ONDOKUZ MAYIS ÜNİVERSİTESİ UZAKTAN EĞİTİM MERKEZİ

Ondokuz Mayıs Üniversitesi
Fen Edebiyat Fakültesi
Matematik Bölümü
Dijital Ders Platformu

Temel Kavramlar

Prof. Dr. Şenol EREN

Ders 5

Teorem 2.2.22 (Euler Teoremi) $m \in \mathbb{Z}$ olsun. $(a,m)=1$ olan $\forall a \in \mathbb{Z}$ için $a^{\varphi(m)} \equiv 1 (\bmod m)$ veya $\bar{a}^{\varphi(m)} = \bar{1}$ dir.

Ispat: $\mathbb{Z}_m^*$ kümesini düşünelim. $\bar{a} \in \mathbb{Z}_m^*$ sabit bir asal kalan sınıfını alalım. $\forall \bar{b} \in \mathbb{Z}_m^*$ için $f(\bar{b}) = \bar{a} \odot \bar{b}$ ile $f: \mathbb{Z}_m^* \longrightarrow \mathbb{Z}_m^*$ fonksiyonunu tanımlayalım. $\bar{a} \odot \bar{b} \in \mathbb{Z}_m^*$ (2.2.18) $f(\bar{b}) = f(\bar{c}) \Rightarrow \bar{a} \odot \bar{b} = \bar{a} \odot \bar{c} \Rightarrow \bar{b} = \bar{c}$ olup f 1-1 dir. $\mathbb{Z}_m^* = \{\bar{a}_1, \ldots, \bar{a}_{\varphi(m)}\}$ sonlu olduğundan f aynı zamanda örtendir.

$\bar{a}_1 \odot \bar{a}_2 \cdots \odot \bar{a}_{\varphi(m)} = f(\bar{a}_1) \cdots f(\bar{a}_{\varphi(m)}) = \bar{a}^{\varphi(m)} \cdot \odot \bar{a}_1 \cdots \odot \bar{a}_{\varphi(m)}$ dir. Gerekli kısaltmalar yapılarak $\bar{a}^{\varphi(m)} = \bar{1}$ bulunur.

Sonuç 2.2.23 (Fermat Teoremi) Özel olarak $m=p$ asal tam sayı ise $p \nmid a$ olan $\forall a \in \mathbb{Z}$ için $a^{p-1} \equiv 1 (\bmod p)$ dir.

Örnek 2.2.24 7^{9999} sayısının son üç basamağını bulunuz.

Çözüm: Bir sayının son üç rakamını bulmak için 1000 ile bölümünden elde edilen kalanı bulmak demektir. O halde $7^{9999} \equiv x \pmod{1000}$ bulalım.

$(7, 10^3) = 1$ olduğundan Euler teo. göre

$7^{\varphi(10^3)} \equiv 1 \pmod{10^3}$ dür. $\varphi(10^3) = \varphi(2^3) \cdot \varphi(5^3) = 400$

$7^{400} \equiv 1 \pmod{10^3} \Rightarrow \left(7^{400}\right)^{25} = 7^{10000} \equiv 1 \pmod{10^3}$

$7^{10000} = 1 + 10^3 k = 1001 + (k-1)10^3, \quad k \in \mathbb{Z}$

$1001 = 7 \cdot 143$, $7 \nmid 10^3$ olduğundan $7 \mid k-1$

$7^{9999} = 143 + \frac{k-1}{7} \cdot 10^3 \Rightarrow 7^{9999} \equiv 143 \pmod{1000}$ bulunur.

Tanım 2.2.25 $ax \equiv b \pmod m$ şeklindeki denkleme bir bilinmeyenli lineer kongrüans denir. Bu denklemi sağlayan x tam sayılarının kümesine de kongrüansın çözüm kümesi denir. $ax \equiv b \pmod m$ nin bir çözümü $x_0 \in \mathbb{Z}$ ise $\bar{x}_0 \in \mathbb{Z}_m$ sınıfındaki tüm sayılar da bir çözümdür.

Teorem 2.2.26 $(a,m)=1$ ise $ax \equiv b \pmod m$ nin çözümü var ve $\bmod m$ tek sınıftır.

Teorem 2.2.27 $ax \equiv b \pmod m$ nin bir çözümünün olması için gerek ve yeter şart $(a,m) \mid b$ olmasıdır.

Sonuç 2.2.28 $ax \equiv b \pmod m$ için $d=(a,m) \mid b$ ise bu kongrüansın çözümleri $\bmod m$, d sınıftır.

Örnek 2.2.29 $6x \equiv 9 \pmod{15}$ kongrüansının çözümlerini bulalım. $(6,15)=3 \mid 9$ olduğundan çözüm var. mod 15 çözümleri sayısı 3 tür. $6x \equiv 9 \pmod{13} \Leftrightarrow 2x \equiv 3 \pmod{5} \Leftrightarrow x \equiv 4 \pmod{5}$

$x \in \mathbb{Z}$ olmak üzere $x = 4+5k$ çözümlerdir.

Şimdi çözümleri mod15 kalan sınıflarıyla ifade edelim.

$k = 3t$ için $x = 4 + 15t$

$k = 3t+1$ için $x = 9 + 15t$

$k = 3t+2$ için $x = 14 + 15t$, $t \in \mathbb{Z}$

mod15 çözümler kümesi $\{\bar{4}, \bar{9}, \overline{14}\}$ bulunur.

Uyarı 2.2.30 Bir lineer kongrüansın çözümlerini bulma problemi, $ax \equiv b(\mathrm{mod}\, m)$, $(a,m)=1$ kongrüans denkleminin çözümünü bulma problemine indirgenebilir ve bunun için 3 yol izlenir.

1) $\bar{a}$ nın tersi kolaylıkla bulunabiliyorsa, $\bar{a}^{-1}=\bar{c}$ olmak üzere $x \equiv bc(\mathrm{mod}\, m)$ dir.

2) Verilen denklem diophant denklemine çevrilir; $ax \equiv b(\mathrm{mod}\, m) \Longleftrightarrow ax-my=b$, $x,y \in \mathbb{Z}$. a ve m sayılarına ard arda kalanlı bölme uygulayarak $1=ax'+(-m)y'$ olacak şekilde x', y' bulunur. Her iki yan b ile çarpılarak bir x çözümü veya $\bar{x}$ çözüm sınıfı bulunur.

3) Verilen kongrüans denk kongrüanslara dönüştürülerek mod küçültülür.

Örnek 2.2.31 $28x \equiv 15 \pmod{107}$ kongrüensını çözelim.

$(28,107)=1 \mid 15$ çözüm var.

1 yol: $\overline{28}$ nin mod 107 tersini bulmak kolay değil bu yolu kullanmayalım.

2 yol: $28x \equiv 15 \pmod{107} \Leftrightarrow 28x - 107y = 15, \ \exists x,y \in \mathbb{Z}$

$$107 = 2.28 + 23 \qquad 1 = 3-2 = 3-(5-3) = 2.3-5$$

$$28 = 1.23 + 5 \qquad = 2.(23-4.5)-5 = 2.23-9.5$$

$$23 = 4.5 + 3 \qquad = 11.23-9.28 = 11.(107-3.28)-9.28$$

$$5 = 1.3 + 2 \qquad = 11.107-42.28 \text{ buradan}$$

$$3 = 1.2 + 1 \qquad 15 = (15.11)107 - (15.42).28$$

$$2 = 2.1 + 0 \qquad x = -630 \Rightarrow \overline{x} = \overline{-630} = \overline{12} \text{ bulunur.}$$

$$(-630 + 6.107 = -630 + 642 = 12)$$

3. yol: $28x \equiv 15 \pmod{107} \Leftrightarrow 28x - 107y = 15$

$\Leftrightarrow -107y \equiv 5y \equiv 15 \pmod{28}$

$\Leftrightarrow 5y - 28z = 15$

$\Leftrightarrow 3z \equiv 15 \pmod{5}$

$\Leftrightarrow 3z \equiv 0 \pmod{5}$

$z = 0$ alınırsa $5y - 28z = 15 \Rightarrow y = 3$ bulunur.

$28x - 107y = 15 \Rightarrow x = \dfrac{15 + 321}{28} = 12$ olup

$\bar{x} = \overline{12} \mod 107$ çözüm bulunur.

Teorem 2.2.32 (Çin kalan teoremi) $m_1, \ldots, m_k \in \mathbb{N}^* - \{1\}$, $i \neq j$ için $(m_i, m_j) = 1$ ve $a_1, \ldots, a_k \in \mathbb{Z}$ keyfi tamsayılar olsun. Bu taktirde $x \equiv a_i \pmod{m_i}$ $i = 1, 2, \ldots, k$ olacak şekilde bir $x \in \mathbb{Z}$ vardır. x_1 ve x_2 bu kongrüansı sağlayan iki tam sayı ise $m = m_1 \ldots m_k$ olmak üzere $x_1 \equiv x_2 \pmod{m}$ dir.

İspat: $j = 1, \ldots, k$ için $M_j = \prod_{\substack{i=1 \\ j \neq i}}^{k} m_i$ olsun. $(m_i, M_i) = 1$, $i = 1, \ldots, k$ olduğundan $b_i M_i \equiv 1 \pmod{m_i}$ $b_i \in \mathbb{Z}$, $i = 1, \ldots, k$ vardır.

$c_i = a_i b_i M_i$, $i = 1, \ldots, k$ olmak üzere $x = \sum_{i=1}^{k} c_i$ çözümdür

zira $c_i - a_i = a_i (b_i M_i - 1) \Rightarrow c_i \equiv a_i \pmod{m_i}$ $i = 1, 2, \ldots, k$

$i \neq j$ için $m_i | c_j \Rightarrow c_j \equiv 0 \pmod{m_i}$, $i \neq j$

$x_1 \equiv a_i \pmod{m_i}$ ve $x_2 \equiv a_i \pmod{m_i}$ $i = 1, 2, \ldots, k$ olsun.

$m_i | x_1 - a_i$, $m_i | x_2 - a_i \Rightarrow m_i | x_1 - x_2 \Rightarrow m_1 \ldots m_k = m | x_1 - x_2$ olup $x_1 \equiv x_2 \pmod{m}$ bulunur.

Örnek 2.2.33 $x \equiv 2 \pmod 3$
$x \equiv 3 \pmod 5$
$x \equiv 4 \pmod 7$
kongrüens sisteminin çözümünü bulalım.

$(3,5)=(3,7)=(5,7)=1$ çözüm var.

$M_1 = 35 \quad M_2 = 21 \quad M_3 = 15$

$a_1 = 2 \quad a_2 = 3 \quad a_3 = 4$

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

$c_1 = 140 \quad c_2 = 63 \quad c_3 = 60$

$35 b_1 \equiv 1 \pmod 3$ ise
$2 b_1 \equiv 1 \pmod 3$
$b_1 \equiv 2 \pmod 3$

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

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

$x = 140 + 63 + 60 = 263$

$\bar{x} = \overline{263} = \overline{53}$ bulunur.

ONDOKUZ MAYIS ÜNİVERSİTESİ
UZAKTAN EĞİTİM MERKEZİ

Ondokuz Mayıs Üniversitesi
Fen Edebiyat Fakültesi
Matematik Bölümü
Dijital Ders Platformu

Teşekkürler

Prof. Dr. Şenol EREN

Cebir I

Ders 5