ASAL SAYILAR DENİZİNDE GEZİNTİ

Nesrin Tutaş
Akdeniz Üniversitesi, Matematik Bölümü,
07058-ANTALYA

---

1 'den büyük bir tamsayının 1 ve kendisinden başka pozitif böleni yoksa, bu sayıya asal, aksi halde bileşik sayı denir. $n \in \mathbb{N}$ için n-inci asal sayıyı p_n ile gösterirsek, $p_1 = 2, p_2 = 3, p_{99} = 523$ ve $p_{303} = 1999$ 'u örnek verebiliriz. Bu nedenle, pozitif tamsayıları üç sınıfa ayırabiliriz:

Asal sayılar: $2, 3, 5, 7, 11, 13, 17, 19, 23, ...$

Bileşik sayılar: $4, 6, 8, 9, 10, 12, ...$ ve 1.

Bir sayı kümesi ile ilgilenilirken sorulan; "Kaç tane elemanı vardır?", "Verilen bir sayının bu kümenin elemanı olup olmadığı nasıl belirlenir?", "Bir aralıkta nasıl davranırlar?", "Onları tanımlayan fonksiyonlar var mıdır?" gibi sorular asal sayılar kümesi için de sorulmuştur. Bunların sonucu olarak, Euclid 'in asal sayıların sonsuz olduğunu ispatlamasından bu güne kadar bir çok problem ortaya konulmuş ve bunların bazıları hala çözülememiştir.

Bu yazıdaki amacımız: asal sayıların doğasında var olan gizem ve muhteşemliğin keşfedilişini, yapılan çalışmalarda elde edilen sonuçlar ile çözülemeyen problemlerden bir kaçını tanıtmak olacaktır. Euler 'in şu sözü ile başlayalım: "Asal sayılar yalnız sonsuz çoklukta değil, kare sayılar kadar da dağınık değildir." Euclid'in, yukarıda sözü edilen ve bilinen ispatı oldukça basit olmasına rağmen asallar hakkında fazla bilgi vermemektedir. Elbette, Euclid 'den sonra da yeni ispatlar yapılmıştır. Kummer (1878) Euclid 'in, Shorn da Polya' nın ispatına benzer ispatlar vermiş, Washington ispatında (1980) değişmeli cebir kavramlarını , Fürstengberg ise topolojik fikirler kullanmıştır (1955). Bu ispatlardan ilginç sayılabilecek iki tanesini burada tekrarlayalım.

Polya'nın ispatı:

$$1 < a_1 < a_2 < a_3 < \ldots$$

olacak biçimde aralarında asal sonsuz çoklukta sayı bulunması fikrine dayanır. Eğer p_1, a_1'i; p_2, a_2 'yi; ... ; p_n, a_n 'yi, . . . , bölen asal sayılar ise $p_1, p_2, \ldots, p_n, \ldots$ hepsi farklı asal sayılar olacaktır.

İspat için a_n sayıları Fermat sayıları $F_n = 2^{2^n} + 1$ $(n \geq 0)$ seçilebilir. Şöyle ki, m üzerinde tümevarımla,

$$F_m - 2 = F_0 F_1 ... F_{m-1}$$

olduğunu görmek kolaydır. Böylece, $n < m$ ise, F_n; $F_m - 2$ 'yi böler. p, F_n ve F_m 'yi bölen bir asal sayı ise $F_m - 2$ ve F_m 'yi de böler, dolayısıyla 2 'yi de bölmelidir. Bu nedenle, $p = 2$ 'dir. Ama F_n, tek sayı olduğundan 2 ile bölünemez. Böylece, Fermat sayılarının aralarında asal olduğunu göstermiş olduk ki bu ispat için yeterlidir.

Diğer bir ispat da Euler 'in ispatıdır. p asal ise, $\frac{1}{p} < 1$; böylece,

$$\sum_{k=0}^{\infty} \frac{1}{p^k} = \frac{1}{1 - \frac{1}{p}}$$

'dir. q başka bir asal sayı ise de benzer bir ifade geçerlidir. Bu iki seriyi çarparsak,

$$1 + \frac{1}{p} + \frac{1}{q} + \frac{1}{p^2} + \frac{1}{pq} + \frac{1}{q^2} + \ldots = \frac{1}{1 - \frac{1}{p}} \frac{1}{1 - \frac{1}{q}}$$

elde edilir. Burada, sol taraf $p^h q^k$, $h \geq 0$, $k \geq 0$ formunda tek türlü yazılan doğal sayıların terslerinin toplamıdır. İspatın temel fikri budur. Kabul edelim ki, $p_1, p_2, \ldots, p_n$, tüm asal sayılar olsun. $i = 1, \ldots, n$ için

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

Bu eşitliklerin n tanesini çarparsak,

$$\Pi_{i=1}^{n} \left(\sum_{k=0}^{\infty} \frac{1}{p_i^k}\right) = \Pi_{i=1}^{n} \frac{1}{1 - \frac{1}{p_i}}$$

elde edilir ve buradaki toplam tüm doğal sayıların terslerinin toplamıdır. Sol taraftaki toplam ıraksak, sağ taraf yakınsaktır ki bu bir çelişkidir. O halde, asal sayılar sonsuz çoklukta olmalıdır.

$x \in \mathbb{R}$, $x > 0$ olmak üzere $p < x$ olan tüm p asal sayılarının sayısını $\pi(x)$ ile göstereceğiz. $\pi(x)$ 'e asal sayma fonksiyonu denir. $f(x)$ ile $h(x)$, $x > 0$ için tanımlı ve reel değerli pozitif sürekli fonksiyonlar olsun. $\lim_{x\to\infty} \frac{f(x)}{h(x)} = 1$ ise, $f(x)$ ve $h(x)$ asimptotik eşittir denir ve $f(x) \sim h(x)$ yazılır. $\pi(x)$ fonksiyonu ile ilgili ilk ciddi çalışma Legendre tarafından yapılmıştır. Çalışmaları sonunda 1798-1808 'de $\lim_{x\to\infty} A(x) = 1,08366...$ olmak üzere

$$\pi(x) = \frac{x}{\log x - A(x)}$$

tahminini ortaya atmış, fakat yaklaşık 40 yıl sonra Tschebycheff tarafından tahminin yanlış olduğu gösterilmiştir. Gauss 15 yaşında, $\pi(x)$ 'in $Li(x) = \int_0^x \frac{dt}{\log t}$ ile tanımlanan x 'in logaritmik integraline asimtotik eşit olduğunu iddia etmiştir. 1850 'lerde Tschebycheff elemanter metotlarla,

$$0 < c' < 1 < c\,,$$

$$c'\frac{x}{\log x} < \pi(x) < c\frac{x}{\log x}, \quad (x \geq 2)$$

olacak biçimde c, c' sabitlerinin varlığını ve c, c' değerlerinin aslında 1 'e yaklaştığını göstermiştir.

$$c' = \frac{2^{1/2}3^{1/3}5^{1/5}}{30^{1/30}} = 0,92129...,$$

$$c = \frac{6}{5}c' = 1,10555...$$

1859 'da zeta fonksiyonu için fonksiyonel eşitlikler yazan Riemann daha sonraları $\pi(x)$ fonksiyonunu bu eşitliklerle ifade etmiş ve Temel Asal Sayı Teoremi:

$$\pi(x) \sim \frac{x}{\log x}$$

'in ispatı için bir çok araç bırakmıştır. Asal Sayı Teoremi "en çok çözülmek istenen teorem" statüsündeydi, kim tarafından çözüleceği, kime "ölümsüzlük" kazandıracağı bir folklor idi. Teorem birbirinden habersiz, tanınmış iki analizci tarafından aynı yıl çözüldü (1896). Fakat, onlar da ölümsüz olamadılar. Hadamard 98, la Valle'e Poussin 96 yıl yaşadı.

Bertrand 'ın 1845 'de yaptığı bir gözlem:

"$n \geq 2$ ve $2n$ arasında daima bir asal sayı vardır"

denk olarak,

$$\pi(2n) - \pi(n) \geq 1, \quad n \geq 2$$

ya da

$$p_{n+1} < 2p_n, \quad (n \geq 1)$$

olarak ifade edilebilir. Bu ifade "Bertrand Postulatı" olarak bilinir ve doğruluğu 1852' de Tschebycheff tarafından gösterilmiştir. Daha genel olarak, her $\lambda > 1, x = x(\lambda) > 1$ için

$$\pi(\lambda x) - \pi(x) > c\frac{x}{\log x}$$

olduğu 1949 'da Erdös tarafından ispatlanmıştır. $\pi(x)$ fonksiyonunun ispatlanan bir kaç özelliğini şöyle sıralayalım:

* $x \geq y \geq 2,\ y \geq 6 \Rightarrow \pi(xy) > \pi(x) + \pi(y)$ (Ishikawa, 1934)

* $\pi(x+y) \leq \pi(x) + \frac{2y}{\log y}$ (Vaughan)

veya

* $\pi(x+y) \leq \pi(x) + 2\pi(y)$.

Aşağıdaki iddialar ise hala ispatlanmayı beklemektedirler.

*

"$n > 1$ için $\pi(n^2+n) > \pi(n^2) > \pi(n^2-n)$."

(Opperman, 1882)

*

"$n \geq 2,\ \pi(p_{n+1}^2) - \pi(p_n^2) \geq 4$."

(Brocard, 1904)

Temel Asal Sayı Teoreminden $p_n \sim n \log n$, yani $\lim_{n\to\infty} \frac{p_n}{n \log n} = 1$ olduğu görülebilir. p_n ile ilgili ispatlanan bazı özellikleri şöyle sıralayabiliriz:

*

$$n \log n + n(\log\log n - 10) < p_n$$
$$< n \log n + n(\log\log n + 8)$$

(Rosser, 1938)

*

$$n \geq 2 \text{ ise, } p_n + p_{n+1} > p_{n+2}$$

(Ishikawa, 1934)

*

$$m, n \geq 1 \text{ ise, } p_m p_n > p_{n+m}$$

(Ishikawa)

*

1979 'da Pomerance, Selfridge tahminini ispatladı: "Her pozitif sayı $i < n$ için $p_n^2 > p_{n-i}p_{n+i}$ olacak biçimde sonsuz çoklukta n tamsayısı vardır. Hatta, her $i < n$ için $2p_n > p_{n-i}p_{n+i}$ olacak biçimde sonsuz çoklukta n vardır."

İki ardışık asal sayı arasındaki fark; $d_n = p_{n+1} - p_n$, üzerinde hala soru işareti bulunan bir çok problemin temeli olmuştur. $d_1 = 1$ ve $n \geq 2$ için d_n çift tamsayıdır. d_n ne kadar büyük seçilebilir?

Rankin, sonsuz çoklukta n için

$$d_n > \frac{c \ln n \ \ln\ln n \ \ln\ln\ln n}{(\ln\ln\ln n)^2}$$

olduğunu göstermiş ve Erdös, c sabitinin yeterince büyük alınabileceğini gösterene 10000$ vaad etmiştir. Rankin 'nin en iyi yaklaşımı, γ Euler sabiti olmak üzere $c = e^\gamma$ 'dır.

d_n ile ilgili en meşhur tahminlerden birisi Twin Primes Conjecture 'dır (İkiz Asallar Tahmini). p ve $p+2$ asal sayılar ise, twin prime (ikiz asal) olarak isimlendirilirler. İkiz asal sayı çiftlerine örnek olarak $(3,5)$, $(5,7)$, $(11,13)$ ve $(17,19)$ verilebilir. 1949 'da Clement ikiz asalların belirlenmesi için kullanılabilecek bir kriter ispatlamış:

" n, $n+2$ ikiz asal sayı çifti
$\Leftrightarrow 4[(n-1)! + 1] + n \equiv 0 \ (mod\ n(n+2))$."

Bununla beraber, bu kriter ikiz asalların belirlenmesi için pratik değildir. Asıl soru: "İkiz asal sayılar sonsuz çoklukta mıdır?" 'dır. Bu soru ikiz asallar tahmini olarak bilinir.

Her $x > 1$ için $\pi_2(x)$ 'in p ve $p+2 < x$ olan asal sayıların sayısını gösterdiğini kabul edelim. $\pi_2(x)$ fonksiyonu ile ilgili en ilginç sonuçları Brun 1920 'de ispatlamıştır. Bunlardan bir kaçını şöyle sıralayabiliriz:

* "Öyle $x_0 \in \mathbf{R}$ vardır ki $x \geq x_0$ ise, $\pi_2(x) < \frac{100x}{(\log x)^2}$."

* "Her $m \geq 1$ için ikiz asal olmayan m tane ardışık asal sayı vardır."

Hardy & Littlewood 1923 'de

$$\pi_2(x) \leq 2.c \ \Pi_{p>2}(1 - \frac{1}{(p-1)^2}) \frac{x}{(\log x)^2}$$

ifadesinde $c = 1$ tahmininde bulundular. c değeri için elde edilen en iyi sonuç $c = 3,13$ 'tür. $c_2 = \Pi_{p>2}(1 - \frac{1}{(p-1)^2})$ değeri ikiz asal sabiti olarak bilinir ve Wrench tarafından 1961 'de $c_2 = 0,66016...$ olarak hesaplanmıştır. $\pi_2(x)$ için bilinen en büyük değer 1976 'da Brent tarafından $\pi_2(10^{11}) = 224376048$ olarak elde edilmiştir. Bilinen en büyük ikiz asal sayı çiftleri; B. Parady, J. Smith ve S. Zarantanelle 'nin hesapladığı $1706595 \times 2^{11235} \pm 1$ ve $571305 \times 2^{7701} \pm 1$ 'dir. Fakat, asıl sorunun cevabı hala verilememiştir.

Goldbach 1742 'de Euler 'e yazdığı bir mektupta,

(G) "Her $n > 5$ tamsayısı üç asal sayının toplamı olarak yazılabilir."

iddiasında bulunmuş, Euler ise cevabında bu iddianın,

(G′) "Her $2n \geq 4$ çift tamsayısı iki asal sayının toplamıdır."

önermesi ile denk olduğunu belirtmiştir. (G) ile (G′) 'nün denk olduğunu görmek oldukça basittir:

(G′) $\Rightarrow$(G): (G′) 'nün doğru olduğu kabul edilir ve p, p' asal sayılar olmak üzere $2n \geq 6$ ise, $2n - 2 = p+p'$, $2n = p+p'+2$. Hatta, $2n+1 = 3+p+p'$ 'dür ki bu (G) 'yi ispatlar.

(G) $\Rightarrow$(G′): (G) doğru kabul edilir ve p, p', p''

asal sayılar olmak üzere $2n \geq 4$ ise, $2n + 2 = p + p' + p''$ 'dür. Buradan, $p'' = 2$ ve $2n = p + p'$ olur.

Burada sözü edilen (G) veya (G′) Goldbach Conjecture (Goldbach Tahmini) olarak bilinir. (G′) 'nün sonsuz çoklukta çift tamsayı için doğru olduğu aşikardır, $2p = p + p$. Bu tahmin ile ilgili elde edilen ilk önemli sonuç Hardy & Littlewood 'undur:

"Öyle n_0 sayısı vardır ki her $n \geq n_0$ tek sayısı üç asal sayının toplamıdır."

1937 'de Vinogradov sözü edilen n_0 sayısını 3^{15} olarak hesaplamıştır. $k = \sum_{i=1}^{r} e_i$ olmak üzere bir $n = \sum_{i=1}^{r} p^{e_i}$ doğal sayısına k-asalımsı (k-almost prime) denir ve k-asalımsı sayılar kümesi P_k ile gösterilir. Golbach tahmini ile ilgili olarak en iyi sonuçlar Chen 'nin elde ettikleridir. Bunlardan bazıları şunlardır:

"p asal ve $m \in P_2$ olmak üzere yeterince büyük her çift tamsayı $p + m$ biçiminde yazılabilir."

"Sonsuz çoklukta p asal sayısı için $p + 2 \in P_2$ 'dir."

"$2k \geq 2$ için $p + 2k \in P_2$ olacak biçimde sonsuz çoklukta p asal sayısı vardır."

1959 'da Schinzel, Goldbach tahmininin "her $n > 17$ tamsayısı üç farklı asal sayının toplamı olarak yazılabilir" önermesi ile denk olduğunu göstermiştir. 1940 'da Nipping 100000 'e kadar olan tamsayılar için Goldbach tahmininin doğru olduğunu göstermiştir. Aşağıdaki tabloda elde edilen benzer sonuçların listesini veriyoruz. Fakat problemimiz hâla çözülememiştir:

Adı	Yıl	Üst Sınır
M. K. Shen	1964	$3,3 \times 10^7$
M. L. Stein, P. R. Stein	1965	10^8
A. Graville, J. V. D. Lune, H. J. J. te Reile	1989	2×10^{10}
M. Sinisalo	1993	4×10^{11}
J. M. Deshouillers, H. J. J. te Reile, Y. Saouter	1998	10^{14}

KAYNAKLAR

[1] Paulo Ribenboim, The Little Book of Big Primes, Springer-Verlag, 1991.

[2] Richard K. Guy, Unsolved Problems on Number Theory, 1980.

[3] The Prime Glossary.