

CENG 114 BİLGİSAYAR BİLİMLERİ İÇİN AYRIK YAPILAR

Prof. Dr. Tufan TURACI

tturaci@pau.edu.tr

- Pamukkale Üniversitesi
- Mühendislik Fakültesi
- Bilgisayar Mühendisliği Bölümü
- Hafta 10

Ders İçereği

Sayılar Teorisine Giriş

--- Öklit Algoritması

--- Diyafont Denklemler ve Çözümleri

--- Asal Sayılar ve Asal Sayıların Bulunması

- **Modüler Aritmetik**

--- Doğrusal Denklikler

Öklit Algoritması

Tanım: $a \neq 0$, a ve $b \in \mathbb{Z}$ olsun. q bir tam sayı olmak üzere, $b = qa$ ise a bölür b denir veya b , a 'nın katıdır denir. $a|b$ şeklinde gösterilir.

$$5|10 \Rightarrow 10 = 5 \cdot 2$$

Teoremler

(i) $a|b$ ise $a|k \cdot b$ 'dir.

(ii) $a|b$ ve $b|a$ ise $a = \pm b$

(iii) $a|b$ ve $b|c$ ise $a|c$ 'dir.

(iv) $a|b$ ve $a|c$ ise $a|sb+tc$ 'dir.

(v) $k \neq 0$ ve $k \in \mathbb{Z}$ için, $a|b \Leftrightarrow a \cdot k | b \cdot k$ 'dir.

(vi) $a > 0, b > 0$ ve $a|b$ ise $\Rightarrow a \leq b$ 'dir.

İspatlar:

ispat (i) $5|10$ ise $5|10 \cdot z = 5|20$ 'dir.

$$a|b \Rightarrow b = a \cdot q$$

$a|k \cdot b?$

$$k \cdot b = k \cdot a \cdot q$$

$$k \cdot b = a \cdot (\underbrace{k \cdot q}_{x \in \mathbb{Z} \text{ olsun}})$$

tanımın

$\Rightarrow a|k \cdot b$ 'dir.

iv

$a|b$ ve $a|c$ ise $a|s.b + c.t$ 'dir.

$$2|6 \text{ ve } 2|10$$

$$s=3 \\ t=5$$

||

$$2|3.6 + 5.10$$

$$= 2|60$$

ispat

(i) $a|b \Rightarrow a|b.s \Rightarrow bs = a.t_1$ 'dir.

$a|c \Rightarrow a|c.t \Rightarrow ct = a.t_2$ 'dir

$$bs + ct = a.(t_1 + t_2)$$

$bs + ct = a.q \Rightarrow a|bs + ct$

Teorem: $a \in \mathbb{Z}^+$, b ve $q \in \mathbb{Z}^+$ olsun.

$b = q.a + r$, $0 \leq r < a$ şartını sağlayan tek şekilde q ve r temsilcileri vardır.

b	q	a	r
36	$= 3 \cdot 10$	$+$	6

Tanım: $a, b, c \in \mathbb{Z}^+$ olsun.

$c|a$ ve $c|b$ ise c 'ye a ile b 'nin ortak bölünü denir.

Ortak bölenlerin en büyüğü (OBEB) $\gcd(a,b)$ veya (a,b) ile gösterilir.

= Oklid Algoritması =

Farzedelim ki $a, b \in \mathbb{Z}^+$ olsun. Aşağıdaki işlemler ardışık şekilde devam etsin.

$$a = b \cdot q_0 + r_0, \quad 0 \leq r_0 < b \quad \begin{array}{l} r_0, q_0 \in \mathbb{Z}^+ \cup \{0\} \\ \text{0'ın dışında} \end{array}$$

$$b = r_0 \cdot q_1 + r_1, \quad 0 \leq r_1 < r_0$$

$$r_0 = r_1 \cdot q_2 + r_2, \quad 0 \leq r_2 < r_1$$

$$\vdots \quad \vdots \quad \vdots \quad \vdots$$
$$r_k = r_{k+1} \cdot q_{k+2} + r_{k+2}, \quad 0 \leq r_{k+2} < r_{k+1}$$

Eğer $r_{k+2} = 0$ ise $\boxed{\gcd(a, b) = r_{k+1} \text{ 'dir.}}$

Q12) $\gcd(205, 99) = ?$

$$205 = 99 \cdot 2 + 7$$

$$99 = 7 \cdot 14 + 1$$

$$7 = 1 \cdot 7 + 0$$

$$\gcd(205, 99) = 1$$

Öklid algoritmasını kullanarak
 $\text{gcd}(203, 91)$ 'i hesaplayınız.

$$203 = 91 \cdot 2 + 21, \quad 0 \leq 21 < 91$$

$$91 = 21 \cdot 4 + 7, \quad 0 \leq 7 < 21$$

$$21 = 7 \cdot 3 + \underline{\underline{0}} \quad \text{gcd}(a,b) = 7$$

$\text{gcd}(a,b) \Rightarrow$ greatest common divisor (Ortak bölenlerin en büyüğü - OBEB)

$\text{lcm}(a,b) \Rightarrow$ least common multiple (Ortak katların en küçüğü - OKEK)

Teorem: a ve b iki pozitif tamsayı olmak üzere

$$\text{gcd}(a,b) * \text{lcm}(a,b) = a * b$$

NOT: Öklit algoritması ve yukarıdaki teorem yardımıyla iki sayının OKEK değeri de bulunabilir.

Pseudo Kodu

print '2 tamsay, jirini z' $a > b$
read a, b

bes2: $k \leftarrow a$

bas1: $k \leftarrow k - b$

if $(k >= b)$ then go to bas1 end if

if $(k = 0)$ then print 'obab = ', b

go to son;
end if

$a \leftarrow b$

$b \leftarrow k$

go to bes2;

SON: END.

C kodu: `#include<stdio.h>`
`#include<conio.h>`
`int main()`
`{ int a,b,s,t;`
`printf("a degerini giriniz: ");`
`scanf("%d",&a);`
`printf("b degerini giriniz: ");`
`scanf("%d",&b);`
`if (a<b) {s=a; a=b; b=s;}`
`bas:`
`t=a%b;`
`if (t==0) {printf ("iki sayinin obebi= %d", b);`
`goto son;}`
`a=b;`
`b=t;`
`goto bas;`
`son:`
`getch ();`
`return 0;`
`}`

```
a degerini giriniz: 16
b degerini giriniz: 24
iki sayinin obebi= 8
-----
```

```
a degerini giriniz: 12
b degerini giriniz: 29
iki sayinin obebi= 1
-----
```

```
a degerini giriniz: 8
b degerini giriniz: 1
iki sayinin obebi= 1
-----
```

```
a degerini giriniz: 205
b degerini giriniz: 99
iki sayinin obebi= 1
-----
```

```
a degerini giriniz: 203
b degerini giriniz: 91
iki sayinin obebi= 7
-----
```

Diyafont Denklemler

Tanım:

$a, b, d \in \mathbb{Z}^+$, x, y bilinmeyen ve $x, y \in \mathbb{Z}$

Örnekte örnekte:

$$d = ax + by \quad \text{şeklinde k:}$$

denklemlerle diyafont denklemleri denir.

Teoremi:

$a, b \in \mathbb{Z}^+$ ve $d = \gcd(a, b)$ Örnekte

Örnekte; d , a ile b 'nin lineer kombinasyonu şeklinde yazılabilir.

$$\text{yeni } d = a.x + b.y \text{ 'dir.}$$

(2) $a=240$, $b=936$ olsun. $\gcd(a, b) = ax + by$

denklemini: sağlayan x ve y tam sayılarını bulmak

$$936 = 240 \cdot 3 + 216$$

$$240 = 216 \cdot 1 + 24 \longrightarrow \gcd(240, 936) = 24$$

$$216 = 24 \cdot 9 + 0$$

$$24 = 240x + 536y \quad 'y': \text{başlangıç } x \text{ ve } y \text{ değerleri?}$$

$$\begin{aligned} 24 &= 240 - 216.1 \\ &= 240 - (536 - 240.3) \\ &= 240 - 536 + 240.3 \\ &= \boxed{4} \cdot 240 + \boxed{-1} \cdot 536 \\ &\quad \times \qquad \qquad y \end{aligned}$$

En

$8 = 64x + 202y$ eşitliğini sağlayan
 x ve y değerleri Öklid algoritması kullanarak
bulunabiliriz.

$$202 = 64 \cdot 3 + 10$$

$$64 = 10 \cdot 6 + 4$$

$$10 = 4 \cdot 2 + 2$$

$$4 = 2 \cdot 2 + 0$$

$$2 = 64x + 202y$$

$$2 = 10 - 4 \cdot 2$$

$$= 10 - (64 - 10 \cdot 6) \cdot 2$$

$$= 10 - 64 \cdot 2 + 10 \cdot 12$$

$$= 13 \cdot 10 - 64 \cdot 2$$

$$= 13 \cdot (202 - 64 \cdot 3) - 64 \cdot 2$$

$$= 13 \cdot 202 - 39 \cdot 64 - 64 \cdot 2$$

*4/

$$2 = 13 \cdot 202 - 41 \cdot 64$$

$$8 = 52 \cdot 202 - 164 \cdot 64$$

$$= 52 \cdot 202 + (-164) \cdot 64$$

$$\begin{aligned} x &= -164 \\ y &= 52 \end{aligned}$$

↓
y

↓
x

Çalışma Sorusu: $d = a.x + b.y$ şeklinde diyafont denklemleri çözen bir program yazınız.
($d = \text{gcd}(a, b)$, a ve b pozitif tamsayılardır.)

Asal Sayılar

Tanım!

Sadece 1'e ve kendine bölünen sayılar
asal sayılar denir. 1'den büyük asal olmayan
sayılara bileşik sayılar denir.

5 → asal sayı

10 → bileşik "

① 1'den büyük 2 farklı sayının çarpımı şeklinde
yazılamayan sayılara asal sayılar denir.

② 1 ne asal, ne bileşik sayıdır.

③ 2'de çift sayı denir tek asıldır.

Teoremi:

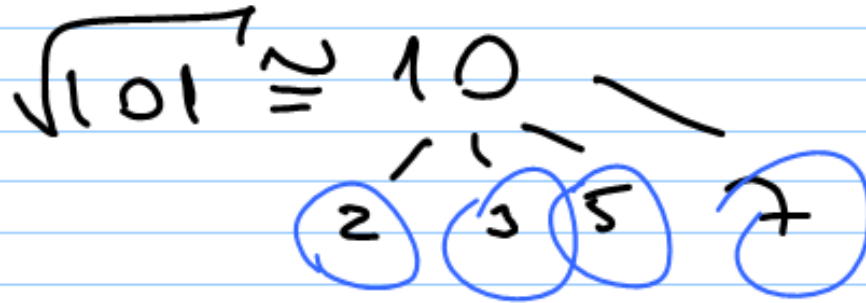
(i) 1'den büyük her tam sayının en az bir asal böleni vardır.

(ii) n bir bileşik sayı ise n sayısının \sqrt{n} 'den büyük olmayan bir asal çarpanı vardır.

$$50 \Rightarrow \sqrt{50} \approx 7 \\ \begin{array}{c} 2 \quad 5 \\ \diagup \quad \diagdown \\ 2 \quad 5 \end{array}$$

(iii) $n > 1$ için n tam sayısının \sqrt{n} 'den küçük bir asal böleni yoksa n bir asal sayıdır.

$n = 101$ asaldır mı?



$\frac{101}{2}$ tam bölünmez

2

$\frac{101}{3}$ " "

$\frac{101}{5}$ " "

$\frac{101}{7}$ " "

4'üne bölünmediğinden
101 sayısı asaldır!!!

C kodu:

```
#include <stdio.h>
#include<conio.h>
#include <math.h>
int main()
{ int i,j,x,a,z,s=0;
  printf("x degerini giriniz: ");
  scanf("%d",&x);
  a=floor(sqrt(x));
  //printf("a degeri= %d", a);
  for(i=2;i<=a;i++)
  { z=0;
    for(j=2;j<=i-1;j++)
    { if (i%j==0) z++;
      }
    if (z==0) printf("%d sayisi asal sayidir, %d sayısına bolunup bolunmedigi kontrol edilecektir...\n", i,x);
    if ((z==0) && (x%i==0)) s++; // x sayısına bölünüp bölünmediği kontrol ediliyor!
  }
  if (s==0) printf ("%d sayisi asal sayidir...",x);
  else
    printf ("%d sayisi asal sayi degildir...",x);
  getch ();
  return 0;
}
```

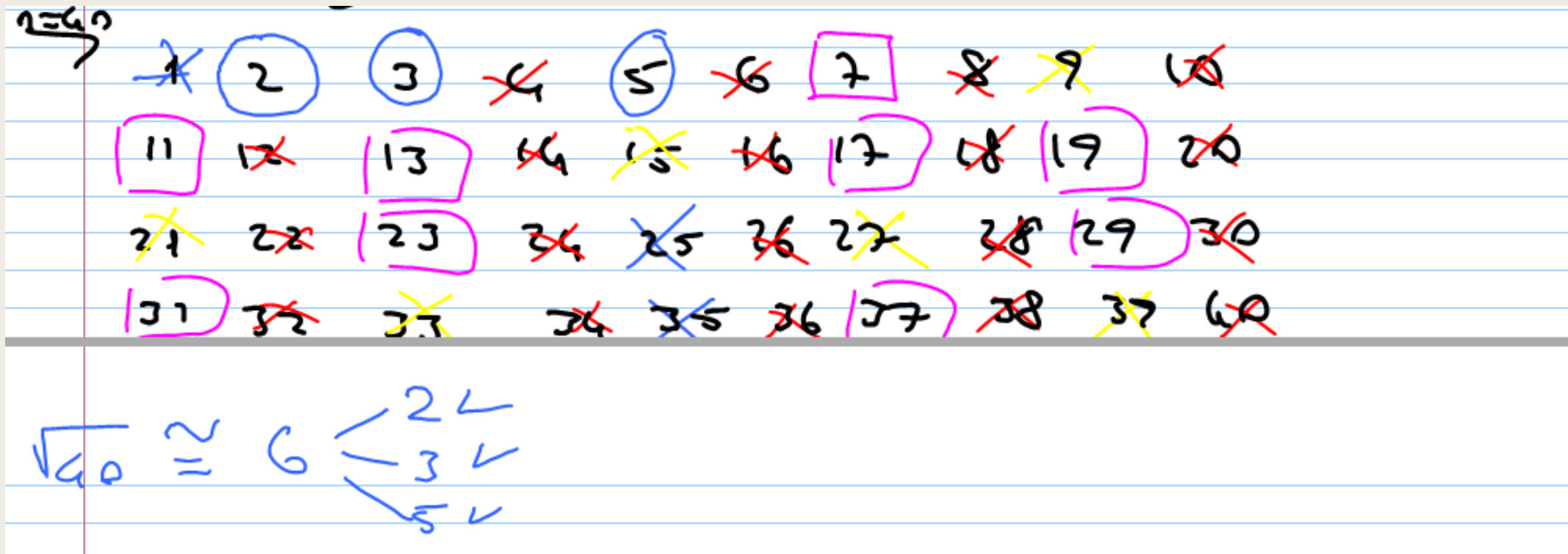
```
x degerini giriniz: 105
2 sayisi asal sayidir, 105 sayisina bolunup bolunmedigi kontrol edilecektir...
3 sayisi asal sayidir, 105 sayisina bolunup bolunmedigi kontrol edilecektir...
5 sayisi asal sayidir, 105 sayisina bolunup bolunmedigi kontrol edilecektir...
7 sayisi asal sayidir, 105 sayisina bolunup bolunmedigi kontrol edilecektir...
105 sayisi asal sayi degildir...
-----
```

```
x degerini giriniz: 137
2 sayisi asal sayidir, 137 sayisina bolunup bolunmedigi kontrol edilecektir...
3 sayisi asal sayidir, 137 sayisina bolunup bolunmedigi kontrol edilecektir...
5 sayisi asal sayidir, 137 sayisina bolunup bolunmedigi kontrol edilecektir...
7 sayisi asal sayidir, 137 sayisina bolunup bolunmedigi kontrol edilecektir...
11 sayisi asal sayidir, 137 sayisina bolunup bolunmedigi kontrol edilecektir...
137 sayisi asal sayidir...
-----
```


Eratosthenes Kalburu Yardımıyla Asal Sayıların Bulunması

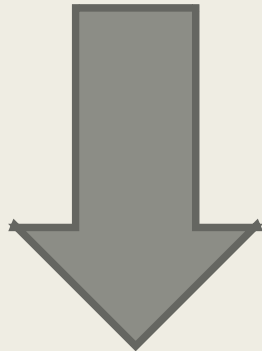
1 den n ye kadar olan tüm asal sayıların listelenmesi Eratosthenes Kalburu yardımıyla yapılır.

$n=40$ a kadar olan tüm asal sayıları listeleyelim.



```
#include <stdio.h>
#include<conio.h>
#include <math.h>
#include <stdlib.h>
```

```
int main()
{ int i,j,x,*asal;
  printf("x degerini giriniz: ");
  scanf("%d",&x);
  asal=(int *)malloc((x+1)*sizeof(int));
  for (i=2;i<=x;i++) // Dizinin tüm elemanlarını 1 yaptık. (2 den itibaren)
    { asal[i]=1;}
```



```
// Karekök x e kadar asal sayıların katlarını sıfıra işaretleriz.
```

```
for (i=2;i<sqrt(x);i++)  
    { if (asal[i]==1){ for (j=i;i*j<=x;j++)  
                        { asal[i*j]=0;}  
      }  
    }
```

```
// İşaretlenmemiş sayılar ekrana yazdırılır.
```

```
j=0;  
for (i=2;i<=x;i++)  
    if (asal[i]==1) {j++;  
                    printf("%d. Asal Sayı = %d\n",j,i);}   
  
getch();  
return 0;  
}
```

Örnekler:

```
x degerini giriniz: 40
```

1. Asal Sayi = 2
2. Asal Sayi = 3
3. Asal Sayi = 5
4. Asal Sayi = 7
5. Asal Sayi = 11
6. Asal Sayi = 13
7. Asal Sayi = 17
8. Asal Sayi = 19
9. Asal Sayi = 23
10. Asal Sayi = 29
11. Asal Sayi = 31
12. Asal Sayi = 37

```
-----
```

```
x degerini giriniz: 60
```

1. Asal Sayi = 2
2. Asal Sayi = 3
3. Asal Sayi = 5
4. Asal Sayi = 7
5. Asal Sayi = 11
6. Asal Sayi = 13
7. Asal Sayi = 17
8. Asal Sayi = 19
9. Asal Sayi = 23
10. Asal Sayi = 29
11. Asal Sayi = 31
12. Asal Sayi = 37
13. Asal Sayi = 41
14. Asal Sayi = 43
15. Asal Sayi = 47
16. Asal Sayi = 53
17. Asal Sayi = 59

```
-----
```

Aritmetiğin Temel Teoremi:

1'den büyük her tam sayı asal sayıların çarpımı olarak yazılır ve bu yazılış tek biridir.

$$\begin{aligned} 100 &= 25 \cdot 4 \\ &= 5^2 \cdot 2^2 = 5 \cdot 5 \cdot 2 \cdot 2 \end{aligned}$$

Modüler Aritmetik

Tanım: $m \in \mathbb{Z}^+$ olsun. Eğer m sayısı 2 tam sayının farklı $a-b$ 'yi böliyorsa, modül b 'ye göre a denktir b denir ve $a \equiv b \pmod{m}$ şeklinde gösterilir.

$$\begin{array}{ccc} 64 & \equiv & 4 \pmod{10} \\ a & & b \end{array}$$

$$m | a-b \stackrel{?}{=} 10 | 64-4$$
$$10 | 60 \checkmark$$

Teorem 1:

i) $a \equiv b \pmod{m}$ ise, $b \equiv a \pmod{m}$ dir.

ii) $a \equiv b \pmod{m}$ ve $b \equiv c \pmod{m}$ ise $a \equiv c \pmod{m}$ dir.

iii) $a \equiv b \pmod{m}$ ve $c \equiv d \pmod{m}$ ise $a + c \equiv b + d \pmod{m}$ dir.

iv) $a \equiv b \pmod{m}$ ise $ca \equiv c \cdot b \pmod{m}$ dir, $C \in \mathbb{Z}^+$.

v) c, a ve b nin bir ortak böleni olmadık üzere

$$a \equiv b \pmod{m} \Leftrightarrow \frac{a}{c} \equiv \frac{b}{c} \pmod{\frac{m}{c}} \text{ dir.}$$

ispat iv: $a \equiv b \pmod{m}$ ise $ca \equiv cb \pmod{m}$ dir?

$\Leftrightarrow m \mid a-b$ dir (terimden)

$a-b = m \cdot q$ (bölen terimden)

$$c \cdot (a-b) = m \cdot \underbrace{c \cdot q}_{x \in \mathbb{Z}}$$

$ca - cb = m \cdot x \rightarrow$ (bölen terimden) $m \mid ca - cb$ dir

$ca \equiv cb \pmod{m}$ \Leftarrow elde edilir.

Teorem 2:

- i) $a \equiv b \pmod{m}$ ve $c \equiv d \pmod{m}$ ise $a.c \equiv b.d \pmod{m}$ dir.
- ii) $a \equiv b \pmod{m}$ ise $a^n \equiv b^n \pmod{m}$, $n \in \mathbb{Z}^+$.
- iii) $p(x)$ tam katsayılı bir polinom olmak üzere
 $a \equiv b \pmod{m}$ ise $p(a) \equiv p(b) \pmod{m}$ dir.

is ~~not~~
 ii

$$a \equiv b \pmod{m} \text{ ise } a^n \equiv b^n \pmod{m}, n \in \mathbb{Z}^+.$$

//

$$\Rightarrow m \mid a-b \text{ 'dir (mod terimi)}$$

$$\Rightarrow \textcircled{*} a-b = m \cdot q \text{ 'dir (bökm teriminde)}$$

$$\boxed{a = b + m \cdot q}$$

$$a^n - b^n = (a-b) \cdot \overbrace{\left[a^{n-1} \cdot b^0 + a^{n-2} \cdot b^1 + a^{n-3} \cdot b^2 + \dots + a^0 \cdot b^{n-1} \right]}^{x \in \mathbb{Z}}$$

$$a^n - b^n = m \cdot q [x]$$

$$a^n - b^n = m \cdot \underbrace{[a \cdot x]}_{\substack{\text{w} \in \mathbb{Z} \text{ dan} \\ \text{abakardan}}}, \quad a^n - b^n = m \cdot w$$

$$\text{mod} \longleftarrow m \mid a^n - b^n \text{ dir.}$$

$$a^n \equiv b^n \pmod{m} \text{ dir.} \star$$

Doğrusal Denkleler

Tanım: $ax \equiv b \pmod{m}$ denkleğinin çözümü x_1 ise
a $x_1 \equiv b \pmod{m}$ yazılabilir. Gerçekten x_1 bir
çözüm ve $x_1 \equiv x_2 \pmod{m}$ ise, x_2 'de bir çözümdür.

Bu durumda x_1 ve x_2 aynı çözüm sayılır.

Buna $x \equiv x_1 \pmod{m}$ şeklinde gösterip,
 $ax \equiv b \pmod{m}$ denkleğinin çözümü diye oluruz.

①

$$27 \equiv x \pmod{5} \text{ ise } x = ?$$

②

2'nin bölümlük sınıfı = $\overline{2}$

$$\overline{2} = 2 + 5k \text{ yani } \overline{2} = \{ \dots, -3, \boxed{2}, 7, 12, \dots \}$$

①

$$10 \cdot x \equiv 1 \pmod{13} \text{ ise } x = ?$$

⇓

x=1 için sağlanmaz

x=2 "

x=3 "

"

"

"

"

$$x = \overline{4}$$

$$x = 4 + 13k$$

$$x = 4 \text{ sağlar}$$

$$40 \equiv 1 \pmod{13}$$

x=5,6,7,8,9,10,11 ve 12 için de sağlanmaz!!!

$$x = 4$$

$$17$$

$$30$$

$$43$$

⋮

①

$$11 \cdot x \equiv 28 \pmod{1943} \text{ ise } x \text{ 'in çık ?}$$

Çözümü birazdan yapılacaktır...

Rasyonel sayılarda mod alma işlemi:

① $\frac{1}{3} \equiv x \pmod{5}$ ise $x = ?$

$0, \bar{1}, \bar{2}, \bar{3}, \bar{4}$

$$\frac{1+5}{3} = \frac{6}{3} = \bar{2} \quad x = \bar{2}$$

② $\frac{1}{3} \equiv x \pmod{4}$

$$\frac{1+4}{3} = \frac{5+4}{3} = \frac{9}{3} = \bar{3} \Rightarrow x = \bar{3}$$

Teoremi!

$ax \equiv b \pmod{m}$ denkleminin bir çözümü
olduğu demektir $ax - my = b$ diğafat denkleminin
bir çözümü olduğu demektir.

Örnek

$$10x \equiv 14 \pmod{24} \text{ ise } x = ?$$

Çözüm: $10x \equiv 14 \pmod{24}$ ise $x = ?$

$\boxed{10x - 24y = 14}$ denkleminin çözümünü bulmamız gerekir.
→ diğerkart denklem.

$$24 = 10 \cdot 2 + 4$$

$$10 = 4 \cdot 2 + 2$$

$$4 = 2 \cdot 2 + 0$$

$$2 = 10 - 4 \cdot 2$$

$$2 = 10 - (24 - 10 \cdot 2) \cdot 2$$

$$2 = 10 - 2 \cdot 24 + 4 \cdot 10$$

$$2 = 5 \cdot 10 - 2 \cdot 24$$

obab $x \cdot a \quad y \cdot m$

7 ile
çarpalım →

$$14 = \boxed{35} \cdot 10 - 14 \cdot 24$$

$b \quad x \cdot a \quad y \cdot b$

bir çözüm.

Böylece;

$$35 \equiv 11 \pmod{24}$$

\Downarrow

$$x = \overline{11} = 11 + 24k$$

$$x = 11$$

$$x = 35$$

$$x = 59$$

$$x = 83$$

\vdots

elde edilir.

① rnt: $\frac{11x}{a} \equiv \frac{28}{b} \pmod{1943}$ ise $x=?$

11x-1943y=28 diyafont denkleminin çözümünün olması gerekir.

$$1943 = 11 \cdot 176 + 7$$

$$11 = 7 \cdot 1 + 4$$

$$7 = 4 \cdot 1 + 3$$

$$4 = 3 \cdot 1 + 1$$

$$3 = 1 \cdot 3 + 0$$

$$1 = 4 - 3 \cdot 1$$

$$1 = 4 - (7 - 4)$$

$$= 4 \cdot 2 - 7$$

$$= (11 - 7) \cdot 2 - 7$$

$$= 2 \cdot 11 - 2 \cdot 7 - 7$$

$$= 2 \cdot 11 - 3 \cdot 7$$

$$= 2 \cdot 11 - 3 \cdot (1943 - 11 \cdot 176)$$

$$= 2 \cdot 11 + 528 \cdot 11 - 3 \cdot 1943$$

$$1 = 530 \cdot 11 - 3 \cdot 1943$$

Her iki taraf 28 ile çarpılırsa:

$$28 = \underline{14840} \cdot 11 - 84 \cdot 1943$$

$x \Rightarrow$ herhangi bir çözüm

$$14840 \equiv \underline{1239} \pmod{1943}$$

$$x = \overline{1239} \text{ yani } x = 1239 + 1943k$$

$$x = 1239$$

$$x = 3182$$

:

elde edilir.

Çalışma Sorusu:

$16x \equiv 12 \pmod{60}$ doğrusal denklik sisteminin çözümü sağlayan en küçük pozitif x tamsayı değeri nedir?

Yanıt: 12

Gelecek Haftanın Konuları:

- **Sayılar Teorisi ile İlgili Önemli Teoremler**
 - Çinli Kalan Teoremi
 - Wilson Teoremi
 - Fermat Teoremi
 - Euler Teoremi
- **Sayılar Teorisinin Kriptolojiye Uygulaması**

Kaynaklar

- *Discrete Mathematics and Its Applications*, Kennet H. Rosen
(Ayırık Matematik ve Uygulamaları, Kennet H. Rosen (Türkçe çeviri),
Palme yayıncılık)
- *Discrete Mathematics: Elementary and Beyond*, L. Lovász, J. Pelikán,
K. Vesztergombi, 2003.
- *Introduction to Algorithms*, T.H. Cormen, C.E. Leiserson, R.L. Rivest,
C. Stein, 2009.
- *Introduction To Design And Analysis Of Algorithms*, A. Levitin, 2008.