Bu yazıda hile yapıyorum... Bir yerde bir hata var.

Gerçekten Asal Var mı?

Ali Nesin

Kendinden ve birden başka sayıya bölünmeyen sayılara **asal** denir. Örneğin, 2, 3, 5, 7, 11, 13, 17, 19 asal sayılardır. Ama 35 asal değildir, çünkü 5'e bölünür. Teknik nedenlerden 1 asal sayılmaz.

Sonsuz tane asal olduğu ta eski Yunanlılardan beri biliniyordu. Öklid'in Elemanlar adlı kitabında vardır bunun kanıtı. Öklid'in aktardığı bu kanıt dünyanın en güzel kanıtlarından biri olarak kabul edilir. Öylesine güzeldir ki, bu kanıtı bilmeden ölenlere, matematikçiler, âşık olmadan ölmüş biri gözüyle, yani acıyarak bakarlar. Matematik ve Korku adlı kitabımın *Asal Sayılar* başlıklı yazısında bu güzel kanıtı bulabilirsiniz.

100'den küçük 25 tane asal sayı vardır. İşte o asal sayılar: 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, yüzden küçük sayıların yüzde 25'i, yani dörtte biri asaldır.

Bir başka deyişle, ilk yüz sayı arasından rastgele bir sayı seçecek olursak, bir asal sayı seçme olasılığımız 1/4'tür, yani yüzde 25'tir, yani 0,25'tir[1].

1000'den küçük kaç tane asal vardır? Hepsini teker teker bulabiliriz. Bir bilgisayar zaman kazandırır. 1000'den küçük asallar şunlar:

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, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997.

Tam 168 tane var. Demek ki, 1'le 1000 arası rastgele bir sayı seçecek olsak, bir asal sayı seçme olasılığımız 168/1000'dir, yani 0,168'dir.

Görüldüğü gibi ilk yüz sayıda asallar daha yoğun: İlk yüz sayıda asal bulma olasılığı, ilk bin sayıda asal bulma olasılığından daha fazla.

Eğer n bir tamsayıysa, $p(n)$, n'den küçük asal sayı sayısı olsun. Örneğin, $p(100) = 25$ ve $p(1000) = 168$.

Asalların ne kadar yoğun olduğunu anlamak istiyoruz, yani $p(n)/n$ sayısıyla ilgileniyoruz. Asal sayıların yoğunluğunu ölçen bu sayılara $y(n)$ diyelim. Bu sayı, n'den küçük rastgele seçilmiş bir sayının asal olma olasılığıdır. Yukardaki deneylerden,

$$y(100) = p(100)/100 = 0,25$$
$$y(1000) = p(1000)/1000 = 0,168$$

olduğu anlaşılıyor.

Bu yoğunlukları bilgisayarımda hesaplattırdım. İşte birkaç sonuç:

$y(100) = 25/100 = 0,25$

[1] Matematikte olasılıklar 1 üzerinden hesaplanır.

$y(200)$	=	46/200	= 0,23
$y(300)$	=	62/300	= 0,206666...
$y(400)$	=	78/400	= 0,195
$y(500)$	=	95/500	= 0,19
$y(600)$	=	109/600	= 0,181666...
$y(700)$	=	125/700	= 0,17857...
$y(800)$	=	139/800	= 0,17375
$y(900)$	=	154/900	= 0,17111...
$y(1000)$	=	168/1000	= 0,168
$y(2000)$	=	303/2000	= 0,1515
$y(3000)$	=	430/3000	= 0,143333...
$y(4000)$	=	550/4000	= 0,1375
$y(5000)$	=	669/5000	= 0,1338
$y(6000)$	=	783/6000	= 0,1305
$y(7000)$	=	900/7000	= 0,12857...
$y(8000)$	=	1007/8000	= 0,125875
$y(9000)$	=	1117/9000	= 0,1241111...
$y(10000)$	=	1229/10000	= 0,1229
$y(20000)$	=	2262/20000	= 0,1131
$y(30000)$	=	3245/30000	= 0,1081666...
$y(40000)$	=	4203/40000	= 0,105075
$y(50000)$	=	5133/50000	= 0,10266
$y(60000)$	=	6057/60000	= 0,10095
$y(70000)$	=	6935/70000	= 0,0990714...
$y(80000)$	=	7837/80000	= 0,0979625
$y(90000)$	=	8713/90000	= 0,0968111...
$y(100000)$	=	9593/100000	= 0,09593

Yoğunlukların giderek küçüldüğünden artık hiç kuşkumuz yok sayılır. Belli ki asalların yoğunluğu gitgide azalıyor[2].

Bu yoğunluk nereye dek küçülüyor? Örneğin 0,08'in ya da 0,09'un altına iniyor mu? İniyorsa, 0,01'in altına iniyor mu? Ya daha aşağılara?

Başka türlü yaklaşalım konumuza.

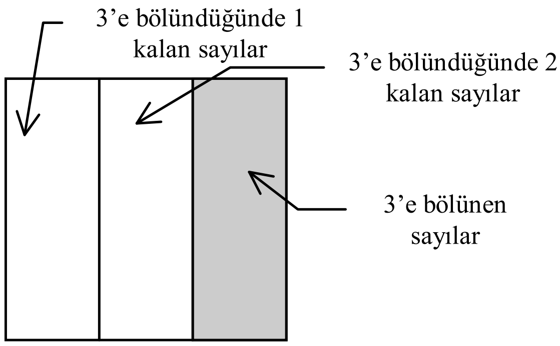
Doğal sayılar arasından rastgele bir sayı seçiyoruz. Bu sayının çift olma olasılığı kaçtır? 1/2'dir elbet. Çünkü sayıların "yarısı" çifttir, "yarısı" da tek. Demek ki, rastgele seçilen bir sayının tek olması yani ikiye bölünmeme olasılığı da 1/2'dir.

Sayıları her kenarının uzunluğu 1 olan bir kareye koyacak olursak, bunu şöyle de gösterebiliriz:

Peki ya rastgele seçilen bir sayının üçe bölünebilme olasılığı kaçtır? 1/3'tür. Çünkü sayıların "üçte biri" üçe bölünür, geri kalan "üçte ikisi" bölünmez. Rastgele seçilmiş bir sayının üçe bölünme olasılığı nasıl 1/3 ise, üçe bölünmeme olasılığı da 2/3'tür. (Toplam olasılık 1, yani yüzde yüz olmalı.)

Bunu, yukardaki gibi bir şemayla gösterebiliriz:

2 Doğru önerme şöyle: "$y(n+1) < y(n)$ ancak ve ancak $n + 1$ asal değilse." Demek ki yoğunluklar her zaman değil, ama genellikle küçülüyorlar.

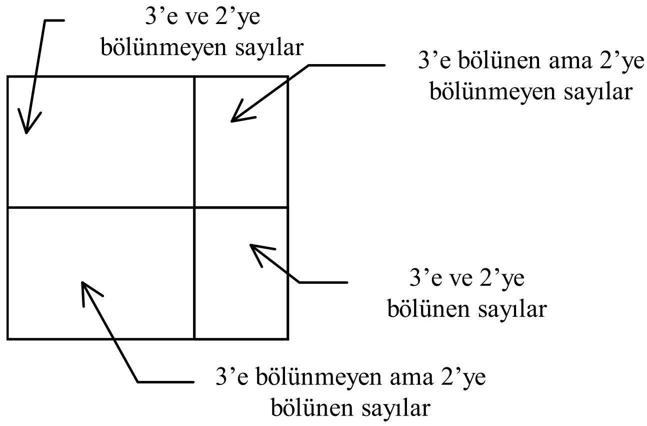


Genel olarak, rastgele seçilmiş bir sayının *n*’ye (tam olarak) bölünme olasılığı 1/*n*’dir, bölünmeme olasılığı da 1 – 1/*n*’dir elbet (toplam olasılık 1, yani yüzde yüz olmalı.)

Şimdi daha zor bir soru soralım. Rastgele seçilmiş bir sayının ne ikiye ne de üçe bölünme olasılığı kaçtır?

Rastgele bir sayının ikiye bölünmeme olasılığı 1/2, üçe bölünmeme olasılığı da 2/3. Bunu biliyoruz. Bu iki bilgiyi kullanarak, rastgele bir sayının ne ikiye ne de üçe bölünmeme olasılığını bulabilir miyiz? Evet! 1/2’yle 2/3’ün çarpımına eşittir bu olasılık.

Neden? Açıklayayım. Yukardaki iki şekli üstüste koyalım:



Rastgele seçilmiş bir sayının ne ikiye ne de üçe bölünmemesi demek, yukardaki kareye rastgele bir taş atıldığında, bu taşın sol üst bölgeye düşmesi demektir. Görüldüğü gibi, ikiye ve üçe bölünmeyen sayıları simgeleyen bu sol üst köşedeki bölge bir dikdörtgendir ve bu dikdörtgenin bir kenarı 1/2, öbür kenarı 2/3’tür. Yani, kareye rastgele atılan bir taşın sol üst dikdörtgenin içine düşme olasılığı 1/2 × 2/3 = 1/3’tür. Demek ki bir sayının ne ikiye ne de üçe bölünme olasılığı 1/3’tür.

Sorularımızı gittikçe zorlaştıralım. Rastgele seçilmiş bir sayının ne ikiye, ne üçe, ne de beşe bölünmeme olasılığı kaçtır? Rastgele seçilmiş bir sayının ne ikiye ne de üçe bölünmeme olasılığının 1/3 olduğunu biraz önce gördük. Rastgele seçilmiş bir sayının beşe bölünmeme olasılğı da 1–1/5, yani 4/5’tir, bunu da yukarda görmüştük. Bu iki bilgiyi kullanarak, rastgele bir sayının ikiye, üçe ve beşe bölünmeme olasılığını bulabiliriz. Yukardaki yöntemi kullanabiliriz. Bu olasılık, 1/3 ile 4/5’in çarpımına eşittir, yani 1/3 × 4/5 = 4/15’tir. Bu sayıyı şöyle yazalım:

$$(1 - 1/2) \times (1 - 1/3) \times (1 - 1/5).$$

Rastgele bir sayının ikiye, üçe, beşe ve yediye bölünmeme olasılığı da,

$$(1 - 1/2) \times (1 - 1/3) \times (1 - 1/5) \times (1 - 1/7)$$

dir.

Genel olarak, p_1, ..., p_n değişik asallarsa, rastgele seçilmiş bir sayının bu asallara bölünmeme olasılığı, $1 - 1/p_1$, ..., $1 - 1/p_n$ sayılarının çarpımıdır.

Küçük p asal sayıları için, bir sayının p ve p'den küçük asallara bölünmeme olasılığını bilgisayarıma hesaplattım:

p	kesirli olasılık	değeri ($\pm 10^{-4}$)
2	1/2	0,5
3	1/3	0,3333
5	4/15	0,2667
7	8/35	0,2286
11	16/77	0,2078
13	192/1001	0,1918
17	3072/17017	0,1805
19	55296/323323	0,1710
23	110592/676039	0,1636
29	442368/2800733	0,1579

Olasılıklar gittikçe küçülüyorlar, çünkü bir önceki sayıyı 0'la 1 arasında bir sayıyla çarpıyoruz. Bu da sezgimizle çatışmıyor, sayı büyüdükçe, rastgele bir sayının o sayıdan küçük asallara bölünmeme olasılığı küçülür.

Bu çarpımlar p büyüdükçe ne olurlar? Küçüldüklerini gördük. Ama bunun da ötesinde? p sonsuza yaklaştıkça, yukarda bulduğumuz değerler hangi sayıya yakınsar?

Yanıtı vereyim: 0'a. Bir başka deyişle,

$$1/2 \times 2/3 \times 4/5 \times 6/7 \times 10/11 \times 12/13 \times 16/17 \times 18/19...$$

sonsuz çarpımı sıfıra eşittir.

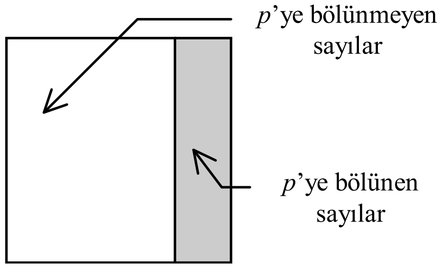
Neden? Çok basit. Çünkü yukardaki sonsuz çarpım, rastgele seçilmiş bir doğal sayının hiçbir asala bölünmeme olasılığıdır ve hiçbir asala bölünmeyen bir tek doğal sayı vardır, o da 1'dir. Sonsuz tane sayı arasından 1'i (rastgele) seçme olasılığı 0 olduğundan, yukardaki sonsuz çarpım da 0'dır.

Şimdi, doğal sayılar arasından rastgele seçilmiş bir sayının asal olma olasılığının 0 olduğunu kanıtlayacağız. Bir başka deyişle, doğal sayılar arasından rastgele seçilmiş bir sayının asal olamayacağını kanıtlayacağız.

"Bal gibi olur, bir asal seçerim, olur biter," demeyin. Olmaz! Rastgele seçerseniz olamaz. İsteyerek, özellikle bir asal seçebilirsiniz elbet. Ama biz burada rastgele bir seçimden sözediyoruz.

Kanıta başlıyorum:

1. Herhangi bir asal ele alalım. Bu asala p adını verelim. Rastgele seçilmiş bir sayının ya p'ye bölünmeme ya da p'ye eşit olma olasılığını hesaplayalım. Bir başka deyişle, aşağıdaki kareye rastgele bir taş attığımızda, bu taşın ya sol bölgeye ya da (sağ bölgede bulunan) p noktasına düşme olasılığını hesaplayacağız.



Rastgele seçilmiş bir sayının p'ye bölünmeme olasılığının $1–1/p$ olduğunu yukarda görmüştük. Rastgele seçilmiş bir sayının p olma olasılığı sıfırdır (çünkü sonsuz tane sayı vardır ve rastgele bir sayı seçersek p'yi seçemeyiz.) Dolayısıyla, rastgele seçilmiş bir sayının ya p'ye bölünmeme ya da p'ye eşit olma olasılığı da $1–1/p$'dir.

Örneğin rastgele seçilmiş bir sayının ya 2'ye eşit olma ya da 2'ye bölünmeme olasılığı 1–1/2'dir. Bunun gibi rastgele bir sayının ya 5'e eşit olma ya da 5'e bölünmeme olasılığı 1–1/5'tir.

2. p bir asal sayı olsun. $A_p(x)$ olayı[3], "ya $x = p$ ya da p, x'i bölmez'' olsun. Bir üstteki paragrafta gördüğümüz gibi, $A_p(x)$ olayının gerçekleşme olasılığı $1 – 1/p$'dir.

Kolayca görüleceği üzere, eğer p ve q değişik asallarsa, "$A_p(x)$ ve $A_q(x)$" olayı, ya

x'in ne p'ye ne de q'ye bölünmeme

ya da

x'in p ve q sayılarından birine eşit olma

olayıdır. Daha önceki açıklamalarımızı anlayan okur, "$A_p(x)$ ve $A_q(x)$" olayının gerçekleşme olasılığının her iki olayın gerçekleşme olasılıklarının çarpımına, yani $(1–1/p)(1–1/q)$ sayısına eşit olduğuna kolayca inanacaktır[4].

Daha da genel olarak, eğer $p_1, p_2, ..., p_k$ değişik asallarsa,

"$A_{p_1}(x)$ ve $A_{p_2}(x)$ ve …. ve $A_{p_k}(x)$ olayı",

x'in ya bu asallardan hiçbirine bölünmeme ya da bunlardan birine eşit olma olayıdır. Bu olayın gerçekleşme olasılığı da,

$$(1–1/p_1)(1–1/p_2)... (1–1/p_k)$$

çarpımına eşittir.

3. Şimdi "her p için $A_p(x)$" olayına bakalım, yani "$A_2(x)$ ve $A_3(x)$ ve $A_5(x)$ ve $A_7(x)$ ve ..." olayına. Bir üstteki paragraftan anlaşılacağı üzere, bu olay, "ya hiçbir asal x'i bölmez (yani $x = 1$) ya da x bir asaldır" olayıdır. Gene bir üstteki paragraftan anlaşılacağı üzere, bu olayın olasılığı, $(1–1/2)(1–1/3)(1–1/5)(1–1/7)$ ... sonsuz çarpımına, yani daha önce de gördüğümüz üzere 0'a eşittir. "$x = 1$" olayının olasılığı 0 olduğundan, x'in asal olma olasılığı da 0'dır.

Demek ki, rastgele seçilmiş bir sayının asal olma olasılığı 0'dır. Bir başka deyişle, sonsuz tane asal vardır, ama asalların sayısı, tüm sayılarla karşılaştırıldığında, o kadar da fazla değildir.

3 Burada "olay" sözcüğünü, Türkçede ne yazık ki çok sık ve gerekli gereksiz kullanılmaya başlanan ve nerdeyse argolaşan anlamında kullanmıyorum. Burda kullanılan "olay" sözcüğü, matematiksel bir terimdir.

4 Ama genel olarak "A ve B" olayının gerçekleşme olasılığı, A olayının gerçekleşme olasılıyla B olayının gerçekleşme olasılığının çarpımına eşit değildir. Bu, burada öyle.