6. BÖLÜM
MODÜLER ARİTMETİK
(KONGRÜANSLAR)

MODÜLER ARİTMETİK KAVRAMI

6.1. Tanım: $a, b, k \in \mathbb{Z}$ ve $p \in \mathbb{Z}^+ - \{1\}$ olmak üzere,

$$a = pk + b, 0 \leq b < p$$

şeklinde olan bir ifade;

$$a \equiv b \pmod{p}$$

biçiminde gösterime modüler aritmetik (kongrüans) denir. Buna göre;

$$a \equiv b \pmod{p}$$
$$p|(a - b)$$
$$a - b = pk, \ k \in \mathbb{Z}$$

şeklindedir.

Örnek: $34 \equiv x \pmod{7}$ ise x'in değerini bulalım.

Çözüm: 34'ün 7'ye bölündüğünde $34 = 7 \cdot 4 + 6$ şeklinde yazılabilir. Bu yazılış,

$$34 \equiv 6 \pmod{7}$$

şeklindedir. Yani $x = 6$ dır.

Örnek: $89 \equiv x \pmod{12}$ ise x'nın değerini bulalım.

Çözüm: 89'un 12'ye bölündüğünde $89 = 12 \cdot 7 + 5$ şeklinde yazılabilir. Bu yazılış,

$$89 \equiv 5 \pmod{12}$$

şeklindedir. Yani $x = 5$ dir.

6.1. Not: Her $a, b \in \mathbb{Z}$ ve $p \in \mathbb{Z}^+ - \{1\}$ olmak üzere $a \equiv b \pmod{p}$ ise,

i) $a - b$ sayısı p ile tam bölünür.

ii) a'nın p ile bölümünden kalan ile b'nin p ile bölümünden kalan aynı sayıdır. Bu durum $\bar{a} = \bar{b}$ biçiminde gösterilir.

iii) $0 \leq a < p$ ise a'nın p ile bölümünden kalan a'dır.

Örnek: $27 \equiv 3 \pmod{p}$ olduğuna göre, p'nin alabileceği değerleri bulalım.

Çözüm: $27 \equiv 3 \pmod{p}$

$p|27 - 3$

$p|24$

olduğundan, p'nin alabileceği değerler 24'ün 3'den büyük pozitif bölenlerin sayısı kadardır. O halde p'nin alabileceği değerlerin kümesi;

$\{4, 6, 8, 12, 24\}$

tür.

Örnek: Bugün günlerden Pazartesi ise, 58 gün sonra hangi güne rast gelir.

Çözüm: Haftanın 7 günü olduğundan modüler 7'ye göre hareket edeceğiz. Yani,

$58 \equiv 2 \pmod{7}$

olup kalan 2'dir. Şu halde bugün Pazartesi olduğundan 2 gün sonra Çarşamba olarak bulunur.

Örnek: $(5 - a) \equiv 3 \pmod{7}$ sağlayan en küçük 2 pozitif a tamsayısının toplamı kaçtır?

Çözüm: $(5 - a) \equiv 3 \pmod{7}$

$(5 - a) - 3 = 7k, k \in \mathbb{Z}$

$2 - a = 7k$

$a = 7k + 2$

olarak bulunur.

$k = 0$ ise $a = 2$

$k = 1$ ise $a = 9$

Buna göre en küçük iki pozitif tamsayının toplamı $2 + 9 = 11$ dir.

Örnek: Bir askeri birlikte 3 günde bir nöbet tutan bir asker, ilk nöbetini Salı günü tuttuğuna göre, 9. nöbetini hangi gün tutar.

Çözüm: 3 günde bir nöbet tutan bir asker ilk nöbetini Salı günü tuttuğuna göre, 9. nöbeti için 8 nöbet kalmıştır. 8. nöbeti $8 \cdot 3 = 24$ gün sonradır. Şu halde,

$$24 \equiv 3 \pmod 7$$

olup Salı gününden 3 gün sonraya gelir. Şu halde 9. nöbet Cuma gününe rast gelir.

KONGRÜANSLARIN ANALİZİ

6.1. Teorem: $a, b, k \in \mathbb{Z}$ ve $p \in \mathbb{Z}^+ - \{1\}$ olmak üzere;

$$a \equiv b \pmod p \text{ ise } a - b \equiv 0 \pmod m$$

dir.

İspat: $a \equiv b \pmod p$

$$a \equiv pk + b$$
$$a - b \equiv pk$$
$$a - b \equiv 0 \pmod p$$

6.2. Teorem: $a, b, k \in \mathbb{Z}$ ve $p \in \mathbb{Z}^+ - \{1\}$ olmak üzere;

$$a \equiv b \pmod p \text{ ise } -b \equiv -a \pmod p$$

dir.

İspat: $a \equiv b \pmod p$

$$a \equiv pk + b$$
$$a - b \equiv pk$$
$$-b - (-a) \equiv pk$$
$$-b \equiv -a \pmod p$$

şeklindedir.

Örnek: $2 - a \equiv 3 \pmod 7$ olduğuna göre, a'nın alabileceği en büyük negatif tamsayı ile en küçük pozitif tamsayının toplamı kaçtır?

Çözüm: $2 - a \equiv 3 \pmod 7$

$$2 - a - 3 \equiv 0 \pmod 7$$
$$-1 \equiv a \pmod 7$$

dir. O halde, a'nın alabileceği değerler kümesi,

$$\bar{6} = \{\cdots, -15, -8, -1, 6, 13, 20, 27, \cdots\}$$

olur. O halde istenen sonuçlar; $a = -1$ ve $a = 6$ olacağından $-1 + 6 = 5$ dir.

6.3. Teorem: $a, b, c, k \in \mathbb{Z}$ ve $p \in \mathbb{Z}^+ - \{1\}$, $a \equiv b \pmod p$ olmak üzere,
i) $a \pm c \equiv b \pm c \pmod p$
ii) $c \cdot a \equiv c \cdot b \pmod m$
dir.

İspat:
i) $a \equiv b \pmod p$
$a - b = pk$
$(a \pm c) - (b \pm c) = pk$
$a \pm c \equiv b \pm c \pmod p$

ii) $a \equiv b \pmod p$
$a - b = pk$
$c(a - b) = cpk$
$c \cdot a - c \cdot b = p(ck)$
$c \cdot a \equiv c \cdot b \pmod p$

6.4. Teorem: Her $a, b, c, d \in \mathbb{Z}$ ve $p \in \mathbb{Z}^+ - \{1\}$ olmak üzere;
$a \equiv b \pmod p$ ve $c \equiv d \pmod p$
olmak üzere,
i) $a \pm c \equiv b \pm d \pmod p$
ii) $a \cdot c \equiv b \cdot d \pmod p$
dir.

İspat:
1. $a \equiv b \pmod p$ ve $c \equiv d \pmod p$
$a - b = pk$ ve $c - d = p\ell, \quad k, \ell \in \mathbb{Z}$
$(a - b) \pm (c - d) = pk \pm p\ell$
$(a \pm c) - (b \pm d) = p(\underbrace{k \pm \ell}_{\in \mathbb{Z}})$
$a \pm c \equiv b \pm d \pmod p$

2. $a \equiv b \pmod p$ ve $c \equiv d \pmod p$
$a - b = pk$ ve $c - d = p\ell, \quad k, \ell \in \mathbb{Z}$
$a = pk + b$ ve $c = p\ell + d$
$ac = (pk + b)(p\ell + d)$
$ac = p^2k\ell + pkd + pb\ell + bd$
$ac = p(pk\ell + kd + b\ell) + bd, \quad (pk\ell + kd + b\ell) = r \in \mathbb{Z})$
$ac - bd = pr$
$ac \equiv bd \pmod p$

6.5. Teorem: Her $a, b, k \in \mathbb{Z}$ ve $p \in \mathbb{Z}^+ - \{1\}$ olmak üzere;

$a \equiv b \pmod{p}$ ve $c \equiv d \pmod{p}$

ise

i) $OBEB(a; b; p) = k$ ise $\frac{a}{k} \equiv \frac{b}{k} \left(\mod \frac{p}{k}\right)$, $(k \neq 0)$

ii) $OBEB(a; b) = k, OBEB(a; p) = OBEB(b; p) = 1$ ise $\frac{a}{k} \equiv \frac{b}{k} \pmod{k}$

dir.

İspat:

i) $a \equiv b \pmod{p}$

$a - b = p\ell, \ell \in \mathbb{Z}$

$\frac{a-b}{k} = \frac{p\ell}{k}$, $(k \neq 0)$

$\frac{a}{k} - \frac{b}{k} = \frac{p\ell}{k}$

$\frac{a}{k} \equiv \frac{b}{k} \left(\mod \frac{p}{k}\right)$

ii) i. özelliğe benzer şekilde yapılır.

6.1. Sonuç: Her $a, b \in \mathbb{Z}$ ve $p \in \mathbb{Z}^+ - \{1\}$ için $ac \equiv bc \pmod{p}$ ise p, $p \nmid c$ olan bir asal sayı ise $a \equiv b \pmod{p}$ dir.

6.6. Teorem: Her $a, b \in \mathbb{Z}$ ve $p \in \mathbb{Z}^+ - \{1\}$ için

$a \equiv b \pmod{p}$ ise $a^n \equiv b^n \pmod{p}$

dir.

İspat: Bu teoremin ispatını tümevarım yöntemi ile yapacağız.

$P(1)$ için $a \equiv b \pmod{p}$ ise $a \equiv b \pmod{p}$ olup doğrudur.

P(k) için $a^k \equiv b^k \pmod p$ ise $a \equiv b \pmod p$ ve $a^k \equiv b^k \pmod p$ olur. Bu iki eşitlik taraf tarafa çarpılırsa,

$$a^{k+1} \equiv b^{k+1} \pmod p, \qquad \text{(6.3. teorem ii'den)}$$

olup doğrudur. Bu ise istenendir.

Örnek: $2a - 1 \equiv 5 \pmod 8$ denklemini sağlayan a tamsayının en büyük negatif değeri ile en küçük pozitif değerinin toplamını bulalım.

Çözüm: $2a - 1 \equiv 5 \pmod 8$

$2a \equiv 6 \pmod 8$

$a \equiv 3 \pmod 4$

$a_1 \equiv 3 \pmod 4$ ve $a_2 \equiv -1 \pmod 4$

$a_1 + a_2 = 3 + (-1) = 2$

Örnek: 24^{30} sayısının 6 ile bölümünden kalan kaçtır?

Çözüm: $24 \equiv 0 \pmod 6$

$24^{30} \equiv 0^{30} \pmod 6 \equiv 0 \pmod 6$

Örnek: 42^{35} sayısının 5 ile bölümünden kalan kaçtır?

Çözüm: $42^{35} \equiv 2 \pmod 5$

$42^2 \equiv 2^2 \pmod 5 \equiv 4 \pmod 5$

$42^3 \equiv 2^3 \pmod 5 \equiv 3 \pmod 5$

$42^4 \equiv 2^4 \pmod 5 \equiv 1 \pmod 5$

42'nin kuvveti 4 veya 4'ün katı ise, 1 kalanını verir. 4 sayısına modülü 5'e göre işlemin periyodu denir. 35 sayısının 4 periyoduna göre,

$$35 = 4 \cdot 8 + 3$$

olacağından

$(42^4)^8 \equiv 1^8 \pmod 5$ ve $42^3 \equiv 3 \pmod 5$

$42^{32} \equiv 1 \pmod 5$ ve $42^3 \equiv 3 \pmod 5$

$42^{32}42^3 \equiv 1 \cdot 3 \pmod 5$

$42^{35} \equiv 3 \pmod 5$

bulunur.

Örnek: $37^{44} + 38^{44}$ sayısının 6 ile bölümünden kalan kaçtır?

Çözüm: $37 \equiv 1 \pmod 6$

$37^{44} \equiv 1^{44} \pmod 6 \equiv 1 \pmod 6$ (1)

ve

$$38 \equiv 2 \pmod 6$$
$$38^2 \equiv 2^2 \pmod 6 \equiv 4 \pmod 6$$
$$38^3 \equiv 2^3 \pmod 6 \equiv 2 \pmod 6$$

öyleyse 38'in modülü 6'ya göre periyodu 2'dir. Buna göre tek kuvvetlerde 2, çift kuvvetlerde 4 kalanını verir. Şu halde,

$$(38^2)^{22} \equiv (2^2)^{22} \pmod 6 \equiv 4 \pmod 6 \qquad (2)$$

dir. (1) ve (2) eşitliğinden

$$37^{44} + 38^{44} \equiv 1 + 4 \pmod 6 \equiv 5 \pmod 6$$

bulunur.

Örnek: $(-11)^{44} \equiv a \pmod 7$ ise a kaçtır?

Çözüm: $\mathbb{Z}_7$ de $\overline{3} = \{\cdots, -11, -4, 3, 10, 17, \cdots\}$ olduğundan

$$-11 \equiv 3 \pmod 7$$
$$(-11)^2 \equiv 3^2 \pmod 7 \equiv 2 \pmod 7$$
$$(-11)^3 \equiv 3^3 \pmod 7 \equiv 6 \pmod 7$$
$$(-11)^4 \equiv 3^4 \pmod 7 \equiv 4 \pmod 7$$
$$(-11)^5 \equiv 3^5 \pmod 7 \equiv 5 \pmod 7$$
$$(-11)^6 \equiv 3^6 \pmod 7 \equiv 1 \pmod 7$$

bulunur. Buna göre –11 sayısının modülü 7 ye göre periyodu 6'dır. Ayrıca,

$$44 = 7 \cdot 6 + 2$$

olup

$$((-11)^6)^7 \equiv 1^7 \pmod 7 \text{ ve } (-11)^2 \equiv 2 \pmod 7$$
$$(-11)^{42} \equiv 1 \pmod 7 \text{ ve } (-11)^2 \equiv 2 \pmod 7$$
$$(-11)^{42}(-11)^2 \equiv 1 \cdot 2 \pmod 7$$
$$(-11)^{44} \equiv 2 \pmod 7$$

bulunur.

Örnek: 18^{70} sayısının birler basamağındaki rakam kaçtır?

Çözüm: Bir sayının birler basamağındaki rakamı bulmak için modülü 10'a bakmalıyız.

$$18 \equiv 8 \pmod{10}$$
$$18^2 \equiv 8^4 \pmod{10} \equiv 4 \pmod{10}$$
$$18^3 \equiv 8^2 \pmod{10} \equiv 2 \pmod{10}$$
$$18^4 \equiv 8^4 \pmod{10} \equiv 6 \pmod{10}$$
$$18^5 \equiv 8^5 \pmod{10} \equiv 8 \pmod{10}$$

Görüldüğü gibi kalanlar {8, 4, 2, 6} periyoduna göre hareket etmektedir. $70 = 4 \cdot 17 + 2$ olduğundan

$$(18)^{70} \equiv (18)^2 \equiv 2 \pmod 7$$

elde edilir.

Örnek: x tamsayısının 8 ile bölümünden kalan 3, y tamsayısının 8 ile bölümünden kalan 5 ise x^3y^4 sayısının 8 ile bölümünden kalan kaçtır?

Çözüm: $x \equiv 3 \pmod 8$

$$x^2 \equiv 3^2 \pmod 8 \equiv 1 \pmod 8$$

$$x^3 \equiv 3^3 \pmod 8 \equiv 3 \pmod 8 \quad (1)$$

ve

$$y \equiv 5 \pmod 8$$

$$y^2 \equiv 5^2 \pmod 8 \equiv 1 \pmod 8$$

$$(y^2)^2 = y^4 \equiv 1^2 \pmod 8 \equiv 1 \pmod 8 \quad (2)$$

(1) ve (2) eşitliklerini taraf tarafa çarparsak,

$$x^3y^4 \equiv 3 \cdot 1 \pmod 8 \equiv 3 \pmod 8$$

bulunur. O halde x^3y^4 sayısını 8 ile bölümünden kalan 3'dür.

Örnek: $1! + 2! + 3! + 4! + 5! + \cdots + 100!$ sayısının birler basamağındaki rakamı bulalım.

Çözüm: $1! = 1,\ 2! = 2,\ 3! = 6,\ 4! = 24,\ 5! = 120$ olup 5!'den sonraki sayılar 10'un katıdır. Şu halde,

$$5! + \cdots + 100! \equiv 0 \pmod{10}$$

$$1! + 2! + 3! + 4! = 33$$

$$33 \equiv 3 \pmod{10}$$

olduğundan

$$1! + 2! + 3! + 4! + 5! + \cdots + 100! \equiv 3 \pmod{10}$$

bulunur.

6.7. Teorem: $\text{OKEK}(p_1, p_2) = p$ ise

$a \equiv b \pmod{p_1}$ ve $a \equiv b \pmod{p_2}$ ise $a \equiv b \pmod p$

dir.

İspat: $a \equiv b \pmod{p_1}$ ve $a \equiv b \pmod{p_2}$

$$a - b = p_1 k \text{ ve } a - b = p_2 \ell, \quad k, \ell \in \mathbb{Z}$$

bu iki eşitlikten $p_1 k = p_2 \ell$ dir. Öte yandan $\text{OKEK}(p_1, p_2) = p$ olduğundan $p \mid p_1$ ve $p \mid p_2$ olduğundan $a - b = pt, t \in \mathbb{Z}$ olacak şekilde yazılabilir. O halde

$$a \equiv b \pmod{p}$$

dir.

6.8. Teorem: Eğer $a_1, a_2, \cdots, a_n$ sayıları mod p'ye göre kalan sistemi, $k, b \in \mathbb{Z}$ ve $OBEB(k, p) = 1$ ise

$$ka_1 + b, ka_2 + b, \cdots, ka_n + b$$

de mod p bir kalan sistemidir.

İspat:

1. Eğer $ka_i + b \equiv ka_j + b \pmod{p}$ ise $ka_i \equiv ka_j \pmod{p}$ ve $OBEB(k, p) = 1$ olduğundan 6.1. Sonucuna göre $a_i \equiv a_j \pmod{p}$ dir. $a_1, a_2, \cdots, a_n$ mod p bir kalan sistemi olduğundan $i = j$ olur.

2. $OBEB(k, m) = 1$ ise herhangi bir $a \in \mathbb{Z}$ için $kx \equiv a - b \pmod{p}$ kongrüansının x_0 gibi bir çözümü vardır. $a_1, a_2, \cdots, a_n$ mod p bir kalan sistemi olduğundan $x_0 \equiv a_i \pmod{p}$ olacak sekilde $1 \leq i \leq n$ olan bir i indisi vardır. Buna göre $kx_0 \equiv ka_i \equiv a - b \pmod{p}$ ve böylece $kx_i + b \equiv a \pmod{p}$ bulunur.

FERMAT ve WİLSON TEOREMLERİ

6.9. Teorem (Fetmat'ın Küçük Teoremi)[1]: p asal sayı olmak üzere $OBEB(a, p) = 1$ ise;

$$a^{p-1} \equiv 1 \pmod{p}$$

dir. Bu teoremin tersi doğru değildir. (Fakat a'nın p–1'den daha küçük kuvvetleri için de denklik 1'e eşit olabilir.)

İspat: p asal a ise ona bölünmeyen bir sayıdır. $a, 2a, 3a, \cdots, (p-1)a$ sayılarına bakalım bunlardan herhangi ikisi p modunda denk olamazlar, olsalardı farkları p ile bölünürdü ki bu p'nin asal olması ve $OBEB(a, p) = 1$ olmasıyla çelişirdi. Öyleyse bu sayılar p modunda farklı kalanlara denk gelmelidir. Yani tüm bir kalanlar sınıfını (0 hariç) oluşturur. Bunları çarpımları da p modundaki sıfır hariç kalanların çarpımına eşit olmalıdır. Buna göre,

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1.2.3 \cdots (p-1) \pmod{p}$$
$$a^{p-1}(p-1)! \equiv 1 \cdot (p-1)! \pmod{p}$$
$$a^{p-1} \equiv 1 \pmod{p}$$

elde edilir.

[1] Pierre de Fermat'ın öne sürdüğü bu teoremi, 1734 yılında Leonhard Euler ispatlamıştır.

Örnek: OBEB$(2;7)=1$ olduğundan $2^6\equiv 1\ (\text{mod } 7)$ dir.

Örnek: 2^{135} sayısının 13 ile bölümünden kalanı bulalım.

Çözüm: OBEB$(2;13)=1$ olduğundan $2^{12}\equiv 1\ (\text{mod } 13)$ tür. O halde 2 sayısının 13'ün modülü 12'dir. Buna göre;

$$135=12\cdot 11+4$$
$$(2^{12})^{11}\equiv 1^{11}(\text{mod } 13) \text{ ve } 2^4\equiv 3\ (\text{mod } 13)$$
$$(2^{12})^{11}2^4\equiv 1\cdot 3\ (\text{mod } 13)$$
$$2^{135}\equiv 3(\text{mod } 13)$$

bulunur.

6.2. Sonuç: Eğer p bir asal sayı ise herhangi bir p sayısı için

$$a^p\equiv a\ (\text{mod } p)$$

dir. //

Küçük Fermat teoremini aşağıdaki biçimde kullanmak işlemlere kolaylık sağlar;

1. Fermat Teoremi, verilen bir modüle göre yapılan hesaplamalardaki işlemleri kolaylaştırmada kullanılabilir.

Örnek: 40^{235} yı mod 79'a göre hesaplayalım: $p=79$ asal, $79\nmid 40$ olduğundan Fermat teoremine göre $40^{78}\equiv 1\ (\text{mod } 79)$ dir. Buna göre

$$40^{235}=(40^{78})^3\cdot 40=1\cdot 40\equiv 40\ (\text{mod } 79)$$

elde edilir.

2. Verilen bir sayısının asal olup olmadığını belirlemede kullanılır.

Örnek: $a\in\mathbb{Z}$ olmak üzere, $a^p\equiv a\ (\text{mod } p)$ kongrüansı, a'nın bazı değerleri için sağlanmıyorsa p asal olamaz. Bu yöntemi $p=247$ için $a=2$ seçerek deneyelim:

$$2^{247}=(2^8)^{30}\cdot 2^7=256^{30}\cdot 2^7\equiv 9^{30}\cdot 2^7\ (\text{mod } 247)$$
$$9^{30}\cdot 2^7=(3^5)^{12}\cdot 2^7=243^{12}\cdot 2^7\equiv(-4)^{12}\cdot 2^7\ (\text{mod } 247)$$

$(-4)^{12} \cdot 2^7 = (2^8)^3 \cdot 2^7 = 256^3 \cdot 2^7 \equiv 9^3 \cdot 2^7 \pmod{247}$
$9^3 \cdot 2^7 = 3 \cdot 3^5 \cdot 2^7 = 3 \cdot 243 \cdot 2^7 \equiv 3 \cdot (-4) \cdot 2^7 \pmod{247}$
$3 \cdot (-4) \cdot 2^7 = -3 \cdot 2^8 \cdot 2 = -6 \cdot 256 \equiv -6 \cdot 9 \pmod{247}$
$-6 \cdot 9 \pmod{247} \not\equiv 2 \pmod{247}$
olduğuna göre 247 sayısı asal değildir.

6.10. Teorem: Eğer p_1 ve p_2, $a^{p_1} \equiv a \pmod{p_1}$ ve $a^{p_2} \equiv a \pmod{p_2}$ şartını sağlayan asal sayılar ise

$$a^{p_1 p_2} \equiv a \pmod{p_1 p_2}$$

dir.

İspat: 6.2. Sonucuna göre $(a^{p_2})^{p_1} \equiv a^{p_2} \pmod{p_1}$ dir. Öte yandan hipoteze göre $a^{p_2} \equiv a \pmod{p_2}$ olduğundan $(a^{p_2})^{p_1} \equiv a \pmod{p_1}$ ve böylece $p_1 \mid (a^{p_1 p_2} - a)$ elde edilir. Benzer şekilde $p_2 \mid (a^{p_1 p_2} - a)$ olduğu gösterilir. $OBEB(p_1; p_2) = 1$ olduğundan $p_1 p_2 \mid (a^{p_1 p_2} - a)$, yani

$$a^{p_1 p_2} \equiv a \pmod{p_1 p_2}$$

dir.

Örnek: Bu teoremi kullanarak $3^{90} \equiv 1 \pmod{90}$ olduğunu bulunuz.

Çözüm: $91 = 7 \cdot 13$
$3^7 = 3 \cdot (3^2)^3 \equiv 3 \cdot (-4)^3 \pmod{13}$
$3 \cdot (-4)^3 = 3 \cdot (-2^6) = -3 \cdot 64 \equiv -3 \cdot 12 \pmod{13}$
$-3 \cdot 12 = -36 \equiv 3 \pmod{13}$
ve
$3^{13} = 3 \cdot (3^2)^6 \equiv 3 \cdot 2^6 \pmod{7}$
$3 \cdot 2^6 = 3 \cdot 64 \equiv 3 \cdot 1 \pmod{7}$
den 6.10. teoreme göre;
$3^{91} \equiv 3 \pmod{91}$
$3^{90} \equiv 1 \pmod{91}$, $(OBEB(3; 91) \equiv 1)$
bulunur. Bu durum aynı zamanda Fermat teoreminin karşıtının doğru olmadığını gösterir.

Robert Daniel Carmichael
01 Mart 1879-02 Mayıs 1967

6.2. Tanım: p bileşik bir tamsayı olmak üzere, eğer OBEB(x; m) = 1 olan bir a tamsayısı için $a^{p-1} \equiv 1 \pmod{p}$ oluyorsa p sayısına **Carmichael sayı** denir. Carmichael sayı asal olmayabilir.

Örnek: 341 sayısının 2 tabanına göre Carmichael sayı olduğunu gösteriniz.

Çözüm: $341 = 11 \cdot 31$ ve
$2^{11} = 2 \cdot (2^5)^2 \equiv 2 \pmod{31}$ ve $2^{31} = 2 \cdot (2^{10})^3 \equiv 2 \pmod{11}$
olduğundan 6.10. teoreme göre
$2^{341} \equiv 2 \pmod{31}$ ise $2^{31} = 2 \cdot (2^{10})^3 \equiv 2 \pmod{11}$
bulunur.

2 tabanına göre en küçük Carmichael sayı 341, 3 tabanına göre en küçük Carmichael sayı ise 91 dir.

Örnek: $561 = 3 \cdot 11 \cdot 17$ olsun. Eğer $3 \nmid a, 11 \nmid a, 17 \nmid a$ ise Fermat Teoremine göre
$a^2 \equiv 1 \pmod{3}$, $a^{10} \equiv 1 \pmod{11}$, $a^{16} \equiv 1 \pmod{17}$
dir. Buna göre
$a^{560} = (a^2)^{280} \equiv 1 \pmod{3}$, $a^{560} = (a^{10})^{56} \equiv 1 \pmod{11}$,
$a^{560} = (a^{16})^{35} \equiv 1 \pmod{17}$ ve böylece $a^{560} \equiv 1 \pmod{561}$ bulunur. O halde 561 sayısı bir Carmichael sayısıdır. Bu sayı aynı zamanda bu şekildeki sayıların en küçüğüdür.

6.11. Teorem: Her $a > 1$ tamsayısı için sonsuz sayıda Carmichael sayısı vardır.

İspat: $p > 2$, $p \nmid a(a^2-1)$ olan bir asal sayı olsun.

$$n = \frac{a^{2p}-1}{a^2-1}$$
$$= \left(\frac{a^p-1}{a-1} \cdot \frac{a^p+1}{a+1}\right)$$
$$= (a^{p-1} + a^{p-2} + \cdots + 1)(a^{p-1} - a^{p-2} + a^{p-3} - \cdots + 1) \in \mathbb{Z}$$

ve çarpanlardan her biri 1'den büyük bir tamsayıdır. O halde n sayısı bir bileşik sayıdır.

$$(a^2-1)(n-1) = a^{p-1} - a^2 = a(a^{p-1}-1)(a^p+a)$$

Ayrıca p–1 çift olduğu için $(a^2-1) \mid (a^{p-1}-1)$, Fermat teoemine göre $p \mid (a^{p-1}-1)$ ve böylece $p \nmid (a^2-1)$ olduğundan $p(a^2-1) \mid (a^{p-1}-1)$ elde edilir. Diğer taraftan a ve a^p nin ikisi birden tek veya ikisi birden çifttir, ohalde $2 \mid (a^p+a)$ dir. Sonuç olarak $2p(a^2-1) \mid (a^2-1)(n-1)$ ve buradan da $2p \mid (n-1)$ bulunur. O halde $n = 1 + 2pt, t \in \mathbb{Z}$ dir.

$$a^{2p} = (a^2-1)n + 1 \equiv 1 \pmod{n}$$

buna göre

$$a^{n-1} = a^{2pt} \equiv 1 \pmod{n}$$

olur.

6.1. Lemma: Eğer $p > 2$ olan bir asal sayı ise

$$a^2 \equiv 1 \pmod{p}$$

şartını sağlayan a tamsayıları, mod p ye göre, sadece $a = 1$ veya $a = p-1$ dir.

İspat: $a = 1$ bu kongrüansın bir çözümüdür.

$a \not\equiv 1 \pmod{p}$, $a^2 \equiv 1 \pmod{p}$

kongrüansının başka bir çözümü ise

$$a^2 - 1 \equiv 0 \pmod{p}$$
$$(a-1)(a+1) \equiv 0 \pmod{p}$$
$$p \mid (a-1)(a+1)$$

dir. p asal olduğundan ya $p \mid (a-1)$ ya da $p \mid (a+1)$ dir. $a \not\equiv 1 \pmod{p}$ olduğundan $p \mid (a+1)$ dir. Şu halde $a \equiv -1 \equiv p-1 \pmod{p}$ bulunur.

John Wilson
06 Ağustos 1741, Westmorland - 18 Ekim 1793, Westmorland, İngiltere

6.12. Teorem (Wilson Teoremi): Eğer p bir asal sayı ise

$$(p-1)! \equiv -1 \pmod{p}$$

dir.

İspat: $p = 2$ için $1! = 1 \equiv -1 \pmod 2$

$p = 3$ için $2! = 2 \equiv -1 \pmod 3$

dir. $p > 3$ için ve a sayısı $1 \leq a \leq p-1$ olan herhangi bir tamsayı olak üzere,

$$ax \equiv 1 \pmod{p}$$

kongrüansını göz önüne alalım. $OBEB(a;p) = 1$ olduğundan bu kongrüansın mod p ye göre tek çözümü vardır. O halde $aa' \equiv 1 \pmod p$ olacak şekilde $1 \leq a' \leq p-1$ olan bir $a' \in \mathbb{Z}$ vardır.

6.1. Lemma ya göre $a = a'$ ise $a = 1$ veya $a = p-1$ dır. Eğer $a \neq 1$ ve $a \neq p-1$ ise $ax \equiv 1 \pmod p$ kongrüansının çözümü olan a', a sayısından farklıdır. Şimdi $2, 3, 4, \cdots, p-2$ sayılarını $a \neq a'$ ve $aa' \equiv 1 \pmod p$ olan çiftlere ayıralım. Bu şekildeki $(p-3)/2$ tane kongrüans taraf tarafa çarpılır ve çarpanlar uygun bir şekilde düzenlenirse

$$2 \cdot 3 \cdot 4 \cdots (p-2) \equiv 1 \pmod p$$

$$(p-2)! \equiv 1 \pmod p$$

bulunur. Bu kongrüansın her iki tarafı $(p-1)$ ile çarpılırsa

$$(p-1)! \equiv -1 \pmod p$$

elde edilir.

Tersine; $(p-1)! \equiv -1 \pmod p$ ise p asal olduğunu gösterelim:

$(p-1)! \equiv -1 \pmod p$ olsun. Eğer p asal değilse $1 < k < p$ olan k gibi bir böleni vardır. Bundan başka $k \leq p-1$ olduğundan $k \mid (p-1)!$ dir. Öte yandan $(p-1)! \equiv -1 \pmod p$ den $p \mid (p-1)! + 1$ ise $k \mid (p-1)! + 1$ dir. Bunun sonucu olarak $k \mid 1$ bulunur. Bu ise $k > 1$ olması ile çelisir. O halde p asal sayıdır.

Örnek: 16! Sayısının 17 ile bölümünden kalan kaçtır?

Çözüm: Wilson teorem gereği 16! Sayısının 17 ile bölümünden kalan -1'dir.

6.13. Teorem: Eğer $p > 2$ olan bir asal sayı ise

$$a^2 \equiv -1 \pmod p$$

kongrüansının çözümlü olması ancak ve yalnız $p \equiv 1 \pmod 4$ olması ile mümkündür.

İspat:

1. a, $a^2 \equiv -1 \pmod p$ kongrüansının bir çözümü olsun. $a^2 \equiv -1 \pmod p$, $p \nmid a$ olduğundan Fermat Teoremine göre

$$1 \equiv a^{p-1} \equiv (a^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2} \pmod p$$

dir. Eğer $p = 4k+3, k \in \mathbb{Z}$ olsa $1 \equiv -1 \pmod p$ bulunur bu ise $p > 2$ olması ile çelişir. O halde $p \equiv 1 \pmod 4$ olur.

2. Tersine $p \equiv 1 \pmod 4$ olsun. $\frac{p-1}{2}$ çift buna göre

$$(p-1)! = 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-2)(p-1)$$

şeklinde yazılabilir.

$$(p-1)! = -1, p-2 \equiv -2, \cdots, \frac{p+1}{2} \equiv -\frac{p-1}{2} \pmod p$$

olduğu göz önüne alınır ve çarpanların sırası yeniden düzenlenirse

$$(p-1)! = (-1)^{\frac{p-1}{2}} \left(1 \cdot 2 \cdots \left(\frac{p-1}{2}\right)^2\right) \equiv \left(1 \cdot 2 \cdots \left(\frac{p-1}{2}\right)^2\right) \pmod p$$

bulunur. Ayrıca Wilson Teoremine göre $(p-1) \equiv -1 \pmod p$, sonuç olarak $\left(\frac{p-1}{2}!\right)^2 \equiv -1 \pmod p$ yani $\frac{p-1}{2}!$ sayısı $x^2 \equiv -1 \pmod p$ kongrüansının bir çözümüdür.

6.14. Teorem: Eğer $p > 2$ olan bir asal sayı ise

$$1^2 \cdot 3^2 \cdot 5^2 \cdots (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod p$$

dir.

İspat: $a \equiv -(p-a) \pmod p$ yazılabilir. Buna göre

$$2 \cdot 4 \cdot 6 \cdots (p-1) \equiv (-1)^{(p-1)/2}(p-2)(p-4) \cdots 5 \cdot 3 \cdot 1 \pmod p$$

$$\begin{aligned} 1 \cdot 2 \cdot 3 \cdots (p-1) &\equiv (1 \cdot 3 \cdot 5 \cdots (p-2))(2 \cdot 4 \cdot 6 \cdots (p-1)) \\ &\equiv (-1)^{(p-1)/2} 1^2 \cdot 3^2 \cdot 5^2 \cdots (p-2)^2 \pmod p \end{aligned}$$

Wilson Teoremine göre $(p-1)! \equiv -1 \pmod p$, sonuç olarak

$$(-1)^{(p-1)/2} 1^2 \cdot 3^2 \cdot 5^2 \cdots (p-2)^2 \pmod p$$

$$1^2 \cdot 3^2 \cdot 5^2 \cdots (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod p$$

bulunur.

Wilson Teoremi $n! + 1$ şeklinde sonsuz sayıda bileşik sayının var olduğunu söyler.

$1 \leq n \leq 100$ için $n! + 1$ in asal olduğu n değerleri 1, 2, 3, 11, 27, 37, 41, 73 ve 77 dir.

LİNEER KONGRÜANSLAR

6.3. Tanım: $p > 1$ bir doğal sayı $a, b \in \mathbb{Z}$ olmak üzere,

$$ax \equiv b(\text{mod } p)$$

şeklindeki bir kongrüansa **bir bilinmeyenli lineer kongrüans** denir. Burada $OBEB(a;\ p) = k$ ise kongrü olmayan k tane sayı vardır denir.

Tanıma göre $ax_0 \equiv b\ (\text{mod } p)$ olması ancak ve yalnız $ax_0 - b = py_0$ olacak şekilde bir $y_0 \in \mathbb{Z}$ olması ile mümkündür. Yani $ax_0 \equiv b\ (\text{mod } p)$ kongrüansını sağlayan bütün tamsayıları bulma problemi ile OKBEB ve OBEK konusundaki $ax - py = b$ Diofant denklemini çözmek problemi aynıdır.

6.3. Not: x_0**,** $ax \equiv b(\text{mod } m)$ kongrüansının bir çözümü ise x_0 ile mod p aynı kalan sınıfına ait bütün tamsayılarda bu kongrüansın bir çözümüdür. $ax \equiv b\ (\text{mod } p)$ kongrüansının birbirinden farklı çözümlerinin sayısı dendiği zaman kongrüansı sağlayan fakat mod p ye göre kongrü olmayan tamsayıların sayısı anlaşılacaktır.

6.15. Teorem: $OBEB(a; p) = k$ olmak üzere, $ax \equiv b\ (\text{mod } p)$ kongrüansının bir çözümünün olması ancak ve yalnız $k \mid b$ olması ile mümkündür. Eğer $k \mid b$, b ise bu kongrüansın mod p ye göre kongrü olmayan tam k tane çözümü vardır.

İspat: Daha önceden verilen kongrüansın $ax - py = b$ Diofant denklemine eşdeğer olduğunu görmüştük. OBEB ve OKEK konusunda Diofant teoremlerine göre bu Diofant denkleminin çözümlü olması için gerek ve yeter kosul $OBEB(a; p) \mid b$ olmasıdır. Eğer bu Diofant denklemi çözümlü ise $x_0, y_0 \in \mathbb{Z}$ bir özel çözüm olmak üzere, diğer çözümler

$$x = x_0 + \left(\frac{p}{k}\right)t, y = y_0 + \left(\frac{a}{k}\right)t, t \in \mathbb{Z}$$

şeklindedir. $t = 0,1, \dots, k-1$ için

$$x_0,\ x_0 + \frac{p}{k}, x_0 + 2\frac{p}{k}, \cdots, x_0 + (k-1)\frac{p}{k} \qquad (1)$$

çözümlerini gözönüne alalım. Bu tamsayılar mod p ye göre kongrü değildirler. Aksi halde

$$x_0 + \frac{p}{k}t_1 \equiv x_0 + \frac{p}{k}t_2(\text{mod } p), 0 \leq t_1 < t_2 \leq k-1$$

olsa $\frac{p}{k}t_1 \equiv \frac{p}{k}t_2 (\text{mod } p)$, OBEB $\left(\frac{p}{k}; n\right) = \frac{p}{k}$, olduğundan $t_1 \equiv t_2 (\text{mod } k)$ elde edilir ki bu mümkün değildir.

Şimdi $x = x_0 + \left(\frac{p}{k}\right)t$, şeklindeki bir çözümün mod p ye göre (1) deki sayılardan herhangi birine kongrü olduğunu gösterelim: t ve k çiftine bölme algoritması uygularsak

$$t = qk + r, 0 \leq r \leq k - 1$$

olacağından

$$\begin{aligned} x &= x_0 + \left(\frac{p}{k}\right)t \\ &= x_0 + \left(\frac{p}{k}\right)(qk + r) \\ &= x_0 + pq + \frac{p}{k}r \\ &= x_0 + \frac{p}{k}r \ (\text{mod } p) \end{aligned}$$

ve $x_0 + \frac{p}{k}r$, (1) de sıralanan tamsayılardan biridir.

6.3. Sonuç: i) Eğer x_0 **,** $ax \equiv b \ (\text{mod } p)$ kongrüansının bir çözümü ve $\text{OBEB}(a; p) = k$ ise, bu kongrüansın mod p ye göre kongrü olmayan

$$x_0, \ x_0 + \frac{p}{k}, x_0 + 2\frac{p}{k}, \cdots, x_0 + (k-1)\frac{p}{k}$$

gibi tam k tane çözümü vardır.

ii) $\text{OBEB}(a; p) = k = 1$ ise $ax \equiv b (\text{mod } p)$ kongrüansının mod p ye göre tek çözümü vardır. //

$ax \equiv b \ (\text{mod } p)$ kongrüansını çözmek için, kongrüansı Diofant denklemine dönüştürmek veya verilen kongrüansın her iki tarafını p ile aralarında asal bir sayı ile çarparak x'in katsayısını 1 yapmak, gibi çesitli çözüm yöntemleri vardır.

Örnek: $140x \equiv 133 \ (\text{mod } 301)$ kongrüansını çözelim.

1. Çözüm: $140x \equiv 133 \ (\text{mod } 301)$ kongrüansını çözmek demek, $140x - 301y = 133$ Diofant denklemini çözmeye denktir.

$$\begin{aligned} 301 &= 2 \cdot 140 + 21 \\ 140 &= 6 \cdot 21 + 14 \\ 21 &= 1 \cdot 14 + 7 \\ 14 &= 2 \cdot 7 + 0 \end{aligned}$$

olduğudan $\text{OBEB}(301; 140) = 7$ ve $133 = 19 \cdot 7$ olup

$$7 = 1 \cdot 21 - 1 \cdot 14$$
$$7 = 1 \cdot 21 - 1 \cdot (140 - 6 \cdot 21) = 7 \cdot 21 - 1 \cdot 140$$
$$7 = 7 \cdot (301 - 2 \cdot 140) - 1 \cdot 140 = 7 \cdot 301 - 15 \cdot 140$$

$$133 = 133 \cdot 301 - 285 \cdot 140$$

elde edileceğinden çözüm vardır. $x_0 = -285,\ y_0 = 133$ Diğer çözümler

$$x = x_0 + \left(\frac{p}{k}\right)t, y = y_0 + \left(\frac{a}{k}\right)t, t \in \mathbb{Z}$$

denkleminden

$$x_0 = -285 + \frac{301}{7}t = -285 + 43t,\ y_0 = -133 + \frac{140}{7}t = -133 + 20t$$

şeklinde bulunur. $x_0 = -285 + 43t$ burada $t = 0, 1, 2, 3, 4, 5, 6$ için mod 301'e göre kongrü olmayan bütün çözümler

$t = 0$ için $x_0 = -285 \equiv 16 \pmod{301}$
$t = 1$ için $x_0 = -242 \equiv 59 \pmod{301}$
$t = 2$ için $x_0 = -199 \equiv 102 \pmod{301}$
$t = 3$ için $x_0 = -156 \equiv 145 \pmod{301}$
$t = 4$ için $x_0 = -113 \equiv 188 \pmod{301}$
$t = 5$ için $x_0 = -70 \equiv 231 \pmod{301}$
$t = 6$ için $x_0 = -27 \equiv 274 \pmod{301}$

olarak bulunur.

2. Çözüm: $140x \equiv 133 \pmod{301}$
$20x \equiv 19 \pmod{43}$
$28 \cdot 20x \equiv 28 \cdot 19 \pmod{43}$
$560x \equiv 532 \pmod{43}$
$x \equiv 16 \pmod{43}$

(mod 301)'e göre kongrü olmayan pozitif çözümler

$x \equiv 16, 59, 102, 145, 188, 231, 274 \pmod{301}$

olarak bulunur.

6.16. Teorem (Çinlilerin Kalan Teoremi): $p_1, p_2, \cdots, p_r, i \neq j$ için $OBEB(p_i; p_j) = 1$ olan 1'den büyük pozitif tamsayılar olmak üzere,

$x \equiv a_1 \pmod{p_1}$
$x \equiv a_2 \pmod{p_2}$
...
$x \equiv a_r \pmod{p_r}$

kongrüans sisteminin modülü $p_1, p_2, \cdots, p_r$ ye göre tek türlü belirli bir çözümü vardır.

İspat: $p_1, p_2, \cdots, p_r$ ve $k = 1,2, \cdots, r$ için

$$N_k = \frac{p}{p_k} = p_1 p_2 \cdots p_{k-1} p_{k+1} \cdots p_r$$

ile gösterelim. Hipoteze göre p_i ler ikişer ikişer aralarında asal olduklarından $OBEB(N_k; p_k) = 1$ dir. Bu nedenle $N_k x \equiv 1 \pmod{p_k}$ kongrüansının mod p_k ya göre tek türlü çözümü vardır, bu çözümü p_k ile gösterirsek,

$$x_0 = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_r N_r x_r$$

verilen sistemin bir çözümüdür. Gerçekten $i \neq j$ için, $n_k | N_i$ olduğundan $N_i \equiv 0 \pmod{p_k}$ dır. Bunun sonucu olarak $x_0 = a_k N_k x_k \pmod{p_k}$ bulunur. Öte yandan p_k, $N_k x \equiv 1 \pmod{p_k}$ nın bir çözümü olduğundan $N_k x_k \equiv 1 \pmod{p_k}$ ve böylece $k = 1,2,\cdots,r$ için $x_0 = a_k N_k x_k \equiv a_k \pmod{p_k}$ bulunur. Bu ise x_0 ın verilen sistemin bir çözümü olduğunu gösterir.

Şimdi bu çözümün modulo $p_1, p_2, \cdots, p_r$ ye göre tek türlü belirli olduğunu gösterelim: Verilen sistemin x'_0 gibi bir başka çözümünün olduğunu kabul edelim. Bu durumda $k = 1,2,\cdots,r$ için , $x_0 \equiv x'_0 \pmod{p_k}$ yani $p_k | (x_0 - x'_0)$ dır. Öte yandan $i \neq j$ için $OBEB(p_i; p_j) = 1$ olduğundan $(p_1, p_2, \cdots, p_r) | (x_0 - x'_0)$ ve buradanda $x_0 \equiv x'_0 \pmod{p_1, p_2, \cdots, p_r}$ bulunur.

Örnek:

$$x \equiv 1 \pmod 2$$
$$x \equiv 1 \pmod 3$$
$$x \equiv 4 \pmod 5$$

sistemini çözelim: $p = 2 \cdot 3 \cdot 5 = 30$ ve $N_1 = \frac{30}{2} = 15$, $N_2 = \frac{30}{3} = 10$, $N_3 = \frac{30}{5} = 6$ dır.

$15x \equiv 1 \pmod 2$ ise $x \equiv 1 \pmod 2$ olup $x_1 = 1$
$10x \equiv 1 \pmod 3$ ise $x \equiv 1 \pmod 3$ olup $x_2 = 1$
$6x \equiv 1 \pmod 5$ ise $x \equiv 1 \pmod 5$ olup $x_3 = 1$

$$x_0 = 1 \cdot 15 \cdot 1 + 1 \cdot 10 \cdot 1 + 4 \cdot 6 \cdot 1 = 49 \equiv 19 \pmod{30}$$

olur. //

$k = 1,2,\cdots,r$ için p_k lar ikişer ikişer aralarında asal olmak üzere,

$$a_1 x \equiv b_1 \pmod{p_1}$$
$$a_2 x \equiv b_2 \pmod{p_2}$$
$$\cdots$$
$$a_r x \equiv b_r \pmod{p_r}$$

gibi bir lineer kongrüans sistemi verilmiş olsun. Bu sistemin çözümlü olabilmesi için ön şart, sistemdeki her bir lineer kongrüansın çözümlü olmasıdır. Bu durumda $k = 1,2,\cdots,r$ için $OBEB(a_k; p_k) = h_k$ olmak üzere $h_k | a_k$ olmalıdır. Bu

şart sağlandıktan sonra her bir k. kongrüans h_k ile sadeleştirilerek, ilk sistemle aynı çözümlere sahip yeni bir

$a'_1x \equiv b'_1 \pmod{p_1}$, $a'_2x \equiv b'_2 \pmod{p_2}$,..., $a'_rx \equiv b'_r \pmod{p_r}$

sistemi elde edilir, burada $p_k = \frac{n_k}{h_k}$ $i \neq j$ için $OBEB(p_i; p_j) = 1$, $OBEB(a'_i; p_j) = 1$ dir. Bu sistemdeki kongrüansların ayrı ayrı çözümleri

$x \equiv c_1 \pmod{p_1}$, $x \equiv c_2 \pmod{p_2}$,..., $x \equiv c_r \pmod{p_r}$ (1)

şeklinde ise problem, (1) sisteminin çözümlerini bulmaya indirgenir.

Örnek:

$2x \equiv 1 \pmod 5$
$3x \equiv 3 \pmod 6$
$4x \equiv 1 \pmod 7$
$5x \equiv 9 \pmod{11}$

sistemini çözelim:

1. Çözüm: 5, 6, 7, 11 ikişer ikişer aralarında asaldır. $OBEB(2; 5) = 1$ olduğundan $2x \equiv 1 \pmod 5$ kongrüansı çözümlü, $OBEB(3; 6) = 3$ olduğundan 2. kongrüans çözümlü ve $3x \equiv 3 \pmod 6$ yani $x \equiv 1 \pmod 2$ dir. $OBEB(4; 7) = 1$ o halde $4x \equiv 1 \pmod 7$ çözümlü ve son olarak $OBEB(5; 11) = 1$ olduğundan $5x \equiv 9 \pmod{11}$ kongrüansı çözümlüdür. Böylece ilk sistemle aynı çözümlere sahip olan

$2x \equiv 1 \pmod 5$, $x \equiv 1 \pmod 2$, $4x \equiv 1 \pmod 7$, $5x \equiv 9 \pmod{11}$

gibi yeni bir sistem elde edilir. Öte yandan bu sistem

$x \equiv 3 \pmod 5$, $x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 7$, $x \equiv 4 \pmod{11}$

sistemine denktir. Problem yukarıdaki sistemi çözmeye indirgenir. Çinlilerin kalan teoremin deki notasyonlara göre,

$p = 770$; $a_1 = 3$, $N_1 = 154$; $a_2 = 1$, $N_2 = 385$; $a_3 = 2$, $N_3 = 110$; $a_4 = 4$, $N_4 = 70$

$154x \equiv 1 \pmod 5$ ise $x \equiv 4 \pmod 2$ olup $x_1 = 4$
$385x \equiv 1 \pmod 2$ ise $x \equiv 1 \pmod 3$ olup $x_2 = 1$
$110x \equiv 1 \pmod 7$ ise $x \equiv 3 \pmod 7$ olup $x_3 = 3$
$70x \equiv 1 \pmod{11}$ ise $x \equiv 3 \pmod{11}$ olup $x_4 = 3$

$$x_0 = 3 \cdot 154 \cdot 4 + 1 \cdot 385 \cdot 1 + 2 \cdot 110 \cdot 3 + 4 \cdot 70 \cdot 3$$
$$= 3\,733 \equiv 653 \pmod{770}$$

bulunur. //

Şimdi bu şekildeki sistemleri çözmek için kullanılan bir başka metodu bu örnek üzerinde gösterelim.

2. Çözüm:

$2x \equiv 1 \pmod 5$ ise $x \equiv 3 \pmod 5$ olup $x = 3 + 5k_1, k_1 \in \mathbb{Z}$ dir. x için bulunan bu değer sistemin 2. kongrüansında yerleştirilir.

$$3x \equiv 3 \pmod 6$$
$$x \equiv 1 \pmod 2$$
$$3 + 5k_1 \equiv 1 \pmod 2$$
$$k_1 \equiv 0 \pmod 2$$
$$k_1 = 2k_2,\ k_2 \in \mathbb{Z}$$
$$k_1 = 3 + 5(2k_2)$$

x için bulunan son değer sistemin 3. kongrüansında yerlestirilirse,

$$4x \equiv 1 \pmod 7$$
$$4(3 + 10k_2) \equiv 1 \pmod 7$$
$$5k_2 \equiv 3 \pmod 7$$
$$k_2 \equiv 2 \pmod 7$$
$$k_2 = 2 + 7k_3,\ k_3 \in \mathbb{Z}$$
$$x = 3 + 10k_2 = 3 + 10(2 + 7k_3) = 23 + 70k_3$$

bulunur ve x'in bu değerini sistemin son kongrüansında yerleştirirsek buradan

$$5(23 + 70k_3) \equiv 9 \pmod{11}$$
$$20k_3 \equiv 4 \pmod{11}$$
$$-2k_3 \equiv 4 \pmod{11}$$
$$k_3 \equiv -2 \pmod{11}$$
$$k_3 = 9 + 11k_4,\ k_4 \in \mathbb{Z}$$
$$x = 23 + 70k_3 = 23 + 70(9 + 11k_4) = 653 + 770k_4$$

bulunur. Buna göre $x \equiv 653 \pmod{770}$ tir.

6.17. Teorem: Eğer $p = p_1p_2 \cdots p_k$ ve $1 \leq i < j \leq k$ için $OBEB(p_i; p_j) = 1$ ise $ax \equiv b \pmod m$ kongrüansı

$ax \equiv b \pmod{p_1}$, $ax \equiv b \pmod{p_2}$,..., $ax \equiv b \pmod{p_k}$ (1)

sistemine denktir, yani kongrüansının her bir çözümü aynı zamanda (1) sisteminin de bir çözümüdür ve bunun tersi de doğrudur.

İspat: x_0, $ax \equiv b \pmod p$ kongrüansının bir çözümü olsun. Bu durumda $ax_0 \equiv b \pmod p$ ve $i = 1,2,\cdots,k$ için $n_i \mid n$ olduğundan $ax \equiv b \pmod{p_i}$ dir.

Karşıt olarak $i = 1,2,\cdots,k$ için $ax_0 \equiv b \pmod{p_i}$ olsun. Bu durumda $n_i \mid ax_0 - b$ ve $OBEB(p_i; p_j) = 1$ olduğundan $n \mid ax_0 - b$ yani $ax_0 \equiv b \pmod p$ bulunur. //

Bu teoreme göre büyük bir bileşik modüle sahip kongrüansları çözmek için Çinlilerin Kalan teoreminden yararlanılabilir.

Örnek: $131x \equiv 21 \pmod{77}$ kongrüansını çözmek için $n = 77 = 7 \cdot 11$ olduğundan bunun yerine

$$131x \equiv 21 \pmod{7}$$
$$131x \equiv 21 \pmod{11}$$

sistemini çözebiliriz. Bu sistemde

$$x \equiv 0 \pmod{7}$$
$$x \equiv 1 \pmod{11}$$

sistemine denktir. Simdi Çinlilerin Kalan teoremini kullanarak bu sistemi çözelim:

$x \equiv 0 \pmod{7}, x = 7k_1, k_1 \in \mathbb{Z}$

bu değeri 2. kongrüansta yerleştirirsek

$$7k_1 \equiv 1 \pmod{11}$$
$$k_1 \equiv 8 \pmod{11}$$
$$k_1 = 8 + 11k_2,\ k_2 \in \mathbb{Z}$$

ve buradan da

$$x = 7k_1 = 56 + 77k_2,\ k_2 \in \mathbb{Z}$$

elde edilir.

6.4. Tanım: $a_1x_1 + a_2x_2 + \cdots + a_mx_m \equiv c \pmod{p}$ kongransına birden fazla bilinmeyen içeren lineer kongrüanslar adı verilir. Bu birden fazla bilinmeyen içeren lineer kongrüansların çözümü, belirli sayıda tek bilinmeyenli kongrüansların arka arkaya çözülmesi ile gerçekleştirilir.

Örnek 4. $4x + 3y \equiv 5 \pmod{8}$ iki bilinmeyenli lineer kongrüansını çözünüz?

Çözüm: Bu kongrüansın $OBEB(4; 3; 8) = 1$, $1 \mid 5$, Çinlilerin Kalan teoremine göre $k \cdot m^{n-1} = 8$ tane (mod 8) kongrü olmayan çözüm vardır? Şimdi bunları inceleyelim:

$k' = OBEB(4; 8) = 4$ ve $3y \equiv 5 \pmod{4}$
$-y \equiv 1 \pmod{4}$
$y \equiv 3 \pmod{4}$

$y \equiv 3 \pmod{8}$ ve $y \equiv 7 \pmod{8}$ için:

$$4x + 9 \equiv 5 \pmod{8}$$
$$4x \equiv 4 \pmod{8}$$
$$x \equiv 1 \pmod{2}$$

böylece $x \equiv 1 \pmod{8}, x \equiv 3 \pmod{8}, x \equiv 5 \pmod{8}, x \equiv 7 \pmod{8}$ bulunur.

Böylece mod 8'in bütün çözüm takımları

$$(x, y) = (0,7), (2,7), (4,7), (6,7), (1,3), (3,3), (5,3), (7,3)$$

dir.

KALAN SINIFLAR KÜMESİ

Bir tamsayı 5 ile bölündüğünde kalanların kümesi $\{0, 1, 2, 3, 4\}$ olduğunu biliyoruz. Bunlardan 5 ile bölündüğünde kalanların kümesi;

$\bar{0} = \{\cdots, -15, -10, -5, 0, 5, 10, 15, \cdots\}$
$\bar{1} = \{\cdots, -14, -9, -4, 1, 6, 11, 16, \cdots\}$
$\bar{2} = \{\cdots, -13, -8, -3, 2, 7, 12, 17, \cdots\}$
$\bar{3} = \{\cdots, -12, -7, -2, 3, 8, 13, 18, \cdots\}$
$\bar{4} = \{\cdots, -11, -6, -1, 4, 9, 14, 19, \cdots\}$

biçiminde gösterilir. Bu yazıma denklik sınıfları adı verilir.

6.5. Tanım: p kongrüansına göre,

$$\mathbb{Z}_p = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \cdots, \overline{p-1}\}$$

ifadesine kalan sınıfların kümesi veya denklik sınıfların kümesi adı verilir.

Örnek:

$\mathbb{Z}_1 = \{\bar{0}\}, \mathbb{Z}_2 = \{\bar{0}, \bar{1}\}, \mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}, \mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}, \mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$
bir kaç kalanların sınıfıdır.

6.6. Tanım: m kongrüansına göre $\mathbb{Z}_p$ kalanların kümesi, her $a, b \in \mathbb{Z}$ ve $p \in \mathbb{Z}^+ - \{1\}$ olmak üzere,

i) $\bar{a} \oplus \bar{b} = \overline{a+b}$
ii) $\bar{a} \otimes \bar{b} = \overline{a \cdot b}$

biçiminde tanımlanır.

Örnek: $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ kümesinde $\bar{3} \oplus \bar{2} = \overline{3+2} = \bar{1}$ dir.

Örnek: $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ kümesinde $\bar{4} \otimes \bar{3} = \overline{4 \cdot 3} = \bar{0}$ dir.

Örnek: $\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ kümesinde $\bar{3} \otimes [(\bar{2} \oplus \bar{4}) \oplus \bar{4} \otimes \bar{2}]$ ifadesini hesap ediniz.

Çözüm:
$$\begin{aligned} \bar{3} \otimes [(\bar{2} \oplus \bar{4}) \oplus \bar{4} \otimes \bar{2}] &= \bar{3} \otimes [\overline{(2+4)} \oplus \overline{(4 \cdot 2)}] \\ &= \bar{3} \otimes [\bar{1} \oplus \bar{3}] \\ &= \bar{3} \otimes \overline{[1+3]} \\ &= \bar{3} \otimes \bar{4} \\ &= \overline{3+4} \\ &= \bar{2} \end{aligned}$$

Örnek: $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ için toplama ve çarpma işleminin tablosunu yapınız.

Çözüm:

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$\odot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

6.7. Tanım: $\mathbb{Z}_p$ de;

$$\bar{a} \oplus \bar{e} = \bar{e} \oplus \bar{a} = \bar{a}$$

şartını sağlayan $\mathbb{Z}_m$ nin $\bar{a}$ sayısına $\oplus$ işleminin etkisiz elemanı denir. Yine,

$$\bar{a} \otimes \bar{e} = \bar{e} \otimes \bar{a} = \bar{a}$$

şartını sağlayan $\bar{a}$ sayısına $\otimes$ işleminin etkisiz elemanı denir.

Örnek: Yukarıdaki $\mathbb{Z}_4$ örneğine göre $\oplus$ işleminin etkisiz elemanı $\bar{0}$, $\otimes$ işleminin birim (etkisiz) elemanı $\bar{1}$ dır. Çünkü

$\bar{0} \oplus \bar{0} = \bar{0}$
$\bar{1} \oplus \bar{0} = \bar{1}$ $\qquad$ $\bar{1} \otimes \bar{1} = \bar{1}$
$\bar{2} \oplus \bar{0} = \bar{0} \oplus \bar{2} = \bar{2}$ $\qquad$ $\bar{2} \otimes \bar{1} = \bar{1} \otimes \bar{2} = \bar{2}$
$\bar{3} \oplus \bar{0} = \bar{0} \oplus \bar{3} = \bar{3}$ $\qquad$ $\bar{3} \otimes \bar{1} = \bar{1} \otimes \bar{3} = \bar{3}$

dir.

6.8. Tanım: $\mathbb{Z}_p$ de $\bar{e}$ birim (etkisiz) eleman olsun.

$$\bar{a} \oplus \bar{a}^{-1} = \bar{a}^{-1} \oplus \bar{a} = \bar{e}$$

şartını sağlayan $\bar{a}^{-1}$sayısına $\mathbb{Z}_p$ nin $\oplus$ işleminin ters elemanı denir. Yine,

$$\bar{a} \otimes \bar{a}^{-1} = \bar{a}^{-1} \otimes \bar{a} = \bar{e}$$

şartını sağlayan $\bar{a}^{-1}$ sayısına $\otimes$ işleminin ters elemanı denir.

Örnek: Yukarıdaki $\mathbb{Z}_4$ örneğine göre $\oplus$ işleminin birim (etkisiz) elemanı $\bar{0}$ olduğuna göre ters elemanlar,

$\bar{0} \oplus \bar{0}^{-1} = \bar{0}^{-1} \oplus \bar{0} = \bar{0}$ olup $\bar{0}^{-1} = \bar{0}$
$\bar{1} \oplus \bar{3}^{-1} = \bar{3}^{-1} \oplus \bar{1} = \bar{0}$ olup $\bar{3}^{-1} = \bar{1}$
$\bar{2} \oplus \bar{2}^{-1} = \bar{2}^{-1} \oplus \bar{2} = \bar{0}$ olup $\bar{2}^{-1} = \bar{2}$
$\bar{3} \oplus \bar{1}^{-1} = \bar{1}^{-1} \oplus \bar{3} = \bar{0}$ olup $\bar{1}^{-1} = \bar{3}$

dir. Yine $\otimes$ işleminin birim (etkisiz) elemanı $\bar{1}$olduğuna göre ters elemanlar,

$\bar{1} \otimes \bar{1}^{-1} = \bar{1}^{-1} \otimes \bar{1} = \bar{1}$
$\bar{3} \otimes \bar{3}^{-1} = \bar{3}^{-1} \otimes \bar{3} = \bar{1}$

dir. $\bar{0}$ ve $\bar{2}$ sayıların tersi yoktur.

Örnek: $\mathbb{Z}_5$ de $(\bar{x} \oplus \bar{3}) \otimes \bar{2} = \bar{4}$ denkleminin çözüm kümesini bulunuz.

Çözüm:

$(\bar{x} \oplus \bar{3}) \otimes \bar{2} = \bar{4}$
$(\bar{x} \oplus \bar{3}) \otimes \bar{2} \otimes \bar{2}^{-1} = \bar{4} \otimes \bar{2}^{-1}$
$(\bar{x} \oplus \bar{3}) \otimes \bar{2} \otimes \bar{3} = \bar{4} \otimes \bar{3}$ ($\otimes$ işlemine göre $\bar{2}^{-1} = \bar{3}$)
$(\bar{x} \oplus \bar{3}) \otimes \overline{2 \cdot 3} = \overline{4 \cdot 3}$
$(\bar{x} \oplus \bar{3}) \otimes \bar{1} = \bar{2}$
$\bar{x} \oplus \bar{3} = \bar{2}$
$\bar{x} \oplus \bar{3} \oplus \bar{3}^{-1} = \bar{2} \oplus \bar{3}^{-1}$
$\bar{x} \oplus \bar{3} \oplus \bar{2} = \bar{2} \oplus \bar{2}$ ($\oplus$ işlemine göre $\bar{3}^{-1} = \bar{2}$)
$\bar{x} \oplus \overline{3+2} = \overline{2+2}$
$\bar{x} \oplus \bar{0} = \bar{4}$
$\bar{x} = \bar{4}$

Örnek: $\mathbb{Z}_5$ de $(x^2 \oplus \bar{1})(x \oplus \bar{4}) = 0$ denkleminin çözüm kümesini bulunuz.

Çözüm: $(x^2 \oplus \bar{1})(x \oplus \bar{4}) = \bar{0}$

$x^2 \oplus \bar{1} = \bar{0}$ veya $x \oplus \bar{4} = \bar{0}$

i) $x^2 \oplus \bar{1} = \bar{0}$ ise $x^2 \oplus \bar{1} \oplus \bar{4} = \bar{0} \oplus \bar{4}$
$x^2 = \bar{4}$
$x = \bar{2}$ veya $x = \bar{3}$

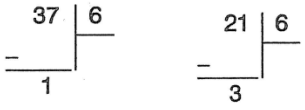
ii) $x \oplus \bar{4} = \bar{0}$ ise $x \oplus \bar{4} \oplus \bar{1} = \bar{0} \oplus \bar{1}$
$x = \bar{1}$

$Ç = \{\bar{1}, \bar{2}, \bar{3}\}$

ÇÖZÜM ALIŞTIRMALAR

Modüler Aritmetik Tanımı

1. Aşağıda iki bölme işlemi verilişitir.



Buna göre, aşağıdakilerden hangisi yanlıştır?

A) $21 \equiv 3 \pmod 6$ B) $37 \equiv 1 \pmod 6$ C) $1 \equiv 37 \pmod 6$
D) $3 \equiv 21 \pmod 6$ E) $3 \equiv 1 \pmod 6$

Çözüm: $3 \equiv 1 \pmod 6$ dışındaki kongüanslar doğrudur.

2. Aşağıdakilerden hangisi yanlıştır?

A) $34 \equiv -1 \pmod 5$ B) $48 \equiv 0 \pmod 6$ C) $51 \equiv 9 \pmod 7$
D) $83 \equiv 9 \pmod{12}$ E) $-94 \equiv 2 \pmod 8$

Çözüm:
A) $34 \equiv -1 \pmod 5 \Leftrightarrow 34 + 1 \equiv -1 + 1 \pmod 5 \Leftrightarrow 35 \equiv 0 \pmod 5$
B) $48 \equiv 0 \pmod 6$
C) $51 \equiv 9 \pmod 7 \Leftrightarrow 51 \equiv 2 \pmod 7$ olup yanlıştır.
D) $83 \equiv 9 \pmod{12}$
E) $-94 \equiv 2 \pmod 8 \Leftrightarrow 94 - 94 \equiv 94 + 2 \pmod 8 \Leftrightarrow 0 \equiv 96 \pmod 5$
$\Leftrightarrow 96 \equiv 0 \pmod 5$

3. I. $58 \equiv 33 \pmod 5$
II. $12x \equiv 0 \pmod 4, x \in \mathbb{Z}$
III. $9! \equiv 0 \pmod{42}$
Yukarıdaki bilgilerden hangileri doğrudur?

I. $58 \equiv 3 \pmod 8$ ve $33 \equiv 3 \pmod 5 \Leftrightarrow 58 \equiv 33 \pmod 5$ doğrudur.
II. $12 \equiv 0 \pmod 4$ ve $x \equiv x \pmod 4 \Leftrightarrow 12x \equiv 0 \pmod 4$ doğrudur.
III. $9! \equiv 0 \pmod{42}$ doğrudur. Çünkü;
$1! \equiv 1 \pmod{42}$

$2! \equiv 2 \pmod{42}$
$3! \equiv 6 \pmod{42}$
$4! \equiv 24 \pmod{42}$
$5! \equiv 36 \pmod{42}$
$6! \equiv 6 \pmod{42}$
$7! \equiv 0 \pmod{42}$
$8! \equiv 0 \pmod{42}$
$9! \equiv 0 \pmod{42}$

4. $8527 \cdot 4256 \equiv a \pmod{5}$
olduğuna göre, a aşağıdakilerden hangisidir?

Çözüm: $8527 \equiv 2 \pmod{5}$ ve $4256 \equiv 1 \pmod{5}$
$8527 \cdot 4256 \equiv 2 \cdot 1 \pmod{5}$
$8527 \cdot 4256 \equiv 2 \pmod{5}$

5. $46 \equiv 10 \pmod{a}, a \in \mathbb{N}\backslash\{0,1\}$
olduğuna göre, a'nın birbirinden farklı alacağı değer nelerdir?

Çözüm: $46 \equiv 10 \pmod{a}$
$46 - 10 \equiv 10 - 10 \pmod{a}$
$36 \equiv 0 \pmod{a}$
olduğundan a'nın değeri 2, 3, 4, 6, 10, 12, 18, 36 olur.

Modüler Aritmetikte Üstlü İfadeler

6. $(-7)^{30} \equiv x \pmod{8}$
olduğuna göre, x aşağıdakilerden hangisidir?

Çözüm:
$(-7)^{30} \equiv x \pmod{8} \Leftrightarrow (-1)^{30} \cdot 7^{30} \equiv x \pmod{8} \Leftrightarrow 7^{30} \equiv x \pmod{8}$

$7 \equiv 7 \pmod{8}$
$7^2 \equiv 1 \pmod{8}$
$(7^2)^{15} \equiv 1^{15} \pmod{8}$
$7^{30} \equiv 1 \pmod{8}$
$(-7)^{30} \equiv 1 \pmod{8}$

7. $5^{571} \equiv m \pmod 6$
olduğuna göre, x aşağıdakilerden hangisidir?

Çözüm: $5 \equiv 5 \pmod 6$
$5^2 \equiv 1 \pmod 6$
$(5^2)^{285} \equiv 1^{285} \pmod 6$
$5^{570} \equiv 1 \pmod 6$
$5^{570} \cdot 5 \equiv 1 \cdot 5 \pmod 6$
$5^{571} \equiv 5 \pmod 6$

8. $x \equiv 3 \pmod 8$
olduğuna göre, x^4 sayısı 8 ile bölündüğünde kalan kaç olur?

A) 0 B) 1 C) 2 D) 3 E) 4
Çözüm: $x \equiv 3 \pmod 8$
$x^2 \equiv 1 \pmod 8$
$(x^2)^2 \equiv 1^2 \pmod 8$
$x^4 \equiv 1 \pmod 8$

9. $10^{16} \equiv a \pmod{17}$ olduğuna göre, a'nın değeri nedir?

A) 1 B) 2 C) 3 D) 4 E) 5
Çözüm: $10 \equiv 10 \pmod{17}$
$10^2 \equiv 15 \pmod{17}$
$10^3 \equiv 14 \pmod{17}$
$10^4 \equiv 4 \pmod{17}$
$(10^4)^4 \equiv 4^4 \pmod{17}$
$10^{16} \equiv 1 \pmod{17}$

10. x doğal sayısı 12 ile bölündüğünde kalan 5 oluyor. x^2 sayısını 6 ile böldüğünde kalan nedir?

Çözüm:
$x \equiv 5 \pmod{12} \Leftrightarrow x = 12k + 5, k \in \mathbb{Z}$
$\Leftrightarrow x = 6(2k) + 5, 2k \in \mathbb{Z}$
$\Leftrightarrow x \equiv 5 \pmod 6$
$\Leftrightarrow x^2 \equiv 5^5 \pmod 6$
$\Leftrightarrow x^2 \equiv 1 \pmod 6$

11. $x = 17^4$ olduğuna göre, x sayısı 15 ile bölündüğünde kalan kaç olur?

Çözüm: $17 \equiv 2 \pmod{15}$
$17^2 \equiv 2^2 \pmod{15} \equiv 4 \pmod{15}$
$(17^2)^2 \equiv 4^2 \pmod{15} \equiv 1 \pmod{15}$

12. $2^{26} + 3^{26} = a \pmod 5$ olduğuna göre, a'nın değeri nedir?

Çözüm:
$2 = 2 \pmod 5$ ve $3 = 3 \pmod 5$
$2^2 = 4 \pmod 5$ ve $3^2 = 4 \pmod 5$
$2^3 = 3 \pmod 5$ ve $3^3 = 2 \pmod 5$
$2^4 = 1 \pmod 5$ ve $3^4 = 1 \pmod 5$
$(2^4)^6 = 1^6 \pmod 5$ ve $(3^4)^6 = 1^6 \pmod 5$
$2^{24} = 1 \pmod 5$ ve $3^{24} = 1 \pmod 5$
$2^{24} \cdot 2^2 = 1 \cdot 4 \pmod 5$ ve $3^{24} \cdot 3^2 = 1 \cdot 4 \pmod 5$
$2^{26} = 4 \pmod 5$ ve $3^{26} = 4 \pmod 5$
$2^{26} + 3^{26} = 4 + 4 \pmod 5$
$2^{26} + 3^{26} = 3 \pmod 5$

13. n pozitif tamsayı olmak üzere,
$5^{12n+5} \equiv x \pmod 7$
olduğuna göre, x'in değeri nedir?

Çözüm: $5 \equiv 5 \pmod 7$
$5^2 \equiv 4 \pmod 7$
$5^3 \equiv 6 \pmod 7$
$5^4 \equiv 2 \pmod 7$
$5^5 \equiv 3 \pmod 7$
$5^6 \equiv 1 \pmod 7$
$(5^6)^{2n} \cdot 5^5 \equiv 1^{2n} \cdot 3 \pmod 7$
$5^{12n+5} \equiv 3 \pmod 7$

Modüler Aritmetik Uygulamaları

14. Bugün Çarşamba ise 100 gün sonra hangi gündür?

Çözüm: $100 \equiv 2 \pmod 7$ olduğundan 2 gün sonra Cuma'dır.

15. Bugün Pazartesi ise 53 gün önce hangi gündür?

Çözüm: $53 \equiv 4 \pmod 7$ olduğundan 4 gün sonra Cuma'dır.

16. Bugünden 151 önceki gün Cuma ise, bugün hangi gündür?

Çözüm: $151 \equiv 4 \pmod 7$ olduğundan 4 gün önce Pazartesi'dir.

17. 8 günde bir nöbet tutan astsubay, ilk nöbetini Pazartesi tutarsa 5. Nöbetini hangi gün tutar.

Çözüm: İlk nöbet tutulunca geriye 4 nöbet kalır. $8 \cdot 4 = 36$ ise $36 \equiv 1 \pmod 7$ olduğundan 1 gün sonra Salı'dır.

18. Pazartesi saat 08.00 da havalanan bir uçak 80 saat sonra geri döneceğine göre, bu uçak hangi gün, saat kaçta geri dönecektir.

Çözüm: $80 \equiv 8 \pmod{24}$ olduğundan 3 gün 8 gün saat sonra yani Perşembe günü saat 16.00 dir.

Modüler Aritmetikte Denklemler

19. x ve y doğal sayıları 8 ile bölündüğünde kalanlar sırasıyla 5 ve 4 oluyor. $x \cdot y$'nin 8 ile bölümünden kalan nedir?

Çözüm: $x \equiv 5 \pmod 8$ ve $y \equiv 4 \pmod 8$
$x \cdot y \equiv 5 \cdot 4 \pmod 8$
$x \cdot y \equiv 4 \pmod 8$

20. $3x + 11 \equiv 5 \pmod 7$
olduğuna göre, x'in en küçük doğal sayı değerini nedir?

Çözüm: $3x + 11 \equiv 5 \pmod 7$
$11 \equiv 4 \pmod 7$ ise $3x \equiv 1 \pmod 7$
$5 \cdot 3x \equiv 5 \cdot 1 \pmod 7$
$x \equiv 5 \pmod 7$

21. $2x + 3 \equiv 5 - x \pmod 8$
olduğuna göre, x'in en küçük doğal sayı kaçtır?

Çözüm: $2x + 3 \equiv 5 - x \pmod 8$
$2x + x \equiv 5 - 3 \pmod 8$
$3x \equiv 2 \pmod 8$
$3 \cdot 3 \cdot x \equiv 3 \cdot 2 \pmod 8$
$x \equiv 6 \pmod 8$

22. $(x + 1)(x - 2) \equiv 0 \pmod{11}$
olduğuna göre, x'i sağlayan değerler nelerdir?

Çözüm: $(x + 1)(x - 2) \equiv 0 \pmod{11}$ olması
$x + 1 \equiv 0 \pmod{11}$ ve $x - 2 \equiv 0 \pmod{11}$
$x = 10$ ve $x = 2$

23. 5 sayısının 11 modülüne göre tersi aşağıdakilerden hangisidir?

A) 9 B) 10 C) 11 D) 12 E) 13

Çözüm: 5 sayısının 11 modülüne göre tersini bulmak $5x \equiv 1 \pmod{11}$ lineer kongrüansının çözmek gerekir.
$9 \cdot 5x \equiv 9 \cdot 1 \pmod{11}$
$45x \equiv 9 \pmod{11}$
$x \equiv 9 \pmod{11}$

24. $x \equiv 3 \pmod{12}$ ve $x \equiv 6 \pmod 8$ kongrüans sisteminin çözümünü bulunuz.

Çözüm: $x \equiv a \pmod p$ ve $x \equiv b \pmod q$ ve $OBEB(p;\ q) = c$ kongrans olsun. $c \mid b - a$ ise sistemin çözümü var. $c \nmid b - a$ ise sistemin çözümü yoktur. Buna göre $OBEB(12;\ 8) = 4$ tür. $4 \nmid 6 - 3$ olduğundan çözüm yoktur.

25. $x \equiv 9 \pmod{12}$ ve $x \equiv 5 \pmod 8$ kongrüans sisteminin bir x_0 çözümü nedir?

Çözüm: $OBEB(12;\ 8) = 4, 4 \mid 9 - 5$ dir. Sistemin çözümü vardır.

$$\frac{12}{4}x \equiv \frac{9-5}{4} \left(\text{mod } \frac{8}{4}\right)$$

çözümünü bulalım.

$3x \equiv 1 \pmod 2$

$x \equiv 1 \pmod 2$

dir. Buna göre;

$x_0 \equiv 12 + 9 \pmod{\text{OKEK}(12;8)}$

$x_0 \equiv 21 \pmod{24}$

olur.

Kalan Sınıfları

26. $\mathbb{Z}_8$ de $\bar{5} \cdot \bar{6} \cdot \bar{7}$ işleminin sonucu aşağıdakilerden hangisidir?

Çözüm: $5 \cdot 6 \cdot 7 \equiv 2 \pmod 8$ olduğundan $\mathbb{Z}_8$ de $\bar{5} \cdot \bar{6} \cdot \bar{7}$ işleminin sonucu $\bar{2}$ olur.

27. $\mathbb{Z}_9$ de $x \in \bar{5}$ olduğuna göre, x'in iki basamaklı en büyük tamsayını toplamı nedir?

Çözüm: $\mathbb{Z}_9 = \{\dots, -\bar{4}, \bar{5}, \overline{14}, \overline{23}, \dots, \overline{95}, \dots\}$ olduğundan cevap $\overline{95}$ olur.

28. $\mathbb{Z}_6$ için $\bar{5} \cdot (\bar{4} + \bar{3}) + \bar{2}$ işleminin sonucu nedir?

Çözüm: $5 \cdot (4 + 3) + 2 \equiv 1 \pmod 6$ olduğundan $\mathbb{Z}_6$ de $\bar{5} \cdot (\bar{4} + \bar{3}) + \bar{2}$ işleminin sonucu $\bar{1}$ olur.

29. $\mathbb{Z}_5$ te $(\bar{2}x + \bar{3}) \cdot (\bar{3}x + \bar{5})$ işleminin sonucu nedir?

Çözüm: $(\bar{2}x + \bar{3}) \cdot (\bar{3}x + \bar{5})$

$= \bar{2}x \cdot \bar{3}x + \bar{2}x \cdot \bar{5} + \bar{3}x \cdot \bar{3} + \bar{3} \cdot \bar{5}$

$= \bar{1}x^2 + \bar{0}x + \bar{4}x + \bar{0}$

$= x^2 + \bar{4}x$

30. $\mathbb{Z}_7$ de aşağıdakilerden hangisi $x^2 = \bar{2}$ denklemini sağlar?

A) 0 B) 1 C) 2 D) 3 E) 4

Çözüm: Cevap 3 dür. Çünkü $3^2 \equiv 2 \pmod 7$ dir.

KAYNAKÇA

1. Doç. Dr. Mustafa BAYRAKTAR, Soyut Cebir ve Sayılar Teorisi, Atatürk Üniversitesi Basımevi, Erzurum, 1988.
2. Prof. Dr. Bülent KARAKAŞ, Yrd. Doç. Dr. Hacı AKTAŞ, Sayılar Teorisi, Gaziosmanpaşa Üniversitesi Yayınları, Tokat, 1998.
3. Doç. Dr. Neşe Yelkenkaya, Sayılar Teorisi Ders Notları, İstanbul Kültür Üniversitesi, İnternet Ders Notları, 2020.
4. H. Hilmi HACISALİHOĞLU, Lise Matematik I – II – III, Serhat Yayınları A.Ş. İstanbul, 2001.
5. Ömer Faruk ERTÜRK, Galip KIR, İsmail BİLGİN, Devlet Kitapları, Lise 1, 2, 3, Milli Eğitim Basımevi, 4. Baskı, İstanbul, 2002.
6. Sait AKKAŞ, H. Hilmi HACISALİHOĞLU, Zühtü ÖZEL, Arif SABUNCUOĞLU, Soyut Matematik**,** 4. Baskı, Aralık, 2010.