DÜSTAD
Dünya Sağlık ve Tabiat Bilimleri Dergisi
JOGHENS
Journal of Global Health & Natural Science
ISSN: 2687-637X Yıl: 2022 Cilt: 5 Sayı: 2

Çelik Asal Sayıları

Kadir Can ÇELİK[1]

Özet: Asal sayılar günümüzde pek çok alanda kullanılmaktadır. Bu alanların başında matematik ve kriptoloji alanları bulunmaktadır. Asal sayıların arasındaki olası düzenin bulunması veya yeni asal sayıların keşfi, başta bu alanlar olmak üzere tüm alanları etkileyecektir. Bu sebeple asal sayılar çok uzun zamandır matematikçilerin dikkatini çekmektedir. Eğer asal sayıların arasındaki olası düzen bulunursa internet şifrelemeleri kökten etkilenecektir. Bunun yanında bulunacak yeni asal sayılar da şifrelemelerde kullanılarak güvenlik düzeyini arttıracaktır. Günümüzde tüm asal sayıları tespit edecek veya bir sayının asal olup olmadığını anında çözümleyecek bir yöntem yoktur ancak farklı formüllerle yeni asal sayı bulma çalışmaları devam etmektedir. Bu makalede anlatılacak yöntem sayesinde yeni asal sayıların tespiti için önemli bir kapı aralanmış olacaktır.

Anahtar kelimeler: asal sayı, matematik, şifreleme, yeni asal sayı tespiti

Celik Prime Numbers

Abstract: Prime numbers are used in many fields today. Mathematics and cryptology are the leading areas of these fields. Finding the possible order among prime numbers or the discovery of new prime numbers will affect all areas, especially these areas. For this reason, prime numbers have attracted the attention of mathematicians for a very long time. Internet passwords will be radically affected if the possible sequence between prime numbers is found. In addition, the new prime numbers to be found will also increase the security level by using them in encryption. Today, there is no method to detect all prime numbers or to instantly analyze whether a number is prime or not, but studies are continuing to find new prime numbers with different formulas. Thanks to the method it will be explained in this article, it will be possible to determine new prime numbers.

Keywords: prime number, mathematics, encryption, detection of prime numbers

GİRİŞ

Asal sayı, 1 ve kendisi dışında hiçbir sayıya tam olarak bölünemeyen sayıları tanımlamak amacıyla kullanılan bir ifadedir. Asal olmayan sayılara ise bileşik sayı adı verilir (Yerlikaya, 2017). 0 ve 1 sayısı dışında kalan tüm doğal sayılar ya bileşik sayıdır ya da asal sayıdır (Yerlikaya, 2017)

Örneğin 17 sayısı bir asal sayıdır. Çünkü 17 sayısı 17 ve 1 sayıları dışında hiçbir doğal sayıya tam olarak bölünemez. 6 sayısı ise bir bileşik sayıdır. Çünkü 6 sayısı kendisi ve 1 dışında, 2 ve 3 sayılarına da tam olarak bölünebilir.

2 dışında tüm asal sayılar tek sayıdır (Dönmez, 2010). Yani 2 sayısı hem çift hem de asal olma özelliğine sahip özel bir sayıdır. 2 dışında kalan çift sayıların asal sayı olmama sebebi bunların kendisi ve 1 sayısı dışında çift oldukları için 2 sayısına da mutlaka bölünecekleri gerçeğidir.

Asal sayılar hakkında ilk çalışmalar Antik Yunan döneminde M.Ö 500-300 yılları arasında yapılmaya

[1] Uludağ Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Bursa, Türkiye, kadircancelik17@gmail.com,
0000-0003-1453-2510

başlamıştır. Bu tarihten sonra Euler, Fermat, Mersenne ve daha pek çok bilim adamı asal sayılar hakkında çalışmalar yapmış ve bu özel sayıların tespit edilmesi adına bazı yöntemleri geliştirmişlerdir.

Fermat Yöntemi

17. yüzyılda Pierre de Fermat, n sayısı doğal sayı olmak şartıyla aşağıdaki formülü sağlayan sağlayan sayıları Fermat asalı olarak isimlendirmiştir (Özdemir, 2017).

$$F_n = 2^{2^n} + 1 \qquad (1)$$

Fermat, tüm Fermat sayılarının asal sayılar olduğunu öne sürse de Euler F_5 sayısının asal olmadığını kanıtlamış ve böylece Fermat'ın bu öngörüsünün yanlış olduğu ispatlanmıştır (Altun, 2004). Bu sayılar n sayısının artışına bağlı olarak oldukça büyüdüğü için günümüzde daha büyük Fermat asal sayılarının olup olmadığı gizemini korumaktadır (Fermat Sayıları, 2022).

Erastotenes Kalburu

Erastotenes Kalburu yöntemi hala asal sayı testlerinde sık kullanılan yöntemlerden biridir. Bu yöntemde sayı, karekökünden daha küçük pozitif tam sayılara bölünür. Eğer 1 dışında herhangi bir sayıya tam olarak bölünme olmazsa bu o sayının asal olduğu anlamına gelir (Yerlikaya, 2017).

Mersenne Yöntemi

Marin Mersenne 17. Yüzyılda yaşamış Fransız bir matematikçi ve müzik teorisyenidir ve "akustiğin babası" olarak adlandırılır.

Aşağıdaki formüle uygun sayılar Mersenne sayısı olarak isimlendirilir.

$$M_n = 2^n - 1 \qquad (2)$$

Bu formüle uygun sayılara Mersenne sayısı denir. Ancak hem Mersenne sayısı hem de asal sayı olma özelliğine sahip sayılara Mersenne asal sayısı ismi verilmiştir (Mersenne Sayısı, 2022). Mersenne sayılarının bir başka özelliği ise bu sayıların aynı zamanda mükemmel sayıları da tespit edebilmesidir.

Mükemmel sayılar, kendisi hariç doğal sayı bölenlerinin toplamı kendisine eşit olan sayılardır (Pollack, 2012). Günümüzde 51 adet Mersenne asalı ve 51 adet mükemmel sayı bulunmaktadır.

Mersene yöntemini özel yapan konuysa, bu yöntemin günümüzde bilinen en büyük 10 asal sayıdan 9 tanesinin tespitine katkı sağlamış olmasıdır (Largest Known Prime Numbers, 2022). 1996 yılından itibaren gerçekleştirilen özel bir çalışma ile Mersenne yöntemi kullanılarak asal sayıların tespit edilmesine dair bir çalışma yürütülmektedir. Günümüze kadar tespit edilmiş en büyük 10 asal sayı ve hangi yöntemle keşfedildiğine dair bir tablo, tablo1 başlığı altında bulunmaktadır.

Tablo 1. Günümüze değin bulunmuş en büyük 10 asal sayı ve bulunma yöntemleri (Largerst Known Prime Numbers, 2022).

Sıralama	Sayı	Yöntem
1	$2^{82589933} - 1$	Mersenne
2	$2^{77232917} - 1$	Mersenne
3	$2^{74207281} - 1$	Mersenne
4	$2^{57885161} - 1$	Mersenne
5	$2^{43112609} - 1$	Mersenne
6	$2^{42643801} - 1$	Mersenne
7	$2^{37156667} - 1$	Mersenne
8	$2^{32582657} - 1$	Mersenne

9	$10223x2^{31172165}+1$	Proth
10	$2^{30402457}-1$	Mersenne

MATERYAL ve METOT

P, 2 sayısında farklı olmak şartıyla bir asal sayı olmak üzere, P+1 sayısı bir çift sayıdır. P+1 sayısı çift sayı olması nedeniyle $2^n.x^a$ şeklinde yazılabilir. Bu durumda P asal sayısı için 3 numaralı denklem yazılabilir.

$$P = (2^n.x^a) - 1 \qquad (3)$$

Burada x sayısını doğal sayıların özel bir kümesi olan asal sayılar kümesiyle sınırlandırarak şöyle bir örnek verelim. P sayısını 19 alalım formülde gerekli sayıları yerine koyduğumuzda 4 numaralı denklemi elde ederiz.

$$19 = (2^2.5^1) - 1 \qquad (4)$$

Burada x sayısı olarak belirlenen 5 sayısı sayı doğrusunda 19 sayısından önce gelen bir asal sayıdır. Aynı yöntemden yola çıkarak x yerine bu sefer seçilen 19 sayısı yazılığında ise 5 numaralı denklem elde edilir.

$$P = (2^n.19^a) - 1 \qquad (5)$$

5 numaralı denklemde n ve a değişkenleri için uygun değerler belirlendiğinde yeni P asal sayısı elde edilir. Bu denklemde n ve a yerine 1 yazıldığında P sayısı 37 değerine eşit olur ve 37 bir asal sayıdır.

3numaralı denklem baz alınarak şöyle bir sonuca varılabilir: P asal sayısı 3 numaralı denkleme yerleştirildiğinde x değişkeni yerine yazılan x asal sayısı, sayı doğrusunda p asal sayısından daha önce gelen bir asal sayıdır ve bu P asal sayısı da 5 numaralı denklemdeki örnekte açıklandığı gibi sayı doğrusunun başka bir noktasında bir başka R asal sayısı için bu denklemi sağlayacaktır.

Yukarıdaki Yöntemi Mersenne Yöntemi ile Karşılaştırma

Mersenne yöntemi ile yukarıda belirtildiği üzere günümüzde bilinen en büyük 8 asal sayı bulunmuştur. Bu çalışmada önerilen özel yöntem için bir örnek verilerek Mersenne yöntemiyle kıyaslamak gerektiğinde: Hesaplama kolaylığı açısından günümüzde bilinen en büyük Mersenne asal sayısını bu örnek için $2^{31}-1$ olarak kabul edelim. Bu asal sayı daha önce Euler tarafından Mersenne formülü kullanılarak tespit edilmiştir. Yine Mersenne yöntemi kullanılarak bu örnek içeriğinde tespit edilecek yeni en büyük asal sayı $2^{61}-1$ olacaktır. Bu sayı da yine Mersenne yöntemi ile Pervushin tarafından tespit edilmiştir. Örnekte de görüldüğü gibi Mersenne yönteminde $2^{31}-1$ asal sayısından hemen sonra 2^{61}-1 asal sayısı tespit edilmiş ve aradaki asal sayılar atlanmıştır. Oysa bu çalışmada önerilen formül ile basit şekilde $(2^{33}.31)-1$ (266287972351) asal sayısı tespit edilmiştir.

Henüz Tespit Edilememiş Asal Sayıları Bulma

Günümüzde bilinen en büyük 4 asal sayı arasında başka asal sayılar olup olmadığı henüz bilinmemektedir (Great Internet Mersenne Prime Search, 2022). Bu aralıkta büyük olasılıkla bulunan asal sayılar aşağıdaki yöntemle tespit edilebilir.

$$2^{82589933} - 1 > (2^n.(2^{77232917} - 1) - 1) \qquad (6)$$

Bu eşitsizlikte bilinen en büyük asal sayıdan küçük asal sayıların tespiti için, bilinen en büyük 2. asal sayı (3) numaralı denkleme yerleştirilmiştir. Buradaki eşitsizlik için doğru n sayısının tespiti ile yeni en

büyük 2. asal sayı bulunabilir.

Yeni En Büyük Asal Sayının Tespiti

Yukarıda formül anlatılırken açıklandığı üzere bir asal sayı, sayı doğrusu üzerinde kendisinden daha büyük başka bir a asal sayısı için (3) numaralı denklemde x değişkenine değer teşkil eder. Bu durumda bilinen en büyük asal sayı da kendisinden daha büyük başka bir asal sayı için x değişkenine değer teşkil etmelidir ve bu çıkarımdan aşağıdaki (7) numaralı denklem elde edilir.

$$P = (2^n.(2^{82589933} - 1)) - 1 \qquad (7)$$

(7) numaralı denklemde gerekli düzenleme ile 2^n değişkeni parantez içine dağıtılırsa 8 numaralı denklem elde edilecektir.

$$P = 2^{82589933+n} - 2^n - 1 \qquad (8)$$

(8) numaralı denklemde doğru n sayısının tespiti ile yeni en büyük asal sayı elde edilir. Günümüzde en büyük 8 asal sayının Mersenne yöntemi ile tespit edildiğini, bir sonraki asal sayının da bu yöntemle tespit edileceğini ve bunun $2^{82589933 + n} - 1$ olacağı göz önüne alındığında, bu çalışmada bahsedilen yöntemde bulunan ve (8) numaralı denklemde gösterilen 2^n değerinin sonuçtan çıkarılması nedeniyle bu yöntem ile bulunacak yeni asal sayı, Mersenne yöntemiyle bulunacak asal sayıdan küçük olacak ve bu sayede gözden kaçırılma ihtimali olan bir asal sayının yakalanması sağlanacaktır.

BULGULAR

Mersenne yöntemi ile bilinen en büyük 8 asal sayı tespit edilmiş ve bu asal sayılardan en büyük 4 tanesinin arasında bulunan başka asal sayılar olup olmadığı henüz kesin olarak bilinmemektedir. Eğer varsa henüz bulunamamış bu asal sayıların tespiti ve yeni en büyük asal sayının bulunması için bu çalışmada önerilen yöntem kullanılabilir.

Bunun yanında bu yöntemle keşfedilecek yeni asal sayılar, siber güvenlik, kriptoloji, matematik gibi alanları da etkileyecektir. Çünkü büyük boyutlardaki asal sayılar bu alanlarda özellikle kullanılmaktadır.

TARTIŞMA ve SONUÇ

Formül hakkında çıkarılabilecek ilk sonuç asal sayı tespiti alanına yeni bir yöntem kazandırmasıdır. Bu alanda şu an için en aktif şekilde kullanılan daha önce de sıkça bahsettiğim Mersenne yöntemi ile asal sayı keşfetme projesi 1996 yılında başlatılmıştır. Rasyonel bir değerlendirme yapıldığında şu sonuca varılabilir ki, 1996 yılından beri çok daha verimli bir asal sayı keşfetme yöntemi kullanılmamasına rağmen 20 yılı aşkın bir süreçte sadece bu yöntemle pek çok asal sayı keşfedilmiştir. Bu çalışmada önerilen nispeten daha kapsamlı olan yöntemle gerekli imkanlar sağlandığında mevcut durumdan çok daha başarılı bir asal sayı keşfetme yöntemi elde edilebilir ve bu yöntemle keşfedilecek her asal sayı Çelik Asal Sayısı olarak adlandırılır.

KAYNAKÇA

Altun, M., (2004). Asal sayıların, bileşik sayılardan ayırımına istatistiksel bir yaklaşım. *Eğitim Fakültesi Dergisi, 17*(1), 1-12.

Dönmez, A., (2010). Matematikte ilginç sayılar. *ABMYO Dergisi*, *20*, 4-11.

Fermat Sayıları, (2022). https://tr.wikipedia.org/wiki/Fermat_say%C4%B1lar%C4%B1#:~:text=F7%20%

3D %202128%20%2B%20%201,ve%20bunlara %20Fermat%20asal%C4%B1%20denir.

Great Internet Mersenne Prime Search, (2022). https://www.mersenne.org/primes/

Largest Known Prime Numbers, (2022). https://en.wikipedia.org/wiki/Largest_known_prime_number#:~:text=The%20largest%20known%20prime%20number,Search%20(GIMPS)%20in%202018.

Mersenne Sayısı, (2022). https://tr.wikipedia.org/wiki/Mersenne_say%C4%B1s%C4%B1#:~:text=Mersenne%20say%C4%B1lar%%20C4%B1%2C%20matematikte%20ikinin%20kuvvetlerin in,bilinen%20Marin%20Mersenne'den%20alm%%20C4%B1%C5%9Ft%C4%B1r.

Özdemir, F., & Özdemir, G., (2017). Matematik eğitiminde sayıların önemi: özel sayı ve sistemlerininkeşfedilmesi örneği. *Researcher: Social Science Studies, 5*(4), 28-45.

Pollack, P., & Shevelev, V., (2012). On perfect and near perfect numbers. *Journal of Number Theory, 132,* 3037-3046.

Yerlikaya, T., & Kara, O., (2017). Kriptolojide kullanılan asal sayı test algoritmaları. *Trakya University Journal of Engineering Sciences, 18*(1), 85-94.