Asal Sayılar

Ali Nesin

Birden ve kendisinden başka sayıya bölünmeyen sayılara **asal sayı** denir[1]. Örneğin 17 asaldır, çünkü 1 ve 17'den başka sayıya (tam olarak) bölünmez. Öte yandan 35 asal değildir, 5'e ve 7'ye bölünür. Teknik nedenlerden 1 asal kabul edilmez.

100'den küçük asalları bulmak pek zor değildir. İşte o asallar: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97. Demek ki 100'den küçük 25 tane asal varmış. Yani 100'den küçük rastgele seçilmiş bir sayının asal olma olasılığı 1/4'tür.

Matematiksel kanıtlar arasında bir güzellik yarışması yapılsa, Öklid'in (MÖ. 300) "**sonsuz tane asal sayı vardır**" önermesinin kanıtı hiç kuşkusuz ilk on sırada yer alırdı. Bu teorem Öklid'in ünlü **Öğeler** adlı yapıtının dokuzuncu cildinde kanıtlanır. Öklid'in teoreminin güzelliğinin göklere çıkarılmadığı ve kanıtlanmadığı popüler matematik kitabı yok gibidir. Birazdan bu güzel teoremi – ve çok daha fazlasını – kanıtlayacağız.

Bir sayının asal olup olmadığını nasıl anlarız? Sayımıza n diyelim. n'yi n'den küçük sayılara bölmeye çalışalım. Eğer n'den küçük, 1'den büyük bir sayı n'yi tam bölüyorsa, n, tanımı gereği, asal olamaz. Öyle bir sayı bulamazsak, n asaldır.

Ne var ki bu yöntemle büyük sayıların asallığına karar vermek çok zaman alır. Bu yöntem ve çeşitlemeleri dışında bir sayının asallığına karar verebilecek genel bir yöntem de bilinmemektedir. Örneğin, şu çeşitleme düşünülebilir: n'yi n'den küçük her sayıya böleceğimize, n'yi $\sqrt{n}$'den küçük sayılara bölmeye çalışabiliriz. Çünkü $n = ab$ ve $a \geq \sqrt{n}$ ise, $b \leq \sqrt{n}$'dir. Dolayısıyla n asal değilse, $\sqrt{n}$'den küçük bir sayıya bölünür. Böylece yapmamız gereken bölme sayısı azalır. Bir başka kolaylık da şöyle sağlanabilir: n'nin asal olup olmadığına karar vermek için n'yi $\sqrt{n}$'den küçük her sayıya bölmeye çalışacağımıza, $\sqrt{n}$'den küçük asallara bölmeye çalışmamız yeterlidir. Bu birazdan kanıtlayacağımız birinci teoremden çıkar. Böylece, n'nin asallığına karar vermek için yapmamız gereken bölme sayısı daha da azalır. Öte yandan bu yöntemi kullanabilmek için $\sqrt{n}$'den küçük asalları bilmek gerekir. Bu asalları bildiğimizi varsaysak bile, bölme sayısı gene de büyük sayılar için çok fazladır. Örneğin, n = 100.000.000.001'in asal olup olmadığını anlamaya çalıştığımızı varsayalım bir an. Eğer n asal değilse ve küçük bir asala (örneğin 97'ye) bölünebiliyorsa, n'nin asal olmadığına oldukça çabuk karar veririz. Ama ya n asalsa ya da küçük bir asala bölünmüyorsa? Onbinlerce bölme işlemi yapmamız gerekecek.

Yukarda açıkladığımız yöntem Yunanlı matematikçi Eratosthenes tarafından M.Ö. 3. yüzyılda bulunmuştur. Bu yöntemle 50 rakamlı bir sayının en gelişmiş bilgisayar yardımıyla asal olup olmadığını anlamak trilyonlarca yıl alır. Yaşam gerçekten kısa!

Bazı özel sayıların asallığına karar vermek için özel yöntemler geliştirilebilir. Örneğin son rakamı çift olan bir tek asal sayı vardır, o da 2'dir. Çünkü son rakamı çift olan bir sayı 2'ye bölünür.

Asal olmayan sayılara bir başka örnek vereyim. $x^a - 1$ biçiminde yazılan sayılar $x - 1$'e bölünürler:

1 Bu yazıda, "sayı" sözcüğünü 1, 2, 3, 4 gibi tamsayılar için kullanacağız.

$$x^a - 1 = (x - 1)(x^{a-1} + x^{a-2} + ... + x + 1).$$

Dolayısıyla, bir $a > 1$ sayısı için, $x^a - 1$ biçiminde yazılan bir sayının asal olabilmesi için x'in 2 olması gerekmektedir. Madem öyle, $2^a - 1$ biçiminde yazılan sayılara bakalım. Bu sayılar asal mıdır?

Sav: *Eğer a asal değilse $2^a - 1$ de asal olamaz.*

Kanıt: Bunu kanıtlamak için önce $a = bc$ yazalım. a asal olmadığından bu eşitliği sağlayan b ve c sayıları vardır. Sonra x'i 2^b olarak tanımlayıp küçük bir hesap yapalım: $2^a - 1 = 2^{bc} - 1 = (2^b)^c - 1 = x^c - 1$. Ama $x^c - 1$ sayısının $x - 1$'e bölündüğünü yukarda görmüştük. Demek ki $2^a - 1$, $x - 1$'e bölünür ve asal olamaz. Dolayısıyla, $2^a - 1$'in asal olması için a'nın asal olması gerekmektedir. Kanıtımız bitmiştir.

Asal bir a için $2^a - 1$ biçiminde yazılan sayılara **Mersenne sayıları** denir[2]. Peki, a asalsa,

$$M_a = 2^a - 1$$

olarak tanımlanan sayı da asal mıdır? İlk Mersenne sayılarına bakalım:

$$M_2 = 3$$
$$M_3 = 7$$
$$M_5 = 31$$
$$M_7 = 127$$

Bu sayıların herbiri asal. Ama bundan sonraki ilk Mersenne sayısı, yani M_{11}, asal değil: $M_{11} = 23 \times 89$.

Hangi asallar için M_a asaldır? Yanıt bilinmiyor.

1972'de M_{19937}'in asal olduğunu Bryant Tuckerman bilgisayar yardımıyla keşfetti.

1975'te, on beş yaşında iki lise öğrencisi, Laura Nickel ve Curt Noll, M_{19937}'in o zamana dek bilinen en büyük asal olduğunu bir gazeteden öğrenince, çalışmaya koyuldular ve üç yıl sonra, 1978'te, bilgisayarlarını 350 saat çalıştırdıktan sonra, M_{21701}'in asal olduğunu buldular. Ve birdenbire ünlendiler.

Şubat 1979'da Noll, M_{23209}'un asal olduğunu buldu.

İki ay sonra, Slowinski M_{44497}'nin asal olduğunu gösterdi.

Mayıs 1983'te Amerikalı David Slowinski, M_{86243}'ün asal olduğunu, bilgisayar yardımıyla tam 1 saat 3 dakika 22 saniyede kanıtladı. Ama 86.243 sihirli sayısını bulmak için aylarca uğraştı. Bilinen klasik yöntemle (yani kendisinden küçük sayılara bölmeye çalışarak) bu sayının asal olduğunu kanıtlamak, evrenin ömrünü aşardı! M_{86243}'ün tam 25.962 rakamı olduğunu da ayrıca belirtelim. Bu kadar bozuk parayı üstüste yığsanız, para kuleniz evrenin sınırlarını aşar! [43]

Yukardaki asalı bulan Slowinski, 19 Eylül 1983'te M_{132049}'un asal olduğunu bilgisayarlarla anladı. Bundan çok daha önce, Manfred Schroeder adlı bir matematikçi, matematiksel yöntemlerle, sezgisinin de yardımıyla, $2^{130.000} - 1$ civarlarında bir asal olduğunu tahmin etmişti zaten.

Mart 1992'de M_{756839}'un asal olduğu anlaşıldı.

12 Ocak 1994'te, Paul Gage ve yine David Slowinsky bilgisayar ağlarında M_{859433}'ün asal olduğunu kanıtladıklarını duyurdular. Hesaplarını gene bilgisayarla yapmışlardı elbet.

2 Mersenne ("mersen" diye okunur), Fermat, Pierre de'yla çağdaş ve Fermat'nın mektup arkadaşı bir Fransız matematikçisidir.

Şimdi, $S_o = 4$, $S_{k+1} = S_k^2 - 2$ olsun. Örneğin, $S_1 = 4^2 - 2 = 14$'tür. Bunun gibi, $S_2 = S_1^2 - 2 = 14^2 - 2 = 194$'tür. Bir q asalı için, M_q'nün asal olması için gerekli ve yeterli koşul, M_q'nün S_q'yü bölmesidir. Bu teste **Lucas testi** denilir. Lucas testi sayesinde çok büyük asallar oldukça kolay sayılacak işlemlerle bulunabilir.

Bu sonuçlara bilgisayarlara güvenebildiğimiz derecede güvenebiliriz elbet. Bilgisayarlar da hata yaparlar!

Büyük sayıların asal olup olmadıklarını anlamak, şifreli mesajlarda (kriptoloji) çok önemlidir ve gelişmiş ülkelerin orduları bu yüzden asal sayılarla çok ilgilenirler. Gizli mesaj yollamak isteyen, mesajıyla birlikte iki büyük asal sayının çarpımını da yollar. Şifreyi çözmek için, şifreyle birlikte yollanan sayıyı bölen o iki asalı bilmek gerekir, ki bu da dışardan birisi için (sayılar büyük olduğundan) hemen hemen olanaksızdır. İki sayıyı çarpmak kolaydır ama bir sayıyı çarpanlarına ayırmak çok daha zordur.

Şifrelemede Mersenne sayıları kullanılmaz. Çünkü az sayıda (30 küsur tane olmalı) asal Mersenne sayısı bilindiğinden, şifreyle birlikte yollanan sayının asal bir Mersenne sayısına bölünüp bölünmediğini anlamak kolaydır.

Asal olmayan bir sayıyı bölenlerine ayırmanın Fermat'nın bulduğu şu yöntem vardır. Eğer n sayısı iki pozitif doğal sayı için $x^2 - y^2$ biçiminde yazılıyorsa, o zaman,

$$n = (x - y)(x + y)$$

eşitliği doğrudur ve x, y +1 olmadığı sürece, n'yi çarpanlarına ayırmış oluruz. Bunun tersi de aşağı yukarı doğrudur. Eğer $n = ab$ ise ve n çift değilse, o zaman,

$$x = \frac{a+b}{2}$$

ve

$$y = \textbf{Hata!}$$

alarak, $n = x^2 - y^2$ eşitliğini elde ederiz. Demek ki, çift olmayan bir n doğal sayısını çarpanlarına ayırmak için, $n = x^2 - y^2$ eşitliğini sağlayan x ve y bulmalıyız. Bu eşitlik yerine $y^2 = x^2 - n$ yazalım ve x yerine teker teker sayıları koyup $x^2 - n$ sayısını hesaplayalım. Bu sayı tam bir kare (y^2) olduğunda $n = x^2 - y^2$ eşitliğini bulmuş oluruz. Elbette x'in $\sqrt{n}$'den büyük olması gerekmektedir, yoksa $x^2 - n$ pozitif bile olamaz. Ayrıca, $x^2 - n$ sayısının tam bir kare olması için 0, 1, 4, 5, 6 ve 9'la bitmesi gerekmektedir, 2, 3, 7 ve 8'le biten sayılar kare olamazlar.

Bu yöntemi $n = 91$ için deneyelim. $x > \sqrt{91}$ olması gerektiğinden, $x = 10$'dan başlamalıyız. $x = 10$ ise, $x^2 - n = 10^2 - 91 = 9 = 3^2$ dir ve $y = 3$ olabilir. Demek ki,

$$91 = n = 10^2 - 3^2 = (10 - 3)(10 + 3) = 7 \times 13$$

eşitliği geçerlidir.

Aynı yöntemi $n = 143$ için deneyecek olursanız, gene yanıtı hemen bulursunuz: $x = 12$, $y = 1$.

Mersenne sayılarına çok benzeyen başka sayılara bakalım. $2^a + 1$ biçiminde yazılan sayılar asal mıdır? Bu sayıların hangi a'lar için asal olduklarını bilmiyoruz ama hangi a'lar için asal olamayacaklarını biliyoruz: Eğer a, 2'nin bir gücü değilse, yani 2^n biçiminde yazılamazsa, bu sayılar asal olamazlar. Bunu birazdan kanıtlayacağız (Teorem 9.) Fermat,

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

biçiminde yazılan bütün sayıların asal olduklarını sanıyordu. Bu yüzden bu sayılara **Fermat sayıları** denir. Gerçekten de ilk beş Fermat sayısı,

$$F_o = 3$$

$$F_1 = 5$$
$$F_2 = 17$$
$$F_3 = 257$$
$$F_4 = 65537$$

asaldır. Fermat, bütün Fermat sayılarının asal olduklarını kanıtlamaya uğraştı ama başaramadı. Başarısızlığının nedeni vardı: Sanısı doğru değildi. F_5 asal değildir. F_5 on basamaklı bir sayı olduğundan asallığını kanıtlamak kolay değildi. Euler (1707–1783), F_5'in 641'e bölündüğünü gösterdi:

$$F_5 = 641 \times 6700417.$$

Demek ki $a = 2^n$ biçiminde yazılabilse bile, $2^a + 1$ asal olmayabiliyor.

Lucas F_6'nın asal olmadığını kanıtladı. Daha sonra, 1880'de, Landry,

$$F_6 = 274177 \times 67280421310721$$

eşitliğini buldu. F_7 ve F_8 de asal değiller. Bu sayıların asal olmadıkları, çok geç bir tarihte, 1970 ve 1981'de anlaşıldı. W. Keller, 1980'de F_{9448}'in asal olmadığını gösterdi. Bu sayı $19 \times 2^{9450} + 1$'e bölünür. 1984'de gene W. Keller, F_{23471}'in asal olmadığını kanıtladı. Bu sayının 10^{7000}'den fazla basamağı vardır ve $5 \times 2^{23473} + 1$'e bölünür.

$n \geq 5$ için, asal bir F_n'nin olup olmadığı şimdilik bilinmiyor. Asallığı bilinmeyen en küçük Fermat sayıları şunlar: F_{22}, F_{24}, F_{28}.

Son yıllarda bir sayının asallığına yüzde olarak oldukça çabuk karar verebilen yöntemler geliştirildi. Örneğin, "Şu sayı yüzde 99,978 olasılıkla asaldır," gibi önermeler bilgisayarların yardımıyla oldukça kısa sayılabilecek zamanda kanıtlandı. Bu konuda bilgim kısıtlı olduğundan daha fazla söz söyleyemeyeceğim.

11, 111, 1111, 11111 gibi her rakamı 1 olan sayılar asal mıdır? İçinde n tane 1 olan sayıya B_n diyelim. Eğer çift sayıda 1 varsa, yani n çiftse, B_n, 11'e bölünür ve B_2 dışında bunlardan hiçbiri asal olamaz. Eğer n üçe bölünüyorsa B_n de üçe bölünür ve asal olamaz.

Hangi n'ler için B_n asaldır? Bu asallardan kaç tane vardır? B_2, B_{19}, B_{23}, B_{317}, B_{1031} asal sayılar, bu biliniyor. Bunlardan başka? Ben bilmiyorum. Bu sayılardan daha büyük bir asal varsa, $n > 10.000$ olması gerektiğini Harvey Dubner adlı biri kanıtlamış, daha doğrusu hesaplamış. [43]

Asallar matematikte çok önemlidir elbet. Bu yazıda bu önemli konuda bir iki teorem kanıtlayacağız. İlk teoremimizi okurların çoğu biliyordur.

Teorem 1. *1'den büyük her sayı*[3] *bir asala bölünür.*

Kanıt: Bunun kanıtı oldukça kolaydır: $a > 1$ bir sayı olsun. a'nın bir asala bölündüğünü kanıtlamak istiyoruz.

Eğer a asalsa bir sorun yok: a, a'yı böler ve teoremimiz kanıtlanmış olur (a bir asala (kendisine!) bölünür.)

Eğer a asal değilse, a'yı bölen ve $1 < b < a$ eşitsizliklerini sağlayan bir b vardır. Eğer b asalsa bir sorun yok: b, a'yı böler ve teoremimiz kanıtlanmış olur.

Eğer b asal değilse, b'yi (ve dolayısıyla a'yı da) bölen ve $1 < c < b$ eşitsizliklerini sağlayan bir c vardır. Eğer c asalsa bir sorun yok: c, a'yı böler ve teoremimiz kanıtlanmış olur.

3 Bu yazıda, "sayı" sözcüğünü, 0, 1, 2, 3 gibi "doğal sayılar" için kullanacağız.

Eğer c asal değilse, c'yi (ve dolayısıyla a'yı da) bölen ve $1 < d < c$ eşitsizliklerini sağlayan bir d vardır. Eğer d asalsa bir sorun yok: d, a'yı böler ve teoremimiz kanıtlanmış olur.

Eğer d asal değilse.....

Nereye dek gidebiliriz? Bulacağımız her sayı bir öncekinden küçük ve 1'den büyük olduğundan sonsuza dek bunu böyle sürdüremeyiz. Bir zaman sonra durmalıyız, yani bir zaman sonra a'yı bölen bir asal buluruz. Teoremimiz kanıtlanmıştır. □

Birazdan yukarda güzelliğinden sözettiğimiz Öklid Teoremini kanıtlayacağız: *Sonsuz tane asal sayı vardır*. Aynı yöntemle başka sonuçlar da çıkaracağız. İlk önce biraz ilkokul aritmetiği yapalım.

Eğer a ve b sayıları n'ye bölünüyorsa, bu iki sayının toplamı da n'ye bölünür. Örneğin hem 78, hem 66 üçe bölündüğünden, 78 + 66 da, yani 144 de, üçe bölünür.

Öte yandan eğer a ve b sayılarından yalnızca biri n'ye bölünüyor, öbürü bölünmüyorsa, bu iki sayının toplamı n'ye bölünmez. Örneğin 78 üçe bölünür, 67 bölünmez. Dolayısıyla 78 + 67 üçe bölünmez.

Bir üst paragraftaki b'yi 1 olarak alırsak, a'yı bölen 1'den büyük bir sayının $a + 1$'i bölemeyeceği çıkar. Demek ki a ve a+1 sayılarının 1'den başka ortak böleni yoktur.

Hem ikiye, hem de üçe bölünen bir sayıya 1 eklersek, elde ettiğimiz sayı ne ikiye ne de üçe bölünür. Bunun gibi, $2 \times 3 \times 4 \times 5 \times 6 \times 7$, yani 5040, 2'ye, 3'e, 4'e, 5'e, 6'ya, 7'ye bölünür, ama bu sayıya 1 ekleyerek elde ettiğimiz 5041, bunlardan hiçbirine bölünmez.

Aynı şey a ve $a - 1$ sayıları için de geçerlidir. Örneğin, 5040'ı bölen 1'den büyük hiçbir sayı 5039'u bölemez.

5039 ve 5041 sayılarının 7 ve 7'den küçük hiçbir asala bölünmediklerini gördük. Öte yandan, Teorem 1'e göre, bu sayılardan herbiri bir asala bölünmeli. Demek ki 7'den büyük bir asal vardır. Bunun gibi 2'yle 11 arasındaki sayıların çarpımına 1 eklersek, elde edilen sayı bir asala bölünür ve bu asal 11'den büyük olmak zorundadır. Bu akıl yürütmeyi genelleştireceğiz:

Teorem 2. *Sonsuz tane asal sayı vardır*.

Kanıt: $n > 1$ herhangi bir sayı olsun. 2'den n'ye kadar bütün sayıları birbiriyle çarpalım: $2 \times 3 \times ... \times (n–2) \times (n–1) \times n$. Kocaman bir sayı elde ettik. Bu sayı $n!$ olarak simgelenir. $n!$ sayısı $n + 1$'den küçük bütün sayılara bölünür elbet, çünkü $n!$ bu sayıların çarpımı. Demek ki $n! + 1$ sayısı 1'le n arasındaki hiçbir sayıya bölünemez. Öte yandan, Teorem 1'e göre $n! + 1$ sayısı bir asala bölünmeli. Demek ki n'den büyük bir asal vardır.

Ne bulduk? Her sayıdan büyük bir asal bulduk. Dolayısıyla sonsuz tane asal vardır, çünkü her asaldan büyük bir başka asal vardır. İkinci teorem kanıtlanmıştır. □

Ne denli yalın bir kanıt değil mi? Ve şaşırtıcı. Şu nedenden şaşırtıcı: Kanıt, n'den sonra gelen ilk asalı bulmuyor; yalnızca n'den büyük bir asalın varlığı kanıtlanıyor. Örneğin 1 milyondan büyük bir asal vardır. Hangi asal? Yanıt yok! Kanıt, hangi asalın 1 milyondan büyük olduğunu göstermiyor. "Öyle bir asal var" demekle yetiniyor.

Aslında kanıtımız n'den büyük asallar üzerine hiç de bilgi vermiyor değil. En azından, her n için, $n < p \leq n! + 1$ eşitsizliklerini sağlayan bir p asalının olduğunu kanıtlıyor.

Teorem 3. *Her $n > 1$ için, $n < p \le n! + 1$ eşitsizliklerini sağlayan bir asal vardır.* □

Hangi n asal bir sayıları için $n! + 1$ asaldır? Bence bu pek ilginç bir soru değil ama, meraklılar böyle sorular soruyorlar. Yanıt bilinmiyor. 1987'de H. Dubner, $n = 13649$ için, ki bu asal bir sayıdır, 5862 basamaklı $n! + 1$ sayısının asal olduğunu gösterdi.

Yukardaki teoeremde, $n! + 1$ sayısını biraz daha küçültebiliriz. Teorem 2'nin kanıtının hemen hemen aynısı, $n!$ yerine, n'den küçük ya da eşit asalların çarpımını alabileceğimizi gösteriyor. Örneğin, $n = 29$ ise,

$$29 < p \le 2\times3\times5\times7\times11\times13\times17\times19\times23\times29 + 1$$

eşitsizliğini sağlayan bir asal vardır.

Bütün bunlar akla bir başka soru getiriyor. Ardarda gelen, örneğin, her bin sayıdan en az biri asal mıdır? Başka bir deyişle, n herhangi bir sayıysa,

$$n + 1, n + 2, n + 3, ..., n + 1000$$

sayılarından biri asal mıdır?

Bu soruyu yanıtlamak için yeterli bilgiye sahibiz. Yanıt olumsuzdur. Yanıtın olumsuz olduğunu kanıtlayalım.

Bir örnekle başlayalım. $7! = 2 \times 3 \times 4 \times 5 \times 6 \times 7$, yani 5040, 2'ye, 3'e, 4'e, 5'e, 6'ya ve 7'ye bölünür. Dolayısıyla

5042, 2'ye
5043, 3'e
5044, 4'e
5045, 5'e
5046, 6'ya
5047, 7'ye

bölünür ve bu sayılardan hiçbiri asal olamaz. Bunun gibi, aşağıdaki bin sayı,

$$1001! + 2, 1001! + 3, ... , 1001! + 1001$$

sırasıyla 2'ye, 3'e, ..., 1001'e bölünürler ve hiçbiri asal olamaz. Bu yaptığımızı genelleştirmek işten bile değildir:

Teorem 4. *Ardarda gelen her n sayıdan birinin mutlaka asal olduğu bir n yoktur.* □

Asallarla ilgili bir başka soruya geçelim. Sayıları üç kümeye ayırabiliriz:

A kümesi = {3'e bölünen sayılar }
B kümesi = {3'e bölündüğünde kalanın 1 olduğu sayılar}
C kümesi = {3'e bölündüğünde kalanın 2 olduğu sayılar}

Yani,

$A = \{3,6,9,12,15,18,...\}$
$B = \{4,7,10,13,16,19,...\}$
$C = \{5,8,11,14,17,20,...\}$

B kümesinden herhangi iki sayı alalım: n_1 ve n_2. Bu sayılar 3'e bölündüğünde 1 kalıyor. Dolayısıyla $n_1 = 3q_1 + 1$ ve $n_2 = 3q_2 + 1$ olarak yazabiliriz. Şimdi n_1 ve n_2'yi birbiriyle çarpalım:

$$n_1n_2 = (3q_1+1)(3q_2+1) = 9q_1q_2 + 3q_1+3q_2 +1 = 3(3q_1q_2+q_1+q_2)+1$$

Dolayısıyla n_1n_2 sayısı 3'e bölündüğünde 1 kalır. Ne kanıtladık? B kümesindeki sayıların çarpımlarının gene B kümesinde olduğunu kanıtladık. Bunu kullanarak aşağıdaki teoremi kanıtlayacağız:

Teorem 5. *C kümesinde sonsuz tane asal vardır.*

Kanıt: C kümesindeki bir sayı, A kümesindeki bir sayıya bölünemez, çünkü A kümesindeki sayılar 3'e bölünüyor, oysa C kümesindekiler 3'e bölünmüyorlar. Demek ki C kümesindeki bir sayıyı bölen sayılar B ve C kümesinde olmalıdır. Ama hepsi birden B'de olamaz, çünkü B'nin öğeleri kendileriyle çarpıldığında gene B'den bir sayı verir. Demek ki C kümesinin her sayısı, gene C kümesinden bir asala bölünür.

Şimdi $n \geq 3$ herhangi bir sayı olsun. $n! - 1$ sayısını ele alalım. Bu sayıya x diyelim. x, C'dedir, çünkü, $x = (n! - 3) + 2$ olarak yazılabilir ve $n! - 3$ üçe bölünür. Demek ki C kümesinde x'i bölen bir asal vardır. Öte yandan x'i bölen sayılar n'den büyüktür elbet. Ne kanıtladık? n kaç olursa olsun, C kümesinde n'den büyük bir asal vardır. Yani C'de sonsuz tane asal vardır. □

Okur buna benzer bir kanıtla aşağıdaki teoremi kanıtlayabilir:

Teorem 6. *4'e bölündüğünde kalanı 3 olan sonsuz tane asal vardır.*

18. yüzyılın sonlarına doğru, Fransız matematikçisi Legendre (1752–1833) son iki teoremi genelleştirmek istedi. Şu soruyu sordu:

Soru. *a ve b, 1'den başka ortak böleni olmayan iki sayı olsun. $ax+b$ biçiminde yazılan sonsuz tane asal var mıdır?*

Teorem 5'ten $a = 3$, $b = 2$ için, Teorem 6'dan da $a = 4$, $b = 3$ için yanıtın olumlu olduğu anlaşılıyor. Legendre bu soruyu genel olarak yanıtlamak istedi. Örneğin $25x + 6$ biçiminde yazılan sonsuz tane asal var mıdır? Eğer $x = 1$ ise 31 buluruz ki, 31 asaldır. Eğer $x = 2, 3, 4$ ise, sırasıyla 56, 81, 106 buluruz ve bunlardan hiçbiri asal değildir. $x = 5$ olduğunda 131 çıkar ve 131 asaldır.

Legendre sorunun yanıtının olumlu olduğundan hiç kuşku duymadı, ancak kanıtlamakta güçlük çekti. 1785'te defterine "bunu bilimsel olarak kanıtlamalı" diye not düşmüş. On dört yıl sonra, 1798'de, "doğruluğundan kuşku duymamalıyız" diye yazmış. Sonra da kanıtlamaya çalışmış. Başaramadan... İkinci denemesini **Sayılar Kuramı** adlı kitabına aldığını biliyoruz [26]. Ama bu denemesi de yanlış. Kanıtın yanlışlığının ne zaman anlaşıldığını bilmiyorum. 1837'de, meslektaşı Legendre gibi Fransız olan G. L. Dirichlet (1805–1859) teoremi doğru olarak kanıtladı [8]:

Teorem 7. *a ve b ortak böleni olmayan iki doğal sayıysa, $ax+b$ biçiminde yazılan sonsuz tane asal sayı vardır.*

Dirichlet'nin yönteminden bir başka teorem daha elde edilebilir:

Teorem 8. *a, b ve c ortak böleni olmayan üç pozitif doğal sayı olsunlar.* $ax^2 + bxy + cy^2$ *biçiminde yazılan sonsuz tane asal vardır.*

Sadece ve sadece asal sayıları ve her asal sayıyı veren bir formül var mıdır? Genel olarak sanılanın tersine böyle bir formül vardır. Öyle bir formül vardır ki, bu formülle yalnız ve yalnız asal sayılar elde edilir ve her asal sayı bu formülle elde edilir. Oldukça kolay bir formüldür bu. İşte formül:

n ve m herhangi iki doğal sayı olsun.

$$k = m(n + 1) - (n! + 1)$$

olarak tanımlansın. Şimdi,

$$p = \textbf{Hata!} + 2$$

her n ve m sayısı için asaldır! Ayrıca her asal sayı bu biçimde elde edilebilir.

Bu formülle sık sık 2 elde ederiz, ama 2 dışındaki her asal sayı bu formülle ancak bir kez, yani bir tek n ve m değerleri için elde edilebilir.

Eğer $k^2 - 1 \geq 0$ ise, yukardaki formül hep $p = 2$ verir. Ama $k^2 - 1 < 0$ ise, yani $k^2 < 1$ ise, yani $k^2 = 0$ ise, yani $k = 0$ ise, yani $m(n + 1) - (n! + 1) = 0$ ise, yani,

$$m = \textbf{Hata!}$$

ise, yukardaki formül $p = n + 1$ verir. Bu sayı asaldır, çünkü Wilson'ın ünlü teoremine göre, m'nin tamsayı olabilmesi için, yani $n + 1$'in $n! + 1$'i bölebilmesi için, $n + 1$'in asal olması gerekmektedir.

Örneğin, $n = 2$ ve $m = 1$ ise, $p = 3$ bulunur. Eğer $n = 4$ ve $m = 5$ ise, $p = 5$ bulunur. Eğer, $n = 6$ ve $m = 103$ ise, $p = 7$ bulunur. Gelecek asalı, yani 11'i bulmak için, yani $p = 11$ çıkması için, n'nin 10 olması, m'nin de

Hata!

yani 329.891 olması gerekmektedir. Hangi n ve m sayıları için $p = 13$ bulunacağını okur kolaylıkla bulabilir.

Hardy ve Wright, bir $\omega = 1{,}9287800\ldots$ sayısı için,

$$f(n) = \left\lfloor 2^{2^{\cdot^{\cdot^{2^{\omega}}}}} \right\rfloor$$

sayısının (n tane 2 var) bir asal olduğunu gösterdiler [47][4]. Örneğin $f(1) = 3$, $f(2) = 13$, $f(3) = 16381$. $f(4)$'ü hesaplamak zor, basamak sayısı 5000 civarında. Öte yandan, ω sayısını belirlemek için, asal sayıları bilmek gerektiğinden, bu formül pek işe yaramaz. Gene de öyle bir ω sayısının varlığı ilginç.

Her asalı veren bir formül var ama, her asalı veren bir polinomun[5] olmadığı biliniyor. Eğer katsayıları tamsayı olan her polinomun sonsuz tane asal olmayan sayı verdiği bilinir.

1772'de Euler, $n^2 + n + 41$ polinomunun $n = 0,1,2,\ldots,39$ için asal sayılar verdiğini buldu. Ancak bu polinom $n = 40$ için 41'e bölünür ve asal değildir.

Fermat sayıları üzerine bir teorem kanıtlayacağımıza sözvermiştik. Sözümüzü tutuyoruz:

Teorem 9. *Eğer* $a = 2^n$ *biçiminde yazılamazsa,* $2^a + 1$ *asal olamaz.*

4 [48]'de bu teoremin özet kanıtını bulabilirsiniz.

5 x ve x'in katlarını toplayarak ve çıkartarak elde edilen terimlere polinom denir.

Kanıt: Önce şunu belleyelim: x herhangi bir sayı ve $a > 1$ bir tek sayıysa, $x^a + 1$ sayısı asal olamaz, çünkü $x + 1$'e bölünür. Şöyle bölünür:

$$x^a + 1 = (x+1)(x^{a-1} - x^{a-2} + x^{a-3} - x^{a-4} + \ldots - x + 1.)$$

Şimdi a'nın bir tek sayıya bölündüğünü varsayalım. $2^a + 1$'in asal olamayacağını kanıtlamak istiyoruz. a'yı bölen tek sayıya m diyelim. Demek ki $a = nm$ ve m bir tek sayı. $x = 2^n$ olsun. Küçük bir hesap yapalım:

$$2^a + 1 = 2^{nm} + 1 = (2^n)^m + 1 = x^m + 1.$$

m tek olduğundan, ilk paragrafta gördüğümüz gibi, $x + 1$, $x^m + 1$'i böler. Yani $x + 1$, $2^a + 1$'i böler.

Demek ki a bir tek sayıya bölünüyorsa, $2^a + 1$ asal olamaz. Dolayısıyla a, 2'nin bir katı olmalı. □

Asallar üzerine bildiklerimiz bilmediklerimizin yanında hiç kalır. Bildiklerimiz arasından en önemlilerinden biri Fermat'nın Küçük Teoremi adıyla anılan şu teoremdir:

Teorem 10. (Fermat'nın Küçük Teoremi.) *n bir sayıysa ve p asalsa, p, $n^p - n$ sayısını böler. Dolayısıyla eğer p, n'yi bölmüyorsa, $n^{p-1}-1$'i böler.*

Bu teorem, n üzerine tümevarımla kolaylıkla kanıtlanabilir. Örneğin 23, $2^{23}-2$ sayısını böler, çünkü 23 asaldır. 23, 2'yi bölmediğinden, 23, $2^{22}-1$ sayısını da böler. Bunun tersi doğru mudur? Yani $p > 1$ bir sayıysa ve p, $2^{p-1} - 1$'i bölüyorsa, p asal mıdır? Eski Çinliler de bu soruyu sormuşlar ve yaptıkları hesaplarda p hep asal çıkmıştır. Gerçekten de $1 < p < 300$ için bu doğrudur. Öte yandan $p = 341 = 11 \times 31$ için doğru değildir: 341 asal olmamasına karşın $2^{340} - 1$'i böler. Demek ki Çinliler yanılmışlar. Bir iki deney yaparak matematiksel bir gerçek bulunmaz. Kanıt gerekir. [11]

Eğer p, $2^p - 2$'yi bölüyorsa ve asal değilse, p'ye **yalancı asal** adı verilir. Örneğin 341 bir yalancı asaldır[6]. 561, 645, 1105, 1387, 1729, 1905 de yalancı asallardır. Kaç tane yalancı asal vardır? Sonsuz tane vardır, çünkü eğer p bir yalancı asalsa, 2^p-1 de bir yalancı asaldır. Okur bunu alıştırma olarak kanıtlayabilir. Demek ki $2^{341} - 1$ bir yalancı asaldır.

Her p için, $2^p - 1$ tek bir sayıdır. Dolayısıyla yukardaki yöntemle bulunan yalancı asallar hep tektirler. Bundan da şu "doğal" soru çıkar: çift yalancı asal var mıdır? Evet! 1950'de D.H. Lehmer 161.038'in bir yalancı asal olduğunu kanıtladı. 161.038 sayısını bulmak kolay değil ama, bu sayının yalancı asallığını kanıtlamak oldukça kolay. Kanıtlayalım. 161.038'in $2^{161.038} - 2$'yi böldüğünü kanıtlamak istiyoruz. Önce 161.038'i asallarına ayıralım: $161.038 = 2 \times 73 \times 1103$. Demek ki 73 ve 1103'ün $a := 2^{161.037}-1$'i böldüğünü kanıtlamalıyız. 161.037'yi asallarına ayıralım: $161.037 = 3^2 \times 29 \times 617 = 9 \times b$. Burda $b = 29 \times 617$ olarak aldık elbet. Eğer $c = 2^9$ ise, bundan da şu çıkar: $a = 2^{161.037} - 1 = (2^9)^b - 1 = c^b - 1$. Demek ki $c - 1$, yani $2^9 - 1$, yani 511, yani 7×73, a'yı bölüyormuş. Dolayısıyla 73 de a'yı bölüyordur. Şimdi sıra 1103'ün a'yı böldüğünü kanıtlamakta. Aynı akıl yürütmeyi yapacağız. $d := 3^2 \times 617$ ve $e = 2^{29}$ olsun. Hesaplayalım: $a = 2^{161.037} - 1 = (2^{29})^d - 1 = e^d - 1$. Demek ki

$$e - 1 = 1103 \times 486.737,$$

a'yı bölüyormuş. Kanıtımız bitmiştir.

6 341'in yalancı asal olduğu 1819'da Sarrus tarafından bulunmuştur.

1951'de N.W.H. Beeger sonsuz tane çift yalancı asal olduğunu kanıtladı.

Eğer $p > 1$, her n için $n^p - n$'yi bölüyorsa ve asal değilse, p'ye **çok yalancı asal** adı verilir. Çok yalancı asal sayı var mıdır? Evet. En küçük çok yalancı asal sayı 561'dir. $561 = 3 \times 11 \times 17$ olduğundan 561 asal değildir. Öte yandan, 561, her n için $a^{561}-561$'i böler. Bunu da kanıtlamak oldukça kolaydır. Kanıt için okur [23]'e bakabilir.

Fermat'nın Küçük Teoremi'ne göre, eğer p asalsa,

$$1^{p-1}, 2^{p-1},..., (p-1)^{p-1}$$

sayıları p'ye bölündüğünde 1 kalır. Dolayısıyla bu $p-1$ sayının toplamı olan

$$1^{p-1} + 2^{p-1} + ... + (p-1)^{p-1}$$

sayısı p'ye bölündüğünde kalan $p - 1$'dir. Bunun tersi de doğru mudur? Yani n herhangi bir sayıysa ve

$$1^{n-1} + 2^{n-1} + ... + (n-1)^{n-1}$$

sayısı n'ye bölündüğünde kalan $n - 1$ ise, n asal mıdır? 1950'de Bedocchi adında bir matematikçi 1985'de yanıtın $n < 10^{1700}$ için "evet" olduğunu gösterdi. Genel sorunun yanıtı bugün de bilinmiyor:

Soru: *n herhangi bir sayıysa ve $1^{n-1}+2^{n-1}+ ...+(n-1)^{n-1}$ sayısı n'ye bölündüğünde kalan $n - 1$ ise, n asal mıdır?*

Gerçek asallara geri dönelim. Wilson Teoremi, hemen hemen Fermat'nın Küçük Teoremi kadar önemlidir:

Teorem 11. *Eğer p asalsa, p, $(p - 1)! + 1$'i böler.*

Asallar üzerine yanıtı bilinmeyen bir başka soru geçeyim. Goldbach, bir mektubunda aşağıdaki soruyu Euler'e sordu (1972):

Goldbach Sanısı (1): *5'ten büyük her sayı üç asalın toplamına eşittir.*

Euler, Goldbach'a sorunun yanıtını bilmediğini, ama sorunun aşağıdaki soruyla eşdeğer olduğunu yazdı:

Goldbach Sanısı (2): *4'ten büyük her çift sayı iki asalın toplamıdır.*

Örneğin,

$4 = 2+2$
$6 = 3+3$
$8 = 3+5$
$10 = 3+7 = 5+5$
$12 = 5+7$
$14 = 3+11 = 7+7$
$16 = 3+13 = 5+11$
$18 = 5+13 = 7+11$
$20 = 3+17 = 7+13$
$22 = 3+19 = 5+17 = 11+11$
$24 = 5+19 = 7+17 = 11+13$
$26 = 3+23 = 7+19 = 13+13$

Yüz milyondan küçük sayılar için Goldbach sanısının doğru olduğu biliniyor. Önermenin her sayı için doğru olduğu bilinmiyor, ancak doğru olduğu sanılıyor. Bu sanıyı kanıtlayabilirseniz ölümsüzler arasında yerinizi alırsınız.

Asal sayılar üzerine dahaca çözülememiş bir başka ünlü sanı vardır:

İkiz Asallar Sanısı: *Sonsuz tane ikiz asal sayı vardır*.

Eğer iki asal sayının arasındaki fark 2 ise, bu iki asal sayıya **ikiz** denir. Örneğin, (3,5), (5,7), (11,13), (17,19), (29,31), (41,43) ikiz asal sayılardır. Sonsuz tane ikiz asalın olup olmadığı bilinmiyor. "Bilinse ne olur, bilinmese ne olur?" demeyin. Yanıtı bilinmeyen her soru ilginçtir, üzerinde düşünmeye değer. İnsan yalnızca "düşünen hayvan" değildir, nedenli nedensiz düşünen hayvandır.

1966'da, sonsuz tane asal p sayısı için, $p + 2$ sayısının ya asal ya da iki asalın çarpımı olduğu kanıtlandı.

Bilinen en büyük ikiz asallar $1.706.595 \times 2^{11235} \pm 1$ asallarıdır, 1990'da Parady, Smith ve Zarantonello bulmuştur.

Üçüz asal var mıdır? (3,5,7)'den başka yoktur. Okur bunu kolaylıkla kanıtlayabilir. Bir ipucu verelim: eğer n bir tamsayıysa, n, n+2, n+4 sayılarından biri 3'e bölünür.

Yukarda sonsuz tane asal sayının olduğunu gördük. Gene de o kadar fazla asal sayı yoktur. Örneğin, çift sayılar (2 dışında) asal olamayacaklarından, sayıların "yarısından fazlası" asal değildir. 1'le n arasından rastgele bir sayı seçsek, bu sayının asal olma olasılığı kaçtır? Bu olasılık n'ye göre değişir elbet. Eğer $n = 100$ ise, bu olasılığın 1/4 olduğunu yazının en başında görmüştük.

Eğer n bir tamsayıysa, $\pi(n)$, n'den küçük asalların sayısı olsun. $\pi(n)/n$, n'den küçük rastgele seçilmiş bir sayının asal olma olasılığıdır. n sonsuza gittiğinde, bu olasılığın değeri kaçtır? Okur, n büyüdükçe, asal seçme olasılığının da küçüleceğini ve n sonsuza gittiğinde bu olasılığın 0'a yakınsayacağını tahmin edebilir. Bu tahmin doğrudur[7]:

$$\lim_{n\to\infty} \pi(n)/n = 0.$$

Bundan çok daha iyi bir sonuç bilinmektedir. $\pi(n)/n$ ve $1/\log(n)$, n büyüdükçe birbirlerine çok yakınsamaktadırlar[8]. Başka bir deyişle, eğer n büyükse, $\pi(n)$ aşağı yukarı $n/\log(n)$ dur, yani $\pi(n) \approx n/\log(n)$. Bu sonuca **Asal Sayılar Teoremi** adı verilir.

Asal sayılar son derece ilginç bir konudur. Asal sayılar konusunda bilgilenmek isteyen okur [33] ve [40]'a bakabilir. Hele Euler'in sonsuz tane asal sayının olduğunu (bir kez daha) kanıtlayan bir kanıtı vardır ki...

7 [44]'teki "Gerçekten Asal Var mı" yazısında bu limitin 0 olduğu kanıtlanmıştır.

8 Buradaki log, e temelindeki logaritmadır.