CENG 114 BİLGİSAYAR BİLİMLERİ İÇİN AYRIK YAPILAR

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

- Pamukkale Üniversitesi
- Mühendislik Fakültesi
- Bilgisayar Mühendisliği Bölümü

- Hafta 11

Ders İçereği

- **Modüler Aritmetik**

--- Doğrusal Denklikler ve Çözümleri

--- Çinli Kalan Teoremi

Modüler Aritmetik

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

$$\underset{a}{64} \equiv \underset{b}{4} \pmod{\underset{m}{10}}$$

$$m \mid a-b \stackrel{?}{=} 10 \mid 64-4$$

$$10 \mid 60 \checkmark$$

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 $a \mp c \equiv b \mp d \pmod{m}$ dir.

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

v) c, a ve b nin bir ortak çarpanı olmak üzere

$$a \equiv b \pmod{m} \iff \frac{a}{c} \equiv \frac{b}{c} \left(\text{mod } \frac{m}{c}\right) \text{ dir.}$$

İspat (iv): $a \equiv b \pmod{m}$ ise $ca \equiv cb \pmod{m}$'dir?

$\Downarrow$

$m \mid a-b$ dir (tanımdan)

$a-b = m \cdot q$ (bölüm tanımından)

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

$ca - cb = m \cdot x \rightarrow$ (bölüm tanımından) $m \mid ca-cb$'dir

$ca \equiv cb \pmod{m}$ 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.

İspat (ii)

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

$$\Downarrow$$

$\Rightarrow m \mid a-b$ 'dir (mod tanımı)

$\Rightarrow a-b = m.q$ 'dir (bölüm teoreminden)

$$\boxed{a = b + mq}$$

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

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

$a^n - b^n = m \cdot \underbrace{[q \cdot x]}_{w \in \mathbb{Z} \text{ dersen}}$, $a^n - b^n = m \cdot w$ olduğundan

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

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

Doğrusal Denklikler

Tanım: $ax \equiv b \pmod{m}$ denkliğinin 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.

Bunu $x \equiv x_1 \pmod{m}$ şeklinde gösterip, $ax \equiv b \pmod{m}$ denkliğinin çözümü diye okuruz.

Örn

$27 \equiv x \pmod 5$ ise $x = ?$

$\parallel$

2

2'nin denklik sınıfı $= \overline{2}$

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

Örn

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

$x=1$ için sağlamaz

$x=2$ " "

$x=3$ " "

$x = \overline{4}$

$$\boxed{x = 4 + 13k}$$

$x=4$ sağlar

$40 \equiv 1 \pmod{13}$

$x = 4$
17
30
43
$\vdots$

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

Örn

$11.x \equiv 28 \pmod{943}$ ise x'in [illegible] ?

Çözümü birazdan yapılacaktır…

Rasyonel sayılarda mod alma işlemi:

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

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

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

2) $\frac{1}{3} \equiv x \pmod{4}$

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

Teorem: $ax \equiv b \pmod{m}$ dekliğinin bir çözümü olması demek $ax - my = b$ diyofant denkleminin bir çözümü olması demektir.

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

Çözüm: $\underset{a}{10}x \equiv \underset{b}{14} \pmod{\underset{m}{24}}$ ise $x=?$

$\boxed{\begin{array}{c} 10x - 24y = 14 \\ 7 \quad\quad 7 \end{array}}$ denkleminin çözümü olması gerekir. → diophant denklem.

$24 = 10 \cdot 2 + 4$

$10 = 4 \cdot 2 + \boxed{2}$

$4 = 2 \cdot 2 + 0$

$2 = 10 - 4 \cdot 2$

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

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

$\underset{obeb}{2} = \underset{x}{5} \cdot \underset{a}{10} - \underset{y}{2} \cdot \underset{m}{24}$

7 ile çarpılır → $\underset{b}{14} = \boxed{\underset{x}{35}} \cdot \underset{a}{10} - \underset{y}{14} \cdot \underset{b}{24}$

bir çözüm.

Böylece;

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

$$\Downarrow$$

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

$x = 11$

$x = 35$

$x = 59$

$x = 83$

$\vdots$

elde edilir.

Örnek: $\underbrace{11}_{a}x \equiv \underbrace{28}_{b} \pmod{\underbrace{1943}_{m}}$ ise $x=?$

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

$1943 = 11.176 + 7$
$11 = 7.1 + 4$
$7 = 4.1 + 3$
$4 = 3.1 + \boxed{1}$ obeb
$3 = 1.3 + 0$

$1 = 4 - 3.1$
$1 = 4 - (7-4)$
$= 4.2 - 7$
$= (11-7).2 - 7$
$= 2.11 - 2.7 - 7$
$= 2.11 - 3.7$
$= 2.11 - 3.(1943 - 11.176)$
$= 2.11 + 528.11 - 3.1943$
$1 = 530.11 - 3.1943$

Her iki taraf 28 ile çarpılırsa:

$$28 = \underbrace{14840}_{x} \cdot 11 - 84 \cdot 1943$$

$x \Rightarrow$ herhangi bir çözüm

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

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

$x = 1239$

$x = 3182$

$\vdots$

elde edilir.

Çalışma Sorusu:

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

Yanıt: 12

Çinli Kalan Teoremi

doğrusal denklik sistemlerini çözmek için bu teorem kullanılır. yani

$$\left.\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 5 \pmod{7} \end{aligned}\right\} \text{ denklik sistemi}$$

$x = ?$

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

Bir çözüm

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

b_i'ler için:

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

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

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

$a_1 = 2 \qquad m_1 = 3 \qquad m = 3 \cdot 5 \cdot 7 = 105$

$a_2 = 3 \qquad m_2 = 5$

$a_3 = 5 \qquad m_3 = 7$

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

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

$\underline{\underline{b_1}}$

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

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

$$\Downarrow$$

$$\boxed{b_1 = 2}$$

$\underline{\underline{b_2}}$

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

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

$$\Downarrow$$

$$b_2 = 1$$

$\underline{\underline{b_3}}$

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

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

$$\Downarrow$$

$$b_3 = 1$$

Böylece;

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

$b_1 = 2 \quad b_2 = 1 \quad b_3 = 1$

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

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

$$\boxed{x = 68 + 105k}$$

$x = 68$

173

278

383

; **elde edilir.**

Örn

$$x \equiv 1 \pmod{5}$$
$$x \equiv 2 \pmod{7}$$
$$x \equiv 3 \pmod{11}$$

ise $x = ?$

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

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

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

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

$$x = 77 \cdot 1 \cdot \underset{3}{b_1} + 55 \cdot 2 \cdot \underset{6}{b_2} + 35 \cdot 3 \cdot \underset{6}{b_3}$$

$$77 \cdot b_1 \equiv 1 \pmod 5 \qquad 55 \cdot b_2 \equiv 1 \pmod 7 \qquad 35 \cdot b_3 \equiv 1 \pmod{11}$$

$$\boxed{b_1 = 3} \qquad \boxed{b_2 = 6} \qquad \boxed{b_3 = 6}$$

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

$$1521 \equiv \underline{\underline{366}} \pmod{385} \qquad \boxed{x = 366 + 385k}$$

$x = 366 \Rightarrow$ pozitif en küçük

751 çözüm $\underline{\underline{366}}$

1136

⋮

elde edilir.

Çalışma Sorusu:

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

$$x \equiv 4 \pmod{5}$$
$$x \equiv 4 \pmod{7}$$
$$x \equiv 8 \pmod{11}$$

Yanıt: 74

Gelecek Haftanın Konuları:

- **Sayılar Teorisi ile İlgili Önemli Teoremler**

  (Wilson Teoremi – Fermat Teoremi –Euler Teoremi)

- **Sayılar Teorisinin Kriptolojiye Uygulaması**

- **Graf Teoriye Giriş**

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.