

## İKİZ ASAL SAYILAR ÜZERİNE

Urfat G. NURİYEYEV

Ege Üniversitesi, Fen Fakültesi, Matematik Bölümü, 35100; Bornova, İZMİR

e-mail: urfat@sci.ege.edu.tr

Halide G. SADİGOVA

Azerbaycan Bilimler Akademisi, Sibernetik Enstitüsü, 370141, Bakü, Azerbaycan

*Beni yıkamayan her şey beni güçlendirir.*

Nietsche

## 1. Giriş

Yakın zamanlara kadar sayılar teorisi matematiğin çok cazip, fakat hemen hemen hiç bir uygulaması olmayan bir alanıydı. Günümüzde kuramsal sayısal algoritmalar çeşitli şifreleme (kriptografi) sistemlerinde geniş bir şekilde kullanılmaktadır. Bu tür sistemlerde kullanılmak üzere büyük asal sayıların bulunması gerekmektedir.

Bu yazıyla amaçlanan asal sayıların uygulama alanlarını ve bu alanda son zamanlardaki gelişmeleri tanıtmak ve ikiz asal sayıları bulmak için bir algoritma vermektir.

Bir zamanlar ilgi görmeyen alanlardan biri olan çarpanlara ayırma çalışmaları, şifreleme ve bilgisayar güvenliğiyle ilgili olduğu için bugün matematiğin en popüler alanlardan birisidir.

Günümüzdeki bilgisayarlar, son derece hızlı olmalarına rağmen büyük sayıların çarpanlarını doğru bulmayı başaramıyorlar. Bu, bir tamsayıyı çarpanlarına ayırmak için şimdiye kadar etkin bir yöntemin bulunamamasından kaynaklanmaktadır. Bu tür algoritmaların olmamasından dolayı farklı şifreleme sistemlerinin kullanılma olanağı ortaya çıkmıştır. Eğer böyle algoritmalar bulunursa bu sistemlerin hepsi çöker.

Böylece bazen bir algoritmanın olmaması onun olmasından daha yararlı olabilir. Bu, belki de insanlığın, matematiğin başarısından çok başarısızlığından yararlandığı tek durumdur.

## 2. Asal sayılar

Sayma sayılarına *pozitif tamsayılar* denir. Bu kümeyi

$$S = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \dots\}$$

ile gösterelim. Yalnızca 1 ve kendisi ile tam olarak (yani kalan bırakmadan) bölünebilen tamsayılara *asal sayılar* denir. Örnek olarak 5, 11 veya 23'ü verebiliriz. Bu tür sayıların sonsuz sayıda olduğu bilinmektedir.

**Öklid (Euclides) Teoremi:** Sonsuz tane asal sayı vardır.

Asal sayılar kümesini

$$P = \{2, 3, 5, 7, 11, 13, 17, 19, 23, \dots\}$$

olarak gösterelim. Bunların dışında kalan bütün tamsayılara *bileşik sayılar* denir. Bütün bileşik sayılar kendilerinden daha küçük olan tamsayıların çarpımlarından elde edilebilirler; örneğin 72 sayısı 8 ile 9'un çarpımından elde edilir. Daha küçük olan bu tamsayılara, büyük sayının *çarpanları* denir. Bunlar arasında daha özel olan çarpanlar bulunur; *asal çarpanlar*. Yukarıdaki örnekte verilen 8 ve 9'un her ikisi de asal olmadığından onların her biri tekrar çarpanlarına ayrılabilir. Çarpanlara ayırma sonucu elde edilen sayılar içinde sadece asal çarpanlar kalana kadar çarpanlarına ayırma işlemi sürdürülebilir. Bileşik sayı olan 72 için işlem  $72 = 2 \times 2 \times 2 \times 3 \times 3 = 2^3 \cdot 3^2$  ifadesine ulaşıncaya kadar sürdürülmüştür. Burada üç tane 2 ve iki tane 3, 72 sayısının asal çarpanlarıdır. Asal çarpanlar özeldir; çünkü her bileşik sayı için bir tane ve sadece bir tane asal çarpanlar takımı vardır. Bu nedenle asal sayılar, bütün diğer sayıların onların çarpımı yoluyla elde edildiği atomlardır (veya en küçük parçalardır).

**Aritmetiğin Temel Teoremi:**  $n > 1$  olmak üzere, her bir  $n$  pozitif tamsayısı

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_s, s \geq 1$$

şeklinde  $p_1, p_2, \dots, p_s$  asal sayılarının çarpımı olarak yazılabilir. Bu yazılış, çarpanların sırası göz önüne alınmazsa, tek türdür.

Bu özelliğe, *pozitif tamsayıların tek çarpanlama (factorization) teoremi* denilmektedir. Bu ayrılış şeklini yeniden düzenlemek ve yalnız farklı asalları almak suretiyle

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_t^{k_t}$$

yazabiliriz. Burada  $k_i \geq 1$  ve  $p_1, p_2, \dots, p_t$  farklı asallardır.

**Not 1:** 1 sayısı ne asal, ne de bileşik sayıdır.

### 3. Asal sayıların bulunması algoritması üzerine

Eski zamanlardan beri matematikçiler asal sayılarla ilgilenmişlerdir. Asal sayılarla ilgili temel problemlerden biri, verilen bir sayının asal olup olmadığını kontrol etmektir. Şifrelemede geniş şekilde kullanıldığı için bir sayının asallığının testi önem kazanmıştır.

Antik Çinlilerden ve Yunanlılardan başlayarak çok kişi asallığı test etmek için efektif bir algoritma bulmaya çalışmıştır. Asallığın testi için ilk yöntemi M.Ö. 240 yıllarında Erastotenes (Eratosthenes) önermiştir.

**Erastotenes Kalburu (Eleği):** Verilmiş bir  $n$  sayısından büyük olmayan asal sayılar tablosunu yazmak için 2'den başlayarak  $n$ ' e kadar tamsayılar dizisini yazalım.

$$2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \dots, n.$$

Dizinin ilk sayısı olan 2 asaldır. Bu dizide 2'den sonraki sayılar için, birer atlayarak 4, 6, 8, ... i (yani 2'nin katlarını) silelim. Bu işlemden sonra kalan ilk silinmemiş sayı 3 olur ki, o da asaldır, çünkü 2'ye bölünmez. 3'ü silmeden ikişer atlayarak 6, 9, 12, 15, ... i (yani 3'ün katlarını) silelim. Çift sayı oldukları için bunlardan bazıları önceden silinmiştir. Sonraki adımda ilk silinmemiş sayı 5'dir ve o asaldır, çünkü 2 ve 3'e bölünmez. 5'i silmeden dörder atlayarak 10, 15, 20, ... i (yani 5'in katlarını) silelim. Yine bu sayılardan bazıları 2'nin, bazıları 3'ün katı olduklarından daha önceki adımda silinmişti. Şimdi en küçük silinmemiş sayı 7'dir ve o asaldır, çünkü ondan küçük asal sayılara,

yani 2, 3, ve 5'e bölünmez. Böylece  $n'$  den küçük asal sayıların tablosu  $\sqrt{n'}$ 'i geçmeyen sayıların katlarının silinmesiyle (başka deyişle elenmesiyle) biter.

Bu algoritmayı verilen bir  $n$  sayısını çarpanlarına ayırmak için de kullanabiliriz. Örneğin 60 sayısı verildiğinde, en küçük asal sayıdan başlayarak sırasıyla asal sayılardan her birine (yani 2, 3, 5, ...) bölünüp bölünmediği test edilir. Burada 60'ı bölen ilk sayı en küçük çarpan olur. Bu sayıyı bulduktan sonra aynı süreç tekrarlanarak daha büyük asal çarpanlar bulunur. Sayı büyüdükçe çarpan bulma işi de zorlaşır Buna rağmen bu yöntem en azından ilke olarak her tamsayıya uygulanabilen bir yöntemdir. Eğer sayının kareköküne kadar olan bütün asal sayılar denenmiş ve bir çarpan bulunmamışsa, sayının kendisinden ve 1'den başka çarpanı yok demektir; dolayısıyla bu bir asal sayıdır.

Yukarıda verilen kaba kuvvete dayanarak çarpanlara ayırma yönteminin uygulanması basamak sayısı arttıkça daha da zorlaşır. Örneğin  $2^{193} - 1$  sayısının ondalık ifadesinde 58 basamak vardır. Günümüzde her nanosaniyede (milyonda bir saniyede) bir bölme işlemi yapabilen en hızlı bilgisayarlar kullanıldığında bile, gösterilen yöntemle çarpanları bulmak 35.000 yıllık bir bilgisayar süresi gerektirir.

Büyük sayıların çarpanlarının bu yöntemle elde edilemeyeceği aşikardır. XVII yüzyılda Fermat 'ın küçük teoremi olarak bilinen teorem ispatlandı ve çarpanlara ayırma işleminde yeni bir sayfa açılmış oldu.

**Fermat Teoremi:**  $p$  asal sayı ise, her  $a$  tamsayısı için  $p$ ,  $(a^p - a)$ 'yı böler.

Ancak bu teoremin tersi Carmichael sayıları için geçerli değildir. Bu sonuç asallığı test eden algoritmalar için çıkış noktası olmuştur. 1976 yılında Miller, sonra da Rabin Genişletilmiş Riemann hipotezine dayanan ve hızlı çalışan, olasılıklı algoritmalar ürettiler. O zamandan bu yana bu konuda pek çok algoritma önerilmiştir. Bunlara örnek olarak 1983'de Adleman, Pomeance ve Rumely algoritmasını gösterebiliriz. 1986'da Coldwasser ve Kilian eliptik eğrilere dayanan bir algoritma önerdiler. Asallığı test etmek için en son algoritma 2002 yılının Ağustos ayında Hindistan'ın Kanpur kentindeki Teknoloji Enstitüsünde Manindra Agrawal ve onun öğrencileri tarafından önerilmiştir. Algoritma polinomial zamanda çalışır (karmaşıklığı  $O((\log n)^{12})$  dir). Bu çalışmasıyla Agrawal Clay araştırma ödülünü almıştır ve Fields madalyasını almaya adaydır.

Sayıları çarpanlara ayırma algoritmasına örnek olarak Pollard, Lensta ve Pomerance algoritmalarını gösterebiliriz. Çarpanlara ayırmanın zirvesi, "tek bir süper bilgisayar"la değil, birçoğunun ortak çabasıyla başarılmıştır. En son eğilim, çok sayıda farklı bilgisayarın hesaplamalarını bir araya getirme yönündedir. Bunların her biri tek bir çarpanlara ayırma probleminin ayrı yönleri üzerinde (genellikle yoğun olmayan gece saatlerinde) çalışır. Daha sonra yaptıklarını birleştirmek için bunları elektronik posta yoluyla bir bilgi işlem merkezine bildirir.

Bu yaklaşımın en başarılı sonucu olarak GIMPS (The Great Internet Mersenne Prime Search), farklı ülkelerde binlerce bilgisayarı 2,5 sene kullanarak 14 Kasım 2001 tarihinde 4053946 basamaklı  $2^{13466917} - 1$  sayısını, yani 39. Mersenne asal sayısını bulmuştur. Bu sayının asal olup olmadığını kontrol etmek 45 gün sürmüştür.

**Not 2:**  $M_n = 2^n - 1$  şeklinde gösterilebilen asal sayılara *Mersenne asal sayıları* denir. Yukarıdan anlaşıldığı gibi şimdiye kadar 39 tane böyle sayı bulunmuştur:  $M_2 = 2^2 - 1 = 3$ ,  $M_3 = 2^3 - 1 = 7$ ,  $M_5 = 2^5 - 1 = 31$ ,  $M_7 = 2^7 - 1 = 127$  v.s.

#### 4. İki asal sayılar

Asal sayılar teorisinde ilk bakışta çok basit gibi görünen farklı sorularla karşılaşırız. Fakat bunlardan bazıları kolaylıkla cevaplanabilir. Örneğin en küçük iki asal sayı olan 2 ve 3 asal sayıları ardışık doğal sayılardır. Buradan aklımıza şu soru gelebilir: Aynı şekilde ardışık olan başka asal sayılar

var mıdır? Bunun olmadığını kolaylıkla gösterebiliriz. İki ardışık doğal sayıdan birisi mutlaka çift sayıdır. Sadece 2 sayısı çift asal sayı olduğundan bu sayının asal olmadığını söyleyebiliriz. Ancak bir çok ardışık tek sayılar vardır ki, ikisi de asaldır, örneğin 3 ve 5, 5 ve 7; 11 ve 13, 17 ve 19, 29 ve 31, 41 ve 43 ve diğerleri. Bu tür ikililere *ikiz asal sayılar* denir. 30 milyona kadar 152892 tane ikiz asal sayı ikilisi vardır. İkiz asal sayılar kümesini

$$PP = \{3, 5, 7, 11, 13, 17, 19, 29, 31, 41, 43, \dots\}$$

ile gösterelim. Çok eski zamanlardan beri bu kümenin sonsuz olup olmadığı problemi araştırılmaktadır ve günümüze kadar bu problem çözümlenememiştir. Yani biz 2 sayısının sonsuz yolla iki asal sayının farkı gibi gösterilebileceğini ispatlayamıyoruz.

Her çift sayının sonsuz yolla iki asal sayının farkı gibi gösterilebileceği düşünülmesine rağmen bunun hiç olmazsa bir yolla yapılabileceği bile ispatlanamamasına karşın bu bir çok ardışık çift sayılar için gösterilmiştir. Örneğin  $2 = 5 - 3$ ,  $4 = 11 - 7$ ,  $6 = 29 - 23$ ,  $8 = 97 - 89$ ,  $10 = 149 - 139$ .

Asal sayılar teorisinde buna benzer kolay gibi gözükken, fakat daha ispatlanamamış yüzlerce problem vardır ve bu problemler günümüzde bir çok matematikçinin ilgisini çekmektedir.

#### 4.1. İkiz Asal Sayılar Üzerine Bazı Teoremler

$L^6 = \{l | l = 6n \pm 1, n \in S\}$  şeklinde gösterelim. Buna göre aşağıdaki teoremler doğrudur:

**Teorem 1.**  $PP \setminus \{3\} \subseteq L^6$ .

$K^6 = \{k | l_1 = 6k + 1 \in P \wedge l_2 = 6k - 1 \in P\}$  şeklinde gösterelim. Buna göre aşağıdaki teorem doğrudur:

**Teorem 2.**  $\exists m, n \in S, k = 6mn \pm m \pm n \Rightarrow k \notin K^6$ .

$$M_j^6 = \{k | k = 6mn \pm m \pm n, m = j, j \in S, n \in S\} = \\ = \{k | k = (6j - 1)n \pm j, n \in S\} \cup \{k | k = (6j + 1)n \pm j, n \in S\}$$

şeklinde gösterelim. Örneğin;

$$j = 1 \Rightarrow M_1^6 = \{k | k = 5n \pm 1, n \in S\} \cup \{k | k = 7n \pm 1, n \in S\}$$

$$j = 2 \Rightarrow M_2^6 = \{k | k = 11n \pm 2, n \in S\} \cup \{k | k = 13n \pm 2, n \in S\}$$

$$j = 3 \Rightarrow M_3^6 = \{k | k = 17n \pm 3, n \in S\} \cup \{k | k = 19j \pm 3, n \in S\}$$

$$A_i^6 = \{k \in S | 6i^2 - 2i \leq k < 6(i+1)^2 - 2(i+1), i \in S\}$$

$M_j^6 \cap A_i^6 = P_{ij}^6$ ,  $A_i^6 \setminus \cup_{j=1}^i P_{ij}^6 = P_i^6$  ve  $P^6 = \cup_{i=1}^{\infty} P_i^6$  şeklinde gösterelim. Buna göre aşağıdaki teoremler doğrudur:

**Teorem 3.**  $P_i^6 \subset K^6, i = 1, 2, 3, \dots$

$P_0^6 = \{1, 2, 3\}$  kabul etsek aşağıdaki teorem doğrudur.

**Teorem 4.**  $K^6 = \{1, 2, 3\} \cup (\cup_{i=1}^{\infty} P_i^6) = P_0^6 \cup P^6 = \cup_{i=0}^{\infty} P_i^6$

Aşağıdaki problemler bu konuda açık problemlerdir, yani henüz ispatlanamamıştır.

**Problem 1.**  $|P^6| = \infty$ ?

Burada  $|P^6|$ ,  $P^6$  kümesinin eleman sayısını ifade etmektedir

**Problem 2.**  $s \geq 3$ ,  $s \in S$  için  $|P^s| = \infty$ ?

Yukarıda  $P^s$  kümesi  $M_j^6, A_i^6, P_{ij}^6, P_i^6$  ve  $P^6$  kümelerinin ifadelerinde 6 yerine  $s$  yazılarak elde edilir.

#### 4.2. İkiz Asal Sayıları Bulma Algoritması :

Bu bölümde, yukarıda verilmiş teoremlerden yararlanılarak ikiz asal sayıları bulmak için bir algoritma önerilmiştir. Bu algoritma önceden verilmiş bir  $M$  sayısı için  $(6M + 1)$ ' den küçük tüm ikiz asal sayıları bulmaktadır.

##### Algoritma

0.  $M$  sayısını oku
1.  $n = 1$
2.  $A_2 :$   $i_1 = 6n^2 - 2n$
3.  $i_2 = i_1 + 12n + 3$
4.  $i = i_1$
5.  $A_3 :$   $k = 1$
6.  $A_4 :$   $k_1 = 6k - 1$
7.  $k_2 = 6k + 1$
8.  $k_3 = k_1 - k$
9.  $k_4 = k_2 - k$
10.  $k_5 \equiv i \pmod{k_1}$
11. Eğer  $(k_5 = k)$  veya  $(k_5 = k_3)$  ise,  $A_5$ 'e git
12.  $k_6 \equiv i \pmod{k_2}$
13. Eğer  $(k_6 = k)$  veya  $(k_6 = k_3)$  ise,  $A_5$ 'e git
14.  $k = k + 1$
15. Eğer  $(k_5 \leq k)$  ise,  $A_4$ 'e git
16.  $l_1 = 6i - 1$
17.  $l_2 = 6i + 1$
18.  $l_1$  ve  $l_2$ 'yi yaz
19.  $A_5 :$   $i = i + 1$
20. Eğer  $(i \leq i_2)$  ise,  $A_3$ 'e git
21.  $n = n + 1$

22. Eğer  $(n \leq M)$  ise,  $A_2'$ 'ye git  
 23. Dur

Bu algoritmanın çalışması sonucunda önceden verilmiş bir  $M$  sayısı için  $M$ ' den küçük olan ve bölüm 4.1'de tanımlanmış olan  $K^6$  kümesinin elemanları olan  $i$ ' ler bulunur ve bu  $i$ 'lerden  $l_1 = 6i - 1$  ve  $l_2 = 6i + 1$  ikiz asal sayıları hesaplanır. Böylece  $(6M + 1)$ 'e kadar olan bütün ikiz asal sayılar hesaplanmış olur. Bu algoritmadan yararlanılarak  $M$  sayısını artırıp istediğimiz büyüklükte ikiz asal sayılar bulabiliriz.

**Not 3:** Günümüzde bilinen en büyük ikiz asal sayılar 51090 basamaklı  $33218925 \times 2^{169690} \pm 1$  sayılarıdır. Bu sayılar 28 Eylül 2002 tarihinde bulunmuştur.

### 5. Alıştırmalar.

- 3' ten büyük olan her asal sayının  $6k + 1$  veya  $6k - 1$  şeklinde gösterilebileceğini ispatlayınız.
- 3' ten büyük olan her asal sayının karesinin  $12k + 1$  şeklinde gösterilebileceğini ispatlayınız.
- Bir asal sayının 30'a bölümünden kalanın da asal sayı olduğunu gösteriniz.
- $n > 2$  için  $2^n - 1$  ve  $2^n + 1$  sayılarının ikisinin de aynı zamanda asal sayı olamayacaklarını gösteriniz.
- $p$  ve  $p^2 + 2$  asal sayılarsa,  $(p^3 + 2)$ 'nin de asal sayı olduğunu gösteriniz.

### 6. Kaynak web siteleri üzerine

Asal sayılar konusunda ve benzer bilgileri aşağıdaki web sitelerinden öğrenebilirsiniz:

- <http://www.biltek.tubitak.gov.tr/asal> : Bu adreste bazı asal sayılar ve bazı çift sayıların iki asalın toplamı şeklinde yazılışlarının listelerini bulabilirsiniz.
- <http://www.utm.edu/research/primes> : Asal sayılar hakkında bilmek isteyeceğiniz bir çok şey bu sitede var. Küçük asal sayıların listesi, bilinen en büyük asal sayılar, büyük sayıların asal olup olmadıklarını ispatlamak için yöntemler v.s.
- <http://www.eff.org/coopawards/award-prime-rules.html> : EFF'nin en büyük asal sayı rekorunu kıranlara verdiği ödüllerin detaylarını bu sitede bulabilirsiniz
- <http://www.cse.iitk.ac.in/news/primality.html>

EFF (Elektronik Frontier Foundation - "Elektronik Sınırlar Vakfı") aslında bilgisayar dünyasında özgürlükleri savunan bir vakıftır. Vakfın büyük asallarla ilgisiyse, veri iletişimde kullanılan bazı kriptografik tekniklerin büyük asal sayıları kullanmalarınıdır. Vakıf, asallar hakkında araştırmaları teşvik ederek kriptografik teknikleri güçlendirmek amacıyla bu tip ödülleri veriyor.

EFF' in verdiği ödülleri burada ilan edelim: 10 milyon ondalık basamaklı ilk asal sayıyı bulana 100,000 dolar, 100 milyon basamaklı ilk asal sayıyı bulana 150.000 dolar, bir milyar basamaklı ilk sayıyı bulana 250,000 ödül verilecek

## KAYNAKLAR

- [1] Agrawal M., Kayal, N. and Saxena, N.: Primes is in P. Indian Institute of Technology, 2002  
<http://www.cse.iitk.ac.in/news/primality.html>.
- [2] Apostol, T.M.: Introduction to Analytic Number Theory. Springer - Verlag, 1997.
- [3] Adleman, L.M., Pomerance, C. and Rumely, R.S.: On distinguishing prime numbers from composite numbers. Ann. Math., 117:173-206,1983.
- [4] Miller, G.L.: Riemann's hypothesis and tests for primality. J. Comput. Sys. Sci. 13:300-317,1976
- [5] Rabin, M.O.: Probabilistic algorithm for testing primality. J. Number Theory, 12: 128-138,1980.
- [6] Riesel, H.: Prime Numbers and Computer Methods for Factorization. Progress in Mathematics. Birkhauser,1985