^p = n^p + \binom{p}{1} n^{p-1} + \binom{p}{2} n^{p-2} + ... + \binom{p}{p-1} n + 1 \quad \text{dir.}$$

$1 \leqslant k \leqslant p-1$ için $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ ve paydaki p çarpanı sadeleştirelemeyeceğinden $p \mid \binom{p}{k}$ dir. Yani, $(n+1)^p \equiv n^p + 1 \bmod p$ dir. İddia n için doğru olduğundan $n^p \equiv n \bmod p$ dir. Sonuç olarak,

$$\begin{aligned}(n+1)^p &\equiv n^p + 1 \bmod p \\ &\equiv n + 1 \bmod p\end{aligned}$$

dir. İddia $n+1$ için de doğru olduğundan tümevarımdan ispat tamamlanmış olur.

Eğer $ebob(a,p) = 1$ ise $a^{-1}a \equiv 1 \bmod p$ dir.

$$\begin{aligned}a^p &\equiv a \bmod p \\ a^p a^{-1} &\equiv a a^1 \bmod p \\ a^{p-1} &\equiv 1 \bmod p\end{aligned}$$

olur.

Tanım 3.6 Aşağıdaki özellikleri sağlayan $\{r_1, r_2, ..., r_{\phi(m)}\}$ kümesine modulo m indirgenmiş kalan sistemi denir.

1. $1 \leqslant i \leqslant \phi(m)$ olacak şekilde ki $\forall i$ için $ebob(r_i, m) = 1$

2. $i \neq j$ için $r_i \neq r_j \bmod m$

3. $\forall n \in Z$, $ebob(n,m) = 1$ için $n \equiv r_i (\bmod m)$ olacak şekilde $\exists i \ni 1 \leqslant i \leqslant \phi(m)$

Teorem 3.6 (Euler) Eğer $ebob(a, m) = 1$ ise $a^{\phi(m)} \equiv 1 \bmod p$ dir.

İspat : $ebob(a, m) = 1$ olsun. $\{r_1, r_2, ..., r_{\phi(m)}\}$ bir indirgenmiş kalan sistemi olsun. $ebob(a, m) = 1$ ve $r_1, r_2, ..., r_{\phi(m)}$ sayıları $\bmod m$ de terslenebilir olduğundan $ar_1, ar_2, ..., ar_{\phi(m)}$ sayıları da terslenebilirdir. $ebob(a, m) = 1$ olduğundan

$$ar_i \equiv ar_j \bmod m \Longrightarrow r_i \equiv r_j \bmod m \qquad \text{dir.}$$

Dolayısıyla, $ar_1, ar_2, ..., ar_{\phi(m)}$ sayılarının herhangi ikisi birbirine denk olamaz. Sonuç olarak,

$$\begin{aligned} (ar_1)(ar_2)...(ar_{\phi(m)}) &\equiv r_1 r_2 ... r_{\phi(m)} \bmod m \\ a^{\phi(m)} r_1 r_2 ... r_{\phi(m)} &\equiv r_1 r_2 ... r_{\phi(m)} \bmod m \\ a^{\phi(m)} &\equiv 1 \bmod m \qquad \text{dir.} \end{aligned}$$

Algoritma 3.4 ($\bmod m$ de üs alma)

Bu algoritma $k \geqslant 0$ olmak üzere verilen a, k ve m tamsayıları için $z := a^k \bmod m$ ifadesini hızlı bir şekilde hesaplar.

1. $sonuc := 1$
2. Eğer $k = 0$ ise $z := sonuc$ ve Bitir.
3. Eğer $k \bmod 2 = 1$ ise
   (a) $sonuc := (sonuc.a) \bmod m$

   (b) $k := k - 1$

   (c) Git Adım 2

4. Eğer $k \bmod 2 = 0$ ise

(a) $a := a^2 \bmod m$

(b) $k := k/2$

(c) Git Adım 2