Tanım 2.1.15. $0 \neq m, n \in \mathbb{Z}$ verilsin.

(i) $d \in \mathbb{Z}^+$ (ii) $d \mid m$ ve $d \mid n$ (iii) $k \in \mathbb{Z}$ için $k \mid m$ ve $k \mid n$ ise $k \mid d$

şartlarını sağlayan d tam sayısına m ile n tam sayılarının en büyük ortak bölen (ebob) denir ve (m,n) veya $ebob(m,n)$ ile gösterilir. (ebob yerine obeb de kullanılabilir)

Teorem 2.1.16 Sıfırdan farklı iki tam sayının en büyük ortak böleni vardır ve $d = (m,n)$ ise $d = mx + ny$ o.ş. en az $x, y \in \mathbb{Z}$ bulunabilir.

İspat: $A = \{ mx + ny \mid mx + ny > 0, x, y \in \mathbb{Z} \}$ olsun. $x = m$ ve $y = n$ için $m^2 + n^2 > 0$ olup $A \neq \emptyset$ olur. $\mathbb{Z}^+$ iyi sıralı old.dan A nın d gibi bir en küçük elemanı vardır. $d = (m,n)$ old. gös. m yi d ye kalanlı bölelim. $m = qd + r$, $0 \leq r < d$ o.ş. $\exists q, r \in \mathbb{Z}$ vardır. $d = mx + ny$ old.dan

$$m = qd + r$$
$$= q(mx + ny) + r$$

$\Rightarrow r = m(1 - qx) + n(-qy)$ dir. $r \neq 0$ ise $0 < r < d$ olur ki bu d nin seçimiyle çelişir. ($r \in A$). Dolayısıyla $r = 0$ olup $d \mid m$ dir.

Benzer şekilde d|n olduğu gösterilebilir. elmk eln o.s. e∈Z alalım. d=mx+ny old.dan eld dir. Aynı zamanda d∈A olddan d=mx+ny o.s. ∃ x,y∈Z vardır.

Tanım 2.1.17 İki tam sayının en büyük ortak böleni 1 ise bu iki sayıya aralarında asaldır denir.

Not: m,n∈Z⁺ olsun n yi m ye kalanlı olarak ard arda bölelim.

$n = q_1 m + r_1$ ve $0 \le r_1 < m$ —(1)

$m = q_2 r_1 + r_2$ ve $0 \le r_2 < r_1$ —(2)

— — — — — — —

$r_{k-1} = q_{k+1} r_k + r_{k+1}$ ve $0 \le r_{k+1} < r_k$ ——(k+1)

$r_k = q_{k+2} r_{k+1} + 0$ ——(k+2) şeklinde kalan sıfır olunca kadar devam edelim. $m > r_1 > r_2 \ldots$ olduğuna dikkat edilirse sonlu bir adımdan sonra 0 kalanının bulunacağı aşikârdır.

Teorem 2.1.18 (Euclid Algoritması) Yukarıda yapılan kalanlı bölmeler arasında sıfırdan farklı en son kalan m ile n nin en büyük ortak böleridir yani $r_{k+1} = (m,n)$ dir.

İspat: Yukarıdaki $(k+2)$. satırdan $r_{k+1} | r_k$ yazılabilir.
Buradan $r_{k+1} | q_{k+1} r_k + r_{k+1}$ olup bu şekilde devam edilirse $r_{k+1} | m$ ve $r_{k+1} | n$ olur. Yani, r_{k+1} m ile n nin bir ortak böleridir. Şimdi $e \in \mathbb{Z}$ olmak üzere e|m ve e|n yani e, m ile n nin keyfi bir ortak böleri olsun.

e|m ve e|n $\Rightarrow$ e|n − q₁m = r₁

e|m ve e|r₁ $\Rightarrow$ e|m − q₂r₁ = r₂ . Böyle devam edersek e|r_{k+1} bulunur. En büyük ortak bölen tanımı gereği $r_{k+1} = (m,n)$ dir.

Örnek: 963 ile 657 sayılarının ebob'u Öklid Algoritması yardımıyla bulunuz.

$963 = 1.657 + 306$
$657 = 2.306 + 45$
$306 = 6.45 + 36$
$45 = 1.36 + 9$
$36 = 4.9 + 0$

$\Rightarrow 9 = (963, 657)$ dir.

$9 = 45-36 = 45 - 306+6\cdot45 = 7\cdot45-306 = 7(657-2\cdot306)-306$

$= 7\cdot657 - 15\cdot306 = 7\cdot657 - 15(963-657)$

$= -15\cdot963 + 22\cdot657 \Rightarrow x_0 = -15, y_0 = 22$

Teorem 2.1.19. m ve n sıfırdan farklı ve $c \in \mathbb{Z}$ olsun. Eğer $(m,n)=1$ ve $m \mid nc$ ise $m \mid c$ dir.

İspat: $(m,n)=1 \Leftrightarrow 1 = mx+ny$ o.ş. $\exists x,y \in \mathbb{Z}$ vardır.

$c = cmx+cny = (mc)x+(nc)y \Rightarrow m \mid nc \Rightarrow m \mid (nc)y+(mc)x = c$ olur.

Sonuç 2.1.20. $p \in \mathbb{P}$ ve $p \nmid m$ ise $m \mid nc$ $p \nmid n$ keyfi $p \mid n$ dir.

İspat: $p \in \mathbb{P}$ oldan $p \nmid m$ keyfi $(p,m)=1$ dir.

$(p,m)=1 \Leftrightarrow 1 = px+ny$ o.ş. $\exists x,y \in \mathbb{Z}$ vardır.

$n = npx+npy \Rightarrow p \mid n$ olur.

Tanım 2.1.21. $0 \neq m,n \in \mathbb{Z}$ olsun. (i) $k \in \mathbb{Z}^+$

(i) $m|k$ ve $n|k$ (iii) $m|t$ ve $n|t$ için $k|t$ şartlarını sağlayan $k \in \mathbb{Z}$ sayısına m ile n tam sayılarının en küçük ortak katı (ekok) denir $[m,n]$ veya ekok $[m,n]$ ile gösterilir.

[ekok yerine okek de kullanılabilir]

Aritmetiğin temel teoremi gereği n ve m tam sayıları için

$n = p_1^{n_1} \cdots p_r^{n_r}$ ve $m = p_1^{m_1} \cdots p_r^{m_r}$ şeklinde yazılabilir.

$(n,m) = p_1^{\min(m_1,n_1)} \cdots p_r^{\min(m_r,n_r)}$ ve

$[n,m] = p_1^{\max(m_1,n_1)} \cdots p_r^{\max(m_r,n_r)}$ dir.

Teorem 2.1.22. $m,n \in \mathbb{Z}^+$ için $(m,n)[m,n] = m.n$ dir.

Tanım 2.1.23. Pozitif $n \in \mathbb{Z}$ için $1 \leq a < n$ ve $(a,n) = 1$ olan a tam sayılarının sayısı $\varphi(n)$ ile gösterilir ve Euler fonksiyonu denir.

Euler fonksiyonu aşağıdaki özelliklere sahiptir.

E_1: $p \in \mathbb{P}$ ise $\varphi(p) = p-1 = p\left(1-\frac{1}{p}\right)$

E_2: $p \in \mathbb{P}$ ve $t \in \mathbb{N}$ ise $\varphi(p^t) = p^t - p^{t-1} = p^t\left(1-\frac{1}{p}\right)$

E_3: $(m,n)=1$ ise $\varphi(m.n) = \varphi(m).\varphi(n)$ dir.

E_4: $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ ise $\varphi(m) = p_1^{\alpha_1} \cdots p_r^{\alpha_r}\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_r}\right)$.

Ödev: 72 ile aralarında asal olan tam sayıların sayısını bulunuz. (cevap: 24)

Ödev: $(m,n)=1$ olmak üzere $m|a$ ve $n|a$ olması için $mn|a$ old. göst.

Ödev: 102! sayısının sonunda kaç tane sıfır vardır? (24)

Ödev: $a,b \in \mathbb{Z}^+$ ve $(a,b)=12$, $a+b=108$ ise bu şartı sağlayan kaç farklı (a,b) ikilisi vardır?

Not: $a = p_1^{m_1} \cdots p_r^{m_r}$, $b = p_1^{n_1} \cdots p_r^{n_r}$ $(p_i \in \mathbb{P}, m_i, n_i \in \mathbb{Z}^+)$ cla olması için $\forall i=1,r$ için $m_i \leq n_i$.

2.2. Modüler Aritmetik

Bu bölümde, cebirsel yapıları daha iyi kavrayabilmek için, tam sayıların bazı aritmetik özellikleri üzerinde durulacaktır.

Tanım 2.2.1. $0 \neq m \in \mathbb{Z}$ olmak üzere $a, b \in \mathbb{Z}$ olsun. $a \equiv b \pmod{m}$ olması için gerek ve yeter şart $m \mid a-b$ olmasıdır şeklinde tanımlanır ve a ile b mod m ye göre denktirler denir.

$m \mid a-b \Rightarrow -m \mid a-b$ old.dan $m > 0$ alınabilir.

Teorem 2.2.2 Yukarıda tanımlanan $\equiv$ bağıntısı $\mathbb{Z}$ de bir denklik bağıntısıdır.

Tanım 2.2.3. $\mathbb{Z}$ deki $\equiv$ denklik bağıntısının belirttiği denklik sınıflarına m modülüne göre (mod(m)) kalan sınıfları denir ve tüm kalan sınıflarının kümesi $\mathbb{Z}_m$ ile gösterilir.

$a \in \mathbb{Z}$ nin denklik sınıfı $a = \{x \in \mathbb{Z} \mid m \mid a-x\}$ dir.

Teorem 2.2.4. $a \equiv b \pmod m$ olması için $\iff$ a ve b nin m ile bölümünden elde kalanın aynı olmasıdır.

İspat. ($\Rightarrow$:) $a \equiv b \pmod m$ olsun. a ve b yi m ile kalanlı olarak bölelim. $a = q_1 m + r_1$, $b = q_2 m + r_2$, $0 \le r_1, r_2 < m$ o.ş. $\exists q_1, q_2, r_1, r_2 \in \mathbb{Z}$ vardır.

$a \equiv b \pmod m \iff m \mid a-b \Rightarrow a-b = mk$ o.ş $\exists k \in \mathbb{Z}$ vardır.

$a = b + mk = q_1 m + r_1$, $0 \le r_1 < m$

$\Rightarrow b = m(q_1 - k) + r_1$ old.dan kalanlı bölmenin teşliğinden

$q_1 - k = q_2$, $r_1 = r_2$ elde edilir.

($\Leftarrow$:) a ile b nin m ile bölümünden kalanlar aynı olsunlar.

Yani $a = mq_1 + r_1$, $b = mq_2 + r_2$, $0 \le r_1, r_2 < m$ o.ş. $\exists q_1, q_2, r_1, r_2 \in \mathbb{Z}$ vardır. $a - b = m(q_1 - q_2) \Rightarrow m \mid a-b \iff a \equiv b \pmod m$.

$q_1 - q_2 \in \mathbb{Z}$

Not: Yukarıdaki teorem'e göre bir $a \in \mathbb{Z}$ nin $m>0$ ile bölümünden elde edilen kalanlar $0, 1, 2, \to m-1$ olacağından $\bar{a}$ sınıfı, $\bar{0}, \bar{1}, \to \overline{m-1}$ sınıflarından biridir. O halde $\mathbb{Z}_m$ m elemanlı bir kümedir. $|\mathbb{Z}_m| = m$. dir.

Örnek: $\mathbb{Z}_8 = \{\bar{1}, \bar{2}, \to \bar{7}\}$ dir. $14 \equiv 6 \pmod 8$ ve $21 \equiv 5 \pmod 8$ olduğundan $14 \in \bar{6}$, $21 \in \bar{5}$ dir.

Teorem 2.2.5. $\left.\begin{array}{l} a \equiv a_1 \pmod m \\ b \equiv b_1 \pmod m \end{array}\right\} \Rightarrow a+b \equiv a_1+b_1 \pmod m$
$ab \equiv a_1 b_1 \pmod m$ dir.

İspat: $a \equiv a_1 \pmod m \Rightarrow m \mid a-a_1$
$b \equiv b_1 \pmod m \Rightarrow m \mid b-b_1$
$\Rightarrow m \mid (a-a_1)+(b-b_1)$
$\Rightarrow m \mid (a+b)-(a_1+b_1) \Rightarrow a+b \equiv a_1+b_1 \pmod m$

$m \mid b(a-a_1) \Leftarrow m \mid b(a-a_1)$
$m \mid b-b_1 \Leftarrow m \mid a_1(b-b_1)$
$\Rightarrow m \mid ba - bb_1 + a_1 b - a_1 b_1$
$\Rightarrow m \mid ba - a_1 b_1 \Leftarrow ab \equiv a_1 b_1 \pmod m$

Tanım 2.2.6. $\bar{a}, \bar{b} \in \mathbb{Z}_m$ için $\bar{a} \oplus \bar{b} = \overline{a+b}$ ve $\bar{a} \odot \bar{b} = \overline{ab}$ ile tanımlanır.

Not: Yukarıdaki teoremden $\bar{a}$ ve $\bar{b}$ sınıflarının toplamının (çarpımının) sınıflardan alınan temsilcilere bağlı olmadığı yani $\oplus$ nın ($\odot$ nın) iyi tanımlı olduğu anlaşılır.

Örnek: $\mathbb{Z}_{10}$ da $\bar{4} = \overline{14}$, $\bar{5} = \overline{15}$, $\bar{4} \oplus \bar{5} = \overline{14} \oplus \overline{15}$ olur.

$\bar{4} \odot \bar{5} = \overline{14} \odot \overline{15}$

Teorem 2.2.7. $\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_m$ için (i) $\bar{a} \oplus \bar{b} = \bar{b} \oplus \bar{a}$

(ii) $\bar{a} \oplus (\bar{b} \oplus \bar{c}) = (\bar{a} \oplus \bar{b}) \oplus \bar{c}$

(iii) $\bar{a} \oplus \bar{0} = \bar{a}$

(iv) $\bar{a} \oplus \bar{x} = \bar{0}$ o.ş. $\exists\, \bar{x} \in \mathbb{Z}_m$ vardır.

Teorem 2.2.8. $\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_m$ için (i) $\bar{a} \odot \bar{b} = \bar{b} \odot \bar{a}$

(ii) $\bar{a} \odot (\bar{b} \odot \bar{c}) = (\bar{a} \odot \bar{b}) \odot \bar{c}$ (iii) $\bar{a} \odot \bar{1} = \bar{a}$

(iv) $\bar{a} \odot \bar{0} = \bar{0}$ (yutan eleman)

Teorem 2.2.9. $\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_m$ için $\bar{a} \odot (\bar{b} \oplus \bar{c}) = (\bar{a} \odot \bar{b}) \oplus (\bar{a} \odot \bar{c})$.

$(b,m) = d_2 \Rightarrow d_2 \mid b$

$d_2 \mid m \;,\; m \mid a-b \Rightarrow d_2 \mid a-b \Big\rangle d_2 \mid a$

d_2, a ile m nin keyfi bir ortak bölen olup
$d_2 \mid (a,m) = d_1$ olur. O halde $d_1 = d_2$ dir.

Not: Yukarıdaki teoreme göre bir kalan sınıfındaki tüm sayıların modül ile ebob leri aynıdır.

Tanım 2.2.12. $\bar{a} \in \mathbb{Z}_m$ sınıfının $(a,m)=1$ ise $\bar{a}$ kalan sınıfına asal kalan sınıfı denir. Asal kalan sınıflarının kümesi $\mathbb{Z}_m^*$ ile gösterilir. $\mathbb{Z}_m^* = \{ \bar{a} \in \mathbb{Z}_m \mid (a,m)=1 \}$.
$\mathbb{Z}_m^*$ in eleman sayısı $\varphi(m)$ Euler fonksiyonu ile verilir.

Örnek: $\mathbb{Z}_{12}^* = \{ \bar{a} \in \mathbb{Z}_{12} \mid (a,12)=1 \} = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}$.

$\Rightarrow \varphi(12) = \varphi(2^2 \cdot 3) =$ 4

Örnek: $\mathbb{Z}_9$ da $\bar{4}\odot(\bar{5}\oplus\bar{7}) = \bar{4}\odot\bar{3} = \bar{3}$

$(\bar{4}\odot\bar{5})\oplus(\bar{4}\odot\bar{7}) = \bar{2}\oplus\bar{1} = \bar{3}$ > olur.

Tanım 2.2.10. $\mathbb{Z}_m$ de kendileri $\bar{0}$ dan farklı olduğu halde carpımları $\bar{0}$ olan sınıflara sıfır bölen sınıflar denir.

Örnek: $\mathbb{Z}_6$ de sıfır bölen sınıflar $\{\bar{2},\bar{3},\bar{4},\bar{6},\bar{8},\bar{9},\bar{10}\}$ dır.

Not: $\mathbb{Z}_m$ de carpmaya göre her elemanın tersi olmayabilir.

$\mathbb{Z}_4$ de $\bar{2}$ nin tersi yoktur. Yani $\bar{2}\odot\bar{x} = \bar{1}$ o.ş. $\bar{x}\in\mathbb{Z}_4$ $\Rightarrow \bar{0},\bar{1},\bar{2},\bar{3}$

yoktur. $\mathbb{Z}_4$ de $\bar{3}$ tersi $\bar{3}$ dır.

Teorem 2.2.11. $a\equiv b \pmod m \Rightarrow (a,m)=(b,m)$ dir.

İspat: $(a,m)=d_1$ ve $(b,m)=d_2$ olsun. $d_1 | d_2$ ve $d_2 | d_1$ old.

gösst.

$(a,m)=d_1 \Rightarrow d_1 | a$

$m | a-b$ $\Rightarrow d_1 | -b = |d_1| b$ ve $d_1 | m$ old.dan

d_1, ile b nin keyfi bir ortak böleni olup ebob tanımı gereği $d_1 | (m,b) = d_2$ olur.

Teorem 2.2.13. İki asal kalan sınıfının çarpımı da bir asal kalan sınıfıdır.

İspat: $\bar{a}, \bar{b} \in \mathbb{Z}_m^*$ olsun. $\bar{ab} \in \mathbb{Z}_m^*$ yani $(ab, m) = 1$ old. gös.t.

$\bar{a}, \bar{b} \in \mathbb{Z}_m^*$ old.dan $(a, m) = (b, m) = 1$ yazılabilir.

$(a, m) = 1 \Rightarrow ax + my = 1$ ş.ş. $\exists x, y \in \mathbb{Z}$ vardır

$\Rightarrow bax + bmy = b$ olur. $(ab, m) = t$ olsun. $t = 1$ old. gös.t.

$t | ab$ ve $t | m$ dir. Buradan $t | abx$ ve $t | bmy$ dir.

$t | abx + bmy = b$ olur. $t | m$ ve $t | b$ old.dan t, Ahile b nin bir ortak böleni olup ebob tanımı gereği $t | (b, m) = 1$ dir.

Yani $t = 1$ olur.

Teorem 2.2.14. $\bar{a} \in \mathbb{Z}_m$ ve $\bar{a} \neq \bar{0}$ olsun. $\bar{a}$ sıfır bölen sınıftır $\Leftrightarrow$ $\bar{a} \notin \mathbb{Z}_m^*$ dır.

İspat: $\Rightarrow$) $\bar{0} \neq \bar{a} \in \mathbb{Z}_m$ elemanı sıfır bölen olsun. Bu durumda $\bar{a}\bar{b} = \bar{ab} = \bar{0}$ o.ş. $\exists\ \bar{0} \neq \bar{b} \in \mathbb{Z}_m$ vardır. K.edelim ki $\bar{a}$ bir asal kalan sınıfı olsun. Bu durumda $(a, m) = 1$ dir. $\bar{ab} = \bar{0} \Rightarrow ab \equiv 0 \pmod{m} \Rightarrow m | ab$, $(a, m) = 1$

$\Rightarrow m | b$ dir. Bu ise $b \equiv 0 \pmod{m} \Rightarrow \bar{b} = \bar{0}$ çelişkisi elde edilir.

O halde $\bar{a} \notin \mathbb{Z}_m^*$ olur.

($\Leftarrow$:) $\bar{0} \neq \bar{a} \in \mathbb{Z}_m$ elemanı bir asal kalan sınıfı olmasın.

O halde $(a,m) = d$ ise $d > 1$ dir. $\bar{a} \neq \bar{0}$ yani $m \nmid a$ dır.

Buradan $d \neq m$ olur. Çünkü $m \nmid d$ dir.

$(a,m) = d = 1 \mid a \Rightarrow a = da_1$

$d \mid m \Rightarrow m = dm_1$ $\Big\}$ o.s. $a_1, m_1 \in \mathbb{Z}$ vardır. Öyle ki $(a_1, m_1) = 1$ dir.

$am_1 = da_1m_1 = a_1m$ yani $\overline{am_1} = \bar{0}$ olur. $\overline{m_1} \neq \bar{0}$ olduğundan $\bar{a}$ bir sıfır bölen olur.

Tanım 2.2.15. $\bar{a} \in \mathbb{Z}_m$ olsun. $\bar{a} \odot \bar{c} = \bar{1}$ o.s. $\exists \bar{c} \in \mathbb{Z}_m$ varsa $\bar{c}$ ye $\bar{a}$ nın ters denir.

Teorem 2.2.16. Bir $\bar{a} \in \mathbb{Z}_m$, $\bar{a} \neq \bar{0}$ sınıfının tersinir olabilmesi için ($\Leftrightarrow$) $\bar{a} \in \mathbb{Z}_m^*$ olmasıdır.

İspat: ($\Rightarrow$:) $\bar{0} \neq \bar{a} \in \mathbb{Z}_m$ elemanının tersi mevcut olsun. Bu durumda $\bar{a} \cdot \bar{c} = \bar{1}$ o.s. $\exists \bar{c} \in \mathbb{Z}_m$ vardır. Teorem 2.2.14 e göre $\bar{a}$ nın bir sıfır bölen olmadığını gösterirsek İspat biter. Bir $\bar{0} \neq \bar{b} \in \mathbb{Z}_m$ için $\bar{a} \odot \bar{b} = \bar{0}$ kabul edelim $\bar{c} \odot (\bar{a} \odot \bar{b}) = (\bar{c} \odot \bar{a}) \odot \bar{b} = \bar{1} \odot \bar{b} = \bar{b} = \bar{0}$ çelişkisi elde edilir. O halde $\bar{a}$ bir sıfır bölen değildir.

($\Leftarrow$) $\bar{a} \in \mathbb{Z}_m^*$ olsun. Yani $(a,m)=1$ olduğundan $ax+my=1$ olacak şekilde $x,y \in \mathbb{Z}$ vardır. $ax-1=m(-y) \Rightarrow m \mid ax-1 \Rightarrow ax \equiv 1 \pmod{m} \Rightarrow \bar{a}\cdot\bar{x}=\bar{1}$

$\Rightarrow \bar{x}=a^{-1}$ olur. Yani $\bar{a}$ nın tersi mevcuttur.

Sonuç 2.2.17. $n \in \mathbb{P}$ ise $\mathbb{Z}_n$ deki sıfırdan farklı her kalan sınıfının tersi mevcuttur.

Örnek. $\mathbb{Z}_{10}$ un asal kalan sınıfları $\mathbb{Z}_{10}^* = \{\bar{a} \in \mathbb{Z}_{10} \mid (a,10)=1\}$

$= \{\bar{1},\bar{3},\bar{7},\bar{9}\}$.

$(\bar{1})^{-1}=\bar{1}$, $(\bar{3})^{-1}=\bar{7}$, $(\bar{7})^{-1}=\bar{3}$

$(\bar{9})^{-1}=\bar{9}$

Teorem 2.2.18 (Euler Teoremi) $n \in \mathbb{Z}$ olsun. $(a,n)=1$ olan $\forall a \in \mathbb{Z}$ için $a^{\varphi(n)} \equiv 1 \pmod{n}$ veya $\bar{a}^{\varphi(n)}=\bar{1}$ dir.

Sonuç 2.2.19 (Fermat Teoremi) Özel olarak yukarıdaki teoremde $n=p \in \mathbb{P}$ ise $p \nmid a$ olan $\forall a \in \mathbb{Z}$ için $a^{p-1} \equiv 1 \pmod{p}$ dir.

Örnek: $3^{27} \equiv x \pmod 5 \Rightarrow x = ?$ Yani 3^{27} nin 5 ile bölümünden elde edilen kalanı bulunuz.

Çözüm: Fermat teoremi gereği $3^{\varphi(5)} \equiv 1 \pmod 5 \Rightarrow 3^4 \equiv 1 \pmod 5$ dir.

$(3^4)^6 = 3^{24} \equiv 1 \pmod 5 \Rightarrow 3^{27} \equiv 3^3 \equiv 2 \pmod 5$ olur.

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

Çözüm: Bir sayının son üç basamağını bulmak demek 1000 ile bölümünden kalanı bulmak demektir. Yani $7^{9999} \equiv x \pmod{1000}$ ifadesindeki x i bulalım. $(7, 10^3) = 1$ olduğundan Euler teoremine göre

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

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

$\Rightarrow 10^3 \mid 7^{10.000} - 1 \Rightarrow 7^{10.000} = 1 + 10^3 k, \; k \in \mathbb{Z}$

$= 1001 + (k-1)10^3$

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

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

Tanım 2.2.20. $ax \equiv b \pmod m$ şeklindeki bir denklem ve bir bilinmeyenli lineer kongrüans denir. Bu denklemi sağlayan x tam sayılarının kümesine de kongrüansın çözüm kümesi denir.

Önerme 2.2.21 $ax \equiv b \pmod m$ nin bir çözümü $x_0 \in \mathbb{Z}$ ise $\bar{x}_0 \in \mathbb{Z}_m$ sınıfındaki tüm sayılar da bir çözümdür.

İspat: $\forall x \in \bar{x}_0$ için $x \equiv x_0 \pmod m \Rightarrow ax \equiv ax_0 \equiv b \pmod m$ olduğundan istenen elde edilir.

Teorem 2.2.22. $(a,m)=1$ ise $ax \equiv b \pmod m$ nin çözümü var ve $\bmod m$ tek bir sınıftır.

Teorem 2.2.23 $ax \equiv b \pmod m$ nin bir çözümünün olması için $\Leftrightarrow (a,m) \mid b$ olmasıdır.

Sonuç 2.2.24. $ax \equiv b \pmod m$ için $d=(a,m) \mid b$ ise bu kongrüansın çözümleri $\bmod m$, d sınıftır.

Örnek: $6x \equiv 9 \pmod{15}$ kongrüansının çözümlerini bulunuz.

Çözüm: $(6,15)=3 \mid 9$ olduğundan çözüm var ve mod 15 sınıfından 3 tanedir.

$6x \equiv 9 \pmod{15} \Leftrightarrow 2x \equiv 3 \pmod 5 \Rightarrow x \equiv 4 \pmod 5 \Leftrightarrow 5 \mid x-4$

$\Leftrightarrow x = 4+5t, t \in \mathbb{Z}$. Şimdi çözümleri mod 15 sınıflarıyla ifade edelim. $t=3t$ için $x=4+15t$

$t=3t+1$ için $x=9+15t$ $t \in \mathbb{Z}$ $\{\bar{4}, \bar{9}, \overline{14}\}$.

$t=3t+2$ için $x=14+15t$

Not: Bir lineer kongrüans çözümleri bulma problemi $ax \equiv b \pmod m$, $(a,m)=1$ kongrüans denklemin çözümü " problemine indirgenebilir ve bunun için 3 yol izlenir.

1) a nın tersi bağlılıkla bulunabiliyorsa $\bar{a}^{-1}=\bar{c}$ olmak üzere $x \equiv bc \pmod m$ dir.

2) Verilen denklem diophant denklemine çevrilir. $ax \equiv b \pmod m \Leftrightarrow ax-my=b$ $(x,y \in \mathbb{Z})$. a ve m sayılarına ard arda bölme uygulanarak $1=ax'+my'$ o.ş. $x', y' \in \mathbb{Z}$ 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: $28x \equiv 15 \pmod{107}$ kongruansını çözelim.

$(28,107)=1 \mid 15$ olduğundan çözüm var ve mod 107 sınıfından tek bir çözüm bulmak kolay değil bu yolu kullanmayalım.

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

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

$107 = 3.28 + 23$

$28 = 1.23 + 5$

$23 = 4.5 + 3$

$5 = 1.3 + 2$

$3 = 1.2 + 1$

$2 = 2.1 + 0$

$(28,107)=1$ dir.

$1 = 3 - 2 = 3 - (5-3) = 2.3 - 5$

$= 2(23 - 4.5) - 5 = 2.23 - 9.5$

$= 2.23 - 9(28 - 23)$

$= 11.23 - 9.28$

$= 11(107 - 3.28) - 9.28 = 11.107 - 42.28$

$\Rightarrow 15 = (15.11)107 - (15.42).28$

$\Rightarrow x = -630 \Rightarrow \overline{x} = \overline{-630} = \overline{12}$ 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.

$28x - 107y = 15 \Rightarrow x = \frac{15 + 321}{28} = 12$ olup $\overline{x} = \overline{12} \pmod{107}$ çözüm bulunur.

Teorem 2.2.5 (Çin Kalan Teoremi) $m_1, m_2, \dots, m_k \in \mathbb{N}^* - \{1\}$, $i \neq j$ için $(m_i, m_j) = 1$ ve $a_1, a_2, \dots, a_k \in \mathbb{Z}$ keyfi tam sayılar olsun. Bu takdirde $x \equiv a_i \pmod{m_i}$ $(i = 1, 2, \dots, k)$ olan bir $x \in \mathbb{Z}$ vardır. x_1 ve x_2 bu kongrüansı sağlayan iki tam sayı ise $m = m_1 \cdot m_2 \cdots m_k$ olmak üzere $x_1 \equiv x_2 \pmod m$ dir.

Örnek: $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 4 \pmod 7$ kongrüans denklem sistemini gösteriniz.

Çözüm: $(3, 5) = (5, 7) = (3, 7) = 1$ çözüm var. $M_1 = 35, M_2 = 21, M_3 = 15$

$a_1 = 2, a_2 = 3, a_3 = 4$

$b_1 = 2, b_2 = 1, b_3 = 1$

$c_1 = 140, c_2 = 63, c_3 = 60$

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

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

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

$x = 140+63+60 = 263 \Rightarrow \overline{x} = \overline{263} = \overline{53}$ bulunur.

Ödev: $\left.\begin{array}{l} x \equiv 2 \pmod 6 \\ x \equiv 4 \pmod 8 \end{array}\right\}$ sisteminin çözümünü bulunuz ($\overline{25} = \overline{x}$)

2.yol $x \equiv 2 \pmod 3 \Rightarrow 3 \mid x-2 \Rightarrow x = 2+3t, t \in \mathbb{Z}$

$2+3t \equiv 3 \pmod 5 \Rightarrow 3t \equiv 1 \pmod 5 \Rightarrow t \equiv 2 \pmod 5 \Rightarrow 5 \mid t-2$

$\Rightarrow t-2 = 5v, v \in \mathbb{Z}$, $t = 5v+2$

$x = 2+3t = 2+3(5v+2) = 15v+8$

$15v+8 \equiv 4 \pmod 7 \Rightarrow 15v \equiv -3 \pmod 7 \Rightarrow v \equiv -3 \pmod 7$

$\Rightarrow v \equiv 4 \pmod 7$

$\Rightarrow 7 \mid v-4 \Rightarrow v-4 = 7m \Rightarrow v = 7m+4$, $m \in \mathbb{Z}$

$t = 5v+2 = 5(7m+4)+2 = 35m+22$

$x = 2+3t = 2+3(35m+22) = 68+105m \Rightarrow x \equiv 68 \pmod{105}$

$\Rightarrow \overline{x} = 68$ olur.