CENG 114 BİLGİSAYAR BİLİMLERİ İÇİN AYRIK YAPILAR

Prof. Dr. Tufan TURACI
tturaci@pau.edu.tr

- Pamukkale Üniversitesi
- Mühendislik Fakültesi
- Bilgisayar Mühendisliği Bölümü
- Hafta 12

Ders İçereği

- **Sayılar Teorisi ile İlgili Önemli Teoremler**

  --- Çinli Kalan Teoremi

  --- Wilson Teoremi

  --- Fermat Teoremi

  --- Euler Teoremi

- **Sayılar Teorisinin Kriptolojiye Uygulaması**

Çinli Kalan Teoremi

doğrusal denklik sistemlerini çözmek için bu teorem kullanılır. yani

$$x \equiv 2 \pmod 7$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 5 \pmod 7$$

} denklik sistemi

$x = ?$

Teorem: $m_1, m_2, \ldots, m_r$ ikişer ikişer aralarında asal

pozitif tam sayılar olsun.

$(m_i, m_j) = 1$ ve $i \neq j$ olsun.

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_r \pmod{m_r}$$

denklik sistemi modül

$m = (m_1 \cdot m_2 \cdot \ldots \cdot m_r)$'ye göre bir tek çözüme sahiptir.

Bu çözüm

$$X = \left(\frac{m}{m_1}\right) \cdot a_1 \cdot b_1 + \left(\frac{m}{m_2}\right) \cdot a_2 \cdot b_2 + \ldots + \left(\frac{m}{m_r}\right) \cdot a_r b_r \text{ 'dir.}$$

b_i'ler için:

$\left(\frac{m}{m_i}\right) \cdot b_i \equiv 1 \pmod{m_i}$ formülü kullanılır.

(a)

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 5 \pmod 7$ ise $x = ?$ ($x = 68$ bir çözümdür. Kontrol ediniz...)

$a_1 = 2$ $\quad m_1 = 3$ $\quad M = 3 \cdot 5 \cdot 7 = 105$

$a_2 = 3$ $\quad m_2 = 5$

$a_3 = 5$ $\quad m_3 = 7$

$$x = \left(\frac{105}{3}\right) \cdot 2 \cdot b_1 + \left(\frac{105}{5}\right) \cdot 3 \cdot b_2 + \left(\frac{105}{7}\right) \cdot 5 \cdot b_3$$

$$x = 70 \cdot b_1 + 63 \cdot b_2 + 75 \cdot b_3$$

b_1

$\left(\frac{105}{3}\right) \cdot b_1 \equiv 1 \pmod 3$

$35 \cdot b_1 \equiv 1 \pmod 3$

$\Downarrow$

$b_1 = 2$

b_2

$\left(\frac{105}{5}\right) \cdot b_2 \equiv 1 \pmod 5$

$21 \cdot b_2 \equiv 1 \pmod 5$

$\Downarrow$

$b_2 = 1$

b_3

$\left(\frac{105}{7}\right) \cdot b_3 \equiv 1 \pmod 7$

$15 \cdot b_3 \equiv 1 \pmod 7$

$\Downarrow$

$b_3 = 1$

Böylece;

$$X = 70\,b_1 + 63\,b_2 + 75\,b_3$$

$$= 140 + 63 + 75 = 278$$

$X \Rightarrow 278 \equiv 68 \pmod{105}$

$$x = 68 + 105k$$

$x = 68$

173

278

383

; **elde edilir.**

Örn:

$x \equiv 1 \pmod 5$

$x \equiv 2 \pmod 7$

$x \equiv 3 \pmod{11}$ ise $x = ?$

$m = 5 \cdot 7 \cdot 11 = 385$

$a_1 = 1$ $\quad m_1 = 5$

$a_2 = 2$ $\quad m_2 = 7$

$a_3 = 3$ $\quad m_3 = 11$

$$x = 77 \cdot 1 \cdot b_1 + 55 \cdot 2 \cdot b_2 + 35 \cdot 3 \cdot b_3$$

$b_1 = 3$ $\quad b_2 = 6$ $\quad b_3 = 6$

$$x = 231 + 660 + 630 = 1521$$

$$1521 \equiv 366 \pmod{385}$$

$$x = 366 + 385k$$

$x = 366 \Rightarrow$ pozitif en küçük çözüm 366

75

1136

elde edilir.

Çalışma Sorusu:

Aşağıda verilen doğrusal denklik sistemini sağlayan en küçük pozitif ***x* tamsayı değeri** nedir?

$$x \equiv 4 (\mathrm{mod}\, 5)$$
$$x \equiv 4 (\mathrm{mod}\, 7)$$
$$x \equiv 8 (\mathrm{mod}\, 11)$$

Yanıt: 74

Sayılar Teorisi ile İlgili Önemli Teoremler

Wilson Teoremi

($\Rightarrow$) p asal ise ; $(p-1)! \equiv -1 \pmod{p}$

($\Leftarrow$) Eğer $(p-1)!+1 \equiv 0 \pmod{p}$ ise p asaldır.

Örn) $p=17$ ise $16! \equiv -1 \pmod{17}$

(c) $p=13$ sayısının asal sayı olduğunu wilson teoremi ile gösteriniz.

$12! \equiv -1 \pmod{13}$

$12.11.10.9.8.7.6.5.4.3.2$

$4.10 \equiv 1 \pmod{13}$

$2.7 \equiv 1 \pmod{13}$

$3.9 \equiv 1 \pmod{13}$

$5.8 \equiv 1 \pmod{13}$

$6.11 \equiv 1 \pmod{13}$

$11! \equiv 1 \pmod{13}$

$12.11! \equiv 12 \pmod{13}$

$12! \equiv -1 \pmod{13}$

eşitliğin $p=13$ asaldır.

Fermat Teoremi

p bir asal sayı ve $p \nmid a$ olsun. $a^{p-1} \equiv 1 \pmod{p}$'dir.

Buradan $a^p \equiv a \pmod{p}$ elde edilir.

Örn) $a=3$

$p=5 \Rightarrow$ asal

$5 \nmid 3$ 'tür

$3^{5-1} \equiv 1 \pmod{5}$ $\Rightarrow$ $3^4 \equiv 1 \pmod{5}$

(Ödev) $5^{16} \equiv x \pmod{17}$ ise x'in en küçük 2 tamsayı değerinin toplamı nedir?

Fermat teo.dan $5^{16} \equiv (1) \pmod{17}$

$\overline{1} = 1+17k = \begin{matrix} 1 \\ 18 \\ 35 \\ \vdots \end{matrix}\Big\} \; 1+18 = 19$

Euler ϕ Fonksiyonu ve Euler Teoremi

Tanım: $m > 1$ olmak üzere, $\phi(m)$ gösterimi m'den küçük ve m ile aralarında asal sayıların sayısını verir. $\phi(1) = 1$ olarak tanımlanır. ϕ fonk.'na genellikle Euler ϕ fonk. olarak ifade edilir.

$\Rightarrow$ Her $m > 1$ değeri için $\phi(m) \leq m - 1$ 'dir. Eğer m asal ise $\phi(m) = m - 1$ 'dir.

Örn) $\phi(4) = ?$ 1-4 ✓ 2-4 ✗ 3-4 ✓ $\phi(4) = 2$

$\phi(6) =$ 1-6 ✓ 2-6 ✗ 3-6 ✗ 4-6 ✗ 5-6 ✓ $\phi(6) = 2$

$\phi(7) = 6$ 1-7 ✓ 2-7 ✓ 3-7 ✓ 4-7 ✓ 5-7 ✓ 6-7 ✓ Ardarda asaldır!!

Teorem: m ve n ardarında asal 2 sayı ise $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$ 'dir.

$\phi(6) = \phi(3 \cdot 2) = \phi(3) \cdot \phi(2)$

$= 2 \cdot 1 = 2$

$\phi(15) = ?$ $\phi(3 \cdot 5) = \phi(3) \cdot \phi(5)$

$= 2 \cdot 4 = 8$

Teorem: p asal ise $\phi(p^k) = p^k - p^{k-1}$ 'dir.

$\phi(125) = ?$ $\quad \phi(5^3) = 5^3 - 5^2$

$= 125 - 25 = 100$

Teorem $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_r^{\alpha_r}$ ise

$\phi(m) = \phi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots p_r^{\alpha_r})$ 'dir. $\phi(m)$

Çarpımsal bir fonk. eşl. denir;

$\phi(m) = \phi(p_1^{\alpha_1}) \cdot \phi(p_2^{\alpha_2}) \cdot \cdots \phi(p_r^{\alpha_r})$ 'dir.

(a) $\phi(200) = ?$

$\phi(200) = \phi(2^3 \cdot 5^2) = \phi(2^3) \cdot \phi(5^2)$

$= (2^3 - 2^2) \cdot (5^2 - 5^1)$

$= (8 - 4) \cdot (25 - 5)$

$= 4 \cdot 20 = 80$

$\phi(75) = \phi(3 \cdot 5^2) = \phi(3) \cdot \phi(5^2)$

$= 2 \cdot 5^2 - 5^1$

$= 2 \cdot (25 - 5) = 2 \cdot 20 = 40$

Euler Teoremi: $m \in Z^+$ ve $(m,a)=1$ olsun.

$a^{\phi(m)} \equiv 1 \pmod{m}$ 'dir.

Örn: $m=10$, $a=3$ } $(3,10)=1$

$\phi(10) = \phi(5).\phi(2)$

$4.1=4$

$3^{\phi(10)} \equiv 1 \pmod{10}$

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

Sayılar Teorisi Uygulama
(Şifreleme Uygulamaları)

- Bilginin değiştirilerek korunması ile uğraşan bilim kriptoloji olarak adlandırılır.

- Elektronik ortamda bilginin korunması, yetkisiz kişilerin önlenmesi büyük önem taşır.

- Klasik şifreleme genellikle
  - yerine koyma
  - yer değiştirme

mantığı ile çalışır.

* Bu şifrelemeye örnek olarak Sezar Şifresi (The Caesar cipher) gösterilebilir.

Sezar Şifreleme

Belirlenen bir anahtar değerine göre harflerin yer değiştirmesine dayalı bir şifreleme yöntemidir.

Harfler öncelikle numaralandırılır.

A → 0
B → 1
C → 2
D → 3
i
Z → 25

(İngiliz Alfabesindeki harfler)

Bir harfi şifrelemek için bir f fonksiyonu:

$$f(p) = (p+k) \pmod{26}$$

p, bir harfi temsil eder.

k, kaç birim öteleneceğini temsil eder.

Şifre çözmek için fonksiyon:

$$f^{-1}(p) = (p-k) \pmod{26}$$

şeklindedir.

Örnek: DENIZLI kelimesini Sezar şifreleme ile şifreleyelim.

k=3 alalım

D → 3
E → 4
N → 13
I → 8
Z → 25
L → 11

Tüm dizi: 3, 4, 13, 8, 25, 11, 8

Her sayıyı şifreleme:

$$f(p) = (p + k) \pmod{26}$$

$f(3) = 6$, $f(4) = 7$, $f(13) = 16$
$f(8) = 11$, $f(25) = 2$, $f(11) = 14$ olur.

Şifrelenmiş metin:

6 → G , 7 → H , 16 → Q , 11 → L , 2 → C , 14 → O

Tam sayı dizisi : 6, 7, 16, 11, 2, 14, 11

Şifrelenmiş metin GHQLCOL şeklindedir.

Şifre Çözme:

GHQLCOL ve k = 3.

Sayıya çevir

6, 7, 16, 11, 2, 14, 11

Fonksiyon : $f^{-1}(p) = (p-k) \pmod{26}$

$f^{-1}(6) = 6-3 \pmod{26} = 3$

$f^{-1}(7) = 4$ $\quad f^{-1}(11) = 8$ $\quad f^{-1}(14) = 11$

$f^{-1}(16) = 13$ $\quad f^{-1}(2) = 25$

Tam dizi : 3, 4, 13, 8, 25, 11, 8

metin : DENIZLI

★ Bu tip yöntemler kolaylıkla çözülebilir.

Güvenli bir kripto sistem genellikle Matematiksel açıdan çözümü zor olan NP problemlere dayalı olmalıdır.

RSA kriptosistemi büyük sayıların çarpanlara ayrılmasına dayalı bir yöntemdir.

RSA şifreleme

1977 yılında R.Rivest, A.Shamir ve L.Adleman tarafından geliştirilmiştir.

RSA algoritmasında anahtar üretimi aşağıdaki adımları içermelidir.

1) p ve q şeklinde iki tane büyük asal sayı seçilir.
Büyük asal sayılar seçildiğinde p.q'nun çarpanlara ayrılması zordur.

2) $n = p \cdot q$ ve $\phi = (p-1) \cdot (q-1)$ hesaplanır.

3) $1 < e < \phi$ şeklinde $\gcd(e, \phi) = 1$ olacak şekilde rastgele bir e sayısı alınır.

4) $1 < d < \phi$ aralığında $e \cdot d \equiv 1 \pmod{\phi}$ şartını sağlayan d sayısı hesaplanır.

5) Böylece genel anahtar (n,e) Özel anahtar d elde edilir.

Şifreleme:

1) Mesajın gönderileceği kişinin genel anahtarı (n, e) elde edilir.

2) Şifrelenecek mesaj $[0, n-1]$ aralığında bir m sayısına dönüştürülür.

3) $c = m^e \pmod n$ hesaplanır.

4) Oluşturulan c şifreli mesajı alıcıya gönderilir.

Deşifreleme:

1) d özel anahtarı ile $m = c^d \pmod{n}$ hesaplanır ve orijinal metin elde edilir.

RSA'nın güvenliği:

RSA sistemi n'in çarpanlara ayrılması ile çözülebilir. Bu sayede gizli anahtar bulunabilir.

- n sayısı ne kadar büyükse sistem o kadar güvenlidir.
- $n = p \cdot q$ olduğundan çok büyük iki asal sayı alınırsa sistem güvenli olacaktır.

Örnek: Anahtar üretimi için

$p = 13$

$q = 23$ olsun.

$n = pq = 13 \cdot 23 = 299$ elde edilir.

$\phi = (p-1)(q-1) = 12 \cdot 22 = 264$ olur.

$\gcd(e, \phi) = 1$ olacak şekilde $e = 35$ olsun.

$\gcd(35, 299) = 1$ 'dir.

$35 \cdot d \equiv 1 \pmod{264}$ olacak şekilde

$d = 83$ elde edilir.

$35 \cdot 83 = 2905$

$2905 \equiv 1 \pmod{264}$ sağlanmaktadır.

Genel cevaplar: $(295, 35)$

Özel cevaplar: 83 elde edildi.

Zeka kelimesini RSA ile şifreleyelim.

ASCII kod tablosundan

z → 122

e → 101

k → 107

a → 057

Zeka kelimesi ⟹ 122101107057 şeklinde çözülür.

* Şifrelenecek sayılar n'den küçük olmalıdır.

Bu nedenle sayısal metin n'in basamak sayısının

bir eksik uzunluğundaki parçalara ayrılır.

- Bu sayı Lclear olarak adlandırılır.
- n=299 olduğundan Lclear = 2 elde edilir.

Sayısal metin

Böylece: 12 21 01 10 20 97

şeklinde yazılır.

* Her blok Lclear basamaklı olmak üzere sıfır eklenir.

Gerekiyorsa sıfır eklenir.

Şifreleme:

$$12^{35} \equiv 259 \pmod{299}$$

$$21^{35} \equiv 226 \pmod{299}$$

$$01^{35} \equiv 1 \pmod{299}$$

$$10^{35} \equiv 119 \pmod{299}$$

$$70^{35} \equiv 47 \pmod{299}$$

$$97^{35} \equiv 257 \pmod{299}$$

yeni elde edilen değerler n ile aynı kalacaktır. Bu sayı 2 cipher daha adlandırılır.

2 cipher = 3 elde edilir.

Böylece: 259 226 001 193 047 297 elde edilir.

Sonuç olarak "Zeka" kelimesi için şifreli metin

259226001193047297

şeklindedir.

Deşifreleme:

Şifreli metin L_{cipher} uzunluğu bloklara ayrılır.

255	226	001	195	047	257

$m = c^d \pmod n$ kullanılır.

$259^{83} \pmod{299} = 17$

$226^{83} \pmod{299} = 21$

$001^{83} \pmod{299} = 1$

$195^{83} \pmod{299} = 10$

$047^{83} \pmod{299} = 70$

$257^{83} \pmod{299} = 97$

Bloklar 2 ckar uzunlukta olmalıdır, gerekiyorsa sıfır eklenir.

12 21 01 10 70 97

⇓

12 21 01 10 70 97

⇓

122 101 107 097

" z e k a " elde edilir.

p ve q asal olmalıdır.

Asal olmaması durumunda algoritma çalışmaz.

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.