ASAL SAYI TEOREMİ VE ÖNCESİ

Artık kalemi kağıdı bir kenara bırakın ve asal sayılara cebirsel bir formül aramaktan vazgeçin. Çünkü hiç bir polinomun sürekli asal sayı üretemeyeceği ispatlandı bile! Ama bu hevesinizi kırmasın çünkü asal sayılar henüz cevabı verilmemiş ve ifadeleri basit pek çok sorunun bulunduğu kocaman bir dünya. 2500 yıldır yani insanlar sayı saymaya başladığından itibaren tarih sahnesinde yer alan asal sayılar o günden beri sayılar kuramının gözdesi olan bir konu. Kapsamında insanlığı peşinden koşturan, zaman geçtikçe cevaplanan, cevaplandıkça da yerini başka sorulara bırakan pek çok problem var. Peki *"kendinden ve 1'den başka pozitif böleni olmayan, 1'den büyük tam sayılara asal sayı denir"* tanımı nasıl oluyor da bu kadar kocaman bir dünya yaratabiliyor? Bunu anlamanın tek yolu kapıyı biraz aralayıp asal sayılar dünyasına bir gezinti yapmaktan geçiyor. Dikkatli olun siz de kendinizi bir asal sayı problemi ile uğraşırken bulabilirsiniz. Çünkü birazdan karşınıza hala cevaplanmayı bekleyen pek çok soru çıkacak.

Tarihte Kısa Bir Gezinti

Yüzyıllardır üzerinde uğraşılan bir konu olmasına rağmen 17. yüzyıla kadar asal sayılar tarihinde söylenecek çok bir söz yok. Öncelikle geniş bir şekilde antik yunanlılar tarafından çalışılan kuram, Pisagor okulunun sayıların nümerik özelliklerinde gizem arayan matematikçileri tarafından ilerletildi. Mükemmel ve dost sayılar tanımlanıp üzerine düşünülmeye başlandı. Mükemmel sayı kendisi haricindeki tüm çarpanlarının toplamı kendisini veren sayıdır. Örneğin 6 bir mükemmel sayıdır çünkü kendisi haricindeki çarpanları yani 1, 2 ve 3 toplanınca kendisini verir: 1+2+3=6. Dost sayılara örnek ise 220 ve 284. Bu sayıların da kendileri haricindeki tüm çarpanlarının toplamları birbirlerini verir.

Kaç Asal Vardır?

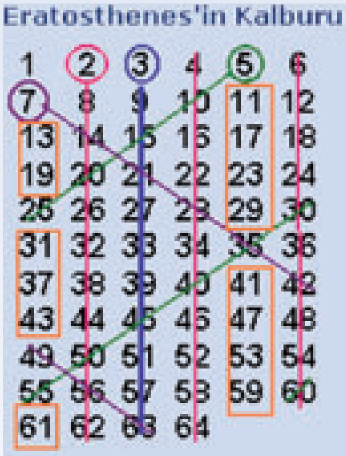
O çağlarda insanların kafasını en çok kurcalayan konu kaç tane asal sayı olduğu idi. Hatta en çok sonsuz tane olup olmadıkları merak ediliyordu. Sonraları, M.Ö. 300 civarlarında Öklid bu tartışmaları sona erdirmek adına matematik tarihinin en eski ve zarif ispatlarından birisini vererek *"sonsuz tane asal sayı vardır"* kestirimini ispatladı. Aynı zamanda Öklid'in bu çalışması şıklığıyla da bugün hala çelişki ile ispat örneklerinin gözdelerindendir. Öklid mükemmel sayılar konusuna da katkıda bulunup "$2^n - 1$ asal ise $2^{n-1}(2^n - 1)$ bir mükemmel sayıdır" ifadesinin ispatını verdi. Euler'in 1747'de ispatladığı "her mükemmel çift sayı $2^{n-1}(2^n - 1)$ biçimdedir" ifadesiyle bu sayılar, üzerlerindeki ilgiyi mükemmel tek sayılara kaptırdılar. Çünkü bugün ne bir mükemmel tek sayı bulunabildi ne de böyle bir sayının varolmadığı ispatlanabildi. Bilinen şu ki, böyle bir sayı varsa 10^{300}'den büyüktür diğer bir deyişle 300'den fazla basamağa sahiptir.

Eratosthenes'in kalburu

Öklid'in ardından Yunanlı Eratosthenes M.Ö. 200 sıralarında kendi adını verdiği bir algoritma ile asal sayıları listelemeye çalıştı. Bu algoritma için şu teoremi kullanırız.

"*d* bileşik (asal olmayan) bir sayı olsun, o zaman *d*'nin hiçbir asal çarpanı $\sqrt{d}$'den büyük olamaz"

Örneğin 64'den küçük asalları mı listeleyeceksiniz. $\sqrt{64}=8$ öyleyse asal çarpanlar: 2,3,5 ve 7 olabilir. 1'den 64'e kadar olan sayıları yazın ve bu dört sayının katlarının üstünü çizin geriye 64'den küçük asallar kalacaktır. Çünkü teoreme göre 64 ve 64'den küçük sayılar ancak 2,3,5 ve 7 asal çarpanlarına sahip olabilir; değilse de zaten asaldır. Eleme yöntemi kullanıldığı için bu yönteme Eratosthenes'in kalburu adı verilir.



Karanlık Yıllar...

İlginçtir ki ilgiyi sürekli üzerinde tutabilen bir konu olmasına rağmen 17. yüzyıla kadar asallar cephesinde pek bir gelişme olmadı. Matematikçilerin karanlık yıllar adını verdikleri ve bilgisayarın hayalinin bile kurulamadığı bu yıllarda asal sayılarla uğraşmak biraz zor, biraz da hatalarla dolu oldu. Doğru olduğu düşünülen sanılar ortaya atıldı ama bunların yanlış olduğunun anlaşılması yıllar hatta yüzyıllar aldı. Örneğin insanlar bir süre $n^2 - n + 41$ polinomunun daima asal sayı üreten bir formül olduğuna inandılar ve asallara karşı haklı bir zafer kazandıklarını düşünerek bir süre de olsa rahat uyku uyudular ta ki birisinin aklına formüle 41 koymak gelene kadar. 0 ve 40 arası n değerleri için sürekli asal üreten bu formül 41'de açıkça görülüyor ki 41^2 halini alarak asal bir değer vermiyor. Bugün cevabı aranan diğer bir soru da şu: acaba bu ve bunun gibi $0 \leq n \leq 79$ için sürekli asal veren $n^2 - 79n + 1601$ formülü verilen n değerleri için sonsuz tane asal sayı üretebilir mi?

Fermat Asalları

17. yüzyılda amatör matematikçi ünvanı ile bilinen Fermat asal sayılar konusuna oldukça önemli katkılarda bulundu. Bu katkılar arasında doğru olduğunu iddia edip ispatlayamadığı kestirimler de vardı. Örneğin $2^{2^n}+1$ biçimindeki sayıların her n doğal sayısı için bir asal verdiğini iddia etti. Bu biçimdeki sayılara Fermat sayıları asal olanlara da Fermat asalları denir. Gerçekten de 5'e kadar tüm doğal sayılar için asal değer veren ifadenin yanlış olduğu ancak 100 yıldan fazla zaman sonra anlaşılabildi. n=5 için $2^{32} + 1 = 4294967297$ sayısının 641 ile bölündüğünün farkına varansa yine Euler oldu. Bugün ispatı yapılması beklenen önermelerden bir diğeriyse "Fermat asalları sonlu tanedir" kestirimi. Bu ifadenin en güçlü gerekçesiyse şimdiye kadar sadece 5 tane Fermat asalının bulunmasıdır($0 \leq n \leq 4$)

Mersenne sayıları

Fermat'ın sıkça fikir alışverişinde bulunduğu çağdaşı Mersenne de $2^n - 1$ şeklindeki sayılar üzerinde çalışıyordu. Mersenne sayıları (M_n) adı verilen bu sayıların başlangıçta n asal olduğunda asal değer verdiği düşünüldü. Gerçekten de n=11'e kadar doğru çalışan fikir 11'de asal olmayan bir değer alınca bu düşüncenin de yanlış olduğu anlaşılabildi ama $2^n - 1$'in asal olması için n'nin asal olması gerektiği şartı doğrudur. Yine de matematikçiler bu sayıların peşini bırakmadı. Sonsuz tane olup olmadıkları hala merak edilen Mersenne sayılarının 41.si geçtiğimiz Mayıs ayında elde edildi. Sonuçsa $2^{24.036.583}$-1 şeklinde 7 235 233 basamaklı bir sayı!

Analitik Sayılar Kuramı

18. yüzyıla gelindiğinde Euler asal sayı çalışmalarına hız verecek çok önemli bir noktayı fark etti. Yeni yeni ortaya çıkıp gelişen analiz dalının ürettiği yöntemler (limit-türev-integral) sayılar kuramında kullanılabilirdi. Böylece Analitik Sayılar Kuramı adı verilen matematik dalı gelişmeye koyuldu. Asallara ilişkin bilgilerin gün ışığına çıkmasında şüphesiz sonsuz küçükler hesabının katkısı ve kazandırdığı hız göz ardı edilemez. Belki de kimi soruların cevaplarının hala bulunmaması, tekniklerin yeterli olmamasından kaynaklanıyordu.

Goldbach Kestirimi

1742'de Goldbach, Euler'e yazdığı bir mektupta "2'den büyük her çift sayı, iki asal sayının toplamı şeklinde ifade edilebilir" önermesinin, ya doğru olduğunu ispatlamasını ya da bunu sağlamayan bir örnek göstererek yanlış olduğunu ispatlamasını istedi. Goldbach kestirimi olarak bilinen bu hipotezle asal sayılar dünyasına yeni bir heyecan geldi. 2'den başlayarak her çift sayıya 3 sayısı (ki bu bir asal sayı) ekleyerek tek sayılar kümesi elde edilebildiğine göre (örneğin:5=2+3; 7=4+3; 9=6+3...) her çift sayı 2 asal sayının toplamı ise her tek sayı da 3 asal sayının toplamıdır denilebilir. Bu ifade de zayıf (ya da tek) Goldbach kestirimi olarak bilinir. Üzerinden 250 yıl geçmesine rağmen hala ispatlanamayan bu iki ifadeden tek sayılarla ilgili olanı oldukça yol kat etmiştir.

Dağınık Asallarda bir Düzen

Matematikte özellikle doğal sayılarla çalışırken bir genelleme yapmak isterseniz önce elinizdeki işlemin ilk birkaç örnek için nasıl sonuçlar verdiğine bakar sonra bunlardaki benzerlikleri kullanarak geneleme yoluna gidersiniz. Şayet şanlıysanız formül hemen göz kırpıverir. Son olarak da bu iddiayı ispatlamaya çalışırsınız. Ama uğraştığınız, asal sayılar gibi dağınık, düzeni olmayan, genellemeye vurulmayı asla sevmeyen bir konuysa işiniz biraz zordur, aritmetik kurallar yeterli olmayabilir. Ortaya çıktıklarından beri akılları meşgul eden "verilen bir sayıdan küçük kaç tane asal sayı vardır" sorusu bu dağınıklık nedeniyle cevaplanması kolay bir soru değildir. 10'dan küçük 4 asal; 100'den küçük 25 asal; 10000'den küçük 168 asal vardır. Daha da ilginci 10000000'den 100 sayı öncesine kadar 9 asala rastlarsınız, oysa ki 10000000'den 100 sonrasına geldiğinizde sadece 2 asal sayabilmişsinizdir. Kim bilir belki bu düzensizlikte de bir düzen vardır?

Bir Dahi...

Bilim dünyasında adı dahiler listesinde yer alan Carl Friedrich Gauss'un yaklaşık 3000000 asal sayıp bunların tablosunu yaptığı bilinir. Gauss kademe kademe 102,000'den küçük asalların miktarlarını listelediği tabloda asal sayıların dağılımını ilişkin bir düzen fark ettiğinde henüz sadece 15 yaşındaydı. Adı geçen bu düzeni anlayabilmek için konuya biraz daha yakından bakalım:

Matematikçiler **π (x)** fonksiyonunu x sayısına eşit ve ondan küçük asalların miktarı olarak matematiğe tanıştırdılar. Gauss yaptığı çalışmada x ile **π (x)** arasındaki oranı inceledi:

x	*x/ π (x)*	*log (x)*
10	**2,5**	**2,3**
100	**4,0**	**4,6**
1000	**6,0**	**6,9**
10000	**8,1**	**9,2**
100000	**10,4**	**11,5**

Tablonun yorumu şöyleydi: ilk 10 sayıda her 2,5 sayıdan 1'i asalken, ilk 100 sayıda her 4 tanesinden 1'i asaldı. Burada cevaplanması gereken soru 2,5 – 4 – 6 - 8,1 - 10,4 diye artış gösteren bu sayıların x ile arasında nasıl bir ilişki vardı? 15 yaşında bu sayılar arasındaki bağlantının x sayısının e tabanındaki logaritmasıyla benzerlik gösterdiğini fark edebilen bir insanın dahi ünvanını almasından doğal bir şey olmasa gerek. Gauss'un söylediği; verilen bir n sayısıdan küçük asalların miktarı yaklaşık n/log(n) kadardır ve sayı büyüdükçe bu yaklaşım daha az hata verecektir. Fakat Gauss bu çalışmasını hiç yayınlamadı. Birkaç yıl sonra Fransız matematikçi Adrien Marie Legendre bu hipotezi ortaya attı ama kendisi de ispatını yapmadı.

Asal Sayı Teoremi

$$\lim_{x\to\infty} \pi(x) \Big/ \frac{x}{\log(x)} = 1.$$

Legendre'nin verdiği hipotez teorem olabilmek için 100 yıl bekledi. 1896'da ayrı ayrı C. de la Vallee Poussin ve Jacques Hadamard tarafından ispatı verilen teoremin sayılar kuramındaki en önemli gelişmelerden birisi olduğu herhalde "asal sayı teoremi" adını almasından da anlaşılıyor.

Daha Verimli Yaklaşımlar

Matematikçiler bundan sonra daha yakın sonuç veren yaklaşımlar üzerine çalıştı. Yaklaşımlar geliştirildikçe formül de bir o kadar genişledi. Örneğin

$$R(n) = 1 + \sum_{k=1}^{\infty} \frac{1}{k\zeta(k+1)} \frac{(\log n)^k}{k!}$$

Buradaki Riemann Zeta Fonksiyonu ifade eden $\zeta(z) = 1 + 1/2^z + 1/3^z + 1/4^z + \dots$ şeklindedir.

Asal sayılara ilişkin bilgiler burada sona ermediği gibi daha bahsetmediğimiz pek çok ünlü kestirim de var. Örneğin n^2 ve $(n+1)^2$ arasında daima bir asal var mıdır? Ya da ikiz asallar yani aralarındaki fark 2 olan asallar sonsuz tane midir? Gibi pek çok soru cevaplanmayı beklemektedir. İnsanların yüzyıllardır herhangi bir karşılık beklemeden uğraştığı asalların 20. yüzyılda nasıl gelişmeler kaydettiğini bir sonraki sayımıza bırakıyoruz. Asal sayıların teknolojiye sunduğu uygulamaları da yine bir sonra ki yazımızda bulabilirsiniz.

Nilüfer Karadağ
karadağnilufer@yahoo.com