T.C.
PAMUKKALE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI

ASAL SAYILARIN TESPİTİ İÇİN FARKLI METOD VE UYGULAMALARI

YÜKSEK LİSANS TEZİ

NAZLI KOCA

DENİZLİ, EKİM - 2020

T.C.
PAMUKKALE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI

ASAL SAYILARIN TESPİTİ İÇİN FARKLI METOD VE UYGULAMALARI

YÜKSEK LİSANS TEZİ

NAZLI KOCA

DENİZLİ, EKİM - 2020

Bu tezin tasarımı, hazırlanması, yürütülmesi, araştırmalarının yapılması ve bulgularının analizlerinde bilimsel etiğe ve akademik kurallara özenle riayet edildiğini; bu çalışmanın doğrudan birincil ürünü olmayan bulguların, verilerin ve materyallerin bilimsel etiğe uygun olarak kaynak gösterildiğini ve alıntı yapılan çalışmalara atfedildiğine beyan ederim.

NAZLI KOCA

ÖZET

ASAL SAYILARIN TESPİTİ İÇİN FARKLI METOD VE UYGULAMALARI

YÜKSEK LİSANS TEZİ

NAZLI KOCA

PAMUKKALE ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ

MATEMATİK ANABİLİM DALI

(TEZ DANIŞMANI:DOÇ.DR. SERPİL HALICI)

DENİZLİ, EKİM - 2020

Bu çalışmada, öncelikle tam sayıların genel özellikleri verilerek bu sayıların alt kümesi olan asal sayıların özellikleri incelendi. Daha sonra, bilinen bazı özel asal sayılara değinilerek literatürde, asal sayı bulmada kullanılan asallık testleri incelendi. Bu çalışmada yeni bir asal sayı bulma yöntemi verilerek bu yöntem üzerinde çalışıldı ve mükemmel güvenli asal sayı dizisi tanımlandı. Bu oluşturulan yeni dizi şifreleme yöntemlerinden biri olan RSA şiflereme yönteminde kullanıldı.

ANAHTAR KELİMELER: Asal sayılar, Mersenne asalları, Asallık testleri, Eratosthenes kalburu, Sophie Germain asalları

ABSTRACT

DIFFERENT METHOD FOR THE DETERMINATION OF PRIME NUMBERS AND APPLICATIONS
MASTER THESIS
NAZLI KOCA
PAMUKKALE UNIVERSITY INSTITUTE OF SCIENCE MATHEMATICS

(SUPERVISOR:ASSOC.PROF.SERPİL HALICI)

DENİZLİ, OCTOBER 2020

In this study, firstly general properties of integers are given. The properties of the prime numbers, which are the subset of integers, were examined. Later, some known special prime numbers are mentioned. In the literature, primality tests, which were created to find prime numbers, were examined. A new prime number finding method was studied and a perfectly safe prime number sequence was defined. This new sequence was used in the RSA encryption method.

KEYWORDS: Prime numbers, Mersenne primes, Test for primes, Sieve of Eratosthenes, Sophie Germain primes

İÇİNDEKİLER

Sayfa

,

ŞEKİL LİSTESİ

Sayfa

TABLO LİSTESİ

Sayfa

SEMBOL LİSTESİ

$\mathbb{R}$	:	Reel Sayılar
$\mathbb{Z}$	:	Tam Sayılar
$\mathbb{Q}$	:	Rasyonel Sayılar
$\mathbb{N}$	:	Doğal Sayılar
$\boldsymbol{F_n}$	:	Fermat Sayıları
$\boldsymbol{M_n}$	:	Mersenne Sayıları
$\mathbb{P}$	:	Asal Sayılar Kümesi
$\boldsymbol{M_s}$	:	Muhtemel Sayı
$\boldsymbol{M_{ss}}$	:	Muhtemel Sayıların Sıra Sayısı
$\mathbb{Z}^{\boldsymbol{Tek}}$	:	Tek Tam Sayılar
M'_{ss}	:	Asal Olmayan Sayıların Sıra Sayısı
$\boldsymbol{a\|b}$	:	a, b yi Böler
$\boldsymbol{\varphi(m)}$	:	Euler phi Fonksiyonu
$\boldsymbol{\pi(x)}$	:	x den Büyük Olmayan Asalların Sayısı
$\boldsymbol{(a,b)=d}$	:	a ile b nin Ebobu
$\boldsymbol{[a,b]=d}$	:	a ile b nin Ekoku

ÖNSÖZ

Tez çalışmamın planlanmasında, araştırılmasında, yürütülmesinde ve oluşumunda desteğini hiç esirgemeyen, engin bilgi ve tecrübelerinden yararlandığım saygıdeğer hocam Doç. Dr. Serpil HALICI' ya, Elektrik-Elektronik yüksek mühendisi Hamit Çacur' a ve çalışma boyunca desteklerini esirgemeyen annem, babam, eşim ve kızıma sonsuz teşekkürlerimi sunarım.

NAZLI KOCA

1.GİRİŞ

1.1 Tarihçe

M.Ö. 300 ile M.Ö. 500 yıllarında Pisagor ve öğrencileri asal sayılar ile ilgili bazı çalışmalar yapmışlardır. Bu çalışmalardan biri, mükemmel sayılardır. n, pozitif bir tamsayı iken, kendisi hariç pozitif tam bölenlerinin toplamı, n sayısına eşit olan n sayısına mükemmel sayı denir (O'Connor ve Robertson 2019). M.Ö. 300 yıllarında yayınlanan, Euclid'in "Elements" adlı kitabının IX $b$ölümünde, sonsuz sayıda asal sayı olduğu ispatlanmıştır ve yine bu kaynakta aritmetiğin temel teoreminin ispatı da yapılmıştır. Aritmetiğin temel teoremi, her tam sayının asal sayıların çarpımı olarak tek türlü yazılabileceğini ifade eder. Ayrıca, Euclid "Elements" adlı bu kitabında mükemmel sayılardan yararlanarak, Mersenne asallarını tanımlamıştır. Herhangi bir p asal sayısı için, $M_p = 2^p - 1$ biçiminde tanımlanan sayılara Mersenne sayıları olarak isim verilmiştir. Her Mersenne sayısı asal sayı değildir. Bir Mersenne sayısının asal sayı olup olmadığını belirlemek için bazı testler uygulanır ki bunlarda biri de Lucas-Lehmer testidir (Yerlikaya ve Kara 2017).

Geçmişten günümüze kadar, asal sayıları bulabilmek için, birçok test ve yöntemler geliştirilmiş ve bunlar üzerinde çalışmalar yapılmıştır. Mesela, M.Ö. 200 yıllarında Eratosthenes, 1 ile n^2 sayıları arasında kalan asal sayıların bulunabilmesini sağlayan Eratosthenes kalburunu oluşturmuştur. Bu yöntemle, çok büyük olmayan iki tam sayı arasındaki asal sayıları bulmak kolaydır. Fakat sayılar büyüdükçe Eratosthenes kalburunu uygulamak zor olacaktır (Erdoğan ve Yılmaz 2008). Daha büyük tam sayıların asal sayı olup olmadığını anlamak için asallık testleri nin geliştirilmesi gerekmektedir. Literatürde bilinen asalık testleri, iki gruba ayrılır: Kesin asallık testleri ve olası asallık testleri. Kesin asallık testleri yardımıyla, bir sayının asal olup olmadığını kesin olarak belirlemek mümkündür. Bu test, sayıların çarpanlarına ayrılmasını kullanır ve büyük sayılar için uygulanırken çok zaman gerektirdiğinden pratik değildir. Olası asallık testlerinde ise, asal sayı bulmak için n bitlik rastsal bir sayı elde edilerek, bu sayıya olası asallık testleri uygulanır. Test sonuçlarına göre, 2^{-100} den daha düşük bir hata payı ile sayının asal olup olmadığı belirlenebilir. Olası asallık

testleri, kesin asallık testlerine göre daha hızlı olduğundan büyük sayılar için daha çok tercih edilir (Yerlikaya ve Kara 2017).

17.yy başında, Fermat $2^{2^n}+1$ şeklindeki bütün sayıların, asal sayı olduğunu iddia etmiştir. Fakat n yerine 5 yazıldığında, elde edilen $2^{32}+1$ sayısı 641 ile bölündüğü için, bu iddia yanlıştır. $2^{2^n}+1$ formülünden bulunan sayılara ise Fermat sayısı adı verilir (O'Connor ve Robertson 2019). 18.yy. Christian Goldbach, her tek doğal $n \geq 9$ sayısının üç tane tek asal sayının toplamı olarak yazılabileceğini ifade etmiştir. Leonard Euler bu sanıyı iki kısıma ayırıp, bugünkü bilinen haline getirmiştir (Özgü. 2002). Yani, $n \geq 4$ olan her çift doğal sayısı, iki asal sayının toplamı olarak yazılabilir
(Binary Goldbach Conjecture). Örneğin, $6=3+3, 8=3+5, 10=3+7=5+5$, ... gibi.
Her tek sayı, üç asal sayının toplamıdır (Ternary Goldbach Conjecture). Örneğin,
$9=3+3+3, 11=3+3+5, 13=3+3+7=3+5+5$, ...

1792 yılında, henüz 15 yaşındayken Carl Friedrich Gauss, belirli bir n sayısından küçük olan asal sayıların sayısını tahmin etmek için yeni bir formül vermiştir. Bu formül, $\pi(n) \sim \frac{n}{\ln n}$ formülü, asal sayı teoremi olarak bilinmektedir. Asal sayı teoremi, asal sayma fonksiyonu $\pi(n)$ için asimptotik bir form vermektedir ve bu teoreme göre, n tamsayısından daha az miktarda asal sayı vardır. 1808 yılında Legendre, n tamsayısı için $B=-1.08366$ olacak şekilde, $\pi(n) \sim \frac{n}{\ln n+B}$ formülünü vermiştir. Burada kullanılan B harfi, Legendre sabiti olarak bilinir (Weisstein). Asal sayılar incelenen aralıkta belirli bir kurala göre sıralanmamaktadır ve üstelik tam sayılar büyüdükçe söz konusu olan aralıkta asal sayıların sıklıkları azalmaktadır. Asal sayıların sıklıklarını belirlemek için, 19.yy ortasında Bernhard Riemann tarafından, Riemann Zeta fonksiyonu hipotezi ortaya atılmıştır. Bu hipoteze göre, Riemann-Zeta fonksiyonunun sıfır değerini aldığı noktalar, asal sayıların bulunuş sıklıklarını belirlemek için kullanılır. $s \neq 1$ olmak üzere, s karmaşık sayı olmak üzere,

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Fonksiyonu, Riemann Zeta fonksiyonu olarak bilinir. Riemann hipotezine göre, $\zeta(s)=0$ denkleminin tüm çözümleri, bir doğru üzerinde yer almaktadır. Daha kısa bir söyleyişle, bu denklemin tüm karmaşık sayı çözümlerinin gerçel kısımlarının $1/2$ olduğu tahmin edilir (O'Connor ve Robertson 2019).

p asal sayısı için, $(p-1)! \equiv -1(mod\ p)$ denkliği sağlanıyorsa bu sayılara Wilson asal sayısı denir. 1953 yılında Goldberg, 1988 yılında E.H. Pearson, K.E. Kloss, W. Keller, H. Dubner ve Gonter ile Kundert, 1997 de Crandall, Dilcher ile Pomerance adlı i yazarlar, Wilson asalları üzerinde çalışmalar yapmışlardır. Wilson asal sayılarının sonlu veya sonsuz sayıda olup olmadığı halen çalışma konusudur. $C_n = n.2^n + 1$ tipindeki sayılar ise, Cullen asalları olarak bilinir. Robinson, Keller, J. Young Cullen [3] asal sayılar ile ilgili bazı temel çalışmalar yapmışlardır. Bertrand ın asal sayılar ile ilgili varsayımı ise şöyledir:
her $x \geq 1$ için, $x < p \leq 2x$ aralığında en az bir asal sayı olduğudur. 1919 yılında, Ramanujan bu varsayımın ispatını yapmıştır (Sondow, 2009). Ramanujan ın verdiği asal sayılardan bazıları ise şöyledir; $2, 11, 17, 29, 41, 47, 59, 67, 71, 97$ ... Fermat ın verdiği son teoreme göre ise, herhangi $x, y\ ve\ z$ pozitif tamsayıları için, $n > 2$ iken $x^n + y^n = z^n$ eşitliğinin sağlanamayacağı ifade edilir. Sophie Germain ise 1823 yılında, Fermat ın son teoremini Sophie asalları için ispatlamıştır. Yani, p Sophie Germain asalı ise, $x^p + y^p = z^p$ eşitliğini sağlayan sıfırdan farklı ve p nin katları olmayan x, y, z tamsayıları yoktur (Wells 2005).

Asal sayılar geçmişte ve günümüzde Kriptografi alanında şifreli mesaj göndermek için de kullanılmaktadır. Kriptografide, her kullanıcının şifreleme ve deşifreleme yapmak için bir açık, bir de gizli olmak üzere iki farklı anahtarı vardır. Açık anahtar herkese açıktır ve isteyen herkes görebilir. Gizli anahtar ise saklı tutulur, sahibinden başka herhangi biri tarafından bilinmemelidir. Şifreleme açık anahtar ile yapılırken şifre çözümü ise gizli anahtarla yapılır. Bu şifreleme anahtarları ikili olarak kullanılır ve birinin şifrelediği bilgiyi diğer anahtar çözmektedir. Günümüzde en çok bilinen ve kullanılan şifreleme yöntemi, açık anahtarlı şifreleme yöntemi olan RSA şifreleme yöntemidir. Bu sistemin adı, 1978 yılında Ron Rivest, Adi Shamir ve Leonard Adlemen isimlerindeki bilim insanlarının soyadlarını taşır yani tamsayıları çarpanlarına ayırma çalışmaları sonrasında yönteme bu isim verilmiştir (Akbar 2015). Başka bir açık anahtarlı şifreleme yöntemi ise Rabin şifreleme tekniğidir. Rabin şifreleme yöntemi, Michael Rabin tarafından, 1979 senesinde bulunan bir kripto sistemdir. Bu kriptosistem, asimetrik şifreleme tekniğine dayanır. RSA yönteminin bir farlı tipi olan Rabin kriptosistemi, RSA da olduğu gibi bileşik sayıların çarpanlara ayrılma zorluğundan yararlanır (Rabin 1979).

1.2 Genel Tanım ve Kavramlar

Tanım 1.2.1 $m, n \in Z,\ n \neq 0\ için\ m = k.n$ eşitliğini sağlayan bir k tamsayısı varsa veya $\frac{m}{n}$ bir tamsayı ise, n sayısı m'yi böler denir. Bu durum $n|m$ şeklinde gösterilmektedir (Gürlü 2015).

Önerme 1.2.2 a, b, c tamsayılar olmak üzere, bölünebilme hakkında, aşağıdaki ifadeler doğrudur (Gürlü 2015);

1. $a|a$ dir.

2. $a|b\ ve\ b|c\ ise\ a|c$ dir.

3. $a|b\ ve\ b \neq 0\ ise,\ |a| \leq |b|$ dir.

4. $a|b\ ve\ a|c\ \ ise, \forall x, y \in Z\ \ a|bx + cy$ dir.

5. $a|b\ ve\ a|(b \pm c)\ ise, a|c$ dir.

6. $a|b\ ve\ b|a$ ise, $|a|=|b|$ dir.

7. $a|b\ ve\ b \neq 0\ ise, \frac{b}{a}|b$ dir.

8. $a|b\ ve\ c \neq 0$ olması için, yeter ve gerek şart $ac|bc$ olmasıdır.

İspat. Yukarıda verilen önermenin bazıları için ispat aşağıda verildi.

2. $a|b\ ve\ b|c$ ise $b = a.m\ ve\ c = b.n$ olacak şekilde $m, n \in Z$ için vardır. Burada, $b = a.m$ eşitliğinden yararlanarak $c = a.m.n$ yazılabilir yani, $a|c$ dir.

4. $a|b\ ve\ a|c$ ise $b = k_1.a\ \ ve\ \ c = k_2.a$ olacak şekilde $k_1, k_2 \in Z$ vardır. Dolayısıyla, $k_1, k_2 \in Z\ \ x, y \in Z$ için $bx + cy = k_1.a.x + k_2.a.y$ yazılabilir. Bu durumda, $a|bx + cy$ olur.

5. $a|b$ ve $a|(b \pm c) olur. b = k_1.a \; ve \; (b \pm c) = k_2.a$ olacak şekilde $k_1, k_2 \in Z$ vardır (Sondow 2009). Buradan,

$\pm c = k_2.a - b = k_2.a - k_1.a = a.(k_2 - k_1)$, $k_1, k_2 \in Z$ olduğundan $a|c$ olur.

8. $a \neq 0 \; ve \; c \neq 0 \iff a.c \neq 0 \; dır. \; b = k.a \iff b.c = k.a.c$ olacak şekilde $\exists k \in Z$

vardır. O zaman, $ac|bc$ olur (Gürlü 2015).

Tanım 1.2.3 b ve c iki tamsayı olsun. Eğer, $a \neq 0$ tamsayısı için $a|b \; ve \; a|c$ koşulları sağlanıyor ise, a ya, b ve c tamsayılarının bir ortak böleni denir. Ortak bölenlerin en büyüğüne, en büyük ortak bölen denir ve (b, c) ile gösterilir (Yelkenkaya 2014).

Tanım 1.2.4 b ve c iki tamsayı olsun. Eğer, $a \neq 0$ tamsayı, $b|a \; ve \; c|a$ koşullarını sağlıyor ise, a sayısına b ve c tamsayılarının bir ortak katı denir. Ortak katların en küçüğüne, en küçük ortak katı denir ve $[b, c]$ ile gösterilir (Yelkenkaya 2014). Ayrıca; $[b, c](b, c) = a.b$ olduğu da bilinir.

Şimdi, aşağıda bazı bölünebilme testlerini vereceğiz.

Bölünebilme Testleri. Bölünebilme testleri, asal sayıları tespit etmek için büyük önem taşır. Bir tam sayının çarpanlarını bulmak için, öncelikle bölünebilme testlerine bakılmaktadır. Bu bölümde, bazı sayılarla bölünebilme testleri verilmiştir. Bölünebilme testlerini uygulayarak, asal sayıları tespit etmek kolay gibi gözükse de, tam sayılar büyüdükçe bu testleri uygulamak zorlaşır. Daha sonraki bölümlerde ise, bu konuya değinilecektir.

Kongrüanslar kullanılarak, onluk tabanda verilen tam sayılar için bölünebilme kuralları oluşturulabilir. Burada, $0 \leq a_j \leq 9$ için $j = 0, 1, \cdots, k$ olacak şekilde, $n = (a_k a_{k-1} \cdots a_1 a_0)_{10}$ tamsayısı

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10^1 + a_0 10^0$$

yazılabilir. Buna bir örnek vermek gerekirse, $a_0 = 3, a_1 = 2, a_2 = 5$ sayıları için n= $(523)_{10}$ sayısı, $n = 5.10^2 + 2.10^1 + 3$ yazılır.

2 nin Kuvvetleri ile Bölünebilme. $10 \equiv 0(mod2)$ eşitliğini kullanarak, her pozitif j tamsayısı için, $10^j \equiv 0(mod2^j)$ yazılabildiğinden

$n \equiv (a_0)_{10}(mod2)$

$n \equiv (a_1 a_0)_{10}(mod2^2)$

$n \equiv (a_2 a_1 a_0)_{10} (mod 2^3)$

$\vdots$

$n \equiv \left(a_{j-1} a_{j-2} \cdots a_1 a_0\right)_{10} \left(mod 2^j\right)$

olur. Buna göre, herhangi bir n tamsayının 2 ile bölünebilmesi için, son basamağının 2 ile bölünebilmesi gerekmektedir. Benzer şekilde, n tam sayısının 4 sayısı ile bölünmesi için ise, son iki basamağının 4 ile bölünebilmesi ve genel olarak n sayısının 2^j ile bölünebilmesi için de, son j basamağının 2^j ile bölünmesi gerekmektedir.

Örneğin, $n = 32688048$ sayısını ele alalım. $2|8$ olduğundan $2|n$ olur. $2^2|48$ olduğundan $2^2|n$ ve benzer olarak $2^3|048$ olduğundan $2^3|n$ dir. Fakat, $2^4 \nmid 88048$ olduğundan $2^4 \nmid n$ dir.

5 in Kuvvetleri ile Bölünebilme. $10 \equiv 0\ (mod\ 5)$ eşitliğinden, her pozitif j tamsayısı için $10^j \equiv 0(\ mod\ 5^j)$ olur. Yani,

son j basamak 5^j ile bölünebiliyor ise, verilen n tamsayısı 5^j ile tam bölünür demektir.

Örneğin, $n = 15535375$ sayısını alalım. $5|5$ olduğundan $5|n$ dir. $5^2|75$ olduğundan $5^2|n$ dir. Fakat $5^4 \nmid 5375$ olduğundan $5^4 \nmid n$ dir.

3 ve 9 ile Bölünebilme. $10 \equiv 1\ (mod\ 3) ve\ 10 \equiv 1\ (mod\ 9)$ denkliğinden yararlanarak, ve

$n = (a_k a_{k-1} \cdots a_1 a_0)_{10} = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10^1 + a_0 10^0$ eşitliği kullanılarak

$n = (a_k a_{k-1} \cdots a_1 a_0)_{10} \equiv a_k + a_{k-1} + \cdots + a_1 + a_0\ (mod\ 3)$

$n = (a_k a_{k-1} \cdots a_1 a_0)_{10} \equiv a_k + a_{k-1} + \cdots + a_1 + a_0\ (mod\ 9)$

olur. Yani, n tamsayısının 3 ve 9 ile bölünebilmesi için, bu tamsayısının basamaklarındaki sayıların toplamının 3 ve 9 ile tam bölünebilmesi gerekmektedir.

Örneğin,

$n = 4127835$ sayısının basamaklarındaki sayıların toplam $4 + 1 + 2 + 7 + 8 + 3 + 5 = 30$ olup, $3|30$ olduğundan $3|n$ dir. $9 \nmid 30$ olduğundan $9 \nmid n$ olur.

11 ile Bölünebilme. $10 \equiv -1(mod 11)$ olduğundan

$n = (a_k a_{k-1} \cdots a_1 a_0)_{10} = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10^1 + a_0 10^0$ eşitliği

$n \equiv a_k (-1)^k + a_{k-1} (-1)^{k-1} + \cdots + a_1 (-1)^1 + a_0 (-1)^0 (mod 11)$

olarak yazılabilir. $(a_k a_{k-1} \cdots a_1 a_0)_{10}$ sayısının 11 ile bölünebilmesi için gerek ve yeter şart;

$-a_1 + a_2 - \cdots + (-1)^k a_k$ toplamının 11 ile bölünebilmesidir. Buna göre, n tamsayısının basamaklarındaki rakamların ard arda toplam ve farklarından oluştuğu görülmektedir.
Örneğin, $11|723160823$ doğrudur. Çünkü, basamaklarındaki sayılar ard arda toplanır ve çıkarılırsa; $3 - 2 + 8 - 0 + 6 - 1 + 3 - 2 + 7 = 22$ olup, bu sayı 11 ile tam bölünür. Dolayısıyla, 723160823 sayısı 11 ile tam bölünür.

7, 11 ve 13 Sayılarına Aynı Anda Bölünebilme.

$7.11.13 = 1001 \; ve \; 10^3 = 1000 \equiv -1(mod 1001)$ olduğundan

$n = (a_k a_{k-1} \cdots a_1 a_0)_{10} = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10^1 + a_0 10^0$

$n \equiv (a_0 + 10a_1 + 100a_2) + 1000(a_3 + 10a_4 + 100a_5) + \cdots + (1000)^k (a_{k-2} + 10a_{k-1} + 100a_k)$

$n \equiv (100a_2 + 10a_1 + a_0) - (100a_5 + 10a_4 + a_3) - \cdots + (100a_k + 10a_{k-1} + a_{k-2})$

$n \equiv (a_2 a_1 a_0)_{10} - (a_5 a_4 a_3)_{10} + (a_8 a_7 a_6)_{10} - \cdots (1001)$

yazılabilir. Dolayısıyla, bir sayının 7, 11 ve 13 ile bölünebilmesi için, sayının basamakları üçlü bloklar halinde bir toplam, bir fark şeklinde düzenlenir. Bu toplamın, $7, 11$ ve 13 ile bölünebileceği söylenebilir. Çünkü, bu asal sayıların üçüde 1001 in bölenleridir.

Örnek. $n = 59358208$ olsun. Bu sayının basamaklarının üçlü bloklar şeklinde bir toplam bir farktan oluşan ifadesi, $208 - 358 + 059 = -91$ dir.
$7 \mid (-91)$, $13 \mid (-91)$ olduğundan, n tamsayısı 7 ve 13 ile bölünebilir olmasına rağmen $11 \nmid (-91)$ olduğundan 11 ile bölünemez (Altındiş 1999).

Şimdi de aşağıda asal sayılar ile ilgili bazı temel bilgileri verelim.

Tanım 1.2.5 $\cdots -3, -2, -1, 0, 1, 2, 3 \cdots$ sayılarından oluşan sayı dizisine, tamsayılar dizisi denir ve $\mathbb{Z}$ sembolü ile gösterilir.

Tanım 1.2.6 p bir tamsayı ve $p > 1$ olsun. Eğer, $1|p \; ve \; p|p$ ise, yani p sayısının 1 ve p den başka bir böleni yok ise, p sayısına asal sayı denir (Aşar ve diğ. 2009).

Tanım 1.2.7 $a > 1\ ve\ b > 1$ olan iki tamsayı olsun. $a.b = n$ olarak yazılan n tamsayısına bileşik sayı denir.

Teorem 1.2.8 $\forall n > 1$ tamsayısı ya asaldır ya da sonlu sayıda asal sayıların çarpımı olarak yazılabilir (Aşar ve diğ. 2009).

İspat. $n = 2$ için iddia sağlanır. Çünkü, 2 sayısı asal sayıdır.

O zaman, iddia $n > 2$ ve $2 \leq k < n$ olan k tamsayıları için doğru olsun.

Eğer n asal sayı ise, bu hipotez doğrudur. Eğer, n asal sayı değil ise, öyle $1 < n_1, n_2 < n$ vardır ki, $n = n_1.n_2$ olur. Tümevarım hipotezinden dolayı

$p_1, p_2, \cdots, p_s$ ve $q_1, q_2, \cdots, q_t$ asal sayılar $s > 0\ ve\ t > 0$

olur. Bu durumda,

$$n_1 = p_1 p_2 \cdots p_s \text{ ve } n_2 = q_1 q_2 \cdots q_t$$

olarak yazılabilir. Bu değerler yerine konursa

$$n = (p_1 p_2 \cdots p_s)(q_1 q_2 \cdots q_t)$$

olup ispat tamamlanmış olur (Aşar ve diğ. 2009).

Teorem 1.2.9 (Aritmetiğin Temel Teoremi) $n, n > 1$ olan, bir tamsayı olsun.

O zaman, $r \geq 1$ tamsayı ve öyle $p_1, p_2, \cdots, p_r$ asal sayıları vardır ki, $n = p_1 p_2 \cdots p_r$ dir ve bu gösterim, çarpanların yer değiştirmesi farkıyla tektir (Aşar ve diğ. 2009).

İspat. Bir önceki teoremden dolayı, $r \geq 1$ tamsayı ve $p_1, p_2, \cdots, p_r$ asal sayılar olmak üzere

$n = p_1 p_2 \cdots p_r$ dir. Varsayalım ki, n nin bu biçimde ikinci bir gösterimi de $s \geq 1$ tamsayısı için $q_1, q_2, \cdots, q_s$ asal sayılar olmak üzere, $n = q_1 q_2 \cdots q_s$ olsun. O zaman,

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

dir.($r \leq s$ alınabilir) (Aşar ve diğ. 2009).

$1 \leq j \leq n$ için, $p_1 | q_j$dir. q_j asal olduğundan $p_1 = q_j$ dir. Eşitliğin iki tarafı için $j = 1$ olduğunu varsayalım. Buradan $p_1 = q_1$olur. Eşitliğin iki tarafı p_1 ile bölünürse, $p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s$ elde edilir. Böyle devam edilirse r. adımdan sonra, $p_1 = q_1, \cdots, p_r = q_r$ ve $1 = q_{r+1} \cdots q_s$ olur. Buradan, $s > 1$ ise $q_s | 1$ olur ki bu bir çelişkidir. Dolayısıyla,

$r = s$ ve $p_1 = q_1, \cdots, p_s = q_s$ olmalıdır.

Tanım 1.2.10 n, pozitif bir tamsayı olsun. n sayısının kendisi hariç, pozitif tam bölenlerinin toplamı, n sayısına eşit ise, n sayısına mükemmel sayı denir (Gerstien 2012). Bir n pozitif

tam sayısının tüm pozitif bölenlerinin toplamı $\sigma(n) = \sum_{m|n} m$ ile gösterilir. Eğer $\sigma(n) = 2n$ ise, n mükemmel sayı olur. Örneğin,

$$\sigma(6) = 1 + 2 + 3 + 6 = 12$$

olup ve 6 mükemmel bir sayıdır.

Teorem 1.2.11 Eğer $(m,\ n) = 1$ olacak şekilde m ve n tamsayıları var ise,

$$\sigma(mn) = \sigma(m)\sigma(n)$$

olur.

İspat. $\sigma(mn) = \sum_{d|mn} d = \sum_{d_1|m\ d_2|n} d_1 d_2 = \left(\sum_{d_1|m} d_1\right)\left(\sum_{d_2|n} d_2\right) = \sigma(m)\sigma(n)$ dir.

Teorem 1.2.12 2^{p-1} sayısının asal sayı olması için gerek ve yeter şart $2^{p-1}(2^p - 1)$ sayısı mükemmel bir sayı olmasıdır.

İspat. ($\Rightarrow$): $2^{p-1}(2^p - 1) = n$ olsun ve $2^p - 1$ sayısını asal sayı kabul edelim.
$(2^{p-1}, 2^p - 1) = 1$ olduğundan,
$\sigma(n) = \sigma(2^{p-1})\sigma(2^p - 1) = (1 + 2 + 2^2 + \cdots + 2^{p-1})\left(1 + (2^p - 1)\right) = (2^p - 1)2^p = 2n$
O halde, n mükemmel sayı olur.

($\Leftarrow$): $n = 2^{p-1}(2^p - 1)$ mükemmel sayı olsun.
$p > 1$ ve q tek sayı olacak şekilde n sayısı, $n = 2^{p-1}.q$ olarak yazılabilir. Böylece, $2^p q = 2n = \sigma(n) = \sigma(2^{p-1})\sigma(q) = (2^p - 1)\sigma(q)$ yazılır. Bundan dolayı, $2^{p-1}|q$ ve $q = (2^p - 1)s, \exists s \in Z$ yazılabilir. $\sigma(q) = 2^p s$ olur. Öyle ki s ve q , q nun 2 farklı bölenidir. $q + s = 2^p s = \sigma(q)$ dur. q nun s ve q dan başka böleni yoktur. O zaman, $s = 1$ ve q asal sayıdır. Yani, 2^{p-1} asal sayıdır (Travaglını 2014).

Riemann-Zeta Hipotezi. Tamsayılar büyüdükçe asal sayıların sıklıkları azalır. Yani, asal sayıların reel eksende görülmesinin belirli bir düzeni yoktur. Bundan dolayı, asal sayıların yoğunluklarını hesaplamak için, 19.yüzyılda Bernhard Riemann tarafından, Riemann Zeta fonksiyonu hipotezi ortaya atılmıştır. Riemann, asal sayıların yoğunluklarını incelerken, Euler in Zeta fonksiyonunu genişletmiştir. Bu hipoteze göre, Riemann-Zeta fonksiyonunun sıfır değerini aldığı noktalar, asal sayıların bulunuş sıklıklarını belirlemek için kullanılmıştır.
$s \neq 1$ olmak üzere, tüm s karmaşık sayıları için

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

fonksiyonu, Riemann Zeta fonksiyonu olarak adlandırılır. Riemann hipotezine göre, $\zeta(s) = 0$ denkleminin tüm çözümleri bir doğru üzerinde yer almaktadır .

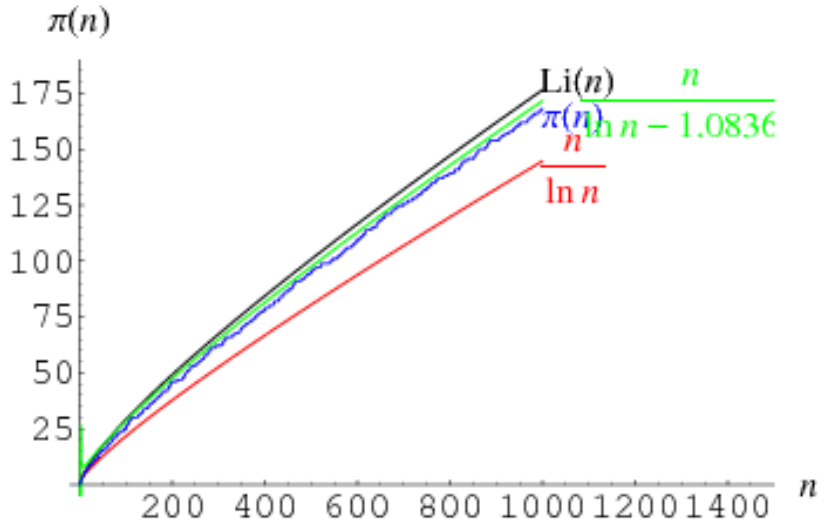
Asal Sayı Teoremi. Carl Friedrich Gauss, bir n sayısından küçük asal sayıların adedini tahmin etmek için, $\pi(n) \sim \frac{n}{\ln n}$ formülünü kullanmıştır. Bu formül asal sayı teoremi olarak bilinmektedir. Asal sayı teoremi, asal sayma fonksiyonu $\pi(n)$ için asimptotik bir form vermektedir ve bu teorem, n tamsayısından daha küçük asal sayı adedini göstermektedir. 1808 yılında, Legendre büyük n sayıları için, Legendre sabiti olarak bilinen $B = -1.08366$ olacak şekilde $\pi(n) \sim \frac{n}{\ln n + B}$ formülünü vermiştir. 15 yıl sonra, Carl Friedrich Gauss, $\pi(n) \sim \frac{n}{\ln n}$ önermesini geliştirdi ve $\pi(n) \sim Li(n)$ benzerliğini yazdı. Burada,

$$Li(n) = \int_2^n \frac{dx}{\ln x}$$

logaritmik integral denklemidir. $Li(n)$ asimptotik serilerinin değerleri sonsuzdur. Yani,

$$Li(n) \sim \sum_{k=0}^{\infty} \frac{k!\, n}{(\ln n)^{k+1}} \sim \frac{n}{\ln n} + \frac{n}{(\ln n)^2} + \frac{2n}{(\ln n)^3} + \cdots$$

dir. Burada, bu serinin ilk üç terimi almanın, sadece $\frac{n}{\ln n}$ den daha iyi bir yaklaşım olduğu gösterilmiştir (Derbyshire 2004).



Şekil 1.1 Asal sayı teoremi grafiği

$Li(n) = \int_2^n \frac{dx}{\ln x}$ ifadesi, $n \leq 1000$ için bir $\pi(n)$ (alt eğri) ve $Li(n)$ grafiği gösterilmiştir ve n nin bazı değerleri için kontrol edilmiştir. Her zaman $\pi(n) < Li(n)$ bağıntısı doğruluğu anlaşılmıştır. Bu iddia, Littlewood tarafından eşitsizliğin yeterince büyük n değeri için, sonsuza gidildikçe tersine döndüğü ispatlanmıştır (Havil, 2017). Skewes, $\pi(n) - Li(n) = 0$ eşitliğinin, skewes sayısı olarak bilinen $10^{10^{10^{34}}}$ sayıdan önce gerçekleştiğini gösterdi. Daha sonra bu üst sınır 10^{371}indirgendi. 1966 tarihinde, Lehman 1166 veya 1167 ondalık basamaklı sayılarda en az 10^{500} için gerçekleştiğini ispatladı ve Chebyshev oranını kısıtladı.

$$\frac{7}{8} < \frac{\pi(n)}{\frac{n}{\ln n}} < \frac{9}{8}$$

eşitliğini ispatlamıştır ve büyük n sayıları için bu eşitsizliğinin doğruluğunu ispatladı.

Burada,

$$0.89Li(n) < \pi(n) < 1.11Li(n)$$

eşitsizliği de yazılabilir. Ayrıca, $Li(n)$ nin logaritmik integraldir ve

$$0.92 < \frac{\pi(n)}{\frac{n}{\ln n}} < 1.05$$

eşitsizliği yazılabilir. Buradan,

$$\lim_{n\to\infty} \frac{\pi(n)}{\frac{n}{\ln n}} = 1$$

dir (Weisstein).

Aşağıdaki tabloda asal sayı teoremi ile ilgili bazı karşılaştırılmalar yapılmıştır:

n	$\pi(n)$	$\frac{\pi(n)}{n}$	$\frac{\pi(n)}{\frac{n}{\ln n}}$
10	4	0.400	0.921
100	25	0.250	1.151
1000	168	0.168	1.161
10000	1229	0.123	1.132
100000	1592	0.096	1.105
1000000	78418	0.078	1.084
10000000	664579	0.066	1.071
100000000	5781455	0.058	1.061
1000000000	50847534	0.051	1.053
100000000000	4118054813	0.041	1.038
1000000000000	37607912018	0.038	1.050
10000000000000	346065536839	0.035	1.048
100000000000000	3204941750802	0.032	1.032
1000000000000000	29844570422669	0.030	1.036
10000000000000000	279238341033925	0.028	1.032
100000000000000000	2623557157654233	0.026	1.018

Tablo 1.1 Bazı sayılar için Asal Sayı Teoreminin sonuçları.

Teorem 1.2.15 (Euclid Teoremi) Sonsuz tane asal sayı vardır. Yani $2,3,5,7,\cdots$ asal sayılar sonsuzdur.

İspat. Varsayalım ki $p_1, p_2, \cdots, p_r$ r tane asal sayı olsun.

$$n = 1 + (p_1 p_2 p_3 \cdots p_r)$$

olarak alalım. n sayısı p_1 veya p_2 veya $\cdots$ p_r sayılarını bölmemektedir. Bundan dolayı, öyle bir p asal sayısı vardır ki $p|n$ dir. n sayısı, asal sayıdır ya da asal çarpanı p dir. Bu da p nin $p_1, p_2, \cdots, p_r$ den farklı bir asal sayı olduğu anlamına gelmektedir. O zaman $p|p_1 p_2 \cdots p_r$ olmalıdır. Fakat $p \nmid 1$dir. Dolayısıyla, asal sayılar sonsuz tanedir (Zuckerman ve diğ. 1991).

Teorem 1.2.16 (Euler Teoremi) n tamsayısını geçmeyen ve n tamsayısı ile aralarında asal olan herhangi pozitif tamsayılarının sayısı $\varphi(n)$ sembolü ile gösterilir. Buna Euler φ fonksiyonu denir. Eğer $n \geq 1$ ve $(a, n) = 1$ ise $a^{\varphi(n)} \equiv 1(mod\ n)$ dir (Yelkenkaya 2014).

Teorem 1.2.17 (Fermat Teoremi) Euler teoreminin özel bir hali olan bu teorem 17. yy da Fermat tarafından bulunmuştur. Fermat teoremine göre;

$p, p \nmid a$ bir asal sayı olsun. Bu durumda

$$a^{p-1} \equiv 1\ (mod\ p)$$

dir (Gerstien 2012).

İspat. a sayısının $a, 2a, 3a, \cdots, (p-1)a$ gibi ilk $(p-1)$ katından oluşan sayıları göz önüne alınsın. $1 \leq r < s \leq p-1$ olmak üzere,

$$ra \equiv sa\ (mod\ p\ )$$

olursa, $r \equiv s\ (mod\ p\ )$ demektir fakat bu mümkün değildir. Dolayısıyla,

$a, 2a, 3a, \cdots, (p-1)a$ sayılarından hiç biri p tarafından bölünmez. Yani,

$$a.2a.3a.\cdots.(p-1)a \equiv 1.2.3.\cdots(p-1)\ (mod\ p\ )$$

olur. Böylece,

$a^{p-1}(p-1)! \equiv (p-1)!\,(modp)\ ve\ p \nmid (p-1)!$ olduğundan

$$a^{p-1} \equiv 1(modp)$$

olur. Dolayısıyla, ispat tamamlanmış olur.

Teorem 1.2.18 Eğer n bir asal sayı ise, herhangi bir a sayısı için

$$a^n \equiv a(mod\ n)$$

dir.

İspat. $n|a$ ise $a^n \equiv a\ (mod\ n)$. Eğer $n \nmid a$ ise, Fermat teoreminden

$a^{n-1} \equiv 1(mod\ n)$ elde edilir. Bu kongrüansın her iki tarafı a ile çarpılırsa

$a^n \equiv a\ (mod\ n)$ elde edilir.

Carmichael Sayıları. Fermat teoremine göre: $(a, n) = 1$ ve $a^{n-1} \equiv 1(mod\ n)$ denkliğini sağlayan her sayının asal sayı olmadığı bilinmektedir. Bu n sayılarına Carmichael sayıları denir. Örneğin,

$n = 561$ sayısını $a = 2$ olsun. $2^{560} \neq 1(mod\ 561)$ olduğundan 571 sayısı carmichael sayısıdır. Bu sayıların kriterlerini 1899 yılında Korselt şu şekilde belirlemiştir:

1. n, tam sayısı karesiz olmalıdır.
2. $n|a$ değerleri için $(n-1)|(a-1)$ değerlerine bölünmelidir.

İlk olarak 1910 yılında R. D. Carmichael bu kriterlere uyan sayıların bir kısmını bulmuş. Bundan sonrada bu sayılara Carmichael sayıları denmiştir. Bu sayılardan bazıları aşağıda verilmiştir.

$$561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, \cdots$$

Bu sayılar sonsuz sayıda olup olmadığı bilinmemektedir.

Bu soruna karşılık 1992 yılında Alford, Granville ve Pomerance, a sayısına kadar $a^{\frac{2}{7}}$ den daha fazla Carmichael sayısı olduğunu ispatlamıştır (Yerlikaya ve Kara 2017).

2. BÖLÜM

BAZI ÖZEL ASAL SAYILAR

Asal sayıları tanımlamak basit olsa da, yeni ve büyük bir asal sayının bulunması işi zordur. Günümüze kadar, asal sayıların dağılımı, bir sonraki büyük asal sayı, asal sayı hesaplama algoritmaları vb. konularda matematikçiler birçok teori geliştirdiler. En yaygın ve bilinen asal sayılarla ilgi çalışma, Öklidin yaklaşık M.Ö.300 lü yıllardaki çalışmasıdır ve bu aynı zamanda aritmetiğin temel esaslarını teşkil etmektedir (O'Connor ve Robertson 2019). Yunan matematikçilerin keşfettiği Eratosthenes Kalburu ise büyük sayıların hesaplanmasında, maliyet ve zaman açışından pek yeterli değildir (Özgü 2002). Daha sonra 17. yüzyılda Fermat ve Euler adlı matematikçiler, asal sayıların özellikleri ve daha anlaşılır olması için çalışmalar yaptılar. Günümüzde de Great Internet Mersenne Prime Search(GIMPS) projesi kapsamında en büyük asal sayıyı bulmak için çalışmalar yapılmaktadır. Bilindiği gibi Euclid, asal sayıların sonsuz sayıda olduğunu ispatlamıştır. Fakat bu asal sayıları bulmak için henüz bir kesin formül günümüzde henüz bulunamamıştır. Bundan dolayı, asal sayılar üzerinde hala çalışmalara devam edilmektedir. Asal sayıları bulmak veya bileşik sayılardan ayırt etmek kolay olmadığı için, asal sayılar bazı özelliklerine göre gruplandırılmıştır. Bu bölümde, bilinen birkaç özel asal sayı tiplerine yer verilmiştir.

Fermat Asalları. Önce tanım verelim.

Tanım 2.1 Her $n \geq 0$ tamsayısı için, $F_n = 2^{2^n} + 1$ biçiminde yazılabilen sayılara Fermat asal sayıları denir. Örneğin,

$n = 0$ için, $F_0 = 2^{2^0} + 1 = 3$ dür.

$n = 1$ için, $F_1 = 2^{2^1} + 1 = 5$ dir.

$n = 2$ için, $F_2 = 2^{2^2} + 1 = 17$ dir.

$n = 3$ için, $F_3 = 2^{2^3} + 1 = 257$ dir.

$n = 4$ için, $F_4 = 2^{2^4} + 1 = 65537$ dir.

Fermat, her $n \geq 0$ için, $F_n = 2^{2^n} + 1$ eşitliğini sağlayan F_n sayısına asal sayı olduğunu iddia etmiştir. Fakat, n= 4 sayısından sonra bu formül işlememektedir. F_5 asal sayı değildir. Yani,

$$F_5 = 2^{2^5} + 1 = 641 \times 6700417$$

dir. Bundan dolayı, her Fermat sayısı asal sayı değildir. Bilinen ilk 25 Fermat sayısı hakkındaki bilgiler aşağıdaki Tablo 2.1 de verilmiştir (Crandall ve Pomerance 2005). Günümüze kadar birçok Fermat sayısı bulunmuş ve üzerinde çalışmalar yapılmıştır. 2019 yılında Fermat sayısı üzerinde yapılan çalışma, Gray Gostin tarafından bilgisayar yardımı ile F_{9863} un bir asal çarpanı olan $332436749 \cdot 2^{9865} + 1$ sayısı verilmiştir. En son 2020 yılında James Scott Brown ve PrimeGrid, bilsayar yardımıyla $F_{5523858}$ nin asal çarpanı olan $13 \cdot 2^{5523858} + 1$ sayısı bulunmuştur .

Aşağıdaki tabloda, bilenen Fermat sayıları verildi. Bileşik Fermat sayıları çarpanlarına ayırarak yazıldı.

F_0 = 3 (asal)
F_1 = 5 (asal)
F_2 = 17 (asal)
F_3 = 257 (asal)
F_4 = 65537 (asal)
F_5 = 641 · 6700417
F_6 = 274177 · 67280421310721
F_7 = 59649589127497217 · 5704689200685129054721
F_8 = 1238926361552897 · p ($p \in$ P)
F_9 = 2424833 · 7455602825647884208337395736200454918783366342657 · p ($p \in$ P)
F_{10} = 45592577 · 6487031809 · 4659775785220018543264560743076778192897 · p ($p \in$ P)
F_{11} = 319489 · 974849 · 167988556341760475137 · 35608419064458339205 13 · p ($p \in$ P)
F_{12} = 114689 · 26017793 · 63766529 · 190274191361 · 1256132134125569 · *C*
F_{13} = 2710954639361 · 2663848877152141313 · 3603109844542291969 ·
319546020820551643220672513 · *C*
F_{14} = *C*
F_{15} = 1214251009 · 2327042503868417 · 1687688170295169723830241270169 61 · *C*
F_{16} = 825753601 · 188981757975021318420037633 · *C*
F_{17} = 31065037602817 · *C*
F_{18} = 13631489 · 81274690703860512587777 · *C*
F_{19} = 70525124609 · 646730219521 · *C*

Tablo 2.1 Bazı Fermat sayıları, P: Kanıtlanmış asal sayı, C: Kanıtlanmış bileşik sayı

Mersenne Asalları. Mersenne sayıları, matematikte ikinin kuvvetlerinin bir eksiği şeklinde olan sayılardır ve n doğal sayısı $M_n = 2^n - 1$ şeklinde hesaplanır. Adını Fransız matematikçi, filozof, keşiş ve müzik teorisyeni ve "akustiğin babası" olarak bilinen Marin Mersenne'den almıştır.

Tanım 2.2 p asal sayı olmak üzere, $M_p = 2^p - 1$ eşitliğini sağlayan sayılara, Mersenne asal sayıları denir.

Örneğin, $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, $M_7 = 127$ birer Mersenne asalıdır.

Fakat her p asal sayısı için M_p asal sayı değildir. Mesela, $p = 11$ için

$$M_p = 2^{11} - 1 = 23 \,.\, 89$$

olur dolaysıyla, M_p asal sayı değildir.

$2^p - 1$ Mersenne sayısının asal sayı olup olmadığını belirlemek için, Lucas-Lehmer testi uygulanır. Bu test, bilinen bir Mersenne sayısının asal sayı olup olmadığını anlamak için kullanılan bir testtir. Bu test, ilk olarak 1856 yılında Lucas ve 1930 da Lehmer tarafından geliştirilmiştir. Özet olarak, $p \geq 2$ asal sayıları ve $M_p = 2^p - 1$ Mersenne sayısı için,

$$M_p \text{ asal sayıdır} \Leftrightarrow S_{p-2} \equiv 0 \ (mod\ M_p)$$

dir. Lucas-Lehmer asallık testine göre, $2^p - 1$ sayısının asal sayı olması için aşağıdaki şartların sağlanması gerekir (Ribenboim, 2004): S_k dizisi, $k \geq 0$ ve $S_0 = 4$ olmak üzere,

$$S_{k+1} = S_k^2 - 2$$

eşitliğinden bulunur. Örneğin, $k = 0$ için,

$$S_1 = S_0^2 - 2 = 16 - 2 = 14$$

olur. k $= 1$ için,

$$S_2 = S_1^2 - 2 = 196 - 2 = 194$$

olur. p asal sayısı için eğer

$$S_{p-2} \equiv 0(mod M_p)$$

eşitliği sağlanıyorsa, o zaman M_p sayısı asal sayı olur. Matematikçiler, ilk Mersenne asallarına bakarak gerçekten bu sayıların nasıl dağıldığına dair asimptotik bir formül geliştirdiler. Örneğin,

$$2^{20.000.000} - 1 \text{ ile } 2^{85.000.000} - 1$$

arasında 12 tane Mersenne asalı vardır. Bu sayı ise formülün iddia ettiğinin 3 katıdır. GIMPS'in internet sitesinde

"Bu anomali, Mersenne asallarının dağılımı ile ilgili teorilerin yanlış olduğuna dair kesin kanıt değildir. Ancak eğilim devam ederse bu konu araştırılmaya değerdir." deniyor. Mersenne asalları, mükemmel sayılar ile olan ilişkisi bakımından da son derece ilginçtir. Mükemmel sayı ise, kendisi hariç doğal sayı bölenlerinin toplamına eşit olan sayıdır. Örneğin;

$$6 = 1 + 2 + 3$$

$$28 = 1 + 2 + 4 + 7 + 14$$

gibi. Mükemmel sayılar, çok seyrek bulunan sayılardır. Önceleri sadece $6, 28, 496$ ve 8128 sayıları biliniyordu. Leonard Euler, bir Mersenne asalı bilinirken mükemmel bir sayının bulabileceğini iddia etti.

$$2^n - 1$$

Mersenne sayısı asal ise, o zaman

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

sayısı da mükemmel sayıdır. Dolayısıyla, o halde artık en büyük asal sayı bilinirse o zaman en büyük mükemmel sayı da bilinir.

$$2^{82.589.932}(2^{82.589.933} - 1)$$

Bu sayı 49 milyon basamaklı olup 51 tane Mersenne asalı ve 51 tane mükemmel sayı var demektir. Asalların sayısının sonsuz tane olduğunu bildiğimize göre her iki sayı tipinin sayısı da sonsuz olacaktır.

Aşağıdaki tabloda, Mersenne asallarının çalışılması, tarihi bir akış içinde verilmiştir.

Asal sırası	$\mathbf{2^p - 1}$	**Tarih**	***Kişi yada kişiler***
1	2^2 -1	c. 500 BCE	Eski Yunanlı matematikçiler
2	2^3 -1	c. 500 BCE	Eski Yunanlı matematikçiler
3	2^5 -1	c. 275 BCE	Eski Yunanlı matematikçiler
4	2^7 -1	c. 275 BCE	Eski Yunanlı matematikçiler
5	2^{13} -1	1456	Anonim
6	2^{17} -1	1588	Pietro Cataldi
7	2^{19} -1	1588	Pietro Cataldi
8	2^{31} -1	1772	Leonhard Euler
9	2^{61} -1	1883	Ivan Mikheevich Pervushin
10	2^{89} -1	1911	RE Yetkileri
11	2^{107} -1	1914	RE Yetkileri
12	2^{127} -1	1876	Édouard Lucas
13	2^{521} -1	1952	Raphael M. Robinson

14	$2^{607}-1$	1952	Raphael M. Robinson
15	$2^{1,279}-1$	1952	Raphael M. Robinson
16	$2^{2,203}-1$	1952	Raphael M. Robinson
17	$2^{2,281}-1$	1952	Raphael M. Robinson
18	$2^{3,217}-1$	1957	Hans Riesel
19	$2^{4,253}-1$	1961	Alexander Hurwitz
20	$2^{4,423}-1$	1961	Alexander Hurwitz
21	$2^{9,689}-1$	1963	Donald B. Gillies
22	$2^{9,941}-1$	1963	Donald B. Gillies
23	$2^{11,213}-1$	1963	Donald B. Gillies
24	$2^{19,937}-1$	1971	Bryant Tuckerman
25	$2^{21,701}-1$	1978	Landon Curt Noll ve Laura Nickel
26	$2^{23,209}-1$	1979	Landon Curt Noll
27	$2^{44,497}-1$	1979	Harry Lewis Nelson ve David Slowinski
28	$2^{86,243}-1$	1982	David Slowinski
29	$2^{110,503}-1$	1988	Walter Colquitt ve Luke Welsh
30	$2^{132,049}-1$	1983	David Slowinski
31	$2^{216,091}-1$	1985	David Slowinski
32	$2^{756,839}-1$	1992	David Slowinski ve Paul Gage
33	$2^{859,433}-1$	1994	David Slowinski ve Paul Gage
34	$2^{1,257,787}-1$	1996	David Slowinski ve Paul Gage
35	$2^{1,398,269}-1$	1996	GIMPS / Joel Armengaud
36	$2^{2,976,221}-1$	1997	GIMPS / Gordon Spence
37	$2^{3,021,377}-1$	1998	GIMPS / Roland Clarkson
38	$2^{6,972,593}-1$	1999	GIMPS / Nayan Hajratwala
39	$2^{13,466,917}-1$	2001	GIMPS / Michael Cameron
40	$2^{20,996,011}-1$	2003	GIMPS / Michael Shafer
41	$2^{24,036,583}-1$	2004	GIMPS / Josh Findley
42	$2^{25,964,951}-1$	2005	GIMPS / Martin Nowak
43	$2^{30,402,457}-1$	2005	GIMPS / Curtis Cooper ve Steven Boone
44	$2^{32,582,657}-1$	2006	GIMPS / Curtis Cooper ve Steven Boone
45	$2^{37,156,667}-1$	2008	GIMPS / Hans-Michael Elvenich
46	$2^{42,643,801}-1$	2009	GIMPS / Garip M. Strindmo
47	$2^{43,112,609}-1$	2008	GIMPS / Edson Smith
48	$2^{57,885,161}-1$	2013	GIMPS / Curtis Cooper
49	$2^{74,207,281}-1$	2016	GIMPS / Curtis Cooper
50	$2^{77,232,917}-1$	2017	GIMPS / Jon Pace
51	$2^{82,589,933}-1$	2018	GIMPS / Patrick Laroche

Tablo 2.2 Bilinen Bazı Mersenne asalları

Wilson Asalları. Wilson teoreminin iddiası aşağıdaki gibidir:

Wilson Teoremi 2.3 p asal sayısı için,

$$(p-1)! \equiv -1(mod\ p)$$

dir. Literatürde, bu teorem yardımıyla elde edilen Wilson katsayısı $W(p) = \frac{(p-1)!+1}{p}$ olarak bilinmektedir.

Tanım 2.3.1 $W(p) \equiv 0(mod\ p)$ veya $(p-1)! \equiv -1(mod\ p)$ eşitliğini sağlayan p sayısına Wilson asal sayısı denir. Örneğin, $p = 5,\ p = 13$ Wilson asalıdır. Diğer bir Wilson asal sayısı ise, 1953 yılında Goldberg tarafından bulunan 563 sayısıdır. 1988 yılında E.H. Pearson, K.E. Kloss, W. Keller, H. Dubner ve Gonter ve Kundert tarafından yapılan araştırmalarda 10^7 den küçük başka bir Wilson asalı bulunamamıştır. 1997 de Crandall, Dilcher ve Pomerance tarafından 5.10^8 e kadar yapılan araştırmalarda ise, herhangi bir Wilson asal sayısına rastlanmamıştır. Wilson asal sayısının sonsuz veya sonlu sayıda olup olmadığı ise bilinmemektedir (Ribenboim 2004).

p	$(p-1)!$	$(p-1)! \equiv -1(mod\ p)$
2	1	Wilson asalı değil.
3	2	Wilson asalı değil.
5	24	Wilson asalıdır.
7	720	Wilson asalı değil.
11	3628800	Wilson asalı değil.
13	479001600	Wilson asalıdır.
17	20922789888000	Wilson asalı değil.
19	6402373705728000	Wilson asalı değil.

Tablo 2.3 Bazı Wilson sayıları

Cullen Asalları. Cullen asal sayıları için önce tanım verelim.

Tanım 2.4 $C_n = n.2^n + 1$ formundaki sayılara, Cullen asal sayıları denir. Örneğin,

$n = 2\ için\ C_2 = 2.2^2 + 1 = 9$ dur.

$n = 3\ için\ C_3 = 3.2^3 + 1 = 25$ dir.

$n = 4\ için\ C_4 = 4.2^4 + 1 = 65$ dir.

$n = 5\ için\ C_5 = 5.2^5 + 1 = 161$ dir.

Bu sayılar Cullen sayılarıdır, fakat Cullen asalları değildir.

1958 yılında Raphael Robinson, her n tamsayısı için, $1 < n \leq 1000$ arasında C_{141} Cullen asal sayısından başka bir asal sayı olmadığını göstermiştir. 1987 yılında (1995'te yayınlandı) Keller, her n tamsayısı için

$n \leq 30000$ e kadar tüm Cullen asal sayılarını bulmuştur. 1997 de J. Young her n için

$n \leq 100000$ e kadar Cullen asalarını buldu (Ribenboim 2004). Bilinen en büyük Cullen asalı $1323365 \times 116^{1323365} + 1$ dir (Marques 2014).

n	Bulan Kişi	Bulunan Tarih
481899	M. Morii and Y. Gallot	1998
361275	D. Smith and Y. Gallot	1998
262419	D. Smith and Y. Gallot	1998
90825	J. Young	1997
59656	J. Young	1997
32469	M. Morii	1997
32292	M. Morii	1997
18496	W. Keller	1984
6611	W. Keller	1984
5795	W. Keller	1984
4713	W. Keller	1984
141	R.M. Robinson	1958

Tablo 2.4 Bazı Cullen Asalları

Palindromik Asallar. Sağdan ve soldan okunuşları aynı olan sayılara palidromik sayı denir. Eğer bu sayılar asal sayı ise palindromik asallar olarak adlandırılır. Bir basamaklı sayılar da palindromik sayılardır. Bazı palindromik asal sayılar;

$2, 3, 5, 7, 11, 101, 131, 151, 181, 191, 313, 353, 373, 383, \cdots$

2019 yılı itibariyle bilinen en büyük palindromik asal sayısı, 474501 basamaklı olan, $10^{474500} + 999 \times 10^{237249} + 1$ sayısıdır.

Faktöriyel Asallar. $n! \pm 1$ formundaki asal sayılara faktöriyel asalllar denir. $n! - 1$ şeklindeki asal sayılar için bazı n değerleri;
$3, 4, 6, 7, 12, 14, 30, 32, 33, 38, 94, 166, 324, 379, 469, 546, 974, \cdots$ dir.

$n! + 1$ şeklindeki asal sayılar için bazı n değerleri;
$1, 2, 3, 11, 27, 37, 41, 73, 77, 116, 154, 320, 340, 399, 427, 872, \cdots$ dir. S. Fukui tarafaından 2016 yılında, bulunan en büyük 1015843 basamaklı faktöriyel asal sayısı, $208003! - 1$ dir .

Ramanujan Asalları. Bertrand, her $x \geq 1$ için, $x < p \leq 2x$ aralığında, en az bir asal sayı olduğunu iddia etmiştir. Bu iddia ilk Chebyshev tarafından kanıtlanmıştır. 1919 yılında Ramanujan, Bertrand iddiasını daha genel olarak ele almıştır (Sondow 2009).

Teorem 2.5 $\pi(x), x$ sayısını aşmayan asal sayılar olsun. O zaman,

$$\pi(x) - \pi\left(\frac{1}{2}x\right) \geq 1, 2, 3, \ldots$$

ise, sırasıyla $x \geq 2, 11, 17, 29, \ldots$ olur.

Tanım 2.5.1 Herhangi n doğal sayısı için, n. Ramanujan asalı en küçük R_n tamsayısıdır öyle ki $x \geq R_n$ iken $\pi(x) - \pi\left(\frac{1}{2}x\right) \geq n$ olur. Yani, $x \geq R_n$ olduğunda

$$R_n = 1 + \max\{k : \pi(x) - \pi\left(\frac{1}{2}x\right) = n - 1\}$$

olur. Buradan, sırasıyla bazı Ramanajuan asalları şöyledir:

$$\{2, 11, 17, 29, 41, 47, 59, 67, 71, 97\}$$

tamsayısıdır (Beşkirli ve diğ. 2019). Bu sayılar aşağıdaki tabloda verilmiştir.

$\boldsymbol{\pi(x)}$	$\boldsymbol{\pi(\frac{1}{2}x)}$	$\boldsymbol{\pi(x) - \pi(\frac{1}{2}x)}$	$\boldsymbol{x}$
1	0	1	2
5	3	2	11
7	4	3	17
10	6	4	29
13	8	5	41

Tablo 2.5 Bazı Ramanajuan Asalları

Sophie Germain Asalları. Sophie Germain (1776-1831), en eski kadın matematikçilerinden biri olarak bilinmektedir. Fransa da bir bankanın müdürü olan babasının kütüphanesindeki kitaplarla kendini eğitmiş ve on üç yaşında Arşimentin ölüm hikayesini okumuştur. Bu olaydan çok etkilenen Sophie, matematikçi olmaya karar vermiştir. Sophie Germain 1823 yılında, Fermatın son teoremininin ilk durumunu, Sophie asallarını kullanarak ispat yapmıştır. Yani, p Sophie Germain asalı ise $x^p+y^p = z^p$ eşitliğini sağlayan, sıfırdan farklı ve p nin katları olmayan x, y, z tamsayıları olmadığını ispatlamıştır (Wells 2005).

Tanım 2.6 p asal bir sayı ve $2p + 1$ sayısı da asal sayı ise, bu p sayısına Sophie Germain asal sayısı denir. Mesela, aşağıdaki sayılar birer Sophie Germain asalıdır:

$2, 3, 5, 11, 23, 29, 41, 53, 89, 113, 173, 179, 191, 233, 239, 251, 281, 293, 359, ..$

p	$2p + 1$	Sophie Germain Asalı
2	5	EVET
3	7	EVET
5	11	EVET
7	15	HAYIR
11	23	EVET
13	27	HAYIR
17	35	HAYIR
19	39	HAYIR
23	47	EVET

Tablo 2.6 Birkaç Sophie Germain sayıları

Sophie Germain ile İlgili Bir Çalışma. Bu kısımda, Recep Baştan Baştan, R., Akın, C. Notes on Sophie Germain Primes. Turkish Journal of Mathematics and Computer Science, 10, 18-21.tarafından yapılan bir çalışmayı ana hatlarıyla verdik.

Lampret, p asal ve $m > 0$ tam sayı olmak üzere $(p, p + 2m)$ gibi asal sayıları $2m$- asalları olarak gösterilmiştir ve $2m$- asallları için,

$m = 1$ için 2- asalları ikiz asallardır.

$m = 2$ için 4- asalları: $(3,7), (7,11), (13, 17), \ldots$

$m = 3$ için 6-asalları: $(5,11), (7,13), (11,17), \ldots$

$m = 4$ için 8-asalları: $(3,11), (5,13), (11, 19), \ldots$

olur. İkiz asallar, $2m$-asallarının özel bir durumu gibi incelenebilir ve ikiz asalların sonsuz sayıda olması $2m$- asalları için genelleştirilebilir. Aşağıdaki teorem bunu verir.

Teorem 2.6.2 k ve n pozitif tam sayıları için,

$(6k + 1, 6k + 6n - 1), (6n - 2)$ asal değildir $\Leftrightarrow$ pozitif tam sayılar için i ve j aşağıdaki eşitliklerden herhangi biri gerçeklenir:

i) $p = 6j - 1$ asaldır, $k = pi - j$ ve $k = pi + j - n$ dir.

ii) $p = 6j + 1$ asaldır, $k = pi + j$ ve $k = pi - j - n$ dir,

Yukarıdaki her iki durum için, $p \leq \sqrt{6k + 6n - 1}$ olur.

3 ten büyük asal sayılar, herhangi k pozitif tamsayısı için $6k - 1$ veya 6k + 1 şeklindedir. Ancak, p asal sayısı $6k + 1$ şeklinde olursa $2p + 1$ asal olmadığı için p bir Sophie Germain asal değildir. Bundan dolayı, $(6k + 1,12k + 3)$ SG-S-asallı olmaz. Buradan, SG-S asalı herhangi k pozitif tamsayısı için $(6k - 1,\ 12k - 1)$ şeklinde olur. Böylece,

$(12k - 1) - (6k - 1) = 6k$ için SG-S asalı, Lampret in 2m-asalı olur, k pozitif tam sayı için $2m = 6k$ olur. k pozitif bir tam sayı olmak üzere, $n = k$ alınırsa aşağıdaki sonuç elde edilir.

$(6k - 1, 12k - 1)$ SG-S asal çifti değildir $\Leftrightarrow$ i ve j pozitif tam sayıları için aşağıdaki denkliklerden biri doğrudur:

i) $p = 6j - 1$ asaldır, $k = pi + j$ ve $k = \frac{pi+j}{2}$,

ii) $p = 6j + 1$ asaldır, $k = pi - j$ ve $k = \frac{pi-j}{2}$.

Her iki durumda da $p \leq \sqrt{12k - 1}$ dir. Verilen bir z pozitif tam sayısına kadar olan SG-S asal çiftleri için aşağıdaki algoritma uygulanır.

1) $k = 1, 2, \ldots, [\frac{z}{6}]$ tamsayıları listelenir.

2) $3 < p \leq \sqrt{z}$ olacak şekilde asallar bulunur.

3) Bulunan her bir $3 < p \leq \sqrt{z}$ asalları için;

- $\frac{p+1}{6}$ ise $j = \frac{p+1}{6}$ dir ve $k = pi + j$ ve $k = \frac{pi+j}{2}$ tam sayıları listeden atılır,
- $\frac{p-1}{6}$ ise $j = \frac{p-1}{6}$ dir ve $k = pi - j$ ve $k = \frac{pi-j}{2}$ tam sayıları listeden atılır,

4) Listede kalan her k tamsayısı, $(6k - 1, 12k - 1)$ SG-S asal çiftlerini verir.

Örneğin, 250 ye kadar olan SG-S asal çiftlerini bulmak için $k = 1, 2, \ldots, 41$ tamsayıları aşağıdaki tabloda listelenmiştir. $3 < p \leq \sqrt{250}$ olacak şekilde asallar $5, 7, 11$ ve 13 tür.

i) $p = 5 = 6.1 - 1$ olduğundan $j = 1$ dir ve dolayısıyla

$k = 5i + 1$ ve $k = \frac{5i+1}{2}$

tamsayıları listeden atılır. Bu durumda listeden atılanlar

$$3, 6, 8, 11, 13, 16, 18, 21, 23, 26, 28, 31, 33, 36, 38, 41$$

tamsayılarıdır.

ii) $p = 7 = 6.1 + 1$ olduğundan $j = 1$ dir. Ve dolayısıyla,

$k = 7i - 1$ ve $k = \frac{7i-1}{2}$

tamsayıları listeden atılır. Bu durumda listeden atılanlar

$$3,6,10,13,17,20,24,27,31,34,38,41$$

tamsayılarıdır.

iii) $p = 11 = 6.2 - 1$ olduğundan $j = 2$ dir ve dolayısıyla,

$k = 11i + 2$ ve $k = \frac{11i+2}{2}$ tamsayıları listeden atılır.

Bu durumda listeden atılanlar,

$$12,13,23,24,34,35$$

tamsayılarıdır.

Bu yapılanlar, aşağıdaki gibi özetlenebilir:

1	2	**3**	4	5	**6**	7	**8**	9	**10**
11	**12**	**13**	14	15	**16**	**17**	**18**	19	**20**
21	22	**23**	**24**	**25**	**26**	**27**	**28**	29	30
31	32	**33**	**34**	**35**	**36**	**37**	**38**	39	40
41									

Tablo 2.7 Sophie Germain eleği

Listede kalan her k tamsayısı için $(6k - 1, 12k - 1)$ olarak SG-S asal çiftleri elde edilir. Listede bulunmayan $(2,5)$ ve $(3,7)$ çiftlerini de eklersek, 250 ye kadar olan bütün SG-S asal çiftlerini bulunur:

$$(2,5), (3,7), (5,11), (11,23), (23,47), (29,59), (41,83), (53,107), (83,167), (89,179), (113,227),$$
$$(131,263), (173,347), (179,359), (192,383), (233,467), (239,479).$$

Lemma 2.6.4 p asal sayıdır ancak ve ancak $(p+1)^2[(p-1)!]^2 \equiv 1\ mod(p)$

$$p\epsilon\mathbb{P} \Rightarrow (p+1)(p-1)! \equiv -1\ mod(p)$$

$$p\epsilon\mathbb{P} \Rightarrow [(p+1)(p-1)!]^2 \equiv (-1)^2 mod(p)$$

$$p\epsilon\mathbb{P} \Rightarrow (p+1)^2[(p-1)!]^2 \equiv 1 mod(p)$$

dir. Fakat,

$$(p+1)^2[(p-1)!]^2 \equiv 1 mod(p) \text{ ve } p \notin \mathbb{P}$$

olsun. Böylece $1 < t < p$ olacak şekilde p nin t tamsayı böleni vardır. Diğer yandan,

$$(p+1)^2[(p-1)!]^2 \equiv 1 mod(p) \text{ ise } [(p-1)!]^2 \equiv 1 mod(p)$$

dir. Bundan dolayı $[(p-1)!]^2 \equiv 1 mod(t)$ dir. t tamsayısı aynı zamanda $[(p-1)!]^2$ nin bir böleni olduğundan bu çelişkidir. O halde, p asal sayıdır.

Lemma 2.6.5 $p > 2$ bir tek sayı olsun. Bu taktirde $2p+1$ asal sayıdır ancak ve ancak $(p+1)^2[(p-1)!]^2 \equiv 1 mod(2p+1)$ dir.

İspat. Wilson teoremininden,

$$2p+1 \in \mathbb{P} \Leftrightarrow (2p)! \equiv -1\ mod(2p+1)$$

dir. Böylece

$$2p+1 \in \mathbb{P} \Leftrightarrow (2p)(2p-1) \dots (2p-p)(2p-p-1)! \equiv -1\ mod(2p+1)$$

$$\Leftrightarrow (-1)(-2) \dots (-p-1)(p-1)! \equiv -1\ mod(2p+1)$$

$$\Leftrightarrow (-1)^{p+1}(p+1)!\,(p-1)! \equiv -1\ mod(2p+1)$$

$$\Leftrightarrow (p+1)!\,(p-1)! \equiv -1\ mod(2p+1)$$

$$\Leftrightarrow (p+1)p(p-1)!\,(p-1)! \equiv -1\ mod(2p+1)$$

$$\Leftrightarrow (p+1)p[(p-1)!]^2 \equiv -1\ mod(2p+1)$$

$$\Leftrightarrow (p+1)(p+p+1-p-1)[(p-1)!]^2 \equiv -1\ mod(2p+1)$$

$$\Leftrightarrow (p+1)(-p-1)[(p-1)!]^2 \equiv -1\ mod(2p+1)$$

$$\Leftrightarrow -[(p+1)]^2[(p-1)!]^2 \equiv -1\ mod(2p+1)$$

$$\Leftrightarrow [(p+1)]^2[(p-1)!]^2 \equiv -1\ mod(2p+1) \text{ dir.}$$

Lemma 2.6.6 $p > 2$ bir sayı olsun. Bu taktirde $(p+1)^2[(p-1)!]^2 \equiv 1\ mod(2p+1)$ $2p+1$ asal sayıdır.

İspat. $(p+1)^2[(p-1)!]^2 \equiv 1\ mod(2p+1)$ve $2p+1 \notin \mathbb{P}$ olsun. Böylece $1 < t < 2p+1$ olacak şekilde $2p+1$ nin tam sayı böleni vardır. Diğer yandan 3.3 Lemma nın ispatı $[(p+1)]^2[(p-1)!]^2 \equiv 1\ mod(2p+1) \Leftrightarrow (p+1)!\,(p-1)! \equiv -1\ mod(2p+1)$

olduğundan 1.2.3 ... $(p+1)(p-1)! \equiv -1\ mod(2p+1)$dir. Buradan

$(-2p)(-2p+1)(-2p+2)\ldots(-2p+p)(p-1)! \equiv -1\ mod(2p+1)$ olup
$(-1)^{p+1}2p(2p-1)\ldots(2p-p)(p-1)! \equiv -1\ mod(2p+1)$ dir. Böylece

$(-1)^{p+1}2p! \equiv -1\ mod(2p+1)$ olduğundan $(-1)^{p+1}2p! \equiv -1\ mod(t)$ elde edilir. t tam sayısı $(2p)!$ sayısını böldüğünden bu bir çelişkidir.

Dolayısıyla, $2p+1$ asaldır.

Teorem 2.6.7 $p > 2$, p Sophie Germain asalıdır ancak ve ancak

$(p+1)^2[(p-1)!]^2 \equiv 1\ mod(p(2p+1))$ dir

İspat, 3.2. Lemma ve 3.3. Lemma dan ispat kolayca görülebilir.

İkiz Asallar. p ve $p+2$ sayıları asal sayı ise, bu sayılar ikiz asallar olarak adlandırılmaktadır. Yani aralarında iki fark olan asal sayılara ikiz asal sayı denir. Bilinen en küçük birkaç ikiz asal sayıları; $(3,5),(5,7),(11,13)\ ve\ (17,19)$ dur. İkiz asallar 1949 yılında Clement tarafından aşağıdaki teoremde tanımlanmıştır (Ribenboim 2004).

Teorem 2.7 $n \geq 2$ olsun. O zaman,

$$(n, n+2) \text{ ikiz asallardır} \Leftrightarrow 4[(n-1)!+1] + n \equiv (mod\ n(n+2))$$

dir.

İspat. Varsayalım ki, $n \neq 2, 4, \ldots ve\ (n-1)!+1 \equiv 0\ (mod\ n)$ ise n, Wilson Teoreminden asaldır. Ayrıca, $4(n-1)!+2 \equiv 0\ (mod\ n+2)$ bu denkliği $n(n+1)$ ile çarpılır ve buradan
$4[(n-1)!+1] + 2n^2 + 2n - 4 \equiv 0\ (mod\ n+2)$ ve
$4[(n-1)!+1] + (n+2)(2n-2) \equiv 0\ (mod\ n+2)$ olur.
Wilson teoremine göre, $n+2$ asal sayıdır. Aksine, $n, n+2$ asal sayı ise, o zaman
$n \neq 2$ ve $(n-1)!+1 \equiv 0\ (mod\ n)$,

$(n-1)! + 1 \equiv 0\ (mod\ n+2)$ dir.

Fakat, $n(n+1) = (n+2)(n-1) + 2$ yani, $2(n-1)! + 1 = k(n+2)$ dir. Burada, k bir tamsayıdır.

$(n-1)! \equiv -1\ (mod\ n)$ den sonra $2k + 1 \equiv 0\ (mod\ n)$ ve $4(n-1)! + 2 \equiv -(n+2)\ (mod\ n(n+2))$ yerine konulduğunda $4[(n-1)! + 1] + n \equiv 0\ (mod\ n(n+2))$ olur.

3. BÖLÜM

ASAL SAYI TESTLERİ

Asal sayılar konusunda birçok çalışma yapılmıştır. Bu çalışmalardan en önemli olanlar, asallık testleridir. Bir sayının asal olup olmadığını incelemek için kullanılan bu testlerin en eskisi "elek testi" olarak bilinmektedir. Sonraları, matematik yöntemlerden yararlanarak elde edilen çeşitli testler bulunmuştur. Bu testler yardımıyla, çok büyük sayıların asal olup olmadıklarının kontrolleri yapılabilmektedir.

Asal sayılara ulaşabilmek, bileşik sayılara ulaşmaktan daha zordur. Bundan dolayı, bir sayının asal sayı mı veya bileşik sayı mı olduğunu bilmek için bazı testler oluşturulmuştur. Ancak günümüzde bu konu üzerinde çalışmalar hala devam etmektedir. Çünkü sayılar büyüdükçe bilinen asallık testlerini uygulamak zorlaşır. Asallık testleri iki gruba ayrılır. Deterministik testler ve Olası asallık testleridir. Bu bölümde asal sayı testleri ve özellikleri incelenecektir.

Kesin(Deterministik) Asallık Testleri. Bu tür asallık testleri yardımı ile bir sayının asal sayı olup olmadığını kesin olarak belirlemek mümkündür. Bu tür yöntemler genellikle çarpanlara ayırma yöntemlerine dayanmaktadır. Kesin asallık testleri büyük sayıları test ederken, çok fazla zaman harcandığından kullanışlı değildir ve bu yöntemler çok karışıktır. Uygulamada asallık testi sırasında hata yapılma olasılığı, olası asallık testinden daha fazladır. Kesin asallık testlerinden bazıları aşağıda verilmiştir (Silverman 1997).

Eratosthenes Kalburu. Dünyanın çevresini hesaplamaya çalışan ve asal sayılarla ilgili çalışmalar yapan Eratosthenes matematik tarihindeki önemli kişilerden biridir. Dünyanın çevresini ölçmek için Aristoteles'in de fikirlerinden yararlanarak iki varsayımda bulunmuştur:

1. Dünya, küre şekline benzeyen geometrik bir cisimdir.
2. Güneş ışınları dünyaya paralel doğrular boyunca gelirler.

Mısırdaki Asvan şehrinde, yılın belirli bir gününde tam öğle vakti güneş ışınları yere dik açıyla gelmektedir. Aynı günde ve aynı saatte Mısır'ı diğer bir kenti olan İskenderiye'de ise güneş ışınları yere dik açıyla gelmemektedir. Bu farklılıklardan yararlanan Eratosthenes, dünyanın çevresini şu şekilde hesapladı:

Biri Asvan'da diğeri İskenderiye'de iki çubuk yere dikilir. Bu iki çubuk yere dik konumda olacak şekilde batırılır. Bu çubuklar, sanal olarak uzatıldığında dünyanın merkezinde kesişeceklerdir. Asvan'daki çubuğun gölgesi 0 olduğu anda İskenderiye' de güneş ışınlarının oradaki çubukla yaklaşık 7 derecelik açı yaparak geldiği ölçülerek belirlenmiştir. Asvan ile İskenderiye arasındaki uzaklık, o zamanki uzunluk ölçüsü olan stad kullanılarak ölçülmüştür. Bu uzaklık 5000 stadtır. Sonrasında Eratosthenes, oran orantı yöntemiyle 360 derecelik açının kaç stad mesafe tarayacağını, yani dünyanın çevresinin yaklaşık hesabını bulmuştur.

M.Ö. 300 yıllarında, Eratosthenes asal sayıları bulmak için basit bir algoritma geliştirmiştir. Bu algoritma Eratosthenes kalburu (İngilizce:Sieve of Eratosthenes) olarak bilinir. Matematikte Eratosthenes kalburu, asal sayıların seçilmesinde temel bir algoritma olarak kullanılır. Algoritma, asal sayıları bir sınır olmadan bulabilmeyi sağlayan bir asallık testi olup, bu asallık testi bileşik sayıları eleyerek ilerlemeye dayanır. Bu işlemler sonucunda, elenmeden kalan sayılar asal sayıdır**.** Sınırlama olmadığı için, istenen sayıya kadar bütün asal sayılar kesin olarak bulunabilir. Fakat sayılar büyüdükçe asal sayıları bulmak zaman alır. Eratosthenes Kalburunu uygulamak için, ilk önce 2 den başlayarak istenen n sayısına kadar tüm tamsayılar yazılır. Ve 2 den başlayarak $2, 3, 4,$ nin katları bu listeden silinir. Dolayısıyla, bu işlemlerler yardımıyla, bileşik sayılar listeden silinmiş olur ve silinmeden kalan sayılar asal sayı olur 5.

Dolayısıyla, yukarıdaki algoritmayı aşağıdaki gibi özetleyebiliriz:

n bileşik tamsayısı için, $p^2 \leq n$ olan yani, $p \leq \sqrt{n}$ eşitsizliğini sağlayan bir p asal böleni bulunabilir. Yani, $n > 1$ olan bir n tamsayısının asal çarpanlar biçiminde yazıldığını biliyoruz. Bu asal çarpanların en küçük asal bölenine p diyelim.

O zaman, $n = p.n_1$ olacak şekilde bir $n_1 > 1$ tamsayısı vardır ve

$$n = p.n_1 \geq p.p = p^2$$

yazılabilir. Bu durumu açık bir örnek ve tablo ile anlatabiliriz.

Örneğin, 127 sayısı olup olmadığını incelemek için, 127 sayısının karekökünden büyük en küçük sayı bulunur. Yani, $\sqrt{127} < 12$ olduğundan dolayı 127 sayısının asal sayı olup olmadığını kontrol etmek için $2, 3, 5, 7, 11$ sayıları ile bölünüp bölünmediğini denemek yeterli olacaktır. 127 , bu sayıların hiçbirine bölünmediği için asal sayıdır.

Örneğin, 1 den 100 e kadar olan asal sayıları Eratosthenes kuralı ile bulalım.

Önce 1 ile 100 arasındaki bütün tamsayıları yazalım. 1 den 10 a kadar olan asal sayılar $2, 3, 5$ ve 7 dir. O halde, 1 sayısını sildikten sonra 2 den başlayarak, sırayla 2 ve 2 nin katları, 3 ve 3 ün katları, 5 ve 5 in katları ve nihayet 7 ve 7 nin katlarındaki sıralarda yer alan bütün sayıları silersek geriye kalan $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73,$

$79, 83, 89, 97$ sayıları 1 ile 100 arasında bulunan asal sayılar olacaktır. Aşağıdaki tabloda burada ifade edilenler gösterildi.

	2	3	**4**	5	**6**	7	**8**	**9**	**10**
11	**12**	13	**14**	**15**	**16**	17	**18**	19	**20**
21	**22**	23	**24**	**25**	**26**	**27**	**28**	29	**30**
31	**32**	**33**	**34**	**35**	**36**	37	**38**	**39**	**40**
41	**42**	43	**44**	**45**	**46**	47	**48**	**49**	**50**
51	**52**	53	**54**	**55**	**56**	**57**	**58**	59	**60**
61	**62**	**63**	**64**	**65**	**66**	67	**68**	**69**	**70**
71	**72**	73	**74**	**75**	**76**	**77**	**78**	79	**80**
81	**82**	83	**84**	**85**	**86**	**87**	**88**	89	**90**
91	**92**	**93**	**94**	**95**	**96**	97	**98**	**99**	**100**

Tablo 3.1 Eratosthones Kalburu

Lucas-Lehmer Testi. Bu test, bilinen bir Mersenne sayısının asal sayı olup olmadığını anlamak için kullanılan bir testtir. Bu test ilk olarak 1856 yılında Lucas ve 1930 da Lehmer tarafından geliştirilmiştir.

Özet olarak, $p \geq 2$ asal sayıları ve $M_p = 2^p - 1$ Mersenne sayısı için,

$$M_p \text{ asal sayıdır} \Leftrightarrow S_{p-2} \equiv 0 \ (mod\ M_p)$$

Burada, S_n sayıları Lucas sayıları olarak bilinir ve aşağıdaki gibi bulunmaktadır (Wells 2005).

$$4, 14, 194, \dots, S_n = (S_{n-1})^2 - 2, \dots.$$

Örneğin, $p = 7$ için, $M_7 = 2^7 - 1 = 127$ olup buradan,

$S_0 = 4 \equiv 4\ (mod\ 127),\ S_1 = 14 \equiv 14\ (mod\ 127),\ S_2 = 194 \equiv 67\ (mod\ 127)$

$S_3 = 37634 \equiv 42\ (mod\ 127),\ S_4 = 1416317954 \equiv 111\ (mod\ 127)$ ve

$S_5 = 2005956546822746114 \equiv 0\ (mod\ 127)$ bulunmaktadır. Dolayısıyla, M_7 Mersenne sayısının asal sayı olduğu anlaşılmaktadır.

AKS (Agrawal- Kayal- Saxena) Testi. Ağustos 2002 de M. Agrawal, N. Kayal ve N. Saxena'nın tarafından oluşturulan polinom algoritmik testtir. Verilen bir sayının asal sayı veya bileşik sayı olup olmadığını belirlemektedir. Bu test özellikle veri güvenliği (kriptoloji) konusunda oldukça önem taşımaktadır. AKS asallık testinin ismi, bu testi oluşturan üç kişinin isimlerinden oluşturulmuştur (Agrawal, Kayal, Saxena).

$a \in \mathbb{Z},\ n \in \mathbb{N}\ \ n \geq 2$ ve $(a, n) = 1$ için $(x - a)^n \equiv (x^n - a)\ (\ mod\ n)$
dir. Bu denklem, Fermatın küçük teoreminin genişletilmiş halidir ve n ile aralarında asal a değerleri bulunmaktadır. Algoritmanın çalışması aşağıda verilmiştir:

- $a > 0$ ve $b > 1$ için $n = a^b$ eşitliği sağlanıyorsa, n sayısı asal sayı değildir.
- $O_r(n) > log_2(n)$ denklemini sağlayan en küçük r değeri bulunur.
- $1 < ebob(a, n) < n$ denklemini sağlayan bir $a \leq r$ değeri bulunabiliyorsa sayı asal değildir.
- Eğer n ≤ r ise n asal sayıdır.
- $1 < a < \left|\sqrt{\varphi(r)}\log(n)\right|$ değerine kadar olan değerler için
- $(x + a)^n \neq x^n + a\ (mod\ x^r - 1, n)$ eşitsizliği sağlanıyorsa sayı asal değildir.
- Yukarıdaki şartlardan geçerse, sayı asaldır.

$1 < a < \left|\sqrt{\varphi(r)}\log(n)\right|$ eşitsizliğinde kullanılan $\varphi(r)$ sembolü, Eulerin Totient fonksiyonudur ve $O_r(n)$ fonksiyonu da çarpım derecesini belirtmektedir. Örneğin,
$r = 2$ ve $n = 119$ sayıları için $log_2(n)$ değeri hesaplanır. $log_2(119) = 6{,}89$ dir. Daha sonra $ebob(n, r)$ yani $ebob(119{,}2) = 1$ dir. $O_{119}(2) = 24$ olarak bulunur.
Bulunan bu değer için en küçük r değeri hesaplanır. $O_r(n) > log_2(n)$ büyüklüğündeki en küçük sayı bulunana kadar işlem devam eder.
$r = 3$ için sayı 20 ve r = 5 için derece 25 olmaktadır.

r=4 değeri denenmemiştir çünkü yukarıda da belirtildiği üzere r asal sayı olmak zorundadır. Bir sonraki adımda r = 7 için hesaplama yapılacaktır. Ancak tam bu noktada sayının asal olmadığını söylenebilmektedir, çünkü obeb (119,7) = 7 olmaktadır.

Olası Asallık Testi. Olası asallık testleri, bir sayının yüksek olasılıkla asal olup olmadığını belirlemektedir. Olasılı asallık testi sayesinde, çok küçük bir hata payı ile bir sayının asal olup olmadığı anlaşılabilir. Bu testler ile $\mathbf{2^{-100}}$ den daha düşük bir hata payı ile, bir sayının asal olduğu belirlenebilir. En çok kullanılan olası asallık testlerinden bazıları ise; Fermat testi, Lehman testi, Solovay Strassen testi ve Miller Rabin testleridir (RSA Laboratories 2000).

Fermat Testi. Bu test için aşağıdaki teorem ile başlamak uygundur:

Teorem 3.2 $p, p \nmid a$ bir asal sayı ve a bir tam sayı olsun. Bu durumda $a^{p-1} \equiv 1(mod p)$ dir.

İspat. a sayısının, $a, 2a, 3a, \cdots, (p-1)a$ gibi ilk $(p-1)$ katından oluşan sayı takımını gözönüne alınırsa, bu sayılar $(mod\ p)$ ye göre birbirleri ile kongrüansı değildir, aksi halde $1 \leq r < s \leq p-1$ olmak üzere $ra \equiv sa(mod\ p)$ olsa $r \equiv s(mod\ p)$ bulunur ki, bu mümkün değildir. Ayrıca bu sayı takımındaki hiçbir sayı p tarafından bölünmez. Böylece $a, 2a, 3a, \cdots, (p-1)$ sayı takımı, belirli bir sırada alındığında, $(mod\ p)$ ye göre $1, 2, 3, \cdots, (p-1)$ sayı takımına kongrü olur, yani

$$a.2a.3a \cdots (p-1)a \equiv 1.2.3 \cdots (p-1)(mod\ p),$$

böylece

$$a^{p-1}(p-1)! \equiv (p-1)!\,(mod\ p),\ p \nmid (p-1)!$$

olduğundan

$$a^{p-1} \equiv 1(mod\ p)$$

elde edilir.

Sonuç 3.2.1 Eğer p bir asal sayı ise herhangi bir a sayısı için $a^p \equiv a(mod\ p)$ dir.

İspat. $p|a$ ise $a^p \equiv 0 \equiv a(mod\ p)$. Eğer $p \nmid a$ ise Fermat teoreminden $a^{p-1} \equiv 1(mod\ p)$ elde edilir. Bu kongrüansın her iki tarafı a ile çarpılırsa $a^p \equiv a(mod\ p)$ elde edilir. Bu teoremin karşıtı doğru değildir. Yani $n \nmid a$ ve $a^{n-1} \equiv 1(mod\ n)$ olması n nin asal olmasını gerektirmez (Yelkenkaya, 2014).

Örneğin, $3^{90} \equiv 1(mod\ 91)$ olduğu gösterilsin. $91 = 7.13$, $3^7 \equiv 3.(3^3)^2 \equiv 3(\ mod\ 13)$, $3^{13} \equiv 3.(3^6)^2 \equiv 3(mod\ 7)$ den$3^{91} \equiv 3(mod 91)$, $(3, 91) = 1$ ise $3^{90} \equiv 1(mod\ 91)$ bulunur. O halde Fermat teoreminin karşıtı doğru değildir.

Lehmann Testi. Herhangi bir p sayısının asal sayı olup olmadığını test etmek için rastgele $p > a$ olacak şekilde a sayısı seçilir. Daha sonra

$$b \equiv a^{\frac{(p-1)}{2}} (mod\ p)$$

Sayısı hesaplanır. Eğer burada çıkan sonuç 1 veya -1 değil ise p sayısı asal sayı değildir. Aksi halde $1\ veya\ -1$ sonucu çıkar ise p nin asal sayı olduğu kabul edilir (Yerlikaya ve Kara 2017). Bu test Lehmann Testi olarak bilinir. Aşağıdaki tabloda Legrende sembolü verilmiştir.

$\left(\frac{a}{p}\right)$	$+1$	$+1 \equiv a^{\frac{(p-1)}{2}} (mod\ p)$
	-1	$-1 \equiv a^{\frac{(p-1)}{2}} (mod\ p)$
	0	$a \equiv 0\ (mod\ p)$

Tablo 3.3 Legrende sembolü

Mesela, $a = 8$ ve $p = 13$ için legrende sembolü şöyle bulunur:

$\left(\frac{8}{13}\right) = 8^{\frac{(13-1)}{2}} (mod\ 13) \equiv 12 \equiv -1$ dir.

Miller Rabin Testi.

Miller-Rabin Asallık testi, Michael Rabin tarafından Gary Millerın düşüncelerinden yararlanarak geliştirilmiştir. Asallık testleri içinde en yaygın olan yöntemlerden biridir. Hata payı çok düşüktür (Arnault, 1995). Milller – Rabin testi, Fermatın küçük teoremine karekökü dahil ederek oluşturulmuştur (Rabin, 1980; Miller, 1976).

Miller Rabin testinde p sayısının asal olup olmadığını test etmek için ilk önce $p - 1 = 2^s r$ eşitliğini sağlayan $s\ ve\ r$ sayıları hesaplanır. $1 \leq a \leq p - 1$ aralığındaki a sayısı için

$$a^r = 1\ (mod\ p) \text{ veya } \ 0 \leq j \leq s - 1 \text{ aralığında}$$

$$a^{2jr} = 1\ (mod\ p)$$

eşitlikleri sağlanıyor ise, p sayısının a tabanına göre güçlü asal sayı olduğu kabul edilir (Crandall ve Pomerance 2005).

Örneğin,

$p = 341$ sayısının asal olup olmadığını miller-rabin testini uygulayarak bulalım.

$p - 1 = 340 = 2^2 85$

Buradan, $s = 2$ ve $r = 85$ olur. $1 \leq a \leq 340$ aralığında rastgele olan $a = 2$ sayısını seçelim. $2^{85} = 32\ (mod\ 341)$ kalan 1 veya -1 olmadığı için teste devam edilmelidir.

$(2^{85})^2 = 1\ (mod\ 341)$ dır.

Başka bir örneğe bakalım,

$p = 91$ sayısının asal olup olmadığını miller-rabin testini uygulayarak bulalım.

$p - 1 = 90 = 2^1 45$

Buradan, $s = 1$ ve $r = 45$ olur. $1 \leq a \leq 90$ aralığında rastgele olan $a = 10$ sayısını seçelim. $10^{45} = -1\ (mod\ 91)$ dır.

Slovay Strassen Testi.

Bu test, açık-anahtar kriptografisinde kullanılmış ilk testtir. Slovay-Strassen Algoritmasında p sayısının asal olup olmadığını bulmak için Jacobi Sembolü kullanılmaktadır. Burada, Jacobi Sembolü $J(a,p)$ ile gösterilmektedir. Jacobi sembolü, Legendre sembolünün bir genellemesidir. Yani, Jacobi Sembolü p asal ise Legendre Sembolüne eşit olmaktadır. Algoritmanın aşamaları aşağıdaki gibidir;

1. p den küçük rastgele bir a sayısı seçilir.
2. Eğer $ebob(p,a) \neq 1$ ise o zaman p testi geçemez ve asal olmadığı anlaşılır.
3. $j = a^{\frac{(p-1)}{2}}\ (mod\ p)$, Jacobi sembolü olan $J(a,p)$ hesaplanır.
4. Eğer j$\neq J\ (a,p)$ ise p testi geçemez ve kesin olarak asal değildir.
5. Eğer $j = J\ (a,p)$ ise p nin asal olmama olasılığı %50'den fazla olamaz.

Slovay Strassen testi yerine kendisinden daha hızlı ve en az onun kadar doğru olan Miller Rabin testinin kullanılması önerilmektedir (Yerlikaya ve Kara 2017).

Yeni Asal Sayı Bulma Metodu.

Günümüze kadar, asal sayı üretmek için bulunan ve ispatlanan bir formül henüz literatürde bulunmamaktadır. Deneme-yanılma yoluyla, matematiksel hesaplamalar ve algoritmalar kullanılarak asal sayı bulma işlemlerinin arayışı devam etmektedir. Biz bu çalışmamızda, daha önce yapılan çalışmalardan farklı olarak, bir eleme algoritması verdik. Bu yöntemi, önce izah edip sonra tablolar yardımıyla destekledik.

Tek tam sayılar kümesi üzerinde çalışılacağından ve bu kümenin her elemanının asal olma ihtimali bulunduğundan, bu sayılar kümesini *muhtemel asal sayılar kümesi* olarak adlandırdık ve bu kümeyi M_s harfi ile gösterdik. Tek tam sayılar kümesini, asal olma ihtimaline göre daha da daraltmak için, asal olabilecek sayıların son basamaklarını inceledik. Bu sayıların $1, 3, 7$ ve 9 rakamlarından biri ile bitmesi gerektiğini aşikardır. Fakat, her son basamağı bu rakamlardan biri ile biten sayıların asal olmadığını da belirtmek gerekir.

Bu yöntemde, diğer asal sayı testlerinden farklı olarak, olası asal sayıların sıra sayılarını tanımladık ve bunları kullandık. Şimdi kullandığımız ve literatürde bulunmayan bazı tanımları verelim.

Tanım 3.4 M_s sayılarından 1 çıkarıp 2 ye bölerek elde edilen sayılara, *muhtemel asal sayıların sıra sayısı denir* ve M_{ss} ile gösterilir. Örneğin,

$$M_{ss}(3) = 1,\ M_{ss}(5) = 2,\ M_{ss}(7) = 3, \dots$$

gibi. M_s dizisinde bulunan asal sayıları doğrudan bulmak mümkün değildir. Bundan dolayı, asal olmayan sayıları bulup, geriye kalan sayıların asal sayı olduğu gösterilecektir. Bu işlemler, muhtemel sayıların sıra sayıları kullanılarak yapılacaktır.

Tanım 3.4.1 (Asal Olmayan Sayıların Sıra Sayısı**)**
$b \in Z^{tek}\ ve\ s, a \in Z$ olmak üzere; s sayısı b sayısının sıra sayısı göstersin. Bu b sayısı yardımıyla

$$a = (s,\ s+1,\ s+2,\ s+3, \cdots) = (s+n); n \in \mathbb{N}$$

sayılarını tanımlayalım. Bu sayıları kullanarak aşağıda tanımlanan

$$M'_{ss} = s(1,1,1,\dots) + b(s, s+1, s+2, \cdots)$$

sayılarına, *asal olmayan sayıların sıra sayısı* denir.
Örneğin, $s \in Z^+$ olmak üzere, $b = 3,\ 5,\ 7,\ 9$ sayıları için, sırasıyla, yukarıdaki formül kullanılarak

$$(1,1,1,\cdots) + 3\ (1,\ 2,\ 3, \cdots) = (4,\ 7,\ 10, \cdots),$$

$$(2,\ 2,\ 2, \cdots) + 5\ (2,\ 3,\ 4, \cdots) = (12, 17, 22, \cdots),$$

$$(3,\ 3,\ 3, \cdots) + 7\ (3, 4, 5, \cdots) = (24, 31, 38, \cdots),$$

$$(4, 4, 4, \cdots) + 9\ (4, 5, 6, \cdots) = (40, 49, 58, \cdots), \dots$$

gibi sayı dizisi elde edilir.

Buradaki ilk $(4,\ 7,\ 10,\cdots)$ dizisi, sırasıyla, 3 ün tek katlarının sıra sayılarını, $(12, 17, 22,\cdots)$ dizisi, sırasıyla, 5 in tek katlarının sıra sayılarını, $(24, 31, 38,\cdots)$ dizisi ise, sırasıyla, 7 nin tek katlarının sıra sayılarını vermektedir. Bazı M'_{ss} sayılarını da aşağıdaki tabloda verdik:

M'_{ss}	4	7	10	13	16	19	22	25	28	31	3 ün katları olan sıra sayıları
s	1	1	1	1	1	1	1	1	1	1	
a	1	2	3	4	5	6	7	8	9	10	
M'_{ss}	12	17	22	27	32	37	42	47	52	57	5 in katları olan sıra sayıları
s	2	2	2	2	2	2	2	2	2	2	
a	2	3	4	5	6	7	8	9	10	11	
M'_{ss}	24	31	38	45	52	59	66	73	80	87	7 nin katları olan sıra sayıları
s	3	3	3	3	3	3	3	3	3	3	
a	3	4	5	6	7	8	9	10	11	12	
M'_{ss}	40	49	58	67	76	85	94	103	112	121	9 un katları olan sıra sayıları
s	4	4	4	4	4	4	4	4	4	4	
a	4	5	6	7	8	9	10	11	12	13	
M'_{ss}	60	71	82	93	104	115	126	137	148	159	11 in katları olan sıra sayıları
s	5	5	5	5	5	5	5	5	5	5	
a	5	6	7	8	9	10	11	12	13	14	
M'_{ss}	84	97	110	123	136	149	162	175	188	201	13 ün katları olan sıra sayıları
s	6	6	6	6	6	6	6	6	6	6	
a	6	7	8	9	10	11	12	13	14	15	
M'_{ss}	112	127	142	157	172	187	202	217	232	247	15 nin katları olan sıra sayıları
s	7	7	7	7	7	7	7	7	7	7	
a	7	8	9	10	11	12	13	14	15	16	
M'_{ss}	144	161	178	195	212	229	246	263	280	297	17 un katları olan sıra sayıları
s	8	8	8	8	8	8	8	8	8	8	
a	8	9	10	11	12	13	14	15	16	17	

Tablo 3.4.2 Asal olmayan sayıların sıra sayısı

Yukarıdaki tabloda M'_{ss} sayılarına bakarak verilen bir sayının asal sayı olup olmadığı hakkında bilgi verebiliriz. Çünkü, eğer bize verilen sayı bu tabloda yer alıyorsa asal sayı değildir. Örneğin, 299 sayısının asal olup olmadığını Tablo 3.4.2 yardımıyla inceleyelim. İlk önce Tanım 3.4 den faydalanarak, 299 sayısının sıra sayısı yazalım, $M'_{ss} = 149$ dur. 149 sayısı Tablo 3.4.2 de olduğu için 299 sayısı asal sayı değildir.

M'_{ss} sayılarından, yani asal olmayan sayıların sıra sayılarından yararlanarak, matris üzerinde de asal olmayan sayılar elde edilebilir. Eğer, $s \leq 8$ tamsayısı için, asal olmayan sayıların sıra numaraları, (M'_{ss}) değerleri matris üzerine yerleştirilirse, bu durumda aşağıdaki gibi bir formül elde edilir:

$a \,.\, b + s = M'_{ss}$ bu formül kullanılarak,

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 3 & 3 & 3 & 0 & 0 & 0 & 0 & 0 \\ 4 & 4 & 4 & 4 & 0 & 0 & 0 & 0 \\ 5 & 5 & 5 & 5 & 5 & 0 & 0 & 0 \\ 6 & 6 & 6 & 6 & 6 & 6 & 0 & 0 \\ 7 & 7 & 7 & 7 & 7 & 7 & 7 & 0 \\ 8 & 8 & 8 & 8 & 8 & 8 & 8 & 8 \end{bmatrix} \cdot \begin{bmatrix} 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 7 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 9 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 13 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 15 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 17 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 3 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 3 & 4 & 0 & 0 & 0 & 0 \\ 1 & 2 & 3 & 4 & 5 & 0 & 0 & 0 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 & 0 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 0 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{bmatrix}$$

$$M'_{ss} = \begin{bmatrix} 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 7 & 12 & 0 & 0 & 0 & 0 & 0 & 0 \\ 10 & 17 & 24 & 0 & 0 & 0 & 0 & 0 \\ 13 & 22 & 31 & 40 & 0 & 0 & 0 & 0 \\ 16 & 27 & 38 & 49 & 60 & 0 & 0 & 0 \\ 19 & 32 & 45 & 58 & 71 & 84 & 0 & 0 \\ 22 & 37 & 52 & 67 & 82 & 97 & 112 & 0 \\ 25 & 42 & 59 & 76 & 93 & 110 & 127 & 144 \end{bmatrix}$$

yazılabilir.

$a \,.\, b + s = M'_{ss}$ formülündeki b köşegen matrisi, tek tam sayılardan oluşmaktadır. a matrisi ise b matrisindeki sayıların sıra sayılarından elde edilmektedir. Bu M'_{ss} matrisi, Tablo 3.4.2 deki gibi bize asal olmayan sayıların sıra sayılarını vermektedir. Bu da Tablo 3.4.2 nin matris üzerindeki gösterimidir. Ayrıca, oluşan M'_{ss} matrisi alt üçgensel bir matristir ve M'_{ss} matrisinin asal köşegeni üzerinde bulunan sayılar, asal olmayan tek sayıların tam karelerinin sıra sayılarını vermektedir. Örneğin,

yukarıdaki M'_{ss} matrisinin asal köşegeninde bulunan; $4, 12, 24, 40, 60, 84, 112, 144$ asal olmayan sıra sayıları sırasıyla, $9, 25, 49, 81, 121, 169, 225, 289$ sayılarına denk gelmektedir.

Burada, M'_{ss} matrisi istenirse daha da genelleştirilebilir. M'_{ss} matrisinin genelleştirilmesi için aşağıda bazı formüller verilmiştir.

Sonsuz sayıda satır ve sütun sayısına sahip olan bir matris yardımıyla, asal olmayan sayıların sıra sayısının formülleri de aşağıdaki tanımlarda verilecektir.

Tanım 3.4.3 $k, n \in Z^+$, k: $satır\ sayısı$ olmak üzere,

$$M'^{satır}_{ss} = 2n(n+1) + (k-1)(2n+1), \quad k \geq 1$$

dir. Bu formülü, asal olmayan sayılar için, *matris satır formülü* olarak adlandıracağız. Şimdi bu formülü aşağıdaki bir örnek üzerinde inceleyelim.

1.satır formülü aşağıdaki gibi olur, yani $k = 1$ için

$$M'^{satır}_{ss} = 2n^2 + 2n$$

$k = 2$ için,

$$M'^{satır}_{ss} = 2n^2 + 2n + 1 + 1.(2n+1) = 2n^2 + 4n + 1$$

Bu şekilde devam ederek, $k = 3, 4, 5, \ldots$ satırları için istenen eşitlikler benzer şekilde yazılabilir. Bu işlemler, yine aşağıdaki gibi matris formunda da yazılabilir:

$$\begin{array}{c} \\ 2n^2+2n \\ 2n^2+4n+1 \\ 2n^2+6n+2 \\ \vdots \end{array} \begin{array}{c} \begin{array}{cccc} n=1 & n=2 & n=3 & \cdots \end{array} \\ \begin{bmatrix} 4 & 12 & 24 & \cdots \\ 7 & 17 & 31 & \cdots \\ 10 & 22 & 38 & \cdots \\ \vdots & \vdots & \vdots & \end{bmatrix} \end{array}$$

Burada verilen formül, $a\,.\,b + s = M'_{ss}$ formülün genişletilmiş halidir. Bu matrisin 1. Sütunu, 3 ün tek katlarının sıra sayısını, 2. Sütun, 5 in tek katlarının sıra sayısını, 3. Sütun ise 7 nin tek katlarının sıra sayını vermekte ve bu işlem böyle devam etmektedir.

Şimdi, genişletilmiş M'_{ss} matrisi için sütun formülünü aşağıda verelim. Matris satır formülünden bulunan ve asal olmayan sayıların sıra sayıları matris formunda yazılabildiği gibi, aynı işlemler sütun formülü olarak da düzenlenebilir:

Tanım 3.4.4 $b, a \in Z^+$, $b \geq 1$, b sütun sayısı olmak üzere,

$$M'^{sütun}_{ss} = (3a+1) + (b-1)(2a+1)$$

formülü, sütundaki sıra sayılarını veren formül olarak tanımlanabilir. Bu nedenle, bu yeni formül, asal olmayan sayılar için, *matris sütün formülü* olarak adlandırılır.

Şimdi bu formülü bazı değerler için inceleyelim: Formüle göre, 1. sütun formülü yani, $b = 1$ iken

$$M'^{sütun}_{ss} = (3a+1), \quad b = 1$$

olur. $b = 2$ iken, 2. sütun formülü aşağıdaki gibi olur:

$$M'^{sütun}_{ss} = (3a + 1) + 1(2a + 1) = (5a + 2).$$

Aynı düşünceyle devam edilerek, $b = 3, 4, 5$ ... satırları için de benzer eşitlikler yazılabilir. Bu eşitlikler, yine matris formunda aşağıdaki gibi yazılabilir:

$$\begin{matrix} & a=1, & a=2, & a=3, & \cdots \\ 3a+1 & 4 & 7 & 10 & \cdots \\ 5a+2 & 7 & 12 & 17 & \cdots \\ 7a+3 & 10 & 17 & 24 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \cdots \end{matrix}$$

Dikkat edilirse bu matris, köşegen ve simetrik bir matris özelliği taşımaktadır. Simetrik matris yardımıyla alt ve üst üçgensel matrisler de oluşturulabilir.

$$\begin{bmatrix} 4 & 0 & 0 & 0 \\ 7 & 12 & 0 & 0 \\ 10 & 17 & 24 & 0 \\ 13 & 22 & 31 & 40 \end{bmatrix} \text{ veya } \begin{bmatrix} 4 & 7 & 10 & 13 \\ 0 & 12 & 17 & 22 \\ 0 & 0 & 24 & 31 \\ 0 & 0 & 0 & 40 \end{bmatrix}$$

Şimdi ise asal sayıların sıra sayılarından oluşan bir matris oluşturacağız ve bu asal sayıların sıra sayılarından oluşan matrisi M_{ss} olarak göstereceğiz. Öncelikle, aşağıda bazı asal sayılar verilmiştir.

$$\{3, 5, 7, 11, 13, 17, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, \cdots\}$$

bu asal sayıların sıra sayıları ise,

$$M_{ss} = \{1, 2, 3, 5, 6, 8, 9, 11, 14, 15, 18, 20, 21, 23, 26, 28, 30, 33, \cdots\}$$

dir. Buradan, aşağıdaki x ve y matrislerinin elemanları tam sayılar olup, z matrisinin sütunları ise asal sayıların sıra sayılarından oluşmak üzere aşağıdaki formülü oluşturalım:

$$M_{ss} = xy + z$$

$$M_{ss} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{bmatrix} . \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 4 & 3 & 10 & 24 \\ 1 & 2 & 3 & 5 & 6 \\ 2 & 6 & 6 & 10 & 12 \\ 1 & 4 & 6 & 5 & 6 \end{bmatrix} + \begin{bmatrix} 1 & 2 & 3 & 5 & 6 \\ 1 & 2 & 3 & 5 & 6 \\ 1 & 2 & 3 & 5 & 6 \\ 1 & 2 & 3 & 5 & 6 \\ 1 & 2 & 3 & 5 & 6 \end{bmatrix}$$

$$M_{ss} = \begin{bmatrix} 1 & 2 & 3 & 5 & 6 \\ 2 & 6 & 6 & 15 & 30 \\ 3 & 8 & 9 & 20 & 36 \\ 5 & 14 & 15 & 30 & 48 \\ 6 & 18 & 21 & 35 & 54 \end{bmatrix}$$

dir. Oluşturulan M'_{ss} ve M_{ss} matrisleri, sırasıyla asal olmayan sayıların ve asal sayıların sıra sayılarının tablo gösterimleri haricinde, matrisler üzerinde birer uygulamalarıdır.

Tanım 3.4.5 Köşegen üzerindeki M'_{ss} sayılarını veren formül,

$$K_{ss} = M_{ss}(1 + M_s)$$

Dir. Burada K_{ss} asal olmayan sayıların karesinin sıra numarasıdır. Örneğin,

$M_s = 7$, $M_{ss} = 3$, $K_{ss} = 3(1 + 7) = 24,$ $M'_{ss}(24) = 49 = 7^2$

$M_s = 11,$ $M_{ss} = 5,$ $K_{ss} = 5(1 + 11) = 60,$ $M'_{ss}(60) = 121 = 11^2$

yazılabilir.

Tanım 3.4.6 $M_s = x$ olsun. O zaman, $M_{ss} = \frac{x-1}{2}$

olur ve $K_{ss} = \left(\frac{x-1}{2}\right)(1 + x) = \frac{x^2-1}{2}$ elde edilir. Buradan K_{ss} ile $M'^{sütun}_{ss}$ formüllerinin grafiğinde, satırda ve sütunda bulunan asal olmayan sayıları bulmak için elde edilen formülü geliştirilirse, aşağıdaki tanım verilebilir.

Tanım 3.4.7 $b \in \mathbb{Z}^{tek}$ ve $b > 2$ olsun.

Aşağıdaki formül yardımıyla, asal olmayan sayıların sıra sayıları bulunabilir.

$$\frac{b^2 - 1}{2}, \quad \frac{b^2 + 2b - 1}{2}, \quad \frac{b^2 + 4b - 1}{2}, \quad \frac{b^2 + 6b - 1}{2}, \cdots$$

Yukarıdaki formülde $b = 3$ yazılırsa, 3 ün katlarının sıra sayıları elde edilir: Yani,

$$4, 7, 10, 13, 16, 19, 22, 25, \cdots$$

Mesala, sıra sayısı 13 olan sayı 39 olup asal değildir.

5 in katlarının sıra sayıları: $12, 17, 22, 27,32,37,42, \cdots$ olur.

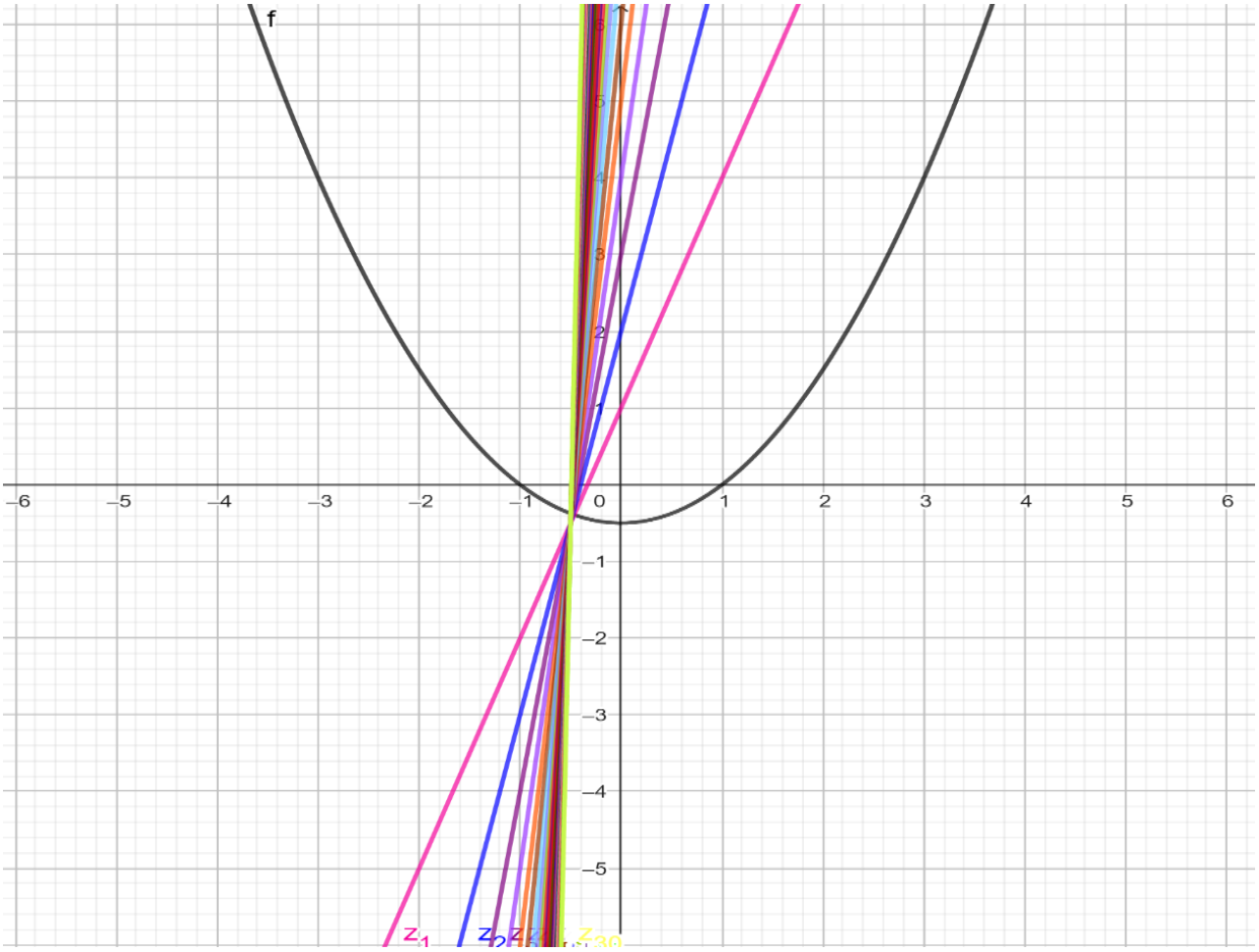
Diğer tek sayılar için aynı işlemler tekrarlanır.

b	$\frac{b^2-1}{2}$	$\frac{b^2+2b-1}{2}$	$\frac{b^2+4b-1}{2}$	$\frac{b^2+6b-1}{2}$	$\frac{b^2+8b-1}{2}$	$\frac{b^2+10b-1}{2}$
2	1,5	3,5	5,5	7,5	9,5	11,5
3	4	7	10	13	16	19
4	7,5	11,5	15,5	19,5	23,5	27,5
5	12	17	22	27	32	37
6	17,5	23,5	29,5	35,5	41,5	47,5
7	24	31	38	45	52	59
8	31,5	39,5	47,5	55,5	63,5	71,5
9	40	49	58	67	76	85
10	49,5	59,5	69,5	79,5	89,5	99,5
11	60	71	82	93	104	115
12	71,5	83,5	95,5	107,5	119,5	131,5
13	84	97	110	123	136	149

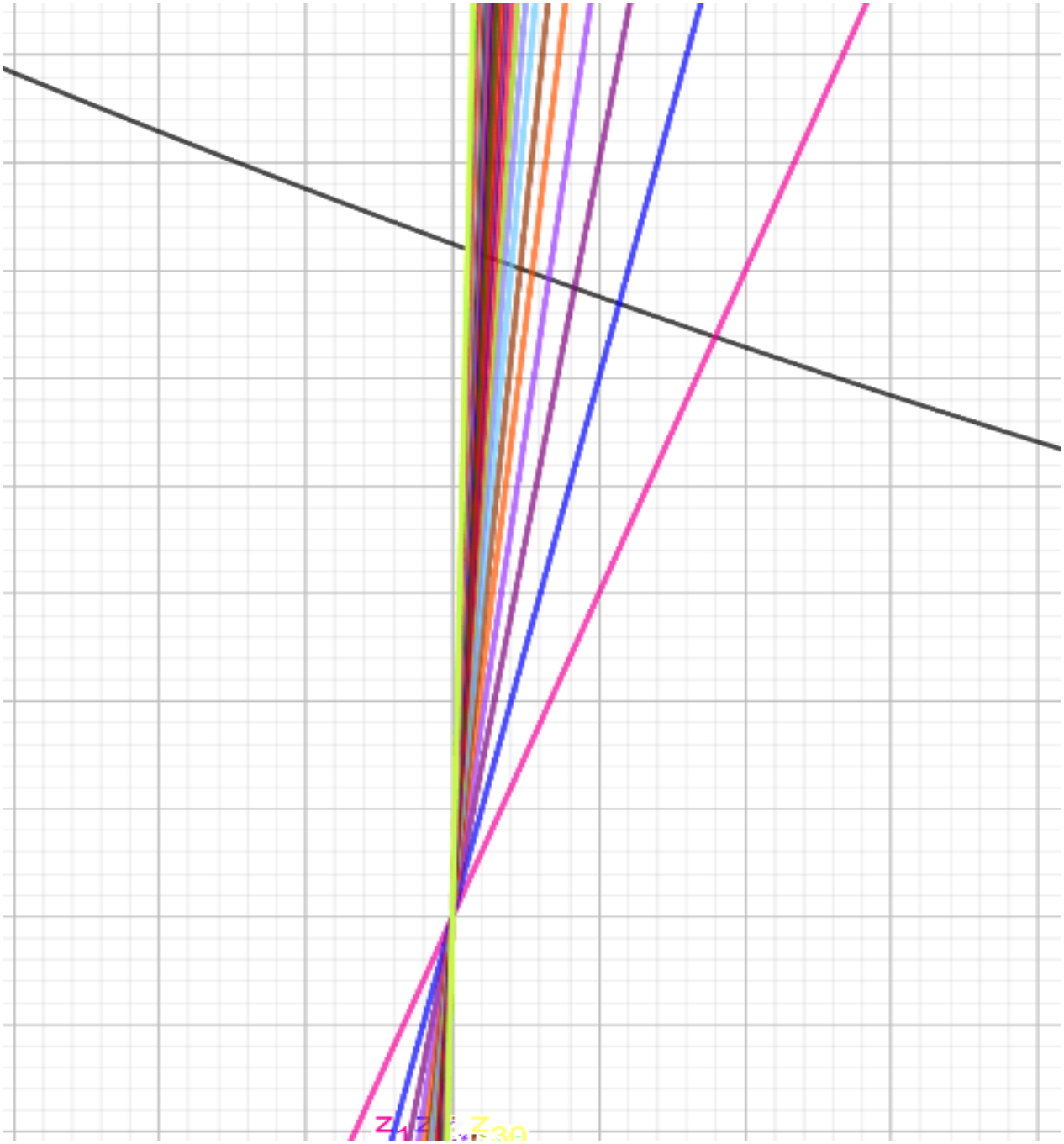
Tablo 3.4 İlk 13 sayısının sıra sayıları

Gözlem sonuçları:

1. Yukarıdaki tabloda hiçbir asal sayının sıra sayısına rastlanmamaktadır.
2. b yerine çift sayı değerleri verildiğinde, çift sayıların sıra sayısına denk geldiği görülmektedir.
3. b yerine tek sayı değerleri verildiğinde, sonucun asal olmayan tek sayılar olduğu görülmektedir.
4. b yerine tek sayılar verildiğinde, sırasıyla b yerine verilen sayının tek katları elde edilir.



Şekil 3.1 Asal olmayan sayıların sıra numarasıyla tam kare asal olmayan sayıların kesişim grafiği



Şekil 3.2 Asal olmayan sayıların sıra numaralarının doğrularının kesişim grafiği

Yukarıdaki her iki grafikte kullanılan fonksiyonlar, aşağıda verilmiştir.

	$f(x) = \frac{x^2}{2} - \frac{1}{2}$		$z_{13}(x) = 27x + 13$		$z_{25}(x) = 51x + 25$
	$z_1(x) = 3x + 1$		$z_{14}(x) = 29x + 14$		$z_{26}(x) = 53x + 26$
	$z_2(x) = 5x + 2$		$z_{15}(x) = 31x + 15$		$z_{27}(x) = 55x + 27$
	$z_3(x) = 7x + 3$		$z_{16}(x) = 33x + 16$		$z_{28}(x) = 57x + 28$
	$z_4(x) = 9x + 4$		$z_{17}(x) = 35x + 17$		$z_{29}(x) = 59x + 29$
	$z_5(x) = 11x + 5$		$z_{18}(x) = 37x + 18$		$z_{30}(x) = 61x + 30$
	$z_6(x) = 13x + 6$		$z_{19}(x) = 39x + 19$		
	$z_7(x) = 15x + 7$		$z_{20}(x) = 41x + 20$		
	$z_8(x) = 17x + 8$		$z_{21}(x) = 43x + 21$		
	$z_9(x) = 19x + 9$		$z_{22}(x) = 45x + 22$		
	$z_{10}(x) = 21x + 10$		$z_{23}(x) = 47x + 23$		
	$z_{11}(x) = 23x + 11$		$z_{24}(x) = 49x + 24$		

Tablo 3.5. Şekil 3.1 ve 3.2 grafiklerini veren formüller

Aşağıda, asal olmayan sayıların sıra numaraları verilmiştir. Bu sayılar bizim asal sayıları bulmamız için Çaçur elek şablonumuz olacaktır. Bu Çaçur elek şablonunu oluştururken, Tanım 3.4.7 sıra sayısı formülümüzden yararlanılmıştır.

														480
													420	449
												364	391	418
											312	337	362	387
										264	287	310	333	356
									220	241	262	283	304	325
								180	199	218	237	256	275	294
							144	161	178	195	212	229	246	263
						112	127	142	157	172	187	202	217	232
					84	97	110	123	136	149	162	175	188	201
				60	71	82	93	104	115	126	137	148	159	170
			40	49	58	67	76	85	94	103	112	121	130	139
		24	31	38	45	52	59	66	73	80	87	94	101	108
	12	17	22	27	32	37	42	47	52	57	62	67	72	77
4	7	10	13	16	19	22	25	28	31	34	37	40	43	46
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

									1300
								1200	1249
							1104	1151	1198
						1012	1057	1102	1147
					924	967	1010	1053	1096
				840	881	922	963	1004	1045
			760	799	838	877	916	955	994
		684	721	758	795	832	869	906	943
	612	647	682	717	752	787	822	857	892
544	577	610	643	676	709	742	775	808	841
511	542	573	604	635	666	697	728	759	790
478	507	536	565	594	623	652	681	710	739
445	472	499	526	553	580	607	634	661	688
412	437	462	487	512	537	562	587	612	637
379	402	425	448	471	494	517	540	563	586
346	367	388	409	430	451	472	493	514	535
313	332	351	370	389	408	427	446	465	484
280	297	314	331	348	365	382	399	416	433
247	262	277	292	307	322	337	352	367	382
214	227	240	253	266	279	292	305	318	331
181	192	203	214	225	236	247	258	269	280
148	157	166	175	184	193	202	211	220	229
115	122	129	136	143	150	157	164	171	178
82	87	92	97	102	107	112	117	122	127
49	52	55	58	61	64	67	70	73	76
16	17	18	19	20	21	22	23	24	25

												2964
											2812	2887
										2664	2737	2810
									2520	2591	2662	2733
								2380	2449	2518	2587	2656
							2244	2311	2378	2445	2512	2579
						2112	2177	2242	2307	2372	2437	2502
					1984	2047	2110	2173	2236	2299	2362	2425
				1860	1921	1982	2043	2104	2165	2226	2287	2348
			1740	1799	1858	1917	1976	2035	2094	2153	2212	2271
		1624	1681	1738	1795	1852	1909	1966	2023	2080	2137	2194
	1512	1567	1622	1677	1732	1787	1842	1897	1952	2007	2062	2117
1404	1457	1510	1563	1616	1669	1722	1775	1828	1881	1934	1987	2040
1351	1402	1453	1504	1555	1606	1657	1708	1759	1810	1861	1912	1963
1298	1347	1396	1445	1494	1543	1592	1641	1690	1739	1788	1837	1886
1245	1292	1339	1386	1433	1480	1527	1574	1621	1668	1715	1762	1809
1192	1237	1282	1327	1372	1417	1462	1507	1552	1597	1642	1687	1732
1139	1182	1225	1268	1311	1354	1397	1440	1483	1526	1569	1612	1655
1086	1127	1168	1209	1250	1291	1332	1373	1414	1455	1496	1537	1578
1033	1072	1111	1150	1189	1228	1267	1306	1345	1384	1423	1462	1501
980	1017	1054	1091	1128	1165	1202	1239	1276	1313	1350	1387	1424
927	962	997	1032	1067	1102	1137	1172	1207	1242	1277	1312	1347
874	907	940	973	1006	1039	1072	1105	1138	1171	1204	1237	1270
821	852	883	914	945	976	1007	1038	1069	1100	1131	1162	1193
768	797	826	855	884	913	942	971	1000	1029	1058	1087	1116
715	742	769	796	823	850	877	904	931	958	985	1012	1039
662	687	712	737	762	787	812	837	862	887	912	937	962
609	632	655	678	701	724	747	770	793	816	839	862	885
556	577	598	619	640	661	682	703	724	745	766	787	808
503	522	541	560	579	598	617	636	655	674	693	712	731
450	467	484	501	518	535	552	569	586	603	620	637	654
397	412	427	442	457	472	487	502	517	532	547	562	577
344	357	370	383	396	409	422	435	448	461	474	487	500
291	302	313	324	335	346	357	368	379	390	401	412	423
238	247	256	265	274	283	292	301	310	319	328	337	346
185	192	199	206	213	220	227	234	241	248	255	262	269
132	137	142	147	152	157	162	167	172	177	182	187	192
79	82	85	88	91	94	97	100	103	106	109	112	115
26	27	28	29	30	31	32	33	34	35	36	37	38

											5100
										4900	4999
									4704	4801	4898
								4512	4607	4702	4797
							4324	4417	4510	4603	4696
						4140	4231	4322	4413	4504	4595
					3960	4049	4138	4227	4316	4405	4494
				3784	3871	3958	4045	4132	4219	4306	4393
			3612	3697	3782	3867	3952	4037	4122	4207	4292
		3444	3527	3610	3693	3776	3859	3942	4025	4108	4191
	3280	3361	3442	3523	3604	3685	3766	3847	3928	4009	4090
3120	3199	3278	3357	3436	3515	3594	3673	3752	3831	3910	3989
3041	3118	3195	3272	3349	3426	3503	3580	3657	3734	3811	3888
2962	3037	3112	3187	3262	3337	3412	3487	3562	3637	3712	3787
2883	2956	3029	3102	3175	3248	3321	3394	3467	3540	3613	3686
2804	2875	2946	3017	3088	3159	3230	3301	3372	3443	3514	3585
2725	2794	2863	2932	3001	3070	3139	3208	3277	3346	3415	3484
2646	2713	2780	2847	2914	2981	3048	3115	3182	3249	3316	3383
2567	2632	2697	2762	2827	2892	2957	3022	3087	3152	3217	3282
2488	2551	2614	2677	2740	2803	2866	2929	2992	3055	3118	3181
2409	2470	2531	2592	2653	2714	2775	2836	2897	2958	3019	3080
2330	2389	2448	2507	2566	2625	2684	2743	2802	2861	2920	2979
2251	2308	2365	2422	2479	2536	2593	2650	2707	2764	2821	2878
2172	2227	2282	2337	2392	2447	2502	2557	2612	2667	2722	2777
2093	2146	2199	2252	2305	2358	2411	2464	2517	2570	2623	2676
2014	2065	2116	2167	2218	2269	2320	2371	2422	2473	2524	2575
1935	1984	2033	2082	2131	2180	2229	2278	2327	2376	2425	2474
1856	1903	1950	1997	2044	2091	2138	2185	2232	2279	2326	2373
1777	1822	1867	1912	1957	2002	2047	2092	2137	2182	2227	2272
1698	1741	1784	1827	1870	1913	1956	1999	2042	2085	2128	2171
1619	1660	1701	1742	1783	1824	1865	1906	1947	1988	2029	2070
1540	1579	1618	1657	1696	1735	1774	1813	1852	1891	1930	1969
1461	1498	1535	1572	1609	1646	1683	1720	1757	1794	1831	1868
1382	1417	1452	1487	1522	1557	1592	1627	1662	1697	1732	1767
1303	1336	1369	1402	1435	1468	1501	1534	1567	1600	1633	1666
1224	1255	1286	1317	1348	1379	1410	1441	1472	1503	1534	1565
1145	1174	1203	1232	1261	1290	1319	1348	1377	1406	1435	1464
1066	1093	1120	1147	1174	1201	1228	1255	1282	1309	1336	1363
987	1012	1037	1062	1087	1112	1137	1162	1187	1212	1237	1262
908	931	954	977	1000	1023	1046	1069	1092	1115	1138	1161
829	850	871	892	913	934	955	976	997	1018	1039	1060
750	769	788	807	826	845	864	883	902	921	940	959
671	688	705	722	739	756	773	790	807	824	841	858
592	607	622	637	652	667	682	697	712	727	742	757
513	526	539	552	565	578	591	604	617	630	643	656
434	445	456	467	478	489	500	511	522	533	544	555
355	364	373	382	391	400	409	418	427	436	445	454
276	283	290	297	304	311	318	325	332	339	346	353
197	202	207	212	217	222	227	232	237	242	247	252
118	121	124	127	130	133	136	139	142	145	148	151
39	40	41	42	43	44	45	46	47	48	49	50

Yukarıdaki Çaçur elek şablonunu kullanarak ilk 300'e kadar olan tek sayılar içindeki asal sayıları bulalım. Bu elek şablonunu oluştururken, Tanım 3.4.7 sıra sayısı formülümüzden yararlanılmıştır.

İlk önce tek sayılar tablosu oluşturalım. Bu tablodaki tek sayılar 3 ten başlayacaktır.

3	5	7	9	11	13	15	17	19	21
23	25	27	29	31	33	35	37	39	41
43	45	47	49	51	53	55	57	59	61
63	65	67	69	71	73	75	77	79	81
83	85	87	89	91	93	95	97	99	101
103	105	107	109	111	113	115	117	119	121
123	125	127	129	131	133	135	137	139	141
143	145	147	149	151	153	155	157	159	161
163	165	167	169	171	173	175	177	179	181
183	185	187	189	191	193	195	197	199	201
203	205	207	209	211	213	215	217	219	221
223	225	227	229	231	233	235	237	239	241
243	245	247	249	251	253	255	257	259	261
263	265	267	269	271	273	275	277	279	281
283	285	287	289	291	293	295	297	299	301

Tablo 3.6 Tek sayılar

Yazdığımız asal sayıların, tanım 3.4 de verilen yöntem ile sıra sayılarını bulup aşağıda tabloda verelim.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150

Tablo 3.7 Tek sayıların sıra sayısı

Son olarak sıra sayılarını bulduğumuz tek sayılar üzerinde, kendi oluşturduğumuz eleğimizi uygulayarak geriye kalan sayılar asal sayıların sıra sayılarını vermektedir.

1	2	3		5	6		8	9	
11			14	15			18	19	20
21		23			26			29	30
		33		35	36			39	
41			44				48		50
51		53	54	55	56				
		63		65			68	69	
			74	75			78		
81		83			86			89	90
91			94	95	96		98	99	
				105	106		108	109	
111		113	114		116			119	120
				125			128		
131			134	135			138		140
141					146				

Tablo 3.8 Asal sayıların sıra sayısı

Bu tabloda asal sayıların sıra sayıları kalmıştır. Böylece kendi oluşturduğumuz Çaçur eleğimizi uygulamış olduk. Oluşturduğumuz eleğin avantajı, incelediğimiz sayı kümesini küçültmesidir. Yani, tablo 3.4.12 deki ilk 300 tek sayıyı incelemek yerine bizim sıra sayısı yöntemi ile oluşturduğumuz tablo 3.4.13 daki sayıları incelemek daha kolay olacaktır.

Tanım 3.4.15 $k > 0$ ve $k \in \mathbb{Z}^+$ için $\frac{k-1}{2}$ formülü uygulandığında, k nın alt sıra sayısı elde edilir. Örneğin, 17 sayısının alt sıra sayısı 8 dir.

$k > 0$ ve $k \in \mathbb{Z}^+$ için $\frac{k+1}{2}$ formülü uygulandığında, k nın üst sıra sayısı elde edilir.

Örneğin, 21 sayısının üst sıra sayısı 11 dir.

Tanım 3.4.16 p asal sayı olsun. Öyle ki p nin alt sıra sayısı ve üst sıra sayısı da asal sayı ise p sayısına mükemmel güveli asal sayı denir. Örneğin, $p = 5$ asal sayısının altı sıra sayısı 2, üst sıra sayısı 7 dir. Yani, $p = 5$ sayısının, alt sıra sayısı ile üst sıra sayısı asal olduğundan dolayı p mükemmel güvenli asal sayıdır. Bazı mükemmel güvenli asal sayılar şöyledir: $5, 11, 23, 83, 179, 359, 719, \ldots$

Aşağıdaki tabloda, beyaz renkli bölgede, ardışık tek sayılar verilmiştir. Bu beyaz bölümde bulunan tek sayıların üzerine, üst sıra sayıları yazılmıştır. Daha sonraki bir üst sıraya, altında yazan sayının üst sıra sayısı yazılacaktır. Ayrıca, beyaz kısımdaki sayıların alt bölümüne ise bu

sayıların alt sıra sayısı yazılmaktadır. Eğer, alt sıra sayısını yazarken sonuç çift sayı çıkar ise devam edilmemektedir. Çünkü işlemlerimizi tek sayılar üzerinden yapacağız. Kırmızı ile belirtilen sayılar asal sayılardır. Arka arkaya gelen 3 asal sayıların ortasındaki asal sayı, mükemmel güvenli asal sayıları oluşturmaktadır. Mükemmel güvenli asal sayıyı yeşil ile belirttik.

255	383	511	639	767	895	1023	1151	1279	1407	1535	1663	1791
127	191	255	319	383	447	511	575	639	703	767	831	895
63	95	127	159	191	223	255	287	319	351	383	415	447
31	47	63	79	95	111	127	143	159	175	191	207	223
15	23	31	39	47	55	63	71	79	87	95	103	111
7	11	15	19	23	27	31	35	39	43	47	51	55
3	5	7	9	11	13	15	17	19	21	23	25	27
1	2	3	4	5	6	7	8	9	10	11	12	13
		1		2		3		4		5		6
						1				2		

Tablo 3.9 Mükemmel güvenli asal sayılar.

1919	2047	2175	2303	2431	2559	2687	2815	2943	3071	3199	3327	3479	3583
959	1023	1087	1151	1215	1279	1343	1407	1471	1535	1599	1663	1739	1791
479	511	543	575	607	639	671	703	735	767	799	831	869	895
239	255	271	287	303	319	335	351	367	383	399	415	431	447
119	127	135	143	151	159	167	175	183	191	199	207	215	223
59	63	67	71	75	79	83	87	91	95	99	103	107	111
29	31	33	35	37	39	41	43	45	47	49	51	53	55
14	15	16	17	18	19	20	21	22	23	24	25	26	27
	7		8		9		10		11		12		13
	3				4				5				6
	1								2				

Tablo 3.10 Mükemmel güvenli asal sayılar.

Asal sayılar düzensiz ilerlediğinden dolayı, mükemmel güvenli asal sayılar da hızlı bir şekilde artış göstermektedir. Çünkü her asal sayı mükemmel güvenli bir sayı değildir. Buradan Mükemmel güvenli asal sayılara ulaşmanın kolay olmadığını söyleyebiliriz. İlerleyen bölümlerde mükemmel güvenli asal sayıların bu özelliğinden yararlanarak, mesajları şifrelemede

kullanacağız. RSA algoritmasında modüler matematik kullanılır. Aşağıda RSA algoritması ana hatlarıyla verdik.

4.BÖLÜM

ASAL SAYILAR İLE ŞİFRELEME

Asal sayılar, bir uygulamanın ne kadar önemli olduğunu ortaya koyan önemli bilgileri güvende tutmak için kullanılır**.** Yeni bir asal sayının bulunma işlemi, kriptografi için büyük bir sürpriz olmasa da matematikçiler asal sayıların daha düşük maliyet ve daha kısa zamanda hesaplanması için yeni yöntemler aramaktadırlar. Çok fazla cebirsel işlem gerektiren asal sayıların hesabı, incelenen sayılar büyüdükçe zorlaşır. Günümüzde, asal sayılar, genelde kişisel bilgilerin korunabilmesi amacıyla şifreleme teknolojilerinde, bankaların kredi kartlarında, fizikçiler için kuantum kaos teorisinde ve haberleşme sistemleri gibi alanlarda kullanılır.

Kriptoloji, haberleşen iki grubun veya daha fazla grubun veri alış-verişini güvenli bir şekilde yapılmasını sağlayan ve bu bilgi alışverişinde matematiksel problemleri ve uygulamaları kullanan bir bilim dalıdır. Kriptoloji, matematiğin hem şifre bilimini hem de şifre analizini (kriptonaliz) kapsayan dalıdır. Şifre bilimi literatürde Kriptografi olarak bilinirken, şifre analizi ise Kriptoanaliz olarak bilinir. İyi bilindiği gibi, Kriptografi kelimesi, Yunanca crypto (gizli) ve grapy (yazmak) kelimelerinden türemiş olup, çeşitli yöntemler ile verilerin şifrelenerek güvenliliğini ve gizliliğini sağlamayı amaçlayan Kriptolojinin bir dalıdır.

Şifrelemenin 1940–1944 yılları arasında II. Dünya Savaşı sırasında kullanıldığı bilinmektedir. Şifre çözümünde amaç, kullanılan şifrenin özelliklerinden ve şifrelenen metin ile ilgili bilgilerden yararlanarak, olası anahtarların denenmesinden kurtulmaktır. Almanların ikinci dünya savaşı sırasında kullandıkları şifreleme cihazı Enigma adlı cihazdır. Bu savaş sırasında, bilgisayar bilimci olan İngiliz A. Turing, Enigma şifresinin yapısal zayıflıklarını kullanarak, nazilerin iletişimlerini çözmeyi başarmıştır. Kriptografide her kullanıcının şifreleme ve deşifreleme yapmak için, bir açık bir de gizli olmak üzere iki anahtarı vardır. Şifrelemek ve şifre çözmek için iki tip şifreleme yöntemi vardır: gizli anahtarlı yöntem ve açık anahtarlı yöntem. Gizli anahtarlı şifrelemede, hem şifrelemek hem de şifre çözmek için aynı anahtar kullanılır. Günümüzde en çok kullanılan gizli anahtarlı şifre sistemi DES yani Data Encryption Standard sistemi olarak bilinir.

Açık anahtar herkese açıktır ve isteyen herkes görebilir. Gizli anahtar ise saklı tutulur, sahibinden başka herhangi biri tarafından bilinemez. Şifreleme açık anahtar ile yapılırken şifre

çözümü ise gizli anahtarla yapılır. Bu şifreleme anahtarları ikili biçimde kullanılır ve birinin şifrelediği bilgiyi diğeri çözer. Günümüzde en çok bilinen ve kullanılan açık anahtarlı şifreleme yöntemi, RSA şifrelemedir. Bu sistemin adı, 1978 yılında Ron Rivest, Adi Shamir ve Leonard Adlemen bilim insanlarının tamsayıları çarpanlarına ayırma çalışmaları sonrasında verilmiştir. Açık anahtar algoritmalarının hepsi, büyük olan sayılarla yapılan bazı işlemlerin bir taraftan kolay olurken diğer taraftan ise zor olmasını kullanır. Mesela, RSA şifreleme yöntemi bundan faydalanır. Bu nedenle, bilim insanları tamsayıların asal çarpanlarını bulmak ile hala uğraşmaktadırlar. RSA algoritmasında modüler matematik kullanılır. Aşağıda RSA algoritması ana hatlarıyla verildi.

Tablo 4.1 şifreleme ve şifre çözme algoritması

Açık Anahtar Oluşturma Algoritması: Her A kişisi açık anahtarını şu şekilde oluşturur:

• iki tane farklı, rasgele ve basamak sayısı aynı olan p ve q asal sayılarını seçer.

• $n = p.q$ ve $\varphi = (p-1).(q-1)$ değerlerini hesaplar.

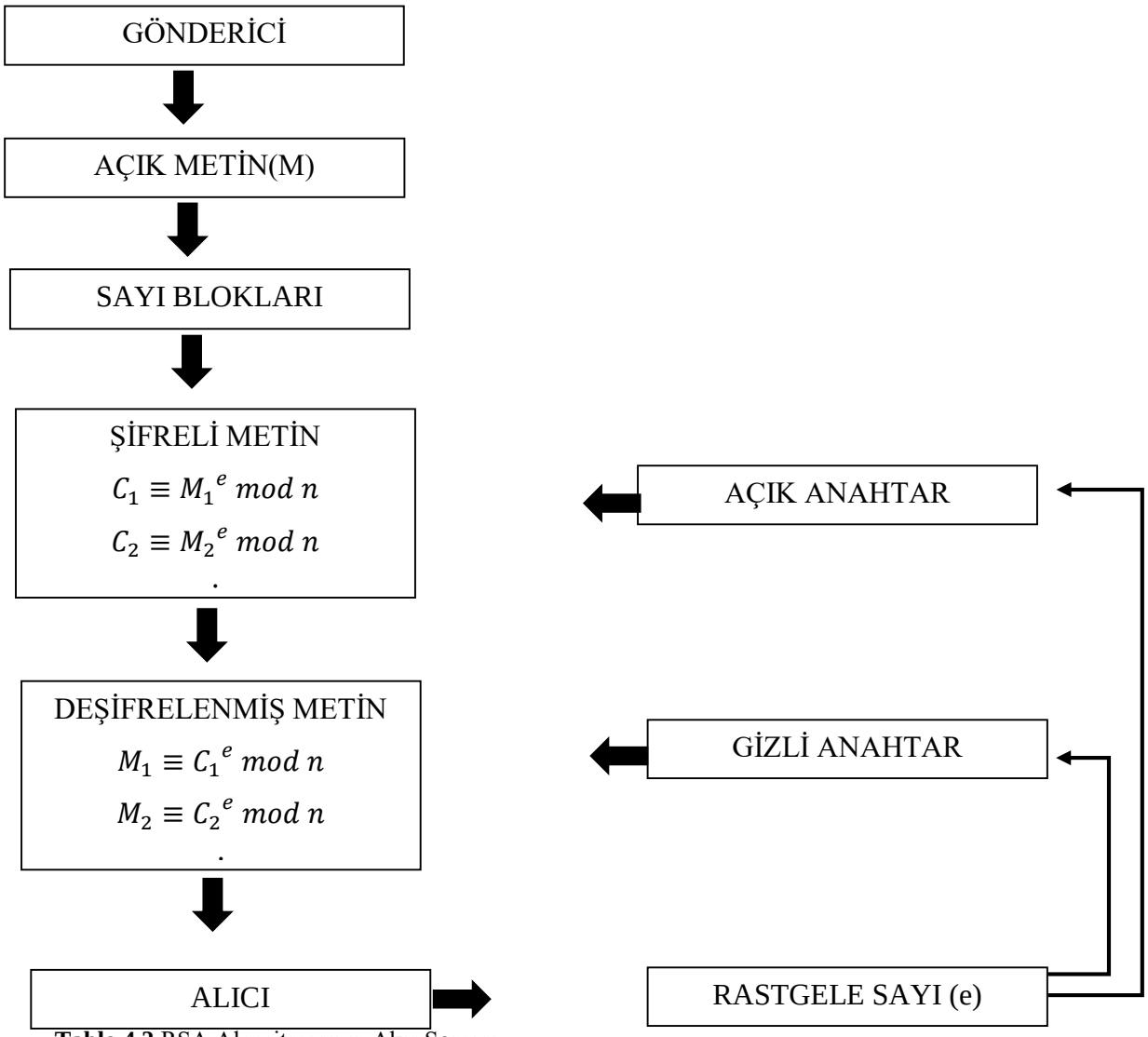
• $1 < c < \varphi$ ve $(c, \varphi(n)) = 1$ olacak şekilde rastgele bir c sayısını seçer.

• Öklid algoritmasını kullanarak, $1 < d < \varphi(n)$ ve $c.d \equiv 1(mod\varphi(n))$ şartını sağlayan d sayısını hesaplar.

• A kişisinin açık anahtarı (n, c) olup gizli anahtarı ise d olur.

Şifreleme genel olarak aşağıdaki ana hatlar ile verilebilir:

- Açık anahtar olan (n, c) çifti, bilgiyi gönderecek kişi tarafından bilinir.
- Açık metin, $M \in [0, n-1]$ aralığında olacak şekilde bir tamsayı dönüştürülür.
- Şifreli metin $C \equiv M^c \ mod \ n$ şeklinde hesaplanır.
- Bilgiyi gönderecek olan kişi, C şifreli metnini bilgiyi alacak kişiye gönderir (Beşkirli ve diğ. 2019).



Tablo 4.2 RSA Algoritmasının Akış Şeması

Şifreleme Algoritması

B şahsı, A ya bir m mesajı göndermek istiyorsa, B kişisi, m mesajını şifrelemek için aşağıdaki işlemleri yapar:

• Öncelikle A nın açık anahtarını (n, e) öğrenir.

• m mesajını, $[0, n-1]$ aralığında yazar.

• Sonra $C \equiv m^c \ (mod\ n)$ değerini hesaplar.

• Oluşan C şifresini A kişisine gönderir.

Şifreli C metninden açık metni bulabilmek için, A kişisi aşağıdaki işlemi uygular:

• d gizli anahtarını kullanarak ve $m \equiv c.d(mod\ n)$ işlemini uygulayarak m açık metine ulaşır (Zuckerman ve diğ. 1991).

Örneğin, $p = 11$, $q = 17$ asal sayıları seçilsin.

$n = 11.17 = 187$ ve $\varphi(n) = (11-1).(17-1) = 160$ olur.

$1 < c < \varphi(n)$ için $c = 3$ seçilsin.

$d.c \equiv 1(mod\varphi(n))$ şartını sağlayan $d = 107\ alınsın. O\ zaman,$

$d.c = 321 \equiv 1(mod\varphi(n))$ olur.

Tanım 4.1.2 p asal sayı olsun. Öyle ki p'nin kendinden bir önceki sıra sayısı ve bir sonraki sıra sayısı da asal sayı ise p sayısına mükemmel güveli asal sayı denir. Mesela, $p = 5$ asal sayısından bir önceki 2 sayısı ve bir sonraki 7 sayısı da asal sayı olduğu için p mükemmel güvenli asal sayıdır. Bazı mükemmel güvenli asal sayılar şöyledir: $5, 11, 23, 83, 179, 359, 719, \ldots$

Mükemmel Güvenli Asal Sayılar için RSA Yöntemi.

Şimdi, bu kesimde RSA güvenlik algoritmasının mükemmel güvenli asal sayılar için bir uygulaması verilecektir.

Örneğin, p ile q ardışık iki mükemmel güvenli asal sayı olsun: $p = 11$, $q = 23$.

$$n = (2p+1).(2q+1) = 23x47 = 1081$$

$$\varphi(n) = \left(\frac{p-1}{2}\right).\left(\frac{q-1}{2}\right) = 5 \times 11 = 55.$$

Rastgele bir e sayısını seçelim.

$1 < e < n$ ve $(e, \varphi(n)) = 1$ olmak üzere, $e = 19$ olsun.

$d.e \equiv 1(mod\varphi(n))$ şartını sağlayan bir sayı $d = 29$ alınabilir.

$d.e = 551 \equiv 1(mod\varphi(n))$ olduğundan açık anahtar $\{n, e\} = \{1081,19\}$ olur.

Kapalı anahtar ise $\{n, d\} = \{1081,29\}$ bulunur.

Örneğin, $p = 5$, $q = 11$ ardışık mükemmel güvenli asal sayı seçilsin.

1. $n = (2p + 1).(2q + 1) = 11.23 = 253$
2. $\varphi(n) = 10$
3. Rastgele bir e sayısını seçelim. $1 < e < n$ ve $\big(e, \varphi(n)\big) = 1$ ile arasında asal olsun.
4. $e = 3$ kabul edelim.
5. $d.e \equiv 1\big(mod\varphi(n)\big) \qquad d = 7 \qquad d.e = 21 \equiv 1\big(mod\varphi(n)\big)$
6. Açık anahtar $\{n, e\} = \{253,3\}$ dır.
7. Kapalı anahtar $\{n, e\} = \{253,7\}$ dır.

Göndermek istenilen metin, ŞİFRE olsun. Harflere sırasıyla numaralandırma yapılırsa,

$Ş = 1, İ = 2, F = 3, R = 4, E = 5$ olur. Mesaj gönderilecek kişiye ve mesajı okuyan herhangi birine, yukarıda hesaplanan n ve rastgele seçilen e sayıları verilir.

Ş$İFRE = 12345$ için $e = 3\ ve\ \ (mod\ 10)$ göre hesaplama yapılır.

$$1^3 \equiv 1\ (mod\ 10)$$
$$2^3 \equiv 8\ (mod\ 10)$$
$$3^3 \equiv 7\ (mod\ 10)$$
$$4^3 \equiv 4\ (mod\ 10)$$
$$5^3 \equiv 5\ (mod\ 10)$$

Yani gönderilmesi gereken şifre 18745 olacaktır. Bu sayıyı kodlarımızı kullanarak ŞİFRE metini haline dönüştürerek deşifreleme tamamlanmıştır.

Örneğin**,** $[0, \varphi(n) - 1]$ tamsayı değerleri arasında harfler rakamlarla eşleştirilir.

A	**İ**	**K**	**M**	**N**	**O**	**R**	**Ş**	**U**	**Y**
0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**

Tablo 4.3 bazı harflerin şifreleme tablosu

Yukarıda numaralandırdığımız harflerle bir mesaj göndermek için ilk önce mesajımızı şifreleyelim. Mesajı şifrelemek için $\varphi(n) = 10$ ve $e = 3$ buluruz.

MESAJ	**M**	**İ**	**R**	**A**	**Y**	**K**	**O**	**N**	**U**	**Ş**	**U**	**Y**	**O**	**R**
Sayi Değeri	3	1	6	0	9	2	5	4	8	7	8	9	5	6
E nin Kuvveti	3^3	1^3	6^3	0^3	9^3	2^3	5^3	4^3	8^3	7^3	8^3	9^3	5^3	6^3
Değer	27	1	216	0	729	8	125	64	512	343	512	729	125	216
$\varphi(n)$ Bölümünden Kalan	7	1	6	0	9	8	5	4	2	3	2	9	5	6
ŞİFRELİ MESAJ	**Ş**	**İ**	**R**	**A**	**Y**	**U**	**O**	**N**	**K**	**M**	**K**	**Y**	**O**	**R**

Tablo 4.4 mesaj şifreleme tablosu

Şifreli mesajımızı alan kişi, bu mesajı anlaşılır bir metine dönüştürmek için aşağıdaki işlemler yapılır.

ŞİFRELİ MESAJ	**Ş**	**İ**	**R**	**A**	**Y**	**U**	**O**	**N**	**K**	**M**	**K**	**Y**	**O**	**R**
D nin Kuvveti	7^7	1^7	6^7	0^7	9^7	8^7	5^7	4^7	2^7	3^7	2^7	9^7	5^7	6^7
$\varphi(n)$ Bölümünden Kalan	3	1	6	0	9	2	5	4	8	7	8	9	5	6
MESAJ	**M**	**İ**	**R**	**A**	**Y**	**K**	**O**	**N**	**U**	**Ş**	**U**	**Y**	**O**	**R**

Tablo 4.5 şifrelenen mesajı çözümleme tablosu

Şifreli mesajı açabilmemiz için gizli anahtar olan $d = 7$ yi bilmemiz gerekir.

Rabin Şifreleme Algoritması. 1979 yılında Michael Rabin tarafından bulunan bir kriptosistemdir. Bu kriptosistem, asimetrik şifreleme tekniğidir. Rabin kriptosistemi, RSA ın bir versiyonudur. RSA da olduğu gibi Rabin kriptosisteminde de bileşik sayıların çarpanlara ayrılma zorluğundan yararlanılmıştır (Rabin 1979). Rabin kriptosisteminin dezavantajı, 4 tane

çıktı içinden hangisinin doğru girdi olduğunu bulmak zordur. Her ne kadar ekleme metoduyla doğru çıktı seçilmeye çalışılsa da RSA ya göre bu bir dezavantajdır [26].

Rabin kriptosistem anahtar üretimi. Yaklaşık olarak aynı boyutta iki büyük rasgele p ve q asal sayıları oluşturulur.

$$n = p.q$$

hesaplanır. n, açık anahtar; (p, q) gizli anahtardır.

Rabin kriptosistemi şifreleme. m, mesajını şifrelemek isteyen biri,
n den az olmayacak şekilde m ikili sayı oluşturulur.
Gönderen kişinin açık anahtarına ulaşılır.
$c \equiv m^2 (mod\ n)$ denkliğini hesaplanır.
Şifrelenmiş c mesajını istediği kişiye gönderir.
Rabin kriptosistemi şifre çözümleme. Şifreli mesaj gelen kişi, kendi özel anahtarını kullanarak $m \equiv \sqrt{c}\ (mod\ n)$ değerini hesaplar.

$m^2 \equiv c(mod\ n)$ nin, ${m_p}^2 \equiv c(mod\ p)$ ve ${m_q}^2 \equiv c(mod\ q)$ şeklinde iki denklem çözümü vardır. Buradan, $m_p \equiv c^{\frac{p+1}{4}}(mod\ p)$ ve $m_q \equiv c^{\frac{q+1}{4}}(mod\ q)$ dur.
Genişletilmiş Öklid algoritmasını kullanarak,

$y_p.p + y_q.q = 1$ hesaplanır.
$m_1 = \left(y_p.p.m_q + m_q.q.m_p\right)(mod\ n)$,
$m_2 = n - m_1$,
$m_3 = \left(y_p.p.m_q - m_q.q.m_p\right)(mod\ n)$,
$m_4 = n - m_3$,

kökler bulunur. Şifreli metini bulan kök kullanılır. Örneğin, A kişisi anahtar üretimi için;
$p = 277$ ve $q = 331$ asal sayılarını seçer. $n = p.q = 91687$ değerini hesaplar.
A kişisinin açık anahtarı $n = 91687$, gizili anahtarı $p = 277$, $q = 331$ dir.

Şifreleme İşlemi. A kişisinin şifrelenecek mesajı $m = 40569$ olsun.
$c \equiv 40569^2 (mod\ 91687) = 62111$ değerini hesaplar.
Bu c mesajı B kişisine gönderilir.

Şifrenin açılması. B kişisi, $n = 91687$ açık anahtarı ile c şifreli metini, c'nin $(mod\ n)$ e göre dört kare kökünü hesaplar. $m_p \equiv c^{\frac{p+1}{4}}(mod\ p)$ ve $m_q \equiv c^{\frac{q+1}{4}}(mod\ q)$ farklı köklerden aşağıdaki dört kök

$$m_1 = 69654,\ m_2 = 22033,\ m_3 = 40569, m_4 = 51118$$

olarak bulunur. Şifreli metini, c'yi açar m_3'ü elde edip, orijinal mesaja ulaşır.

Mükemmel güvenli sayıların Rabin şifrelenmesine uygulanması. Şifrelenecek mesajımız: MRY olsun.

M	**1**
İ	**0**
R	**5**
A	**7**
Y	**8**

Tablo 4.6 bazı harflerin kodlama tablosu

Harfleri keyfi seçtiğimiz sayılarla eşleştirdik. Şimdi $p = 11$ ve $q = 23$ mükemmel güvenli asalları seçelim. Buradan,
$n = p.q = 253$ olur. Açık anahtarımız $n = 253$, gizli anahtarımız $(p, q) = (11, 23)$ dir.
$m < n$ olacak şekilde $m = 158$ olsun.$c \equiv 158^2(mod\ 253) = 170$ dir. Göndereceğimiz gizli mesajımız; MAİ dir. MAI olan gizli mesajımızı alan kişi, açık anahtarı yani $n = 253$ sayısını kullanarak

$$m_{11} \equiv 170^{\frac{11+1}{4}}(mod\ 11) = 4\ ,$$
$$m_{23} \equiv 170^{\frac{23+1}{4}}(mod\ 23) = 3$$

sayılarını bulur.Genişletilmiş Öklid algoritmasını kullanarak,

$$y_p.p + y_q.q = 1$$

eşitliğinden bilinmeyenler bulunur:

$y_p = -2$ ve $y_q = 1$ bulunur. Kökler ise,

$$m_1 = (-2.11.3 + 1.23.4)\ (mod\ 253) = 26,$$

$$m_2 = 253 - 26 = 227,$$

$$m_3 = (-2.11.3 - 1.23.4)(mod 253) = 95,$$

$$m_4 = 253 - 95 = 158 \text{ olur.}$$

Burada gerçek mesajı açan kök, m_4 sayısıdır. Yani, bizim şifrelenen MAI gizli mesajı, $n = 253$ açık anahtarı ile hesaplanarak bulunan $m_4 = 158$ sayısı gerçek mesajı; MRY açar. Aşağıdaki tabloda, sarı ile boyalı olan $m_4 = 158$ değerine karşılık gelen harfler yardımıyla gerçek mesaja ulaşılır.

M	**1**
İ	**0**
R	**5**
A	**7**
Y	**8**

Tablo 4.7 gerçek mesaj tablosu

Sonuç olarak, asal sayıların düzensiz ilerlemesinden faydalanarak mükemmel güvenli asal sayıları oluşturduk. Böylelikle, elde ettiğimiz mükemmel güvenli asal sayıları RSA ve RABİN kriptosistemlerinde kullanarak, şifrelemeyi daha güvenli hale getirdik.

SONUÇ VE ÖNERİLER

Bu çalışmanın birinci bölümünde tam sayıların ve asal sayıların genel bilgilerine ve bölünebilme testlerine yer verilmiştir. İkinci bölümde, bilinen bazı özel asal sayılara ayrıntılı olarak değinilmiştir. Üçüncü bölümde ise, asal sayıları bulmak için oluşturulmuş bazı asallık testleri incelenmiştir. Daha sonra ise, yeni tanımladığımız ve kullandığımız asal sayı bulma yöntemi verilmiştir. Dördüncü bölümde, asal sayıları şifrelemede uygulama teknikleri olan RSA ve Rabin kriptosistemi verilmiştir. Son olarak, bu tezde tanımlanan ve kullanılan mükemmel güvenli asal sayılar ele alınmıştır. Ayrıca, bir uygulama olarak, bu sayıların RSA ve Rabin şifreleme yöntemlerinde kullanılması da verilmiştir. Bu çalışmada tanımlanan asal sayı bulma yöntemi, yapılacak başka çalışmalarda da kullanılabilecektir.

KAYNAKLAR

Akbar, A.A., "Asal Sayıların Şifreleme Teoresindeki Uygulamaları", Yüksek Lisans Tezi, *Atatürk Üniversitesi Fen Bilimleri Enstitüsü*, Matematik Anabilim Dalı, Erzurum, (2015).

Altındiş, H., *Sayılar Teorisi ve Uygulamaları*, Kayseri : Erciyes Üniversitesi, (1999).

Aşar, O., Arıkan, A. And Arıkan, Ay., *Cebir*, Eflatun Yayın Evi : Ankara, (2009).

Baştan, R., Akın, C., "Notes on Sophie Germain Primes". *Turkish Journal of Mathematics and Computer Science*, 10, 18-21,(2018).

Beşkirli, A., Özdemir, D., Beşkirli, M., "Şifreleme Yöntemleri ve RSA Algoritması Üzerine Bir İnceleme", Avrupa Bilim ve Teknoloji Dergisi, (2019).

Crandall, R. and Pomerance, C., *Prime Numbers A Computational Perspective*, New York : Springer Science, 389-392, (2005).

Erdoğan, M., Yılmaz, G., *Soyut Cebir ve Sayılar Teorisi*, Beykent Üniversitesi Yayın Evi : İstanbul, (2008).

Gerstien, L.G., *Introduction To Mathematical Structures And Proofs*, Second, Springer : New York, (2012).

Gürlü, Ö., *Olimpik Matematik Sayılar Teoresine Giriş*, Altın Nokta Yayınevi : İzmir, (2013).

O'Connor, J.J., Robertson, E.F., "Prime Numbers", http://www-history.mcs.st-andrews.ac.uk/HistTopics/Prime_numbers.html, (January 2018).

Özgü, C., "Asal Sayı Örüntüleri ve Goldbach Sanısı Üzerine Bir Çalışma ", Yüksek Lisans Tezi, *Ege Üniversitesi Fen Bilimleri Enstitüsü*, Uluslararası Bilgisayar Anabilim Dalı, (2002).

Primes, https:// primes.utm.edu/notes/rh.html, 13.12.2019.

Ribenboim, P., *The Little Book Of Bigger Primes*, Springer-Verlag : New York, (2004).

RSA Laboraties, *Frequently Asked Questions About Today's Cryptography What's Primality Testing*, RSA Security Inc. : USA, (2000).

Silverman, R.D., *Fast Generation Of Random, Strong RSA Primes*, RSA Laboratories Crypto Bytes Magazine, (1997).

Sondow, J., “Ramanujan Primes and Bertrands Postulate”, The American Mathamatical Monthly, 116 (7), (2009).

Travaglını, G., *Number Theory, Fourier Analysis and Geometric Discrepancy*, Mathematical Society Student Texts 81 : Londan, (2014).

Yelkenkaya, N., “Sayılar Teorisi Ders Notu”, İstanbul Kültür Üniversitesi Fen-Eğitim Fakültesi Matematik Bilgisayar Bölümü, (2014).

Yerlikaya, T., Kara, O., “Kriptolojide Kullanılan Asal Sayı Test Algoritmaları”, Trakya University Journaddl Of Engineering Sciences, 18(1),(2017).

Zuckerman, H.S., Niven, I. And Monygomery H.L., *An Introduction To The Theory Of Numbers,* New York : John Wiley, Sons, 25-26, (1991).

Wells, D., “Prime Number: The Most Mysterious Figures in Math”, United States Of America, (2005).

Weisstein, Eric W., “Prime Number Theorem”, From Mathworld-A Wolfram Web Resource, Http:// mathworld.wolfram.com/PrimeNumberTheorem.html.

http://www.fermatsearch.org/news.html, Erişim Tarihi: 22.07.2019.

https://en.wikipedia.org/wiki/Palindromic_prime#cite_note-1, Erişim tarihi: 26.05.2020.

https://mathworld.wolfram.com/FactorialPrime.html, Erişim tarihi: 26.05.2020.

http://bilgisayarkavramlari.sadievrenseker.com/2009/06/04/rabin-sifreleme/, Erişim tarihi: 1.06.2020.

https://www.mersenne.org/, Erişim tarihi: 13.07.2020

ÖZGEÇMİŞ

Adı Soyadı	:	NAZLI KOCA
Doğum Yeri ve Tarihi	:	DENİZLİ/ 04.10.1992
Lisans Üniversite	:	SELÇUK ÜNİVERSİTESİ
Elektronik posta	:	Nazli_537@hotmail.com
İletişim Adresi	:	Adalet mahallesi, 10083 sokak, NO:11, Daire 4.