2. BÖLÜM
SAYILAR TEORİSİ

ASAL SAYILAR, OBEB-OKEK ve MODÜLER ARİTMETİK BAZI TEORİLERİ

Asal Sayılar, OBEB-OKEK, Modüler Aritmetik kavramı Sayılar Bilimi dersinde bahsedilmiştir. Burada o konuların devamı olarak bazı tanım ve teoremlerden ile o konulara ait bazı fonksiyonlardan bahsedilecektir.

1. Asal Sayıların Bazı Teorileri

"Asal sayıların sonsuz tane olması" teoreminin ispatı, Asal sayılar konusunda biri Öklid'in, diğeri Fransız Matematikçi Dr. Thomas Joannes Stieltjes'in yaptıkları yöntemler verilmişti. Burada da iki tane daha verilecektir. İlk olarak "Euler'in analitik ispatı", sonra da Polya'nın ispatı izah edilecektir.

2.1. Teorem: Asal sayılar sonsuz sayıdadır.

İspat:

1. Euler'in analitik ispatı: $p_1, p_2, \cdots, p_n$ gibi sonlu sayıda asal sayının var olduğunu kabul edelim. Her bir $p_i > 1$ olduğundan $\sum_{k=0}^{\infty} \frac{1}{p_i^k}$ geometrik serisi yakınsak ve toplamı $\frac{1}{1-\frac{1}{p^k}}$ dir. Böylece

$$\prod_{i=1}^{n} \frac{1}{1-\frac{1}{p_i}} = \prod_{i=1}^{n} \sum_{k=0}^{\infty} \frac{1}{p_i^k}$$

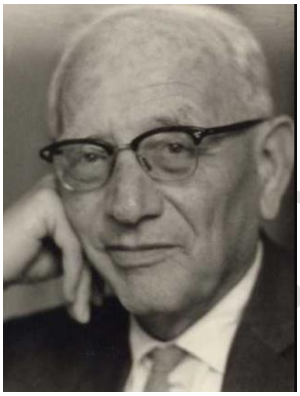
elde edilir. Bütün asal sayılar $p_1, p_2, \cdots, p_n$ den ibaret olduğundan, aritmetiğin esas teoremine göre herhangi bir $n \in \mathbb{N}$ sayısı $n = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$ şeklinde tek türlü olarak yazılır.

Buna göre

$$\prod_{i=1}^{n} \frac{1}{1-\frac{1}{p_i}} \geq \sum_{n=0}^{\infty} \frac{1}{n}$$

dir. Yukarıdaki eşitsizliğin sağ tarafındaki seri (harmonik seri) sonsuza ıraksayan bir seridir.

Öte yandan her bir $p_i > 1$ olduğundan sol taraftaki çarpım sonludur. Bu bizi bir çelişkiye götürür. O halde sonsuz sayıda asal sayı vardır.



George Pólya
13 Aralık 1887, Budapeşte, Macaristan-07 Eylül 1985, Palo Alto, Kaliforniya

2. Pólya'nın ispatı: Her bir F_n Fermat sayısının en az bir asal böleni vardır ve F_n diğer Fermat sayıları ile aralarında asal olduğundan bu asal sayı diğer Fermat sayılarını bölmez. Yani diğer Fermat sayılarını bölen asal sayılardan farklıdır. O halde F_n den büyük olmayan, birbirinden farklı en az $n+1$ tane asal sayı vardır. Fermat sayıları sonsuz sayıda olduğundan bu bize asal sayıların sonsuz sayısı da olduğunu gösterir.

2.2. Teorem: a bir asal sayı ve $a = \log_2(n+1)$ sayısında $(n \in \mathbb{Z})$ ise n sayısı da asaldır.

İspat: $a = \log_2(n+1)$ için logaritmanın tanımından $2^a = n+1$ yani $2^a - 1 = n$ dır. Sayılar bilimi asal sayılar konusunda "a sayısı asal iken $2^a - 1 = n$ da asaldır" teorem gereği n sayısı da asaldır.

Örnek: 2047 asal sayı mıdır?

Çözüm: $\log_2(2047+1) = \log_2 2048 = \log_2 2^{11} = 11$ dir. 11 asal sayı olduğundan 2047'de asal sayıdır.

2.3. Teorem: $a \in \mathbb{Z}$ olmak üzere $a = \log_2(\log_2(n+1))$ ifadesinde $n \in \mathbb{Z}$ sayısı Fermat asal sayısını verir.

İspat: $a = \log_2(\log_2(n+1))$

$2^a = \log_2(n+1)$

$2^{2^a} = n+1$

$2^{2^a} - 1 = n$

2. OBEB-OKEK'in Bazı Teorileri

2.4. Teorem:

$i = 1, 2, \cdots, m; j = 1, 2, \cdots, n$ olmak üzere, $OBEB(a_i; b_i) = 1$ ise

$$OBEB\left(\prod_{i=1}^{m} a_i, \prod_{j=1}^{n} b_j\right) = 1$$

dir.

İspat: İlk önce $OBEB\left(a_1, \prod_{j=1}^{n} b_j\right) = 1$ olduğunu gösterelim: İspatı n'e göre tümevarım ile yapacağız.

1. $n = 2$ için iddianın doğru olduğunu gösterelim:

$OBEB(a_1; b_1) = 1$ ve $OBEB(a_1; b_2) = 1$ den OBEB-OKEK konusunda ilgili teoreme göre $OBEB(a_1; b_1 b_2) = 1$ bulunur.

2. İddianın $n-1$ için doğru olduğunu varsayalım, yani, $OBEB\left(a_1, \prod_{j=1}^{n-1} b_j\right) = 1$ olsun.

3. n için ispat: İndüksiyon hipotezine göre, $OBEB\left(a_1, \prod_{j=1}^{n-1} b_j\right) = 1$, öte yandan $OBEB(a_1; b_n) = 1$ olduğundan OBEB-OKEK konusunda 5.4. teoremine göre, $OBEB\left(a_1, \prod_{j=1}^{n-1} b_j\right) = 1$ elde edilir.

Şimdi $OBEB\left(\prod_{i=1}^{m} a_i, \prod_{j=1}^{n} b_j\right)=1$ olduğunu gösterelim: $\prod_{j=1}^{n} b_j = b$ dersek, yukarıdaki ispata benzer şekilde m'e göre tümevarım ile, $OBEB\left(\prod_{i=1}^{m} a_i, b\right)=1$ olduğu gösterilir.

2.1. Sonuç: $a_1 = a_2 = \cdots = a_m = a, b_1 = b_2 = \cdots = b_m = b$ alınırsa $OBEB(a; b) = 1$ den her $m, n \in \mathbb{N}$ için $OBEB(a^m; b^n) = 1$ elde edilir.

2.5. Teorem: n bir pozitif tamsayı ve p bir asal sayı olsun. p'nin n!'i bölen en büyük kuvveti, $E_p(n)=\sum_{k=1}^{\infty} \left[\!\left[\frac{n}{p^k}\right]\!\right]$ dir. Yani $E_p(n)$, n!'li böler. Burada $p^k > n$ için $\left[\!\left[\frac{n}{p^k}\right]\!\right] = 0$ olmasından dolayı, toplam sonlu sayıda terim içerir.

İspat: n pozitif tamsayı arasında p'nin katları sayısı $\left[\!\left[\frac{n}{p}\right]\!\right]$,

P^2 nin katları sayısı $\left[\!\left[\frac{n}{p^2}\right]\!\right]$,

P^3 nin katları sayısı $\left[\!\left[\frac{n}{p^3}\right]\!\right]$,

...

tanedir. O halde $E_p(n)=\sum_{k=1}^{\infty} \left[\!\left[\frac{n}{p^k}\right]\!\right]$ dir.

2.2. Sonuç: $n!=\prod_{p\le n}^{\infty} p^{\sum_{k=1}^{\infty}\left[\left|\frac{n}{p^k}\right|\right]}$

Örnek: 3'ün 9!'i bölen en büyük kuvvetini bulunuz.

Çözüm: $E_3(9)=\sum_{k=1}^{\infty} \left[\!\left[\frac{9}{3^k}\right]\!\right]$ dır. $3^3 > 9$ olduğundan

$$E_3(9) = \left[\!\left[\frac{9}{3}\right]\!\right] + \left[\!\left[\frac{9}{3^2}\right]\!\right] = 3 + 1 = 4$$

tür.

Örnek: 10! in asal çarpanlara ayrılışını bulunuz.

Çözüm: Eğer p, 10!'in bir asal çarpanı ise p, böler 10! = 1.2.3 ... 10 dur. Asal sayılar konusundaki 4.1. Sonuca göre 10!'in çarpanlarından birini bölmek zorundadır. Öyleyse $p \leq k \leq 10$ dir. Böylece $p \in \{2, 3, 5, 7\}$ olabilir. Öte yandan

$$E_2(10!) = \sum_{k=1}^{\infty} \left[\left[\frac{10}{2^k}\right]\right] = \left[\left[\frac{10}{2}\right]\right] + \left[\left[\frac{10}{2^2}\right]\right] + \left[\left[\frac{10}{2^3}\right]\right] = 5 + 2 + 1 = 8$$

$$E_3(10!) = \sum_{k=1}^{\infty} \left[\left[\frac{10}{3^k}\right]\right] = \left[\left[\frac{10}{3}\right]\right] + \left[\left[\frac{10}{3^2}\right]\right] = 3 + 1 = 4$$

$$E_5(10!) = \sum_{k=1}^{\infty} \left[\left[\frac{10}{5^k}\right]\right] = \left[\left[\frac{10}{5}\right]\right] = 2$$

$$E_7(10!) = \sum_{k=1}^{\infty} \left[\left[\frac{10}{7^k}\right]\right] = \left[\left[\frac{10}{7}\right]\right] = 1$$

$$10! = 2^8 \cdot 3^8 \cdot 5^2 \cdot 7$$

olur.

2.6. Teorem: $0 \leq r \leq n$, $n, r \in \mathbb{Z}$ olmak üzere;

$$E_p(n!) = E_p(r!) + E_p((n-r)!)$$

dir.

Çözüm: $\frac{n}{p^k} = \frac{r}{p^k} + \frac{n-r}{p^k}$ olacağından Parçalı Fonksiyonlar konusunda Tam Değer Fonksiyonunun özelliklerini hatırlayacak olursak;

$$\left[\left[\frac{n}{p^k}\right]\right] \geq \left[\left[\frac{r}{p^k}\right]\right] + \left[\left[\frac{n-r}{p^k}\right]\right]$$

olacağından

$$E_p(n!) = \sum_{k=1}^{\infty} \left[\left[\frac{n}{p^k}\right]\right] \geq \sum_{k=1}^{\infty} \left[\left[\frac{r}{p^k}\right]\right] + \sum_{k=1}^{\infty} \left[\left[\frac{n-r}{p^k}\right]\right] = E_p(r!) + E_p((n-r)!)$$

bulunur.

2.7. Teorem: $m > n \geq 0$ olmak üzere F_n, F_m Fermat asal sayıları aralarında asaldır.

İspat: $OBEB(F_n, F_m) = d$ olsun. Fermat sayıları tek sayılar olduğu için, d sayısı tek sayıdır. $x = 2^{2^n} + 1$ ve $k = 2^{m-n}$ diyelim. Bu durumda

$$\frac{F_m-2}{F_n}=\frac{\left(2^{2^n}\right)^{2^{m-n}}-1}{2^{2^n}+1}=\frac{x^k-1}{x+1}=x^{k-1}-x^{k-2}+\cdots-1$$

ve böylece $F_n \mid (F_m-2)$ dir ve $d \mid F_n$ olduğundan $d \mid (F_m-2)$ bulunur. Öte yandan $d \mid F_m$ olacağından $d \mid 2$ dir. d sayısı bir tek sayı olduğundan $d=1$ olur.

3. İşlemin Modüler Aritmetiğe Uygulaması

Modüler aritmetik Sayılar Bilimi derslerinde izah edilmişti. Orada bir işlemin tersi ile ilgili bilgiler ve örnekler verilmemişti. Yukarıda bir sayının tersinin bulunmasını inceledik. Şimdi de bir sayının tersini bularak modüler aritmetiğe uygulanmasını izah edelim.

2.1. Aksiyom: m kongrüansına göre $\mathbb{Z}_{/m}$ kalanların kümesi olsun. Topla ve çarpma işlemine göre birim (etkisiz) elemanı $\bar{1}$ dir. (İleri de iki işlem için cisim adı verilecektir.)

Örnek: $\mathbb{Z}_{/3}$ de;

$$\bar{2}x+y=\bar{1}$$
$$x+y=\bar{1}$$

denklem sisteminin çözüm kümesini bulunuz.

Çözüm: Verilen iki denklemi taraf tarafa çıkarırsak,

$$x=\bar{1}-\bar{1}=\bar{0}$$

bulunur. Buna göre

$$x+y=\bar{1}$$
$$\bar{0}+y=\bar{1}$$
$$y=\bar{1}$$

$$Ç=\{(x,y): x=\bar{0}, y=\bar{1}\}$$

olur.

Örnek: $\mathbb{Z}_{/7}$ de, $f(x)=\bar{3}x+\bar{2}$ ise $f^{-1}(x)$ i bulalım.

Çözüm: $f(x)=\bar{3}x+\bar{2}$

$$x=\bar{3}y+\bar{2}$$
$$x+\bar{5}=\bar{3}y+\bar{2}+\bar{5}$$
$$x+\bar{5}=\bar{3}y$$
$$\bar{3}^{-1}(x+\bar{5})=\bar{3}^{-1}\cdot\bar{3}y, \quad (\bar{3}^{-1}=\bar{5})$$
$$\bar{5}(x+\bar{5})=\bar{5}\cdot\bar{3}y$$

$\bar{5}x + \bar{4} = y$
$f^{-1}(x) = \bar{5}x + \bar{4}$

Örnek: $\mathbb{Z}_{/10}$ da, $f(x) = \bar{3}x + \bar{5}$ ile tanımlı fonksiyonu için $(f \circ f)(x) = \bar{1}$ ise x'in değeri nedir?

Çözüm: $(f \circ f)(x) = \bar{1}$
$f(f(x)) = \bar{1}$
$f(\bar{3}x + \bar{5}) = \bar{1}$
$\bar{3}(\bar{3}x + \bar{5}) + \bar{5} = \bar{1}$
$\bar{9}x + \bar{0} = \bar{1}$
$\bar{9}^{-1} \cdot \bar{9}x = \bar{9}^{-1} \cdot \bar{1}, \quad (\bar{9}^{-1} = \bar{9})$
$x = \bar{9}$

4. Modüler Aritmetiğin Bazı Teorileri

2.8. Teorem: " $\equiv$ " bağıntısı tamsayılar kümesi üzerinde bir denklik bağıntısıdır.

İspat: Her $m \in \mathbb{N}$ sabit bir sayı olmak üzere, her $x, y, z \in \mathbb{R}$ için

1. $x \equiv x \pmod m$ olduğundan yansıyandır.
2. $x \equiv y \pmod m$ ise $m \mid (x - y)$ olup $m \mid (y - z)$ dir. O halde $y \equiv x \pmod m$ yani simetriktir.
3. $x \equiv y \pmod m$ ve $y \equiv z \pmod m$ ise
   $m \mid (x - y)$ ve $m \mid (y - z)$
   $x - y = mk$ ve $y - z = m\ell$, $(k, \ell \in \mathbb{Z})$
   $x = y + mk$ ve $y = z + m\ell$
   $x = z + m(\ell + k)$
   $m \mid (x - z)$
   $x \equiv z \pmod m$

olur. Bu ise geçişken olduğunu gösterir.

2.9. Teorem: Eğer $f(x_1, x_2, \cdots, x_m)$ katsayıları tamsayı olan bir polinom ve $1 \leq i \leq m$ için $x_1 \equiv y_1 \pmod m$ ise

$$f(x_1, x_2, \cdots, x_m) \equiv f(y_1, y_2, \cdots, y_m) \pmod m$$

dir.

Bu teoremin ispatı aşikardır.

Örnek: $f(x_1, x_2) = x_1^2 + 2x_1x_2 + 3x_2^2 + 1$ olsun.

$f(25,12) \equiv b \pmod 7$

denkleminde b'nin değeri nedir?

Çözüm: $25 \equiv 4 \pmod 7$ ve $12 \equiv 5 \pmod 7$

$f(25,12) = 25^2 + 2 \cdot 25 \cdot 12 + 3 \cdot 12^2 + 1 = 1658$

$f(4,5) = 4^2 + 2 \cdot 4 \cdot 5 + 3 \cdot 5^2 + 1 = 132$

olacağından

$f(25,12) \equiv f(4,5) \pmod 7$

$1658 \equiv 132 \pmod 7$

bulunur ki, bu bize $b \equiv 132$ değeri elde edilir.

2.10. Teorem: a sayısı n basamaklı $a = (c_n c_{n-1} \cdots c_1 c_0)$, $0 \le m \le n$ için $0 \le c_m < 10$, a sayısının ondalık açılımı ve $t = c_0 + c_1 + \cdots + c_n$ olsun. Bu durumda

i) $3 \mid a$ olması ancak ve yalnız $3 \mid t$ olması ile mümkündür.

ii) $9 \mid a$ olması ancak ve yalnız $9 \mid t$ olması ile mümkündür.

İspat: $f(x) = \sum_{k=0}^{n} c_k x^k$ şeklinde sayı çözümlenmesi olsun.

i) $10 \equiv 1 \pmod 3$ 2.9. teoreme göre;

$f(10) \equiv f(1) \pmod 3$ ve $f(10) = a$, $f(1) = t$

$a \equiv t \pmod 3$

olur. Böylece;

$a \equiv t \pmod 3$, $3 \mid a \Leftrightarrow t \equiv a \equiv 0 \pmod 3 \Leftrightarrow 3 \mid t$

dir.

ii) $10 \equiv 1 \pmod 9$ 2.9. teoreme göre;

$f(10) \equiv f(1) \pmod 9$, $f(10) = a$, $f(1) = t$

$a \equiv t \pmod 9$

olur. Böylece;

$a \equiv t \pmod 9$, $9 \mid a \Leftrightarrow t \equiv a \equiv 0 \pmod 9 \Leftrightarrow 3 \mid t$

dir.

2.11. Teorem: a sayısı n basamaklı $a = (c_n c_{n-1} \cdots c_1 c_0)$, $0 \le m \le n$ için $0 \le c_m < 10$, a sayısının ondalık açılımı ve $t = c_0 - c_1 + c_2 - \cdots + (-1)^n c_n$ olsun. Bu durumda $11 \mid a$ olması ancak ve yalnız $11 \mid t$ olması ile mümkündür.

İspat: $f(x)=\sum_{k=0}^{n} c_k x^k$ şeklinde sayı çözümlenmesi olsun.

$10 \equiv -1 \pmod{11}$

$f(10) \equiv f(-1) \pmod{11}$, $f(10) = a$, $f(1) = t$

dir. Böylece $11 \mid a \Leftrightarrow 11 \mid t$ dir.

2.12. Teorem: a sayısı n basamaklı $a = (c_n c_{n-1} \cdots c_1 c_0)$, $0 \le m \le n$ için $0 \le c_m < 10$, a sayısının ondalık açılımı ve $t = c_0 - c_1 + c_2 - \cdots + (-1)^n c_n$ olsun. a sayısının 7, 11 ve 13 sayılarının hepsi ile bölünebilmesi ancak ve yalnız

$t = (100c_2 + 10c_1 + c_0) - (100c_5 + 10c_4 + c_3) + (100c_8 + 10c_7 + c_6) - \cdots$

sayısının 7, 11 ve 13 sayılarının hepsi ile bölünmesidir.

İspat: $7 \cdot 11 \cdot 13 = 1001$ dir.

Eğer m çift ise $10^{3m} \equiv 1, 10^{3m+1} \equiv 10, 10^{3m+2} \equiv 100 \pmod{1001}$

Eğer m tek ise $10^{3m} \equiv -1, 10^{3m+1} \equiv -10, 10^{3m+2} \equiv -100 \pmod{1001}$

O halde

$$a = (100c_2 + 10c_1 + c_0) - (10^{3+2}c_5 + 10^{3+1}c_4 + 10^3 c_3) + \\ +(10^{6+2}c_8 + 10^{6+1}c_7 + 10^6 c_6) - \cdots$$

Buna göre $1001 \mid a$ olması ancak ve yalnız $1001 \mid t$ olması ile mümkündür.

ÇARPIMSAL FONKSİYONLAR

2.1. Tanım: $f : \mathbb{N} \to \mathbb{R}$, $f\left(\prod_{k=1}^{n} a_k\right) = \prod_{k=1}^{n} f(a_k)$ biçiminde tanımlanan fonksiyonlara çarpımsal fonksiyonlar denir. Burada $n = 2$ alınırsa

$$f(a_1 a_2) = f(a_1) f(a_2)$$

olur.

Örnek: A bir pozitif tamsayı $a_1, a_2, a_3, \ldots$ asal sayılar; $m_1, m_2, m_3, \ldots$ doğal sayılar olmak üzere,

$$A = a_1^{m_1} . a_2^{m_2} . a_3^{m_3} . \ldots$$

asal çarpanların çarpımı biçiminde yazılsın. Burada A sayının pozitif bölenleri sayısı

$$\tau = (m_1 + 1)(m_2 + 1)(m_3 + 1) \ldots$$

kadar olduğu Asal Sayılar konusunda izah edildi. $f(m_k) = m_k + 1, (1 \le k \le n)$ biçiminde tanımlanan bir fonksiyon çarpımsal fonksiyondur. Gerçekten;

$$\begin{aligned} f\left(\prod_{k=1}^{n} m_k\right) &= f(m_1)f(m_2)\cdots f(m_n) \\ &= (m_1+1)(m_2+1)\cdots(m_n+1) \\ &= \prod_{k=1}^{n}(m_k+1) \\ &= \prod_{k=1}^{n} f(m_k) \end{aligned}$$

dir. //

Bu soruyu nümerik olarak somutlaştırabiliriz. f fonksiyonunu "4 ve 5 sayılarının bölenlerinin sayısı" biçiminde tanımlanırsa f fonksiyonu çarpımsal fonksiyon olur. Şöyle ki;

"4 sayılarının bölenleri 1, 2, 4" olup sayısı $s(4) = 3$ dür.
"5 sayılarının bölenleri 1, 5" olup sayısı $s(5) = 2$ dür.
"20 sayılarının bölenleri 1, 2, 4, 5, 10, 20" olup sayısı $s(20) = 6$ dür.

$$s(4 \cdot 5) = s(4) \cdot s(5)$$

olur.

Örnek: A bir pozitif tamsayı $a_1, a_2, a_3, \ldots$ asal sayılar; $m_1, m_2, m_3, \ldots$ doğal sayılar olmak üzere,

$$A = a_1^{m_1}.a_2^{m_2}.a_3^{m_3}\ldots$$

asal çarpanların çarpımı biçiminde yazılsın. Burada A sayının pozitif bölenleri toplamı

$$\sigma = \frac{a_1^{m_1}-1}{a_1-1} \cdot \frac{a_2^{m_2}-1}{a_2-1} \cdot \frac{a_3^{m_3}-1}{a_3-1} \cdots$$

olduğu Asal Sayılar konusunda izah edildi. $f(a_k; m_k) = \frac{a_k^{m_k}-1}{a_k-1}, (1 \le k \le n)$ biçiminde tanımlanan bir fonksiyon çarpımsal fonksiyondur. Gerçekten;

$$\begin{aligned} f\left(\prod_{k=1}^{n}(a_k;m_k)\right) &= f((a_1;m_1)(a_2;m_2)\cdots(a_n;m_n)) \\ &= \left(\frac{a_1^{m_1}-1}{a_1-1}\right)\left(\frac{a_2^{m_2}-1}{a_2-1}\right)\cdots\left(\frac{a_n^{m_n}-1}{a_n-1}\right) \\ &= \prod_{k=1}^{n}\left(\frac{a_k^{m_k}-1}{a_k-1}\right) \end{aligned}$$

$$= \prod_{k=1}^{n} f(a_k ; m_k)$$

dir.

2.13. Teorem: Eğer $2^k - 1$ sayısı asal ise $2^{k-1}(2^k - 1)$ sayısı mükemmel bir sayıdır.

İspat: Asal sayılar konusunda bahsedilen mükemmel sayı, bir sayısı bölenlerin toplamı üzerinde tanımlandığından çarpımsal fonksiyon uygulanabilir.

$$\begin{aligned} f(k) &= f\left((2^{k-1})(2^k - 1)\right) \\ &= f(2^{k-1}) \cdot f(2^k - 1) \\ &= \left(\frac{2^{k-1+1}-1}{2-1}\right)(2^k - 1 + 1) \\ &= (2^k - 1)(2^k) \\ &= 2f(k) \end{aligned}$$

sayısı mükemmel bir sayıdır.

Örnek: $2^5 - 1 = 31$ sayısı asal olduğuna göre

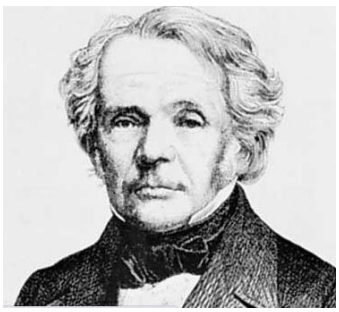
$$(2^{5-1})(2^5 - 1) = 496$$

sayısı mükemmel bir sayıdır. Gerçekten 496 sayısının bölenleri;

1, 2, 4, 8, 16, 31, 62, 124, 248, 496

olup bu sayıların toplamı 496 sayısının 2 katıdır.

MÖBİUS FONKSİYONU



August Ferdinand Möbius
17 Kasım 1790, Naumburg, Almanya-26 Eylül 1868, Leipzig, Almanya

2.2. Tanım: n pozitif bir tamsayı olmak üzere,

$$\mu(n)=\begin{cases} 1\ , & n=1 \\ 0\ , & p^2 \mid n, p \text{ asal} \\ (-1)^r, & n=p_1p_2\cdots p_r,\ (i\neq j, p_i\neq p_j) \end{cases}$$

fonksiyonuna **Möbius fonksiyonu** denir.

Örnek: $\mu(42)=\mu(2\cdot 3\cdot 7)=(-1)^3=-1$

$\mu(50)=\mu(2\cdot 5^2)=0$

Aşikar olarak eğer p bir asal sayı ise $\mu(p)=-1$; $k\geq 2$ için daima $\mu(p^k)=0$ dır.

2.14. Teorem: Möbius fonksiyonu çarpımsal bir fonksiyondur.

İspat: $OBEB(m;n)=-1$ ise $\mu(mn)=\mu(m)\cdot\mu(n)$ olduğunu göstermeliyiz.

i) m ve n sayılarından en az biri bir asal sayının karesi tarafından bölünüyorsa, p bir asal sayı olmak üzere eğer $p^2\mid m$ veya $p^2\mid n$ ise $p^2\mid mn$ olacagından

$$\mu(mn)=0=\mu(m)\cdot\mu(n)$$

dir.

ii) m ve n sayılarının her ikisinin de bir asal sayının karesi tarafından bölünmediğini kabul edelim. $OBEB(m;n)=1$ olduğundan p_i ve p_j ler birbirinden farklı asal sayılar olmak üzere,

$m=p_1p_2\cdots p_r$, $n=p_1p_2\cdots p_s$

şeklindedir. Bu durumda mn nin kanonik gösterilişi

$mn=p_1p_2\cdots p_rp_1p_2\cdots p_s$

şeklindedir. O halde

$$\begin{aligned}\mu(mn)&=\mu(p_1p_2\cdots p_rp_1p_2\cdots p_s)\\&=(-1)^{r+s}\\&=(-1)^r(-1)^s\\&=\mu(m)\cdot\mu(n)\end{aligned}$$

bulunur.

2.15. Teorem: $n\geq 1$ olan her n sayısı için

$$\sum_{d\mid n}\mu(d)=\begin{cases}1\ , n=1\\0\ , n>1\end{cases}$$

dir.

İspat: i) $n = 1$ için $\sum_{d|1}\mu(d) = \mu(1) = 1$ dir.

$n > 1$ olsun. $F(n) = \sum_{d|n}\mu(d)$ diyelim. μ fonksiyonu çarpımsal olduğundan $F(n)$ de çarpımsaldır.

ii) p, bir asal sayı olmak üzere, $n = p^k$ şeklinde olsun. p^k nın bütün pozitif bölenleri $1, p, \cdots, p^k$ gibi $(k+1)$ tane tamsayıdır. Böylece

$$\begin{aligned} F(p^k) &= \sum_{d|p^k}\mu(d) \\ &= \mu(1) + \mu(p) + \cdots + \mu(p^k) \\ &= \mu(1) + \mu(p) \\ &= 1 + (-1) \\ &= 0 \end{aligned}$$

dır.

iii) Eğer $n = p_1^{k_1}.p_2^{k_2}\cdots p_r^{k_r}$ şeklinde ise F fonksiyonu çarpımsal olduğundan $F(n) = F(p_1^{k_1}).F(p_2^{k_2})\cdots F(p_r^{k_r})$, i'ye göre $i = 1, 2, \cdots, r$ için $F\left(p_i^{k_i}\right) = 0$

sonuç olarak $F(n) = 0$ bulunur.

Örnek: $n = 60 = 2^2 \cdot 3 \cdot 5$ olsun.

$$\begin{aligned} \sum_{d|60}\mu(d) &= \mu(1) + \mu(2) + \mu(3) + \mu(2^2) + \mu(5) + \mu(6) + \mu(10) + \mu(12) + \\ &\mu(15) + \mu(20) + \mu(30) + \mu(60) \\ &= 1 + (-1) + (-1) + 0 + (-1) + 1 + 1 + 0 + 1 + 0 + (-1) + 0 \\ &= 0 \end{aligned}$$

2.16. Teorem (Möbius Ters Çevirme Formülü): F ve f doğal sayılar zerine tanımlı iki fonksiyon olsun. Eğer

$$F(n) = \sum_{d|n} f(d)$$

ise

$$f(n) = \sum_{d|n}\mu(d)F\left(\frac{n}{d}\right) = \sum_{d|n}\mu\left(\frac{n}{d}\right)F(d)$$

dir.

İspat: $\sum_{d|n}\mu(d)F\left(\frac{n}{d}\right)=\sum_{d|n}\left(\mu(d)\sum_{c|(n/d)}f(c)\right)=\sum_{d|n}\left(\sum_{c|(n/d)}\mu(d)f(c)\right)$ (1)

dir. Ayrıca $d|n$ ve $c|\left(\frac{n}{d}\right)$ ise $\frac{n}{d}=ct, t\in\mathbb{Z}^+$, böylece $n=cdt$, bu ise $c|n$ ve $d|\left(\frac{n}{c}\right)$ elde edilir. Bunun tersi de doğrudur. Sonuç olarak

$$d|n \text{ ve } c|\left(\frac{n}{d}\right)\Leftrightarrow c|n \text{ ve } d|\left(\frac{n}{c}\right)$$

dir. Bu durumda (1) eşitliğini

$$\sum_{d|n}\left(\sum_{c|(n/d)}\mu(d)f(c)\right)=\sum_{c|n}\left(\sum_{d|(n/c)}\mu(d)f(c)\right)=\sum_{c|n}\left(\sum_{d|(n/c)}\mu(d)\right) \quad (2)$$

şeklinde yazabiliriz. 2.13. teoreme göre $\sum_{d|(n/c)}\mu(d)$ toplamı, $\frac{n}{c}=1$ olması dışında sıfır, bu durumda, yani $n=c$ olması halinde ise 1'e eşittir. Böylece

$$\sum_{c|n}\left(f(c)\sum_{d|(n/c)}\mu(d)\right)=f(n)$$

bulunur. Diğer taraftan $d|n$ ise $n=dd'$ şeklinde yazılabilir. d, n'nin bütün pozitif bölenlerini dolaşırken d′ de n'nin bütün pozitif bölenlerini dolaşır. Böylece

$$f(n)=\sum_{d|n}\mu(d)F\left(\frac{n}{d}\right)=\sum_{d|n}\mu\left(\frac{n}{d}\right)F(d)$$

dir.

2.3. Sonuç: Bir sayının pozitif bölenleri sayısı τ, pozitif bölenleri toplamı σ ile gösterilmek üzere, her $n\geq 1$ için

i) $\sum_{d|n}\mu(d)\tau\left(\frac{n}{d}\right)=\sum_{d|n}\mu\left(\frac{n}{d}\right)\tau(d)=1$

ii) $\sum_{d|n}\mu(d)\sigma\left(\frac{n}{d}\right)=\sum_{d|n}\mu\left(\frac{n}{d}\right)\sigma(d)$

dir.

2.17. Teorem: F bir çarpımsal fonksiyon ve

$$F(n)=\sum_{d|n}f(d)$$

ise f çarpımsaldır.

İspat: m ve n, OBEB(m; n) = 1 olan pozitif tamsayılar olsun. mn'nin d gibi herhangi bir pozitif bölenin $d_1 \mid n, d_2 \mid n$, OBEB(d_1; d_2) = 1 olmak üzere, $d = d_1 d_2$ şeklinde tek türlü olarak yazılabildiğini görmüştük. Möbius Ters Çevirme Formülüne göre

$$f(mn) = \sum_{d|n} \mu(d) F\left(\frac{mn}{d}\right) = \sum_{d_1|m\,;\,d_{21}|n} \mu(d_1 d_2) F\left(\frac{mn}{d_1 d_2}\right) = f(m)\cdot f(n)$$

elde edilir. Yani f çarpımsaldır.

2.18. Teorem: $n = p_1^{k_1}.p_2^{k_2}\cdots p_r^{k_r}$ bir $n > 1$ tamsayısının asal çarpanlara ayrılışının kanonik şekli olsun. Eğer f, en az bir $n \in \mathbb{N}$ için $f(n) \neq 0$ olan, bir çarpımsal fonksiyon ise

$$\sum_{d|n} \mu(d)\cdot f(d) = (1 - f(p_1)).(1 - f(p_2))\cdots(1 - f(p_r))$$

dir.

İspat: $F(n) = \sum_{d|n} \mu(d)\cdot f(d)$ şeklinde tanımlanan F fonksiyonu çarpımsal olduğu aşikardır. O halde

$$\begin{aligned} F(n) &= F(p_1^{k_1}.p_2^{k_2}\cdots p_r^{k_r}) \\ &= F(p_1^{k_1})F(p_2^{k_2})\cdots F(p_r^{k_r}) \\ &= \left(\sum_{d|p_1^{k_1}} \mu(d)\cdot f(d)\right)\left(\sum_{d|p_1^{k_2}} \mu(d)\cdot f(d)\right)\cdots\left(\sum_{d|p_r^{k_r}} \mu(d)\cdot f(d)\right) \\ &= (f(1) - f(p_1)).(f(1) - f(p_2))\cdots(f(1) - f(p_r)), \quad (f(1) = 1) \\ &= (1 - f(p_1)).(1 - f(p_2))\cdots(1 - f(p_r)) \end{aligned}$$

elde edilir.

2.19. Teorem: Tanım kümesi doğal sayılardan oluşan f ve F, $F(n) = \sum_{d|n} f(d)$ biçiminde iki fonksiyon ise herhangi bir m doğal sayısı için

$$\sum_{n=1}^{m} F(n) = \sum_{n=1}^{m} f(k)\left[\frac{m}{k}\right]$$

dır.

İspat: $\sum_{n=1}^{m} F(n) = \sum_{n=1}^{m}\sum_{d|n} f(d)$ (1)

eşitliğin sağ tarafındaki toplamda, f(d) nin eşit değerler aldığı terimleri bir araya getirelim:

$1 \le k \le m$ olan bir k doğal sayısı için f (k) teriminin $\sum_{d|n} f(d)$ içinde yer alması ancak ve yalnız k'nın, n sayısının böleni olması ile mümkündür. Her tamsayı kendi kendisinin bir böleni olduğundan (1) eşitliğinin sağ tarafı $1 \le k \le m$ olan bir k doğal sayısı için f (k) terimini en az bir kere içerir. Simdi içinde f (k) terimini içeren $\sum_{d|n} f(d)$ toplamlarının sayısını hesaplayalım. Bunun için $1, 2, \cdots, m$ tamsayıları içinde k ile bölünenlerin sayısını bulmak yeterlidir, ki bunlar $k, 2k, \cdots, \left(\frac{m}{k}\right)k$ olmak üzere $\left(\frac{m}{k}\right)$ tanedir. Böylece f (k) , m'den küçük veya m'ye eşit, $\left(\frac{m}{k}\right)$ tane farklı pozitif tamsayı için $\sum_{d|n} f(d)$ toplamının bir terimidir. Böylece

$$\sum_{n=1}^{m} F(n) = \sum_{n=1}^{m} \sum_{d|n} f(d) = \sum_{k=1}^{m} f(k) \left[\frac{m}{k} \right]$$

olur.

EULER'İN $\emptyset$ FONKSİYONU

2.3. Tanım: $n \in \mathbb{Z}^+$ olsun. n'den küçük ve n ile aralarında asal olan pozitif tamsayıların sayısı $\emptyset(n)$ ile gösterilir ve $\emptyset$ fonksiyonuna **Euler fonksiyonu** denir. Yani $n > 1$ olsun. $OBEB(k; n) = 1$ ve $1 \le k < n$ şartını sağlayan k tamsayılarının sayısı $\emptyset(n)$ dir.

Örneğin $\emptyset(2) = 1, \emptyset(3) = 2, \emptyset(4) = 2, \emptyset(5) = 4, \emptyset(6) = 3, \cdots$ Eğer $n = p$ bir asal sayı ise p'den küçük her tamsayı p ile aralarında asal olacağından $\emptyset(p) = p - 1$ olur.

Diğer taraftan eğer $n > 1$ olan bir bileşik tamsayı ise n'nin $1 \le \ell < n$ olan ℓ gibi bir böleni var olduğundan, n ile aralarında asal olmayan ve n'den büyük olmayan en az iki tamsayı (ℓ ve n) vardır. O halde $\emptyset(n) \le n - 2$ dir. Buna göre $n > 1$ olan bir tamsayının asal olması ancak ve yalnız $\emptyset(n) = n - 1$ olması ile mümkündür.

2.4. Tanım: $n > 1$ olmak üzere, n ile aralarında asal ve mod n ye göre kongrü olmayan $\emptyset(n)$ tane tamsayının oluşturduğu sisteme **bir mod n ye indirgenmiş kalan sistemi** denir.

Böylece n'den küçük n ile aralarında asal olan bütün pozitif tamsayılar mod n ye göre bir indirgenmiş kalan sistemi oluştururlar.

2.1. Lemma: Eğer $a_1, a_2, \cdots, a_{\emptyset(n)}$ mod n bir indirgenmiş kalan sistemi ise bu sayılar belirli bir sırada, mod n ye göre, n'den küçük ve n ile aralarında asal olan pozitif tamsayılara kongrüdürler.

İspat: Her bir a_i için, $a_i \equiv b_i \pmod n$ ve $0 < b_i < n$ olacak şekilde, b_i gibi bir tamsayı vardır. Öte yandan $OBEB(a_i;\ n) = 1$ olduğundan $OBEB(b_i;\ n) = 1$ olmak zorundadır ve $a_1, a_2, \cdots, a_{\emptyset(n)}$ ler mod n ye göre kongrü olmadığından $b_1, b_2, \cdots, b_{\emptyset(n)}$ ler, n'den küçük ve n ile aralarında asal olan bütün pozitif tamsayılardan ibarettir.

2.20. Teorem: $n > 1$ olmak üzere, eğer $a_1, a_2, \cdots, a_{\emptyset(n)}$ mod n bir indirgenmiş kalan sistemi ve $OBEB(a;\ n) = 1$ ise $aa_1, aa_2, \cdots, aa_{\emptyset(n)}$ de mod n bir indirgenmiş kalan sistemidir.

İspat: $aa_1, aa_2, \cdots, aa_{\emptyset(n)}$ tamsayılarından herhangi ikisi mod n ye göre kongrü değildirler. Gerçekten eğer $1 \le i < j < \emptyset(n)$ için $aa_i \equiv aa_j \pmod n$ ise $OBEB(a;\ n) = 1$ olduğundan $a_i \equiv a_j \pmod n$ bulunur. Bu ise $a_1, a_2, \cdots, a_{\emptyset(n)}$ mod n bir indirgenmiş kalan sisitemi olması ile çelişir. Ayrıca $1 \le i < \emptyset(n)$ için $OBEB(a_i;\ n) = 1$ ve $OBEB(a;\ n) = 1$ olduğundan $OBEB(aa_i;\ n) = 1$ dir. Verilen sayı takımı, n ile aralarında asal ve mod n ye göre kongrü olmayan $\emptyset(n)$ tane tamsayıdan oluştuğuna göre mod n bir indirgenmiş kalan sistemidir.

2.21. Teorem (Euler Teoremi): Eğer $n > 1$ ve $OBEB(a;\ n) = 1$ ise $a^{\emptyset(n)} \equiv 1 \pmod n$ dir.

İspat: $n > 1$ alabiliriz. $a_1, a_2, \cdots, a_{\emptyset(n)}$, ile n'den küçük ve n ile aralarında asal olan bütün pozitif tamsayıları gösterelim. Bunlar mod n ye göre bir indirgenmiş kalan sistemi oluştururlar. Çarpımsal fonksiyon tanımına göre $OBEB(a;\ n) = 1$ olduğundan $aa_1, aa_2, \cdots, aa_{\emptyset(n)}$ de mod n bir indirgenmiş kalan sistemidir ve bu sayılar belirli bir sırada alındıklarında, mod n ye göre, $aa_1, aa_2, \cdots, aa_{\emptyset(n)}$ sayılarına kongrüdürler. Böylece

$$aa_1 \cdot aa_2 \cdots aa_{\emptyset(n)} \equiv a_1 \cdot a_2 \cdots a_{\emptyset(n)} \pmod n$$

$$a^{\emptyset(n)} a_1 \cdot a_2 \cdots a_{\emptyset(n)} \equiv a_1 \cdot a_2 \cdots a_{\emptyset(n)} \pmod n \qquad (1)$$

elde edilir. $1 \le i < j < \emptyset(n)$ için $OBEB(a_i;\ n) = 1$ olduğundan

$$\text{OBEB}(a_1 a_2 \cdots a_{\emptyset(n)};\ n) = 1$$

dir. Böylece (1) den

$$a^{\emptyset(n)} \equiv 1 \pmod{n}$$

elde edilir.

2.4. Sonuç (Fermat Teoremi): p, $p \nmid a$ olan bir asal sayı ise $a^p \equiv a \pmod{p}$ dir.

Örnek: $p = 7$ alalım. $(-2)^7 = -128 = (-19)\cdot 7 + 5$ olup

$$-128 \equiv 5 \equiv -2 \pmod{7}$$

dir.

2.22. Teorem: Eğer p bir asal sayı ve $k > 0$ ise

$$\emptyset(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right) = p^{k-1}(p-1)$$

dir.

İspat: $\text{OBEB}(n;\ p^k) = 1 \Leftrightarrow \text{OBEB}(n,p) = 1$

olduğu göz önüne alınırsa $1 \le n < p^k$ olan tamsayıları arasında p ile bölünebilen

$$p,\ 2p, 3p, \cdots, p^k p$$

gibi p^{k-1} tane tamsayı vardır. Böylece $1 \le n < p^k$ olan ve p^k ile aralarında asal olan tamsayıların sayısı $\emptyset(p^k) = p^k - p^{k-1}$ dir. //

Örnek: $\emptyset(9) = 3(3-1) = 6$ dır. Gerçekten de 9'dan küçük ve 9 ile aralarında asal olan sayılar 1, 2, 4, 5, 7, 8 den ibarettir.

2.23. Teorem: Euler'in $\emptyset$ fonksiyonu çarpımsaldır.

İspat: $\text{OBEB}(m;\ n) = 1$ için $\emptyset(mn) = \emptyset(m)\emptyset(n)$ olduğunu gösterelim: $\emptyset(1) = 1$ olduğundan m ve n'den en az birinin 1 olması halinde teorem dogrudur.

$m > 1, n > 1$ olduğunu kabul edelim. Aşağıdaki şekilde mn tane ardışık tamsayıdan oluşan tabloyu göz önüne alalım:

$$0 \qquad 1 \qquad 2 \qquad \cdots \qquad m-1$$

$$\begin{array}{ccccc} m & m+1 & m+2 & \cdots & m+m-1 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ (n-1)m & (n-1)m+1 & (n-1)m+2 & \cdots & (n-1)m+m-1 \end{array}$$

Bu tablodaki sayılar mod mn bir tam kalan sistemi oluştururlar ve bunların içinden $\emptyset(mn)$ tanesi mn ile aralarında asaldır. İlk sıradaki sayılar mod m bir tam kalan sistemi oluşturur. Herhangi bir sütundaki sayılar ise, mod m ye göre birbirine kongrüdürler. $OBEB(qm+r;\ m) = OBEB(r;\ m)$ olduğundan herhangi bir $r+1$–inci sütundaki sayıların m ile aralarında asal olabilmesi için $OBEB(r;\ m) = 1$ olması gerekir. Bu nedenle m ile aralarında asal olan sayıları bulunduran sütunların sayısı $\emptyset(m)$ tanedir ve bu sütünda yer alan sayıların tamamı m ile aralarında asaldır. Ayrıca $OBEB(r;\ m) = 1$ olan bir $r+1$–inci sütundaki sayılar

$$r,\ m+r, 2m+r, \cdots, (n-1)m+r$$

$OBEB(m;\ n) = 1$ olduğundan Modüler Aritmetik konusundaki 6.8. teoreme göre bu sayılar mod n bir tam kalan sistemi oluştururlar. Bu nedenle bu sütunda n ile aralarında asal olan tam $\emptyset(n)$ tane sayı vardır. O halde yukarıdaki tabloda hem m hem de n ile aralarında asal olan sayıların sayısı $\emptyset(m)\emptyset(n)$ dir. Ayrıca $OBEB(a;\ mn) = 1$ olması ancak ve yalnız $OBEB(a;\ m) = 1$ ve $OBEB(a;\ n) = 1$ olması ile mümkündür. Bu nedenle mn ile aralarında asal olan sayıların sayısı $\emptyset(mn) = \emptyset(m)\emptyset(n)$ dir.

2.24. Teorem: Eğer $n > 1$ tamsayısının asal çarpanlara ayrılışının kanonik şekli $n = p_1^{k_1}.p_2^{k_2}\cdots p_r^{k_r}$ ise

$$\emptyset(n) = n\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right) = \prod_{i=1}^{r} p_i^{k_i-1}(p_i-1)$$

dir.

Bu teoremin ispatı aşikâr olduğundan okuyucuya bırakılmıştır.

Örnek: $\emptyset(4\ 725) = \emptyset(3^3\cdot 5^2\cdot 7)$

$$\begin{aligned} &= 4\ 725\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right) \\ &= 3^2(3-1)5(5-1)(7-1) \\ &= 2\ 160 \end{aligned}$$

2.25. Teorem (Gauss Teoremi): Herhangi bir $n \geq 1$ tamsayısı için

$$n = \sum_{d|n}\phi(d)$$

dir.

İspat: $\{1, 2, \cdots, n\}$ kümesi üzerinde

$$m_1 \approx m_2 \Leftrightarrow OBEB(m_1; n) = OBEB(m_2; n)$$

şeklinde tanımlanan bağıntı bir eşdeğerlik bağıntısıdır ve bu bağıntı $\{1, 2, \cdots, n\}$ kümesini aşağıdaki şekilde tanımlanan sınıflara ayırır:

d, n'nin pozitif bir böleni ve $1 \leq m \leq n$ olmak üzere, $OKEK(m;\ n) = d$ ise $m \in S(d)$, yani

$$S(d) = \{m \mid OBEB(m; n) = d;\ 1 \leq m \leq n\}$$

dir. $OBEB(m; n) = d \Leftrightarrow OBEB\left(\frac{m}{d}, \frac{n}{d}\right) = 1$ olduğundan her bir S(d) sınıfına ait tamsayıların sayısı, $\frac{n}{d}$ den küçük ve $\frac{n}{d}$ ile aralarında asal olan pozitif tamsayıların sayısı $\emptyset\left(\frac{n}{d}\right)$ ye eşittir. Ayrıca $\{1, 2, \cdots, n\}$ kümesine ait her tamsayı tam bir S(d) sınıfında bulunduğundan

$$n = \sum_{d|n} |S(d)| = \sum_{d|n} \left|\phi\left(\frac{n}{d}\right)\right|$$

elde edilir. Diğer taraftan d, n'nin bütün pozitif bölenlerini dolaşırken, $d' = \frac{n}{d}$ de n'nin bütün pozitif bölenlerini dolaşır. Buna göre;

$$n = \sum_{d|n} \left|\phi\left(\frac{n}{d}\right)\right| = \sum_{d|n} \phi(d)$$

elde edilir.

Örnek: $n = 15$ olsun. $k \mid 15$ ise $k \in \{1, 3, 5, 15\}$ olabilir. Böylece

$S(1) = \{m \mid OBEB(m; 15) = 1; 1 \leq m \leq 15\} = \{1, 2, 4, 7, 8, 11, 13, 14\}$, $|S(1)| = 8$

$S(3) = \{m \mid OBEB(m; 15) = 3; 1 \leq m \leq 15\} = \{3, 6, 9, 12\}$, $|S(3)| = 4$

$S(5) = \{m \mid OBEB(m; 15) = 5; 1 \leq m \leq 15\} = \{5, 10\}$, $|S(5)| = 2$

$S(15) = \{m \mid OBEB(m; 15) = 15; 1 \leq m \leq 15\} = \{15\}$, $|S(15)| = 1$

$$\sum_{d|5} \phi(d) = \emptyset(15) + \emptyset(5) + \emptyset(3) + \emptyset(1) = 8 + 4 + 2 + 1 = 15$$

bulunur.

2.26. Teorem: $n > 1$ tamsayısı için n'den küçük ve n ile aralarında asal olan bütün pozitif tamsayıların toplamı $\frac{1}{2}$ $n\ \emptyset(n)$ sayısına eşittir.

İspat: $a_1, a_2, \cdots, a_{\emptyset(n)}$, n'den küçük ve n ile aralarında asal olan bütün pozitif tamsayılar olsunlar.

$$OBEB(a;n) = 1 \Leftrightarrow OBEB(n-a;n)$$

olduğundan, $n-a_1, n-a_2, \cdots, n-a_{\emptyset(n)}$ sayıları bir başka sırada alındıkları taktirde $a_1, a_2, \cdots, a_{\emptyset(n)}$ sayılarına eşittirler. Böylece

$$a_1 + a_2 + \cdots + a_{\emptyset(n)} = n - a_1 + n - a_2 + \cdots + n - a_{\emptyset(n)}$$
$$= \emptyset(n) \cdot n - (a_1 + a_2 + \cdots + a_{\emptyset(n)})$$

ve

$$2(a_1 + a_2 + \cdots + a_{\emptyset(n)}) = \emptyset(n) \cdot n$$
$$a_1 + a_2 + \cdots + a_{\emptyset(n)} = \frac{1}{2}\, n\, \emptyset(n)$$

bulunur.

ÇÖZÜMLÜ ALIŞTIRMALAR

1. $\mathbb{Z}_{/11}$ de tanımlı,

$$f(x) = \overline{7} \cdot x + \overline{6}$$

fonksiyonuna göre, $f^{-1}(x)$ aşağıdakilerden hangisine eşittir?

A) $\overline{7} \cdot x + \overline{3}$ B) $\overline{7} \cdot x + \overline{5}$ C) $\overline{7} \cdot x + \overline{10}$ D) $\overline{8} \cdot x + \overline{4}$ E) $\overline{8} \cdot x + \overline{8}$

Çözüm: Önce x yerine y, y yerine x yazalım.

$$x = \overline{7} \cdot y + \overline{6}$$

olur. $\mathbb{Z}_{/11}$ de $\overline{6} + \overline{5} = \overline{0}$ olduğuna göre

$$x + \overline{5} = \overline{7} \cdot y + \overline{6} + \overline{5}$$
$$x + \overline{5} = \overline{7} \cdot y + \overline{0}$$
$$x + \overline{5} = \overline{7} \cdot y$$

elde edilir. $\mathbb{Z}_{/11}$ de $\overline{7} \cdot \overline{8} = \overline{1}$ olduğuna göre

$$\overline{8}(x + \overline{5}) = \overline{8} \cdot \overline{7} \cdot y$$
$$\overline{8}x + \overline{8} \cdot \overline{5} = \overline{1} \cdot y$$
$$\overline{8}x + \overline{8} = y$$
$$f^{-1}(x) = \overline{8}x + \overline{8}$$

bulunur.

Cevap: E

2. $\mathbb{Z}/4$ de,

+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

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

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

Verile tabloda $(x+\bar{3})\bullet(y+\bar{2})=1$ olduğuna göre xy nin değeri nedir?

A) $\bar{0}$ B) $\bar{1}$ C) $\bar{2}$ D) $\bar{3}$ E) Çözüm yok

Çözüm: $(x+\bar{3})\bullet(y+\bar{2})=\bar{1}$

$x+\bar{3}=\bar{1}$ ve $y+\bar{2}=\bar{1}$

$x=\bar{2}$ ve $y=\bar{3}$

$xy=\bar{2}\bullet\bar{3}=\bar{2}$

Cevap: E

KAYNAKÇA

1. Doç. Dr. Sebahattin BALCI, Modern Cebire Giriş, Ankara Üniversitesi, Fen Fakültesi Döner Sermaye İşletmeleri Yayınları: 15, 1993, ANKARA.
2. Doç. Dr. Neşe YELKENKAYA, Sayılar Teorisi Ders Notları, İstanbul Kültür Üniversitesi, İnternet Ders Notları, 2020.
3. Prof. Dr. Bülent KARAKAŞ, Yrd. Doç. Dr. Hacı AKTAŞ, Sayılar Teorisi, Gaziosmanpaşa Üniversitesi Yayınları, Tokat, 1998.
4. Sait AKKAŞ, H. Hilmi HACISALİHOĞLU, Zühtü ÖZEL, Arif SABUNCUOĞLU, Soyut Matematik**,** 4. Baskı, 2010, Ankara.
5. Doç. Dr. Mustafa Bayraktar, Soyut Cebir ve Sayılar Teorisi, Atatürk Üniversitesi Basımevi, 1988, Erzurum.
6. Prof. Dr. H.İbrahim Karataş, Soyut Cebir, TÜBA, 2010, Ankara.
7. Soyut Cebir ve Sayılar Teorisi-Çözümlü Problemlerle, Prof. Dr. Mehmet ERDOĞAN Yrd. Doç. Dr. Gülşen YILMAZ, Beykent Üniversitesi Yayınevi, 2008, İstanbul.