CENG 114 BİLGİSAYAR BİLİMLERİ İÇİN AYRIK YAPILAR

Doç. 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

Öklit Algoritması

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

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

Teorem

(i) $a \mid b$ ise $a \mid kb$'dir.

(ii) $a \mid b$ ve $b \mid a$ ise $a = \mp b$

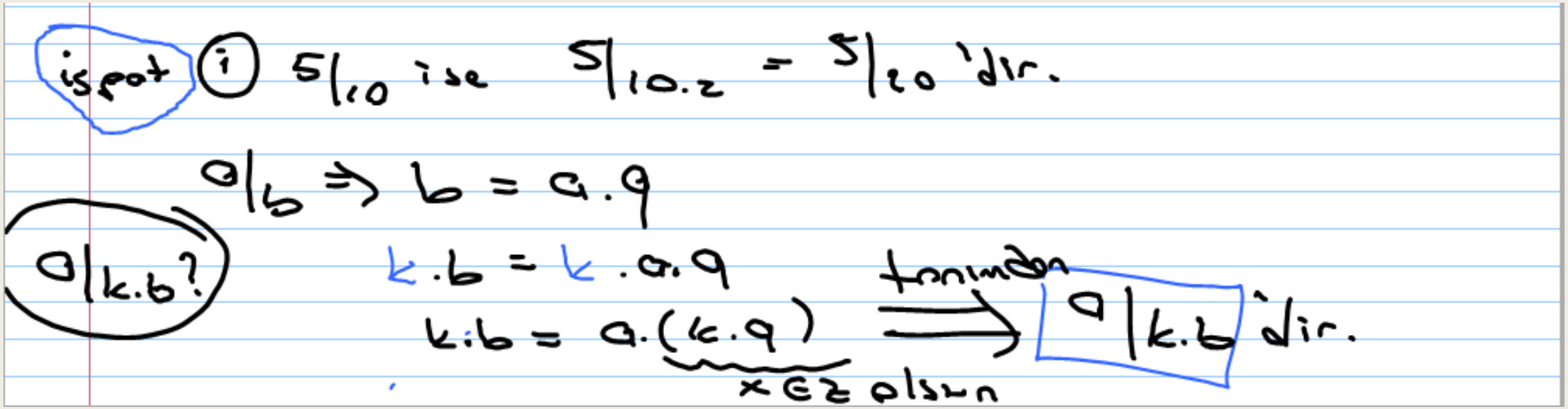
(iii) $a|b$ ve $b|c$ ise $a|c$ 'dir.

(iv) $a|b$ ve $a|c$ ise $a|sb+tc$, $s,t \in \mathbb{Z}$ 'dir.

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

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

İspatlar:


ispat
i) 5|10 ise 5|10.z = 5|20 'dir.
a|b ⇒ b = a.q
a|k.b?
k.b = k.a.q
k.b = a.(k.q)
x ∈ Z olsun
tanımdan
a|k.b 'dir.

(iv) $a \mid b$ ve $a \mid c$ ise $a \mid sb + ct$ 'dir.

$2 \mid 6$ ve $2 \mid 10$ $\quad s=3,\ t=5$ $\quad \Rightarrow 2 \mid 3.6 + 5.10 = 2 \mid 68$

İspat

(i) $a \mid b \Rightarrow a \mid bs$ tanımdan $\Rightarrow bs = a.t_1$ 'dir.

(i) $a \mid c \Rightarrow a \mid ct$ tanımdan $\Rightarrow ct = a.t_2$ 'dir

$bs + ct = a.(t_1 + t_2)$, $q \in \mathbb{Z}$

$bs + ct = aq$ tanımdan $\Rightarrow a \mid bs + ct$.

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

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

b	q	a	r
$36 =$	3	$.10$	$+6$

Tanım: $a, b, c \in Z^+$ olsun.

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

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

= Öklid Algoritması =

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

$$a = b \cdot q_0 + r_0 \quad , \quad 0 \leq r_0 < b$$

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

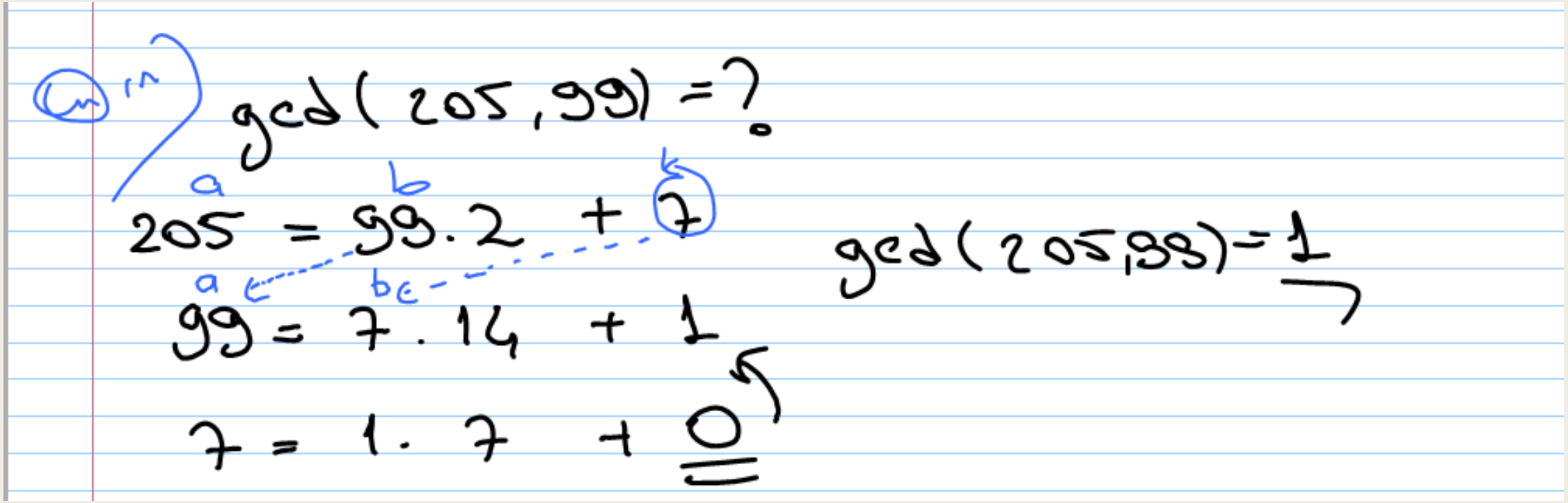
$$r_0 = r_1 \cdot q_2 + r_2 \quad , \quad 0 \leq r_2 < r_1$$

$r_i, q_i \in \mathbb{Z}^+ \cup \{0\}$ olmak zorunda

$$\vdots \qquad \vdots \qquad \vdots \qquad \vdots$$

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

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


gcd(205, 99) = ?
205 = 99 . 2 + 7
99 = 7 . 14 + 1
7 = 1 . 7 + 0
gcd(205, 99) = 1

Öklid algoritmasını kullanarak

gcd(203, 91)'i hesaplayınız.

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

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

$21 = 7 \cdot 3 + \boxed{0}$

$gcd(a,b) = 7$

gcd(a,b)=> greatest common divisor (Ortak bölenlerin en büyüğü - OBEB)

lcm(a,b)=> least common multiple (Ortak katların en küçüğü - OKEK)

Teorem: a ve b iki pozitif tamsayı olmak üzere

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

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

Psedo Kodu

print '2 tamsayı giriniz'

read a,b

a>b

bas2: k ← a

bas1: k ← k - b

if (k>=b) then goto bas1 end if

if (k=0) then print 'obeb = ', b

goto son;

end if

a ← b

b ← k

goto bas2;

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 $x, y \in \mathbb{Z}$ olmak üzere:

$$\boxed{d = ax + by}$$

şeklindeki denklemlere diyafont denklemi denir.

Teorem: $a, b \in \mathbb{Z}^+$ ve $d = \gcd(a, b)$ olmak üzere; d, a ile b'nin lineer kombinasyonu şeklinde gösterilebilir.

yani $d = a.x + b.y$ 'dir.

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

denklemini sağlayan x ve y tamsayılarını bulmak

$$936 = 240 \cdot 3 + 216$$
$$240 = 216 \cdot 1 + 24 \longrightarrow \gcd(240, 936) = 24$$
$$216 = 24 \cdot 9 + 0$$

$24 = 240x + 936y$ 'yi bölgen x ve y değerleri?

$24 = 240 - 216.1$

$= 240 - (936 - 240.3)$

$= 240 - 936 + 240.3$

$= \boxed{4.}240 + \boxed{-17}936$

x y

Örn

$8 = 64x + 202y$ eşitliğini sağlayan x ve y değerlerini Öklid algoritmasını kullanarak hesaplayınız.

$202 = 64.3 + 10$

$64 = 10.6 + 4$

$10 = 4.2 + 2$ $\Rightarrow$

$4 = 2.2 + 0$

$2 = 64x + 202y$

$2 = 10 - 4.2$

$= 10 - (64 - 10.6).2$

$= 10 - 64.2 + 10.12$

$= 13.10 - 64.2$

$= 13.(202 - 64.3) - 64.2$

$= 13.202 - 39.64 - 64.2$

*4/ $2 = 13.202 - 41.64$

$8 = 52.202 - 164.64$

$= 52.202 + (-164).64$

$x = -164$

$y = 52$

y

x

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

Asal Sayılar

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

5 → asal sayı

10 → bileşik "

* 1'den büyük 2 doğal sayının çarpımı şeklinde yazılamayan sayılara asal sayılar denir.
* 1 ne asal, ne bileşik sayıdır.
* 2'de çift sayı dır tek asaldır.

Teorem:

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

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

$50 \Rightarrow \sqrt{50} \approx 7$

2, 3, 5

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

$n = 101$ asal mıdır?

$\sqrt{101} \cong 10$

2 3 5 7

$\frac{101}{2}$ tam bölünmez

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

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

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

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 sayisina 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;
}
```

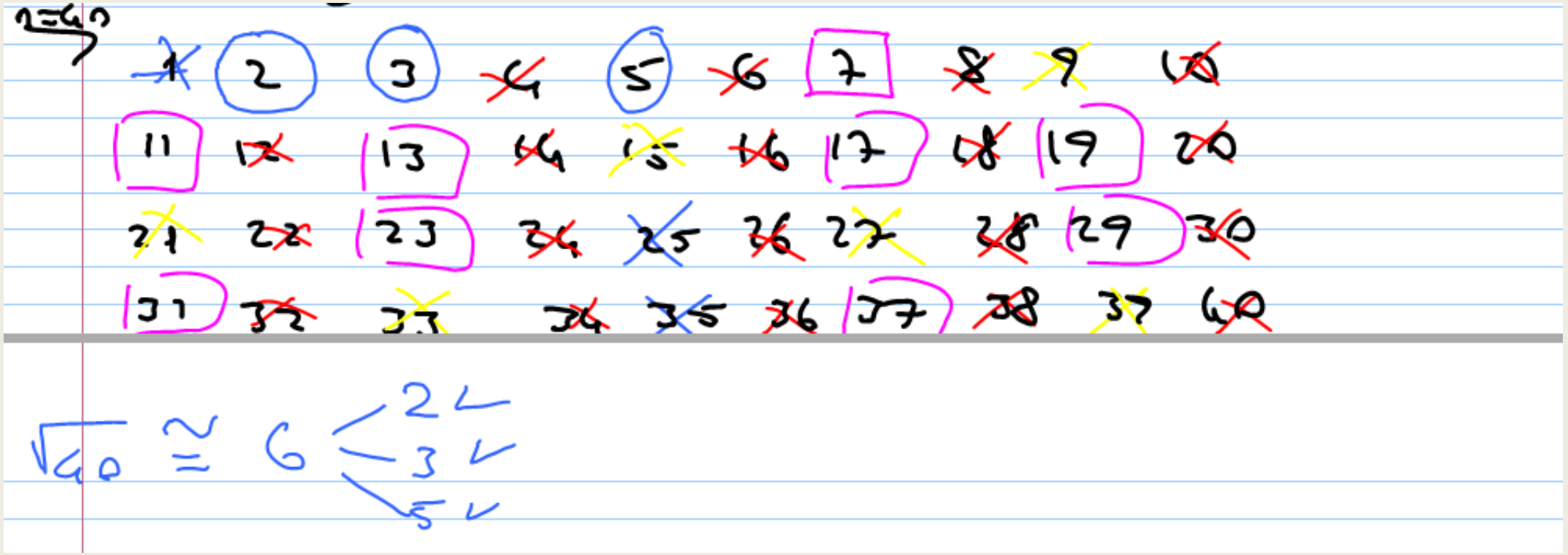
```
x degerini giriniz: 105
2 sayisi asal sayidir, 105 sayisina bolunup bolunmedigi kontrol edilecektir...
3 sayisi asal sayidir, 105 sayisina bolunup bolunmedigi kontrol edilecektir...
5 sayisi asal sayidir, 105 sayisina bolunup bolunmedigi kontrol edilecektir...
7 sayisi asal sayidir, 105 sayisina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

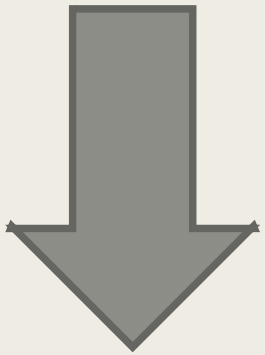
1 den *n* ye kadar olan tüm asal sayıların listelenmesi Eratosthenes Kalburu yardımıyla yapılır.

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 Sayi = %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 tamsayı asal sayıların çarpımı olarak yazılır ve bu yazılış tek türlüdür.

$100 = 25 \cdot 4$

$= 5^2 \cdot 2^2 \quad = 5 \cdot 5 \cdot 2 \cdot 2$

Gelecek Haftanın Konuları:

- **Modüler Aritmetik**

  --- Doğrusal Denklikler

  --- Çinli Kalan Teoremi

  --- Önemli Teoremler (Wilson Teoremi – Fermat Teoremi –Euler Teoremi)

- **Sayılar Teorisinin Kriptolojiye Uygulaması**

Kaynaklar

- *Discrete Mathematics and Its Applications*, Kennet H. Rosen

(Ayrık 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.