GİRESUN
ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

ASAL SAYILAR ÜZERİNE

MATEMATİK
ANABİLİM DALI

Yüksek Lisans Tezi

Recep BAŞTAN
20152110030

Mayıs 2019

GİRESUN

T.C.
GİRESUN ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ASAL SAYILAR ÜZERİNE

YÜKSEK LİSANS TEZİ

Recep BAŞTAN

Enstitü Anabilim Dalı : **Matematik**

Tez Danışmanı : **Dr. Öğr. Üyesi Canan AKIN**

Mayıs 2019

T.C.
GİRESUN ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ASAL SAYILAR ÜZERİNE

YÜKSEK LİSANS TEZİ

Recep BAŞTAN

Enstitü Anabilim Dalı : Matematik

Bu tez 03/05/2019 tarihinde aşağıdaki jüri tarafından oybirliği ile kabul edilmiştir.

Dr. Öğr. Üyesi	**Doç. Dr.**	**Dr. Öğr. Üyesi**
Şerife YILMAZ	**İmdat İŞCAN**	**Canan AKIN**
Jüri Başkanı	**Üye**	**Üye**

Doç. Dr.
Bahadır KOZ
Enstitü Müdürü

BEYAN

Tez içindeki tüm verilerin akademik kurallar çerçevesinde tarafımdan elde edildiğini, görsel ve yazılı tüm bilgi ve sonuçların akademik ve etik kurallara uygun şekilde sunulduğunu, kullanılan verilerde herhangi bir tahrifat yapılmadığını, başkalarının eserlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğunu, tezde yer alan verilerin bu üniversite veya başka bir üniversitede herhangi bir tez çalışmasında kullanılmadığını beyan ederim.

Recep BAŞTAN

03/05/2019

TEŞEKKÜR

Tez çalışmamda her türlü bilimsel desteği sağlayan, sabır gösteren değerli hocam Dr. Öğr. Üyesi Canan AKIN'a ve ayrıca bugüne gelmemde desteklerini esirgemeyen aileme teşekkür ederim.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

$a\|b$	: a, b yi böler
$(a,b)=d$	: a ile b nin ebobu d dir
$ord_m a$	: a nın $mod\ m$ deki mertebesi
$\left[\frac{a}{b}\right]$	: a nın b ye bölümünden elde edilen tam kısım
$(\frac{a}{n})$	: Jacobi sembolü
$(\frac{a}{p})$	: Legendre sembolü
B	: Brun sabiti
Cn	: n basamaklı bileşik sayı
C_n	: Cullen sayısı
$e.k.e.S$	: S nin en küçük elemanı
F_n	: Fermat sayısı
KNR	: Kuadratik nan-rezidü
KR	: Kuadratik rezidü
M_n	: Mersenne sayısı
Pn	: n basamaklı asal sayı
$(p,p+2)$	: İkiz asal çifti
$\mathbb{P}$	: Asal sayılar kümesi
$\pi(x)$	: x den büyük olmayan asalların sayısı
$\varphi(m)$	: Euler phi fonksiyonu
S_n	: Lucas sayısı
$SG-S$	: Sophie Germain ve Güvenli asal çifti

TABLOLAR LİSTESİ

ASAL SAYILAR ÜZERİNE

ÖZET

Bu tezde asal sayıların tarihine kısaca değinilmiş ve asal sayılar ile ilgili tanımlara ve teoremlere yer verilmiştir. Bazı asal sayı çeşitleri ve asal sayıları bulmada kullanılan bir takım yöntemler incelenmiştir. Ayrıca asal sayıların düzensizliğini göstermek için asal sayıların dağılımı hakkında temel bilgiler verilmiştir. İncelediğimiz ve bulgularımıza kaynaklık eden bazı güncel makaleler yer almıştır.

Bu tez çalışmasında, Sophie Germain asalı ve ilgili güvenli asal çifti kısaca *SG-S*-asal çifti olarak adlandırılmıştır. *SG-S*-asal çiftlerini elde etmek için bir eleme yöntemi olarak bazı talimatlardan oluşturulmuş bir elek önerilmiştir. Ayrıca 250 ye kadar olan *SG-S*-asal çiftlerini elde etmek için bu eleği kullandığımız bir örnek verilmiştir. Dahası, bu tezde Sophie Germain asallarının kongrüanslarla elde edilmiş bir karakterizasyonu verilmiştir.

Anahtar kelimeler: Asal sayılar, Sophie Germain Asalları

ON PRIME NUMBERS

SUMMARY

In this thesis, the history of prime numbers is briefly mentioned and definitions and theorems related to prime numbers are included. Some kind of prime numbers and some certain methods which are used to find prime numbers are perused. In addition, basic information on the distribution of prime numbers is given to show the irregularity of prime numbers. Some of the current articles that we have studied and have been the source of our findings are investigated.

In this study, a pair of Sophie Germain prime and connected safe prime is referred to as *SG-S*-prime pair in short. As a sieving method for obtaining *SG-S*-prime pairs, a sieve formed from some instructions is proposed. We also provide an example of using this sieve to obtain *SG-S*-prime pairs up to 250. Moreover, in this thesis, a characterization of Sophie Germain primes by using congruences is given.

Keywords: Prime numbers, Sophie Germain primes

BÖLÜM 1. GİRİŞ

Asal sayılar, matematiğin en köklü konularındandır. Eski Mısır'da asal sayıların kullanıldığına dair işaretler vardır. M.Ö. 300 yıllarında Euclid'in "Elements" kitabında yer alan asal sayıların sonsuz çoklukta olduğunun kanıtı ve yine aynı döneme denk gelen Eratosthenes Kalburu Antik Yunan'da asal sayılarla ilgili çalışmaların olduğunu gösterir. Ancak 17. yüzyıla kadar bu konuyla ilgili önemli gelişmeler olmadığı söylenmektedir. Bu dönemde özellikle Fermat'ın Küçük Teoremi, önemli bir ölçüt olup matematikçilerin bu alanda yoğunlaşmalarını sağlamıştır. Son yüzyılda ise bir sayının asal olup olmadığını anlamak, asal sayıları formülize etmek matematikçiler için uğraş olmuştur. Günümüzde asal sayıları kesin veya olası ihtimallerle bulduran asal sayı test algoritmaları oluşturmak için matematikçiler ve bilgisayar bilimcilerinin çalışmaları vardır.

Aşağıda okuyucunun bu tezi kolaylıkla anlayabilmesine yardımcı olabilmek için bazı temel kavramlara yer verilmiştir. Bu tezde sıklıkla kullanılmış bazı teoremlerin ispatları verilmiş olup diğerlerinin ispatları için belirtilen kaynaklara başvurulabilir. Bu bölümde [1], [2], [3] numaralı kaynaklardan yararlanılmıştır.

1.1. Tanım. $a, b \in \mathbb{Z}$ için $b = ac$ olacak şekilde bir $c \in \mathbb{Z}$ mevcut ise $\boldsymbol{a}$, $\boldsymbol{b}$ **yi böler** denir ve "$\boldsymbol{a|b}$" ile gösterilir. Aksi durumda $\boldsymbol{a \nmid b}$ yazılır.

1.2. Önerme.

i. $\forall a \in \mathbb{Z}$ için $a|a$ dır.

ii. $\forall a \in \mathbb{Z}$ için $a|0$ dır.

iii. $0|b$ ve $b \in \mathbb{Z}$ ise $b = 0$ dır.

iv. $a \in \mathbb{Z}$ ve $\forall b \in \mathbb{Z}$ için $a|b \Leftrightarrow a = \pm 1$ dir.

v. $a, b \in \mathbb{Z}$, $a|b$ ve $b|a$ ise $b = \pm a$ dır.

vi. $a, b, c \in \mathbb{Z}, a|b$ ve $b|c$ ise $a|c$ dir.

vii. $a, b, c \in \mathbb{Z}, c|a$ ve $c|b$ ise $\forall x, y \in \mathbb{Z}$ için $c|ax + by$ dir.

1.3. Tanım. Eğer $a|b$ ve $1 < a < b$ ise a ya b nin bir **öz böleni** denir.

1.4. Tanım. $a, b \in \mathbb{Z}$ olmak üzere aşağıdaki şartları sağlayan bir $d \in \mathbb{N}/\{0\}$ mevcut ise bu d ye a ile b nin **en büyük ortak böleni** (ebob'u) denir ve $d = (a, b)$ ile gösterilir.

i. $d|a$ ve $d|b$

ii. $\forall c \in \mathbb{Z}$ için $c|a$ ve $c|b$ ise $c|d$ dir.

Eğer $d = 1$ olursa a ve b ye **aralarında asal** denir.

1.5. Tanım. Bir A kümesinde bir sıralama bağıntısı varsa bu kümeye **sıralı küme** denir.

Bir kümede tanımlı sıralama bağıntısı " $\leq$ " ile gösterilir.

1.6. Tanım. $(A, \leq)$ sıralı bir küme olsun.

i. $b \in A$ elemanına en küçük eleman denir. $\Leftrightarrow \forall x \in A$ için $b \leq x$ dir.

ii. $a \in A$ elemanına en büyük eleman denir. $\Leftrightarrow \forall x \in A$ için $x \leq a$ dır.

iii. $a \in A$ elemanına maksimal eleman denir. $\Leftrightarrow \forall x \in A$ için $a \leq x \Rightarrow x = a$ dır.

iv. $b \in A$ elemanına minimal eleman denir. $\Leftrightarrow \forall x \in A$ için $x \leq b \Rightarrow x = b$ dir.

v. $(A, \leq)$ kümesine tam sıralı küme (zincir) denir. $\Leftrightarrow \forall a, b \in A$ için $a \leq b$ veya $b \leq a$ dır.

vi. $(A, \leq)$ kümesine iyi sıralı küme denir. $\Leftrightarrow \forall \emptyset \neq X \subseteq A$ için X in en küçük elemanı mevcuttur.

1.7. Örnek. $\mathbb{N}$ iyi sıralıdır.

1.8. Tanım. Doğal sayılar kümesinin boş olamayan her alt kümesinin en küçük elemanı vardır. Buna **iyi sıralama prensibi** denir.

1.9. Tanım. $p > 1$ bir tam sayı olsun. Eğer p nin 1 ve p den başka pozitif böleni yoksa p ye bir **asal sayı** denir. Bu çalışmada asal sayılar kümesi $\mathbb{P}$ ile gösterilecektir. 1 den büyük olan ve asal olmayan bir tam sayıya **bileşik sayı** denir.

1.10. Örnek. $2, 3, 5, 7, 11, 13, 17, 19$ asal sayılardır ve $4, 6, 8, 9, 10$ bileşik tam sayılardır.

1.11. Teorem. $\forall a > 1$ tam sayısının en az bir asal böleni vardır.

İspat. a nın 1 den büyük bölenlerinin kümesi $S = \{d \in \mathbb{Z} \mid d > 1, d|a\}$ olsun. S kümesini göz önüne alalım. $a > 1$ ve $a|a$ olduğundan dolayı $a \in S$ dir. Böylece $S \neq \emptyset$ dır. $S \subseteq \mathbb{N}$ olduğundan iyi sıralama ilkesi gereğince en küçük elemana sahiptir. Kabul edelim ki p, S nin en küçük elemanı olsun. $p \in S$ olduğundan $p > 1$ ve $p|a$ dır. Göstermemiz gereken $p \in \mathbb{P}$ olduğudur. Varsayalım ki $p \notin \mathbb{P}$ olsun. Bu takdirde $\exists q, r \in \mathbb{Z}, 1 < q < p$ vardır öyle ki $p = q.r$ dir. Bundan dolayı $q|p$ dir. 1.2. Önerme. (vi) den dolayı $q|a$ dır. Dolayısıyla $q \in S$ elde edilir ki bu durum p nin en küçük eleman olarak seçilmesiyle çelişir. O halde $p \in \mathbb{P}$ dir. Yani, $a > 1$ sayısının asal bir böleni bulunmuş olur.

1.12. Teorem. $p \in \mathbb{P}$ ve $p \nmid a$ ise $(a, p) = 1$ dir.

1.13. Teorem. $p \in \mathbb{P}$ ve $p|ab$ ise $p|a$ veya $p|b$ dir.

1.14. Sonuç. $p \in \mathbb{P}$ ve $p|b_1 b_2 \dots b_n$ ise en az bir $(i = 1,2,3, \dots n)$ için $p|b_i$ dir.

1.15. Sonuç. Eğer $p, p_1 \dots p_n \in \mathbb{P}$ ve $p|p_2 p_3 \dots p_n$ ise bazı $(i = 1, 2, 3, \dots n)$ için $p = p_i$ dir.

1.16. Teorem. Her $n > 1$ tam sayısı ya asaldır ya da sonlu sayıda asal sayının çarpımı olarak yazılabilir.

İspat. Eğer n tam sayısı asalsa ispat biter. $S := \{t > 1 |\ t|n,\ t < n, t \in \mathbb{N}\}$ olsun. n sayısı asal değilse n nin en az bir öz böleni vardır. Dolayısıyla $S \neq \emptyset$, $S \subseteq \mathbb{N}$ dir ve $\mathbb{N}$ nin iyi sıralı oluşuyla da $e.k.e.S$ vardır. Eğer m bu bölenlerin en küçüğü ise m asaldır. Gerçekten m asal olmasaydı en az bir l tam sayısı vardır ki, $1 < l < m$, $l|m$ olacaktı. O zaman $m|n$ bağıntısını göz önüne alarak $l|n$ bulunur ki bu da m nin tanımıyla çelişir. O halde n ya asaldır ya da kendisinden küçük p_1 asalıyla bölünebilir. Bu durumda $n = p_1 n_1$, $1 < n_1 < n$ dir. Burada ya n_1 asaldır ki o zaman ispat biter ya da n_1 kendisinden küçük p_2 gibi bir asala bölünebilir. Bu durumda $n = p_1 n_1 = p_1 p_2 n_2$, $1 < n_2 < n_1 < n$ dir. Bu düşüncenin tekrarı ile pozitif tam sayılardan oluşan $n, n_1, n_2, n_3, \ldots n_{k-1} \ldots$ dizisi elde etmiş oluruz. Bu dizi için iki durum düşünülebilir. Birinci durumda uygun bir $k \in \mathbb{N}$ için $n_{k-1} = 1$ dir. Başka bir deyişle dizi sonlu olup n_{k-1} de kesilir. İkinci durumda k ne olursa olsun $n_k > 1$ dir. Yani dizi sonsuzdur, ancak bu durum hiçbir zaman mümkün olmaz. Çünkü dizinin oluşum biçiminden $n_k = p_{k+1}.n_{k+1}$ olup, $p_{k+1} > 1$ den $n_k = p_{k+1}.n_{k+1} > n_{k+1}$ yani $n_k > n_{k+1}$ dir. O halde $n, n_1, n_2, \ldots n_{k-1}, \ldots$ tam sayılar dizisi azalan bir dizidir. İyi Sıralama Prensibine göre n_i gibi bir en küçük pozitif tam sayı vardır. Bu nedenle dizi sonsuz olamaz. Aksi halde n_i den sonra yukarıda uygulanan işlemle bir n_{i+1} elde edilir ki dizide n_i den daha küçük bir pozitif tam sayı bulunmuş olur. Bu da n_i nin tanımına aykırıdır. Şu halde $n > 1$ olmak üzere n ne olursa olsun sonlu sayıda adımdan sonra $n_k = 1$ olur ve yukarıda bulunan

$$
\begin{aligned}
n &= p_1 n_1 \\
n_1 &= p_2 n_2 \\
n_2 &= p_3 n_3 \\
&\vdots \\
n_{k-2} &= p_{k-1} n_{k-1} \\
n_{k-1} &= p_k n_k \\
n_k &= 1
\end{aligned}
$$

eşitliklerinden $n = p_1 p_2 \ldots p_k$ elde edilir. Burada her $i = 1, 2, 3, \ldots k$ için p_i asallarının farklı olması gerekmez. Yani herhangi bir p_i ile birçok bölme yapılmış olabilir. Bu durumda $n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ ($\forall i = 1, 2, 3, \ldots k$ için $a_i > 0$, $a_i \in \mathbb{N}$, $p_1 < p_2 < \cdots < p_k$) yazılır ve bu gösterime n nin **standart biçimi** denir.

1.17. Örnek. 60 sayısı asal değildir ve $60 = 12.5 = 3.4.5 = 2^2.3.5$ şeklinde yazılabilir.

1.18. Teorem. (Aritmetiğin Temel Teoremi) $n > 1$ bir tam sayı olsun. O zaman öyle bir $r \geq 1$ tam sayısı ve öyle $p_1, p_2, \dots p_r$ asal sayıları vardır ki $n = p_1 p_2 \dots p_r$ dir ve bu gösterim çarpanların yer değiştirmesi farkıyla tektir.

İspat. 1.14. Sonuç. gereğince $t \in \mathbb{N}^+$, $p|a_1 a_2 \dots a_t$ ise ya $p|a_1$ veya $p|a_2$ veya $\dots p|a_t$ olduğunu biliyoruz. Burada özel olarak $a_1 a_2 \dots a_t$ tam sayıları asal ise 1.15. Sonuç. gereğince p bunlardan biri olmak zorundadır.

Şimdi $p_i (\, i = 1, 2, \dots k)$, q_j $(j = 1, 2, \dots \, l)$ farklı asallar olmak üzere

$$n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} = q_1^{b_1} q_2^{b_2} \dots q_l^{b_l} \qquad (*)$$

olduğunu varsayalım. O zaman açık olarak her $i \in \{1, 2, \dots k\}$ için $p_i | \, q_1^{b_1} q_2^{b_2} \dots q_l^{b_l}$ olup, 1.15. Sonuç. a göre her p bir q olur. Benzer şekilde her q bir p olacaktır. O halde $k = l$ ve asalların her iki kümesi doğal olarak,

$(p_1 < p_2 < \dots < p_k \, , q_1 < q_2 < \dots < q_k)$ şeklinde artan sırada oluşturulduğundan her i için $p_i = q_i$ dir. Eğer $a_i > b_i$ ise (*) ın her iki tarafını $p_i^{b_i}$ ile bölelim. Bu durumda $p_1^{a_1} p_2^{a_2} \dots p_i^{a_i - b_i} \dots p_k^{a_k} = p_1^{b_1} p_2^{b_2} \dots p_{i-1}^{b_{i-1}} p_{i+1}^{b_{i+1}} \dots p_k^{b_k}$ elde edilir. Yukarıdaki eşitliğin sol yanı p_i ile bölünmesine rağmen sağ taraf bölünemez. Bu bir çelişkidir. Benzer olarak $b_i > a_i$ için de böyle bir çelişkiye varmak mümkündür. Böylece sonuçta $b_i = a_i$ elde edilir ki ispat biter.

1.19. Örnek. $60 = 2^2.3.5 = 3.2^2.5 = 5.3.2^2$ olduğu kolaylıkla görülür.

1.20. Teorem. (Euclid) Asal sayılar sonsuz çokluktadır.

İspat. $\mathbb{P} = \{2, 3, \dots p\}$ olsun. Şimdi bu asallar yardımıyla $q = 2.3.5 \dots p + 1$ sayısını oluşturalım. Açık olarak q sayısı $2, 3, 5, \dots p$ asallarından biriyle bölünemez. Böylece ya kendisi asaldır veya 1.11. Teorem gereği p ve q arasındaki bir asal ile bölünür. Her iki durumda da p den büyük bir asal sayı bulunabileceğinden teoremin ispatı biter.

1.21. Tanım. $m > 1$ ve $(a,m) = 1$ olmak üzere $a^t \equiv 1\ (mod\ m)$ olacak şekildeki en küçük pozitif t tam sayısına a tam sayısının m modülüne göre **mertebesi** veya a nın m modülündeki **üssü** denir ve $ord_m a = t$ biçiminde gösterilir.

1.22. Lemma. Eğer, $a \in \mathbb{Z}$ nin m modülüne göre mertebesi t ve $a^u \equiv 1\ (mod\ m)$ ise $t|u$ dur.

1.23. Teorem. Verilen bir pozitif m tam sayısını geçmeyen ve m ile aralarında asal olan sayıların sayısı $\varphi(m)$ ile gösterilir. Buna **Euler'in φ fonksiyonu** denir. Buna göre $m > 1$ tamsayısının asal olması için gerek ve yeter şart $\varphi(m) = m - 1$ olmasıdır.

1.24. Sonuç. Eğer, $a \in \mathbb{Z}$ nin m modülüne göre mertebesi t ise $t|\varphi(m)$ ve p asal olmak üzere a nın p modülüne göre mertebesi t ise $t|p-1$ dir.

1.25. Teorem. (Euler Teoremi) $m \in \mathbb{Z}^+$ ve $a \in \mathbb{Z}$ olmak üzere $(a,m) = 1$ olsun. O halde $a^{\varphi(m)} \equiv 1\ (mod\ m)$ dir.

1.26. Teorem. (Fermat'ın Küçük Teoremi) $p \in \mathbb{P}$ ve $a \in \mathbb{Z}$ olmak üzere $p \nmid a$ olsun. O halde $a^{p-1} \equiv 1\ (mod\ p)$ dir.

1.27. Teorem. (Wilson Teoremi) $p \in \mathbb{P}$ dir $\Leftrightarrow (p-1)! \equiv -1\ (mod\ p)$ dir.

İspat. ($\Leftarrow$:) Karşıt olarak bu kongrüans sağlansın ve $n \notin \mathbb{P}$ olsun. O zaman n nin öyle bir t böleni vardır ki $1 < t < n$ dir. $t|n$ olduğundan $(n-1)! \equiv -1\ (mod\ t)$ dir. Ancak $t|(n-1)!$ Olduğundan $(n-1)! \equiv 0\ (mod\ t)$ olmalıdır. Buradan $-1 \equiv 0\ (mod\ t)$ ve $t|-1$ elde edilir. Fakat $t > 1$ olduğundan bu bir çelişkidir. Dolayısıyla $p \in \mathbb{P}$ olmalıdır.

1.28. Teorem. $p \in \mathbb{P}$ olsun. $a^2 + 1 \equiv 0\ (mod\ p)$ şartını sağlayan bir $a \in \mathbb{Z}$ olması için gerek ve yeter şart $p = 2$ ya da $p \equiv 1\ (mod\ 4)$ olmasıdır.

Bu tezin amacı bazı asal sayı çeşitlerini ve asal sayıları bulmada kullanılan bir takım yöntemleri incelemektir. Bu tezin bazı bölümlerinde özellikle Sophie Germain asallarına ağırlık verilmiştir. Bu tez üç ana bölümden oluşmaktadır. Bölüm 1. Giriş bölümü olup bu bölümde asal sayıların tanımı ve tarihine kısaca değinilmiş ve asal sayılar ile ilgili bazı tanımlara ve teoremlere yer verilmiştir. Bölüm 2. Kaynak Araştırması bölümü olup beş alt başlığa ayrılır. Birinci alt başlıkta aralarında bu tezde özellikle ilgilendiğimiz Sophie German asallarının da bulunduğu asal sayı çeşitleri incelenmiştir. İkinci alt başlıkta asal sayıları bulmada kullanılan ilk algoritma olan Eratosthenes kalburu (eleği) araştırılmıştır. Üçüncü alt başlıkta günümüzde asal sayıları bulmada kullanılan ve şifreleme ile ilgili birçok alanda (bankacılık ve savunma sanayi gibi) uygulaması olan bazı asal sayı test algoritmaları araştırılmıştır. Dördüncü alt başlıkta asal sayıların düzensizliğini göstermek için bu sayıların dağılımı hakkında temel bilgilere yer verilmiştir. Beşinci alt başlıkta incelediğimiz ve bulgularımıza kaynaklık eden bazı güncel makaleler yer almıştır. Bölüm 3. Bulgular bölümüdür. Bu bölümde Sophie German asallarını bulduran bir kalbur elde edilmiş ve ayrıca bu asalların karakterizasyonu için bir kongrüans verilmiştir.

BÖLÜM 2. KAYNAK ARAŞTIRMASI

2.1. Çeşitli Formlardaki Asallar

Bu bölümde çeşitli formlardaki asal sayıları hakkında yapılan çalışmalar ve güncel bilgilere yer verilmiştir. Ayrıntılı bilgi edinmek isteyen okuyucular, bu bölümde kullanılan [4], [5], [6], [7], [8], [9], [10] kaynaklarını inceleyebilirler.

2.1.1. Fermat asalları

2.1. Tanım. Her $n \geq 0$ tamsayısı için $F_n = 2^{2^n} + 1$ tamsayısına bir Fermat sayısı ve F_n asal ise F_n ye **Fermat asal sayısı** denir.

Fermat, her $n \geq 0$ için F_n nin asal olduğunu iddia etmiştir. $n = 0, 1, 2, 3, 4$ için $F_n = 3, 5, 17, 257, 65537$ asaldır. Fakat F_5 sayısı bileşiktir.

Günümüzde F_0, F_1, F_2, F_3, F_4 ten başka Fermat asalı bilinmemektedir. $F_4 = 65537$ bilinen en büyük Fermat asalıdır. Ayrıca $5 \leq n \leq 19$ için bütün F_n lerin bileşik sayı olduğu bilinmektedir. Aşağıdaki teorem bu konuda daha fazla bilgi sağlar.

2.2.Teorem. Herhangi bir $n \geq 2$ tamsayısına karşılık gelen F_n Fermat sayısının bir asal çarpanı $k \in \mathbb{Z}^+$, $2^{n+2} \times k + 1$ biçimindedir.

$5 \leq n \leq 19$ için bütün F_n lerin bileşik sayı olduğunun gösterimi bu teoremin uygulamasıdır.

Euler, 1732'de F_5 in bir asal çarpanının $2^{5+2}k + 1 = 128k + 1$ formunda olduğunu göstermiştir.

$$F_5 = 2^{2^5} + 1 = 641 \times P7$$

Pn, n basamaklı bir asal sayıyı göstermek üzere, aynı şekilde Landry 1880 de F_6 nın bir asal çarpanını $2^{6+2}k + 1 = 256k + 1$ formunda olduğunu göstermiştir.

$$F_6 = 2^{2^6} + 1 = P6 \times P14$$

F_7 nin bir asal çarpanı $2^{7+2}k + 1 = 512k + 1$ formunda olmalıdır. Burada $k =$ 1165031037646443 e karşılık gelen ilk asal çarpan M.J. Morrison ve J.Brillhart tarafından 1975 yılında elektronik bilgisayar yardımıyla bulunmuştur. Daha öncesinden, 1905'de J.C. Morehead, F_7 nin bileşik olduğunu kanıtlamıştır.

$$F_7 = 2^{2^7} + 1 = P16 \times P22$$

1908'de J.C. Morehead ve A.E. Western, F_8 in bileşik olduğunu kanıtladılar. Burada F_8in ilk asal bölenini R.P. Brent 1980'de bulmuştur. 1981'de Brent ve H.C. Williams, F_8 in iki asal çarpanın çarpımı şeklinde olduğunu buldular.

$$F_8 = 2^{2^8} + 1 = P16 \times P62$$

Western 1903'de $k = 2^5.37$ için $2^{11}.k + 1$ sayısının F_9 un bir asal çarpanı olduğunu buldu. A.K. Lenstra, H.W. Lenstra JR. ,M.S. Manasse ve J.M. Polland 1993'te 155 rakamlı $F_9 = 2^{512} + 1$ sayısının bütün asal çarpanlarını Eratosthenes Kalburu yöntemi ile buldular.

$$F_9 = 2^{2^9} + 1 = P7 \times P49 \times P99$$

1953'de J.L. Selfidge elektronik bilgisayar SWAC yardımıyla F_{10} un bir asal çarpanı olan $2^{12}.11131 + 1$ sayısını buldu. Bir başka asal çarpanı olan $2^{14}.395937 + 1$ sayısını J. Brillhart 1962'de IBM 704'ün yardımıyla bulmuştur.

$$F_{10} = 2^{2^{10}} + 1 = P8 \times P10 \times P40 \times P252$$

1899'da Cunningham F_{11} in iki asal çarpanı olan $2^{13}.39 + 1$ ve $2^{13}.119 + 1$ sayılarını buldu. Diğer asal çarpanlarını 1988'de Brent ve Morain buldular.

$$F_{11} = 2^{2^{11}} + 1 = P6 \times P6 \times P21 \times P22 \times P564$$

Daha sonra R.P. Brent, R.E. Crandall, K. Dilcher ve C. Van Halewyn 2000 yılında F_{13}, F_{15}, F_{16} Fermat sayılarının yeni asal çarpanlarını eliptik eğri yöntemini kullanarak buldular.

Yine son yıllarda Fermat asalları üzerine yapılan çeşitli çalışmalar vardır. Peter Strasser, 28 Ocak 2019'da F_{118} sayısının bir asal çarpanı olan $1527888802614951 \times 2^{120} + 1$ ve 19 Aralık 2018'de F_{132} sayısının bir asal çarpanı olan $1075441212722595 \times 2^{135} + 1$ sayılarını bulmuştur. 13 Aralık 2018'de Gary Gostin, F_{3345} sayısının bir asal çarpanı olan $6604326057 \times 2^{3345} + 1$ sayısını bulmuştur. 2 Kasım 2018'de Gary Gostin, F_{2144} sayısının bir asal çarpanı

olan $19789270693 \times 2^{2148} + 1$ sayısını bulmuştur. 24 Temmuz 2018'de Mark Rodenkirch, F_{5199} sayısının bir asal çarpanı olan $1488947679 \times 2^{5201} + 1$ sayısını bulmuştur. 5 Nisan 2018'de Roman Maznichenko, F_{274} sayısının bir asal çarpanı olan $58130105122923 \times 2^{277} + 1$ sayısını bulmuştur. 10 Mart 2018'de Gary Gostin, F_{63480} sayısının bir asal çarpanı olan $242445 \times 2^{63484} + 1$ sayısını bulmuştur. 24 Ocak 2018'de Gary Gostin, F_{45278} sayısının bir asal çarpanı olan $547653 \times 2^{45280} + 1$ sayısını bulmuştur [11].

Şimdiye kadar Fermat asallarının sonlu olup olmadığına dair bir ölçüt geliştirilememiştir. Fermat asallarının bir karakterizasyonu Pepin tarafından verilmiştir.

2.3. Teorem (Pepin Testi) $n \geq 2, F_n = 2^{2^n} + 1$ ve $k \geq 2$ olsun. O halde aşağıdaki koşullar denktir:

1) F_n asal ve $(k|F_n) = -1$ dir.
2) $k^{\frac{F_n - 1}{2}} \equiv -1 (mod\ F_n)$ dir.

2.4. Teorem. Herhangi iki Fermat sayısı aralarında asaldır.

2.5. Teorem. $a \geq 2$ ve $a^n + 1$ asal ise a çift ve $m \in \mathbb{Z}^+$ için $n = 2^m$dir.

2.1.2. Mersenne asalları

2.6. Tanım. $n \in \mathbb{Z}^+$olsun. O halde $M_n = 2^n - 1$ sayısına bir **Mersenne sayısı** ve M_n asal ise M_n ye **Mersenne asal sayısı** denir.

Örneğin; $M_2 = 2^2 - 1 = 3$, $M_3 = 2^3 - 1 = 7$, $M_5 = 2^5 - 1 = 31$ gibi.

1644 yılında Mersenne, Cogitita Physica Mathematica isimli kitabında p asalının $2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ değerleri için $M_p = 2^p - 1$ sayılarının asal, 257 den küçük p nin diğer 44 değeri için bileşik olduğunu iddia etmiştir.

1876 yılında Lucas geliştirdiği metotla $M_{127} = 2^{127} - 1$ in asal olduğunu açıkladı. Bu asal sayı bilgisayar yardımı olmaksızın bulunan en büyük asal sayı olma özelliğini korumaktadır.
1886 yılında Pervusin ve Seelhoff tarafından M_{61} in asal olduğunun keşfedilmesiyle Mersenne'nin iddiasında $p = 61, 67, 89, 107, 257$ için hatalar olduğu görülmüştür.

26 Aralık 2017'de Jon Pace zamanının bilinen en büyük Mersenne asalı olan $M_{77232917} = 2^{77232917} - 1$ asalını bulmuştur. Bu sayı 23249425 basamaklıdır. Günümüzde bilinen en büyük Mersenne asalı olan $M_{82589933} = 2^{82589933} - 1$ sayısı Patrick Laroche tarafından 27 Aralık 2018'de bulunmuştur. Şimdiye kadar 51 tane Mersenne asalı bilinmektedir [12].

1996 yılından itibaren bulunan tüm Mersenne asalları "Great Internet Mersenne Prime Search" tarafından bulunmuştur. Bu araştırma şirketi internet üzerine dağıtılmış bir bilgi işlem projesidir [13].

Aşağıdaki teorem Mersenne asallarının varlığını garanti eder.

2.7. Teorem. $a, n \geq 2$ tam sayılar olsun. Eğer $a^n - 1$ asal ise $a = 2$ ve n asaldır.

2.8. Teorem. Herhangi bir $p > 2$ asalı için, $2^p - 1$ in bir asal çarpanı $k \in \mathbb{Z}^+$, $q = 2kp + 1$ dir.

Euler tarafından 1750'de aşağıdaki sonuç ispatlanmıştır. Ayrıca Lagrange (1775) ve yine Lucas (1878) tarafından da ispatlanmıştır.

2.9. Sonuç. $q > 3$ ve $q \equiv 3\ (mod\ 4)$ biçiminde asal sayı olsun. $(2q + 1) | M_q \Leftrightarrow 2q + 1$ asaldır.

2.1.3. Sophie Germain asalları

Tarih boyunca gizemli ve ilginç bulunan asal sayılar, günümüzde çok önemli uygulama alanlarında yer aldıklarından giderek artan bir öneme sahip olmuştur. Özellikle şifreleme ile güvenliğin sağlandığı savunma sanayii, bankacılık, sosyal medya gibi sektörlerde asal sayılar kullanılmaktadır. Özellikle Sophie Germain asallarının asallık testlerinde, açık anahtar şifrelemelerinde, sayılar teorisinde uygulamaları vardır. Bu bölümde bugünün güvenlik sisteminin temelini oluşturan Sophie Germain asalları tanıtılmıştır.

2.10. Tanım. Eğer p asal iken $2p + 1$ sayısı da asal ise p sayısına **Sophie Germain asalı** denir. Eğer p Sophie Germain asalı ise $2p + 1$ asal sayısına **güvenli asal** denir. İlk birkaç Sophie Germain asalı şunlardır: $2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131, 173, 179, 191, 233 \ldots$

$n = 1, 2, 3, \ldots$ olmak üzere 10^n den küçük Sophie Germain asallarının sayısı $3, 10, 37, 190, 1171, \ldots$ şeklindedir [14]. Ayrıca ilk 1000 Sophie Germain asalı 2 ile 82493 asalları arasındadır ve bu asalların listesi [15] kaynağından bulunabilir.

Fermat'ın Son Teoremini 1994 yılında uzun uğraşlar sonucu Andrew Wiles eski öğrencisi Richard Taylor ile birlikte ispatlamıştır. Aslında 1994 yılından önce Andrew Wiles 200 sayfalık bir ispatta bulunmuştur. Fakat ispatta kısa zamanda uzmanlar tarafından bir hata bulunmuştur. 1994 yılında Andrew Wiles'in hatasını düzeltip doğru ispatı sunan ise Profesör Wiles'in eski öğrencisi Richard Taylor olmuştur [16].

Sophie Germain, Fermat'ın Son Teoremi'nin Sophie Germain asalları için doğru olduğunu gösterdiği aşağıdaki teoremi 1825 yıllarında ispatlamıştır.

2.11. Teorem. Eğer $p > 3$ bir Sophie Germain asalı ise $x^p + y^p = z^p$ şartını sağlayan, sıfırdan farklı ve p nin katları olmayan x, y, z tam sayısı yoktur.

$p > 3$ olmak üzere $p = 4k - 1$ formundaki Sophie Germain asalları 2.9. Sonuç. u sağlar. Bir başka deyişle bu formdaki Sophie Germain asalları M_p bileşik Mersenne

sayısının indisine karşılık gelir. Örneğin $p = 11$, $2^{11} - 1 = 23 \times 89$ bileşik Mersenne sayısının indisidir, yani $M_{11} = 2^{11} - 1$ dir.

Asal sayılar şifreleme alanında her yerde kullanılır, ancak bazıları diğerlerinden daha güvenlidir. Bir sayının büyüklüğü arttıkça sayının asal olup olmadığını bulmamız zaman alır. Özellikle asal çarpanları büyük olduğunda bu durum daha da zor olur. Birçok şifreli sistem, asal sayıların bu özelliğine dayanır. Örneğin bir arkadaşınız size özel bir mesaj göndermek istesin. Bu mesajı iki asal sayının çarpımı olan bir sayı ile şifreleyip mesajı açabilmek için sayının asal çarpanlarını anahtar olarak belirlesin. Herkes şifreyi görebilecek ama anahtar olan asal çarpanları bilmeden kimse mesajı açamayacaktır. Dolayısıyla da diğer kişilerin mesajı görebilmeleri için asal çarpanları hesaplamaları gerekecektir. Şifre olarak seçilen sayı ne kadar büyük olursa süper bilgisayarların bile asal çarpanları hesaplamaları yıllarca sürebilir. Böylece mesajın güvenliği artar. Şifreli sistemler ne kadar karmaşık yapıya sahip olsalar da mantığı aynıdır. Bir şifreli sistemin güvenliği asal çarpanların zorluğuna bağlıdır. Örneğimizdeki asal sayıları ilgili güvenli asallar olarak seçersek asal çarpanları hesaplama işlemi daha da zorlaşır ve sistem daha güvenli bir hal alır. Şimdi, 53 Sophie Germain asalı olduğundan 107 güvenli asaldır, 54 Sophie Germain asalı olmadığından 109, asal olmasına karşın güvenli asal değildir.

$$\text{Güvenli asal: } 107 = (2 \times 53) + 1$$

$$\text{Güvenli olmayan asal: } 109 = (2 \times 2 \times 3^3) + 1$$

Bu örnek, asal sayıların güvenliliğinin asalın büyüklüğüne değil; bir eksiğinin asal çarpanının büyüklüğüne bağlı olduğunu gösterir.

$p > 2$ olacak şekilde asal sayı olsun ve 2 den büyük tüm asallar tek olduğundan $2|(p-1)$ dir. Bu nedenle büyük asallar $p = (2 \times n) + 1$ şeklinde gösterilebilir. Burada $2 \times n$ çarpımındaki asal çarpanı maksimize etmenin en iyi yolu n i asal seçmektir. Dolayısıyla güvenli asallar daima Sophie Germain asallarıyla ilgilidir. Güvenli asallar şifreleme alanında temeldir. Bu Sophie Germain asallarının bugünün güvenlik sisteminin temelini oluşturduğu anlamına gelir [17].

Sophie Germain asallarının sonsuz sayıda olup olmadığı günümüzde halen açık problemdir. Buna karşın birçok araştırmacı tarafından sonsuz sayıda oldukları tahmin

edilmektedir. 29 Şubat 2016 itibariyle kanıtlanmış bilinen en büyük Sophie Germain asalı, $p = 2618163402417.2^{1290000} - 1$ dir [14].

2.1.4. Wieferich asalları

2.12. Tanım. p bir asal sayı olmak üzere, $2^{p-1} \equiv 1(mod\ p^2)$ kongrüansını sağlayan p sayısına **Wieferich asalı** denir.

Wieferich 1909'da Fermat'ın Son Teoremi'ni bu sayılar için doğru olduğunu ispatlamıştır. Lehmer, 1981'de, 1093 ve 3511 dışında 6×10^9 dan küçük başka Wieferich asalı olmadığını göstermiştir. 1997'de Crandall, Dilcher& Pomerance 8×10^{12} den, R. Brown 49×10^{12} den ve J.K. Crump 2×10^{14} den küçük başka Wieferich asalı olmadığını göstermişlerdir. Günümüzde bilinen Wieferich asalları; 1093 ve 3511 dir [18].

2.1.5. Wilson asalları

Wilson Teoremi, $p \in \mathbb{P}$ ise $(p-1)! \equiv -1\ (mod\ p)$dir. Böylece $W(p) = \frac{(p-1)!+1}{p}$ tamsayısı Wilson katsayısıdır.

2.13. Tanım. $W(p) \equiv 0\ (mod\ p)$ veya $(p-1)! \equiv -1\ (mod\ p^2)$ denklikleri sağlanıyorsa p sayısına **Wilson asalı** denir. Bilinen Wilson asalları $5, 13$ ve 563 tür. Wilson asallarının sonlu ya da sonsuz olduğu bilinmemektedir. 563 Wilson asalı 1953'de Goldberg tarafından keşfedildi. 1988'de E. Hearpearson, K.E. Kloss, W. Keller, H.Dubner ve aynı zamanda Ganter& Kundert tarafından yapılan araştırmada 10^7 den küçük başka Wilson asalı bulunamamıştır. Yapılan araştırma 1997'de Crandall, Dilcher& Pomerance tarafından 5×10^8 e genişletildiği halde yeni bir Wilson asalına rastlanılmamıştır [19].

2.1.6. Genelleştirilmiş Fermat asalları

2.14. Tanım. $m \geq 1, b \geq 2k, (k = 1,2,3,\ldots)$ için $b^{2^m} + 1$ formdaki asallara **genelleştirilmiş Fermat asalı** denir.

Haziran 2009 itibariyle bilinen en büyük genelleştirilmiş Fermat asalı $24518^{2^{18}} + 1$ dir [20].

2.1.7. Cullen asalları

2.15. Tanım. $C_n = n \times 2^n + 1$ formdaki asallara **Cullen asalı** denir.

$n = 1$ için $C_1 = 3$ tür.

1958'de Robinson, $1 < n \leq 1000$ için C_{141} den başka asal olmadığını göstermiştir.

1987'de Keller, $n \leq 30000$ için C_{4713}, C_{5795}, C_{6611}, C_{18496} asallarını bulmuştur [21].

2.1.8. İkiz asallar

2.16. Tanım. Eğer p asal iken $p + 2$ de asal ise bu asallara **ikiz asal** denir. Yani aralarındaki fark 2 olan asallara ikiz asal denir. $(p, p + 2)$ çiftine **ikiz asal çifti** denir. İkiz asalların sonlu olup olmadığı kanıtlanamamıştır. İlk birkaç ikiz asal çiftleri şunlardır: $(3,5), (5,7), (11,13), (17,19), \ldots$.

İkiz asallar 1949'da Clement tarafından aşağıdaki gibi karakterize edilmiştir.

2.17. Teorem. $n \geq 2$ için $(n, n+2)$ ikiz asal çiftidir.$\Leftrightarrow$ $4[(n-1)! + 1] + n \equiv 0 \; mod(n(n+2))$ dir.

Bununla birlikte bu karakterizasyon pratik değildir.

1919'da Brun, $(p, p+2)$ ikiz asal çiftleri için $\left(\frac{1}{3} + \frac{1}{5}\right) + \left(\frac{1}{5} + \frac{1}{7}\right) + \cdots + \left(\frac{1}{p} + \frac{1}{p+2}\right) + \cdots$ toplamının, Brun sabiti olarak adlandırılan ve B ile gösterilen bir sayıya yakınsadığını kanıtlamıştır. $(B = 1{,}9021605823 \ldots)$.

Her $x \geq 1$ için, x den küçük $(p, p+2)$ çiftlerinin sayısını belirleyen fonksiyon olarak $\pi_2(x)$ tanımlanmıştır. 1919'da Brun $\pi_2(x) < \frac{100x}{(logx)^2}$ olduğunu belirtmiştir. 1923'de Hardy ve Littlewood $\pi_2(x) \sim C_2 \frac{x}{(logx)^2}$ olduğunu sezgisel olarak tahmin

etmişlerdir. Burada $C_2 = \prod_{p>2}\left(1 - \frac{1}{(p-1)^2}\right)$ dır ve buna **ikiz asal sabiti** denir. $C_2 = 0{,}66016\ldots$ dır.

x	$\pi_2(x)$
10^3	35
10^4	205
10^5	1224
10^6	8169
10^7	58980
10^8	440312
10^9	3424506
10^{10}	27412679
10^{11}	224376048
10^{12}	1870585220
10^{13}	15834664872
10^{14}	135780321665
10^{15}	1177209242304

Tablo 1.1 [4]

Bilinen en büyük ikiz asal çiftleri aşağıdaki tabloda verilmiştir.

Sıra	İkiz asal çifti	Basamak	Tarih
1	$2996863034895 \times 2^{129000} \mp 1$	388342	Eylül 2016
2	$3756801695685 \times 2^{666669} \mp 1$	200700	Aralık 2011
3	$65516468355 \times 2^{333333} \mp 1$	100355	Ağustos 2009
4	$12770275971 \times 2^{222225} \mp 1$	66907	Temmuz 2012
5	$70965694293 \times 2^{200006} \mp 1$	60219	Nisan 2016
6	$66444866235 \times 2^{200003} \mp 1$	60218	Nisan 2016
7	$4884940623 \times 2^{198800} \mp 1$	59855	Temmuz 2015
8	$2003663613 \times 2^{195000} \mp 1$	58711	Haziran 2007
9	$38529154785 \times 2^{173250} \mp 1$	52165	Temmuz 2014
10	$194772106074315 \times 2^{171960} \mp 1$	51780	Haziran 2007

Tablo 1.2 [22]

2.1.9. Ramanujan asalları

2.18. Tanım. Bir $n \in \mathbb{N}$ için, n. Ramanujan asalı en küçük R_n tamsayısıdır öyle ki $x \geq R_n$ ise $\Pi(x) - \Pi\left(\frac{x}{2}\right) \geq n$ dir. Yani $x \geq R_n$ olduğunda $\frac{x}{2}$ ile x arasında asal sayılar mevcuttur. $\Pi(x) - \Pi\left(\frac{x}{2}\right)$fonksiyonu sadece bir asal artabildiğinden bu şekildeki en küçük R_n asal olmalıdır. İlk birkaç Ramanujan asalları şunlardır: $2, 11, 17, 29, 41, 47, 59, 67, 71, 97, 101, 107, 127, 149, 151, 167, \ldots$ Kolayca görülebilir ki sonsuz sayıda Ramanujan asalı vardır.

2.2. Eratosthenes Kalburu

Burada asal sayılarda kullanılan ilk algoritma olan Eratosthenes Kalburu'nu tanıtıp bir örnekle açıklayacağız. Eratosthenes tarafından M.Ö. 300'de geliştirilen ve verilen herhangi bir n tam sayısına kadar olan bütün asalları bulduran Eratosthenes Kalburu yöntemi, 2 den itibaren n ye kadar olan bütün sayıların bir liste şeklinde yazılarak ve sonrasında bileşik sayıların elenmesi esasına dayanır.

Eratosthenes Kalburu şöyledir:

1 den büyük, n e eşit veya küçük tam sayıların listesi yapılır. n in karekköküne eşit ya da küçük olan bütün asal sayıların katları olan sayılar çıkarılır. Geriye kalan sayılar asal sayılardır. Bir başka deyişle, önce n sayısına kadar olan bütün sayılar yazılır. Daha sonra sırası ile 2 nin, 3 ün, 5 in, ... p nin katları olan sayılar elenir. Bu işlem p sayısı, n sayısının karekökünden küçük $(p \leq \sqrt{n})$ olana kadar tekrar eder. Elenmeyen sayılar n sayısına kadar olan asal sayılardır.

2.19. Teorem. Bir bileşik n tam sayısının $p^2 \leq n$ (yani $p \leq \sqrt{n}$) sağlayan bir asal böleni p vardır.

İspat. $n > 1$ olduğundan 1.16. Teorem. den dolayı asal sayıların çarpımıdır. n nin en küçük asal böleni p olsun. O zaman $n = p.n_1$ olacak biçimde bir $n_1 > 1$ tam sayısı vardır ve $n = p.n_1 \geq p.p = p^2$ dir.

2.20. Örnek. 101 sayısı asaldır.

Gerçekten $\sqrt{101} < 11$ olduğundan $2, 3, 5, 7$ asal sayılarını denemek yeterlidir. Bu sayıların hiçbiri 101 i bölmediğinden 101 asaldır.

2.21. Örnek. 80 den küçük sayıları Eratosthenes Kalburu yöntemiyle bulalım:

İlk olarak Tablo1.3 deki gibi 80 e kadar olan sayılar yazılır. En küçük asal sayı olan 2 seçilir ve 2 nin bütün katları kırmızı renkli olup bileşik sayı olduklarından elenirler, sonrasında 2 den büyük en küçük asal sayı 3 seçilir ve 3 ün katları da mavi renkte olup bileşik sayı olduklarından elenirler. Bu işlemler karesi 80 i geçmeyen asallar (yani, $(p \leq \sqrt{n})$) için teker teker denenir ve geriye kalan siyah renkteki sayılar asaldır. Dolayısıyla $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79$ sayıları 80 den küçük asal sayılardır.

	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

Tablo 1.3

Belirli bir sayıya kadar olan bütün asal sayıları bulduran bu yöntem, sayı büyüdükçe çok fazla zaman alır. Bu yüzden büyük asallar için kullanışlı değildir. Tablodan da görüleceği gibi 2 ve 5 i dahil etmezsek, ikinci, dördüncü, beşinci, altıncı, sekizinci ve onuncu sütunlarda asal sayı yoktur. Dolayısıyla 2 ve 5 dışındaki bütün asallar birinci, üçüncü, yedinci ve dokuzuncu sütunlarda bulunur. Buradan ise 2 ve 5 dışındaki bütün asallar $10k + 1$, $10k + 3$, $10k + 7$ ve $10k + 9$ formundadır. Buradan da aşağıda ifadesini vereceğimiz teoremin bir özel halinden bahsedebiliriz. Yani $10k + 1, 10k + 3, 10k + 7$ ve $10k + 9$ tipinde sonsuz sayıda asal sayı vardır.

2.22. Teorem. (Dirichlet) a ve b ikisi de pozitif ve $(a,b) = 1$ olan iki tamsayı olmak üzere $an + b$ biçiminde sonsuz sayıda asal sayı vardır.

2.23. Sonuç. $4k + 3$ biçiminde sonsuz çoklukta asal vardır.

2.24. Sonuç. $4k + 1$ tipinde sonsuz sayıda asal sayı vardır.

2.3. Bazı Asal Sayı Test Algoritmaları

Asal sayıların elde edilmesinde veya tahmininde asal sayı test algoritmaları çok önemli bir yere sahiptir ve bu nedenle bu algoritmaları çalışmak oldukça popülerdir. Burada bir takım asal sayı test algoritmaları [23], [24], [25], [26], [27], [28], [29], [30] kaynakları kullanılarak ifade edilmiş ve bunlardan bazıları açıklanmıştır.

Asallık testleri bir sayının asal olup olmadığını kanıtlama sürecidir. Asallık testi için kullanılan ilk algoritmanın Eratosthenes Kalburu olduğu bilinmektedir. Eratosthenes Kalburu belli bir sayıya kadar olan asal sayıları kesin olarak buldurur fakat sayı büyüdükçe algoritmanın çalışması yavaşladığından bu algoritma büyük asalları bulmakta kullanışlı değildir. 17. Yüzyıldan sonra Fermat'ın Küçük Teoremi, büyük asalları bulmakta kullanışlı asallık testleri için bir çıkış noktası olmuştur.
Asal sayı test algoritmaları, sayının asal olduğunu kanıtlayan ya da büyük olasılıkla asal olduğunu belirleyen algoritmalardır. Bir asal sayı test algoritması ile sayının asal olduğu matematiksel olarak ispatlanıyorsa buna kesin (deterministik) asallık testi denir, eğer sayının asal olduğu muhtemel olarak çıkıyorsa bu tür algoritmalara da olasılıklı (olası) asallık testi denir.

2.3.1. Kesin (Deterministik) Asallık Testleri

Kesin asallık testleriyle bir sayının asal olup olmadığını kesin olarak belirlemek mümkündür. Bu tür yöntemler genellikle çarpanlara ayırmaya dayanmaktadır. Bu yüzden büyük sayılar için kullanışlı değildir. Uygulamada bir hata yapma olasılığının çok yüksek olması nedeniyle kesin asallık testlerinin olası asallık testlerinden daha az

kullanışlı olabildiği bu testlerin kullanıcıları tarafından belirtilmektedir. En çok kullanılan kesin asallık testlerinden bazıları olan Cylclotomic Ring, Lucas- Lehmer ve Aks testlerini aşağıda kısaca açıklayacağız.

2.3.1.1. Lucas- Lehmer testi

Mersenne sayılarının asal olup olmadığını belirlemek için etkili bir kesin asallık testidir.

M_p asal olması için gerek ve yeter şart $S_{p-2} \equiv 0 \left(mod\, M_p\right)$ olmasıdır. Burada $S_0 = 4,\ S_1 = 14,\ S_2 = 194,\ \ldots\ , S_n = (S_{n-1})^2 - 2$ olmak üzere S_n ler Lucas sayılarıdır.

Örneğin; $p = 5$ için $M_5 = 2^5 - 1 = 31$ dir. Bu takdirde

$$S_0 = 4 \equiv 4\ (mod\ 31)$$
$$S_1 = 14 \equiv 14\ (mod\ 31)$$
$$S_2 = 194 \equiv 8 (mod\ 31)$$
$$S_{5-2} = S_3 = 37634 \equiv 0\ (mod\ 31)$$

elde edilir. Böylece M_5 Mersenne sayısının bir Mersenne asalı olduğu gösterilmiş olur.

2.3.1.2. Cyclotomic asallık testi

1980'de L. Adleman, C. Pomarence ve R. Rumely tarafından önerilmiştir ve kısa bir süre sonra 1981'de basitleştirilmiş ve daha verimli halini Lenstra tarafından verilmiştir. Daha sonra, 2008'de Rene Schoof, Lenstra'nın ilkel testinin güncellenmiş versiyonunu sunmuştur. Testin mihenk taşı cyclotomic cisim üzerinde hesaplanan Gauss veya Jacobi toplamlarının, Fermat'ın Küçük Teoremi'ne benzer bir asal kongrüans bağıntısıdır. Cyclotomic asallık testini uygulayabilmek için bu tezin konusu dışındaki cyclotomic cisimler üzerine derin bilgilere gerek vardır. Okuyucular, bu test ile ilgili ayrıntılı bilgiler için Boucher'in yüksek lisans tezini inceleyebilir [26].

2.3.1.3. AKS testi

AKS asallık testi, Manindra Agrawal, Neerj Kayal ve Nitin Saxena tarafından oluşturulmuş deterministik bir asallık testidir. Test, bir sayının polinom zaman içinde asal mı yoksa bileşik sayı mı olduğunu belirler.

2.3.2. Olası Asallık Testleri

Olası asallık testleri, bir sayının yüksek olasılıkla asal olduğunu kanıtlama sürecidir. Kesin asallık testlerine göre daha hızlı olduğu ve gerçekte bir sayının asal olup olmadığını küçük hata payları ile hesaplayabildiği için olası asallık testleri daha çok tercih edilir. 2^{-100} den daha küçük bir hata payı ile bir sayının asal olduğu belirlenebilir ve bu testlerde hata oranının 2^{-100} ü geçmemesi aranan bir ölçüttür.

2.3.2.1. Fermat testi

Fermat'ın Küçük Teoremi, eğer $n \in \mathbb{P}$ ve $(a,n) = 1$ ise $a^{n-1} \equiv 1\ (mod\ n)$ dir. Dolayısıyla da $a^n \equiv a\ (mod\ n)$ dir. Ancak teoremin tersi olan " $(a,n) = 1$ ise $a^{n-1} \equiv 1\ (mod\ n)$ ise $p \in \mathbb{P}$ dir." ifadesi her zaman doğru değildir. Örneğin; $n = 341$ için $a = 2$ seçelirse $2^{341} \equiv 1\ (mod\ 341)$ dir fakat $341 = 11 \times 31$ olduğundan bileşiktir. Aynı şekilde $n = 561$ için $a = 2$ seçelirse $2^{561} \equiv 1\ (mod\ 561)$ dir fakat $561 = 3 \times 11 \times 17$ olduğundan bileşiktir.

Gerçekten de çok sayıda $(n,a) = 1$ olacak şekilde n bileşik sayısı $a^{n-1} \equiv 1\ (mod\ n)$ kongrüansını sağlar. Böyle n bileşik tam sayılarına **Carmichael sayısı** denir. $10000 = 10^4$ tam sayısından küçük 7 tane Carmichael sayısı vardır. 10^{17} sayısından küçük 585355 tane Carmichael sayısı vardır.

Fermat'ın Küçük Teoremi'nin karşıt tersi, eğer $a^{n-1} \not\equiv 1\ (mod\ n)$ ise $(a,n) = 1$ ve $n \notin \mathbb{P}$ dir. Bu yeni ifade kullanılarak bir sayının bileşik olduğu ispatlanabilir. Fermat'ın Küçük Teoremi'nin karşıt tersinin çalışma yöntemi şöyledir:

1. n sayısını tanımla.
2. $(a,n) = 1$ olacak şekilde bir a sayısı seç.
3. $a^{n-1} \equiv ?\ (mod\ n)$ yi hesapla.

4. Eğer $a^{n-1} \equiv 1 \ (mod\ n)$ ise n olası asaldır. 2,3 ve 4 adımlarını farklı a sayıları için tekrarlayın. Her tekrarlamayla n nin asal olma ihtimali artar.
5. Eğer $a^{n-1} \not\equiv 1 \ (mod\ n)$ ise n kesinlikle asal değildir.

Eğer seçtiğimiz n sayısı Carmichael sayısı olursa Fermat testi başarısız olur. 100 veya daha fazla basamaklı sayılardan rastgele seçilen tek bir sayının Carmichael sayısı olma ihtimali o kadar düşüktür ki bu ihtimal sıfır kabul edilebilir. Bu nedenle, Fermat testi, sayının Carmichael sayısı olmama koşuluyla güvenilir bir testtir. Bu durumda dördüncü adımın kaç kez tekrar edileceğine bakılmaksızın test, n nin olası bir asal olduğu sonucuna varacaktır.

Örnek verecek olursak,

1. $n = 5$
2. $a = 2,\ (a,n) = 1$
3. $2^4 = 16 \equiv 1 \ (mod\ 5)$
4. $2^4 \equiv 1 \ (mod\ 5)$ olduğundan 5 sayısı olası asaldır.
   $a = 3,\ (a,n) = 1$ ve $3^4 = 81 \equiv 1 \ (mod\ 5)$ olduğundan 5 sayısı olası asaldır.

2.3.2.2. Solovay& Strassen testi

Olası asallık testlerinden olan Solavay- Strassen testi, açık anahtar şifrelemelerinde kullanılan ilk olası asallık testidir. Solovay& Strassen Testi n sayısının asal olup olmadığını bulmak için Jacobi sembolü kullanılmaktadır. Bu testin yerine daha hızlı ve en az bunun kadar doğru olan Miller- Rabin testinin kullanılması önerilmektedir. Zamanla bu gibi alternatif testlerin artmasıyla tercih edilirliği azalmış olmasına rağmen yine de birçokları tarafından kullanılmaya devam edilmektedir. Aşağıda Solovay- Strassen testinde ve diğer testlerde de kullanılan Jacobi Sembolü ve Euler Kriterine kısaca değinilmiştir.

2.25. Tanım. $p > 2,\ p \in \mathbb{P},\ a \in \mathbb{Z}$ ve $(a,p) = 1$ olsun. Eğer $x^2 \equiv a \ (mod\ p)$ kongrüansının çözümü var ise, a ya $(mod\ p)$ ye göre kuadratik rezidü (KR); eğer $x^2 \equiv a \ (mod\ p)$ kongrüansının çözümü yok ise, a ya $(mod\ p)$ ye göre kuadratik non-rezidü (KNR) denir.

2.26. Tanım. $p > 2$, $p \in \mathbb{P}$, $a \in \mathbb{Z}$ ve $(a,p) = 1$ olsun. $\left(\frac{a}{p}\right)$ sembolüne Legendre Sembolü denir. $\left(\frac{a}{p}\right) = \begin{cases} 1, a\ (mod\ n) ye\ göre\ KR \\ -1, a\ (mod\ n) ye\ göre\ KNR \end{cases}$ dir.

2.27. Tanım. n herhangi bir tek tam sayı olmak üzere $\left(\frac{a}{n}\right)$ ifadesine Jacobi Sembolü denir. Eğer $n = {p_1}^{a_1}.{p_2}^{a_2} \dots {p_k}^{a_k}$, $\forall i \in \{1,2,\dots,k\}$ için $p_i \in \mathbb{P}$ ise $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{a_1}.\left(\frac{a}{p_2}\right)^{a_2} \dots \left(\frac{a}{p_k}\right)^{a_k}$ dır.

2.27. Teorem. (Euler Kriteri) n tek asal sayı olsun. $(a,n) = 1$ olacak şekildeki bütün $a \in \mathbb{Z}$ için $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right)\ (mod\ n)$ dir.

2.28. Tanım. n bileşik tek tam sayı ve $a, 1 \leq a \leq n-1$ olacak şekilde tam sayı olsun. Eğer $(a,n) > 1$ ya da $a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right)\ (mod\ n)$ ise a ya n için Euler tanığı (witness) denir. Eğer $(a,n) = 1$ ve $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right)\ (mod\ n)$ ise n ye a tabanında Euler sahte asalı denir. Yani, n bileşik sayısı Euler Kriteri'ni sağlayıp bir asal sayı gibi davranır. Burada a sayısına Euler yalancısı denir.

Örnek: $91 = 7 \times 13$ sayısı 9 tabanında Euler sahte asalıdır. $9^{45} \equiv 1\ (mod\ 91)$ dir. Ayrıca $\left(\frac{9}{91}\right) = 1$ dir.

2.29. Lemma. n bileşik tek tam sayı ve $a, 1 \leq a \leq n-1$ olacak şekilde tam sayı olsun. a sayılarından en fazla $\frac{\varphi(n)}{2}$ tanesi n için Euler yalancısıdır. Burada $\varphi(n)$, Euler phi fonksiyonudur.

Algoritma aşağıda anlatıldığı gibi çalışmaktadır.

Test edilecek $n > 2$ tek sayısı ve güvenlik parametresi t seçilir. Sonuç olarak n asal mı? sorusuna olası asaldır ya da bileşiktir cevabını verir. t denemeden sonra n için Euler tanığı bulunmazsa n nin asal olma olasılığı $\left(1 - \frac{1}{2^t}\right)$ den daha büyüktür.

1. Rastgele bir $2 \leq a \leq n-2$ olacak şekilde a tam sayısı seç.
2. $a^{\frac{n-1}{2}} \equiv r\ (mod\ n)$ yi hesapla.

3. Eğer $r \neq 1$ veya $r \neq -1$ ise n bileşiktir.
4. $s = \left(\frac{a}{n}\right)$ yi hesapla.
5. Eğer $r \not\equiv s \ (mod\ n)$ ise n bileşiktir.
6. n olası asaldır.

Eğer algoritma n yi bileşik olarak çıktı veriyorsa o zaman n kesinlikle bileşiktir, çünkü asal sayılar Euler Kriteri'ni sağlamak zorundadır.

Algoritmayı $n = 7$ için çalıştıralım:

1. $a = 2$ olsun.
2. $2^3 \equiv 1 \ (mod\ 7)$
3. $r = 1$ olduğundan algoritmaya devam et.
4. $s = \left(\frac{2}{7}\right) = 1$
5. $1 \equiv 1 \ (mod\ 7)$ olduğundan algoritmaya devam et.
6. $a = 3$ olsun.
7. $3^3 \equiv -1 \ (mod\ 7)$
8. $r = -1$ olduğundan algoritmaya devam et.
9. $s = \left(\frac{3}{7}\right) = -1$
10. $-1 \equiv -1 \ (mod\ 7)$ olduğundan algoritmaya devam et.
11. $a = 4$ olsun.
12. $4^3 \equiv 1 \ (mod\ 7)$
13. $r = 1$ olduğundan algoritmaya devam et.
14. $s = \left(\frac{4}{7}\right) = 1$
15. $1 \equiv 1 \ (mod\ 7)$ olduğundan algoritmaya devam et.
16. $a = 5$ olsun.
17. $5^3 \equiv -1 \ (mod\ 7)$
18. $r = -1$ olduğundan algoritmaya devam et.
19. $s = \left(\frac{5}{7}\right) = -1$
20. $-1 \equiv -1 \ (mod\ 7)$ olduğundan algoritmaya devam et.
21. $n = 7$ olası asaldır.

Algoritmayı $n = 91$ için algoritmayı çalıştıralım:

1. $a = 9$ olsun.

2. $9^{45} \equiv 1\ (mod\ 91)$
3. $r = 1$ olduğundan algoritmaya devam et.
4. $s = \left(\frac{9}{91}\right) = 1$
5. $1 \equiv 1\ (mod\ 7)$ olduğundan algoritmaya devam et.
6. $2^{45} \equiv 57\ (mod\ 7)$
7. $r \neq 1$ veya $r \neq -1$ olduğundan $n = 91$ bileşiktir.

2.3.2.3. Lehmann testi

1982'de D.J. Lehmann tarafından oluşturulan Lehmann testi, Fermat'ın Küçük Teoremi'ne dayanmaktadır.

$n \in \mathbb{P}$ için $(a,n) = 1$ olmak üzere $a^{n-1} - 1 \equiv 0\ (mod\ n)$ dir. Burada iki kare farkı özdeşliğini kullanırsak $(a^{\frac{n-1}{2}} - 1)(a^{\frac{n-1}{2}} + 1) \equiv 0\ (mod\ n)$ elde edilir. Bu düşünceden hareketle Lehmann testi aşağıdaki şekilde özetlenmiştir. Lehmann testine göre bir $n > 2$ tek tam sayısının asallığını araştırmak için; $1 \leq a < n$ olacak şekilde rastgele bir a tam sayısı seçilir. Seçilen a sayısına göre $a^{\frac{n-1}{2}} \equiv c\ (mod\ n)$ kongrüansı hesaplanır. Eğer c sayısı 1 ve -1 den farklı ise bu durumda n bileşik bir sayıdır. Aksi durumda, yani c sayısı 1 veya -1 e eşit ise bu c sayısı, $c = c_1$ şeklinde bir dizinin terimi olarak yazılır. İkinci adım olarak farklı bir rastgele a sayısı seçilir ve aynı işlemler sonucunda oluşan c, $c = c_2$ olarak yazılır. Bu adımlar k kez tekrar edilirse $(c_1, c_2, c_3, \dots, c_k)$ dizisi elde edilir. Eğer bütün $c_i, i \in \{1,2,,\dots k\}$, değerleri 1 veya -1 ise fakat yalnız 1 veya yalnız -1 değilse n, $1 - \left(\frac{1}{2}\right)^k$ olasılıkla asal kabul edilir.

2.30. Örnek. $n = 11$ için 11 in asallığını araştıralım.

$1 \leq a \leq 10$ ve $(a,11) = 1$ olacak şekilde a tam sayısı seçelim. $a = 1$ için $1^5 \equiv 1\ (mod\ 11)$ olduğundan $c_1 = 1$ dir. $a = 2$ için $2^5 \equiv -1\ (mod\ 11)$ olduğundan $c_2 = -1$ dir. $a = 3$ için $3^5 \equiv 1\ (mod\ 11)$ olduğundan $c_3 = 1$ dir. $a = 4$ için $4^5 \equiv 1\ (mod\ 11)$ olduğundan $c_4 = 1$ dir. $a = 5$ için $5^5 \equiv 1\ (mod\ 11)$ olduğundan $c_5 = 1$ dir. $a = 6$ için $6^5 \equiv -1\ (mod\ 11)$ olduğundan $c_6 = -1$ dir. $a = 7$ için

$7^5 \equiv -1\ (mod\ 11)$ olduğundan $c_7 = -1$ dir. $a = 8$ için $8^5 \equiv -1\ (mod\ 11)$ olduğundan $c_8 = -1$ dir. $a = 9$ için $9^5 \equiv 1\ (mod\ 11)$ olduğundan $c_9 = 1$ dir. $a = 10$ için $10^5 \equiv -1\ (mod\ 11)$ olduğundan $c_{10} = -1$ dir. Dolayısıyla $i \in \{1, 2, \dots, 10\}$ için c_i değerleri 1 veya -1 ve fakat yalnız 1 veya yalnız -1 olmadığından $n = 11$, $1 - \left(\frac{1}{2}\right)^{10} \cong 0{,}9990234375$ olasılıkla asaldır.

2.3.2.4. Miller- Rabin testi

1976'da Gary L. Miller tarafından başlangıçta deterministik asallık testi olarak oluşturulmuştur. 1980'de Michael O. Rabin deterministik olmayan yeni bir sürüm olarak tasarlamıştır. En çok kullanılan olası asallık testidir. Test aşağıdaki gerçeğe dayanmaktadır. n tek tamsayı ve a tamsayı olmak üzere $(a, n) = 1$ olsun. $n - 1 = r.2^s$ olacak şekilde r tek tam sayı ve s tam sayı olmak üzere;

$$\begin{aligned} a^{n-1} - 1 = a^{r2^s} - 1 &= \left(a^{r2^{s-1}} - 1\right)\left(a^{r2^{s-1}} + 1\right) \\ &= \left(a^{r2^{s-2}} - 1\right)\left(a^{r2^{s-2}} + 1\right)\left(a^{r2^{s-1}} + 1\right) \\ &= \left(a^{r2^{s-3}} - 1\right)\left(a^{r2^{s-2}} + 1\right)\left(a^{r2^{s-1}} + 1\right) \\ &\vdots \\ &= (a^r - 1)(a^r + 1)(a^{2r} + 1)(a^{4r} + 1) \dots \left(a^{r2^{s-1}} + 1\right) \end{aligned}$$

dir.

Eğer n asal ise Fermat'ın Küçük Teoremi'ni kullanarak $a^{n-1} - 1 = a^{r2^s} - 1 = (a^r - 1)(a^r + 1)(a^{2r} + 1)(a^{4r} + 1) \dots \left(a^{r2^{s-1}} + 1\right) \equiv 0\ (mod\ n)$ dir. Böylece n asal olduğunda çarpanlardan biri $(mod\ n)$ de 0 olmalıdır. Bu yüzden $a^r \equiv 1\ (mod\ n)$ veya $a^{r2^j} \equiv -1\ (mod\ n)$, $j \in \{0,1,2, \dots\ s - 1\}$ dir.

Eğer çarpanlardan hiçbiri $(mod\ n)$ de 0 a eşit değil ise $(mod\ n)$ de n nin asal olmadığı kesin olarak bilinir. Ancak en az biri 0 a eşit çıkarsa, n nin asal olduğu kesin olarak söylenemez ve bu durumda n nin asal olduğunun doğruluğunu artırmak için a nın başka değerleri de kontrol edilmelidir.

2.31. Tanım. n, tek bileşik sayı ve r tek sayı olmak üzere $n - 1 = r.2^s$ olsun. $a \in \{1,2, \dots, n - 1\}$ olmak üzere $(a, n) = 1$ şartıyla eğer $a^r \not\equiv 1\ (mod\ n)$ ve

$a^{r2^j} \not\equiv -1 \ (mod\ n),\ \forall j \in \{0,1,2,\dots,s-1\}$ ise a ya n nin **güçlü tanığı** denir. Diğer durumda, kongrüanslardan en az biri bu şartlar altında sağlanırsa a ya n için **güçlü yalancı**, n ye de a tabanında **güçlü sahte asal** denir.

2.32. Örnek. $n = 91$ için $n - 1 = 90 = 2.45$ tir. Bu durumda $r = 45$ ve $s = 1$ olur. $a = 9$ seçilirse $(9,91) = 1$ dir ve $9^{45} \equiv 1 \ (mod\ 91)$ olduğundan 91, 9 tabanında güçlü sahte asaldır.

a nın n için güçlü yalancı olma olasılığı en fazla $\frac{1}{4}$ tür. Farklı a sayıları için güçlü yalancı olma olaslığı $\frac{1}{4^k}$ dır. Burada k, n için test edilen a tam sayıların sayısını gösterir ve bu nedenle testin doğruluğunu kontrol eder.

Miller- Rabin olası asallık test algoritmasını şu şekilde özetleyebiliriz:

1. $n \geq 3$ olacak şekilde bir n tek sayısı seç.
2. n yi, r tek tam sayı ve s tam sayı olmak üzere $n - 1 = r.2^s$ olarak yaz.
3. $a \in \{2,3,4,\dots,n-1\}$ olmak üzere eğer $(a,n) > 1$ ise n bileşiktir. Eğer $(a,n) = 1$ ise $a^r \equiv y \ (mod\ n)$ yi hesapla. $y \neq 1$ ve $y \neq -1$ ise
4. Eğer $b = 1$ veya $b = n - 1$ ise, yani $a^r \equiv 1 \ (mod\ n)$ veya $a^r \equiv -1 \ (mod\ n)$ demektir, n olası asaldır.
5. $a^{r2^j} \equiv b_j \ (mod\ n)$ için $b_j = -1$ olup olmadığını kontrol et, eğer $b_j = 1$ ise n bileşiktir.
6. $s - 1$ kez tekrar edildikten sonra $\left(a^{r2^s} - 1\right) \not\equiv 0 \ (mod\ n)$ ise n bileşiktir.

2.33. Örnek. Miller- Rabin testini kullanarak $n = 247$ nin asal olup olmadığını kontrol edelim:

$n - 1 = 246 = 2^1.213$ böylece $r = 213$ ve $s = 1$ olur. Şimdi 247 nin asallığını test edebilmek için $a \in \{1,2,3,\dots 246\}$ olacak şekilde $(a,247) = 1$ şartını sağlayan a sayısı seçeceğiz. Eğer $(a,247) \neq 1$ ise 247 bileşiktir.

$a = 68$ için $(68,247 = 1$ dir. $68^{213} \equiv 1 \ (mod\ 247)$ olduğundan 247 olası asaldır ya da güçlü sahte asaldır ve $a = 68$ güçlü yalancıdır.

$a = 75$ için $(75,247 = 1$ dir. $75^{213} \equiv -1 \ (mod\ 247)$ olduğundan 247 olası asaldır ya da güçlü sahte asaldır ve $a = 75$ güçlü yalancıdır.

$a = 105$ için $(105, 247 = 1$ dir. $105^{213} \not\equiv \pm 1\ (mod\ 247)$ olduğundan 247 bileşiktir ve $a = 105$ sayısı 247 için güçlü tanıktır.

247 nin güçlü yalancılarının kümesi; $\{1, 12, 56, 68, 69, 75, 87, 88, 103, 144, 159, 160, 172, 178, 179, 191, 235, 246\}$ tır. Eğer a, n için güçlü yalancı ise ve $(n - a)$ da güçlü yalancıdır.

2.34. Örnek. Miller- Rabin testini kullanarak $n = 11$ nin asal olup olmadığını kontrol edelim:

$n - 1 = 10 = 2^1.5$ böylece $r = 5$ ve $s = 1$ olur. Şimdi 11 in asallığını test edebilmek için $a \in \{1, 2, 3, \ldots 10\}$ olacak şekilde $(a, 11) = 1$ şartını sağlayan a sayısı seçeceğiz. Eğer $(a, 11) \neq 1$ ise 10 bileşiktir.

$a = 1$ için $(1,11) = 1$ ve $1^5 \equiv 1\ (mod 11)$ olduğundan 11 olası asaldır.

$a = 2$ için $(2,11) = 1$ ve $2^5 \equiv -1\ (mod 11)$ olduğundan 11 olası asaldır.

$a = 3$ için $(3,11) = 1$ ve $3^5 \equiv 1\ (mod 11)$ olduğundan 11 olası asaldır.

$a = 4$ için $(4,11) = 1$ ve $4^5 \equiv 1\ (mod 11)$ olduğundan 11 olası asaldır.

$a = 5$ için $(5,11) = 1$ ve $5^5 \equiv 1\ (mod 11)$ olduğundan 11 olası asaldır.

$a = 6$ için $(6,11) = 1$ ve $6^5 \equiv -1\ (mod 11)$ olduğundan 11 olası asaldır.

$a = 7$ için $(7,11) = 1$ ve $7^5 \equiv -1\ (mod 11)$ olduğundan 11 olası asaldır.

$a = 8$ için $(8,11) = 1$ ve $8^5 \equiv -1\ (mod 11)$ olduğundan 11 olası asaldır.

$a = 9$ için $(9,11) = 1$ ve $9^5 \equiv 1\ (mod 11)$ olduğundan 11 olası asaldır.

$a = 10$ için $(10,11) = 1$ ve $10^5 \equiv -1\ (mod 11)$ olduğundan 11 olası asaldır.

O halde $n = 11$ sayısı $1 - \left(\frac{1}{4}\right)^{10}$ olasılıkla asaldır.

2.4. Asal Sayıların Dağılımı

2.35. Teorem. Ardışık iki asal sayı arasındaki boşluk istenildiği kadar büyük yapılabilir. Başka bir deyişle her $k \geq 1$ için k ardışık bileşik tam sayı vardır.

İspat. $k \geq 1$ bir tam sayı olsun. O zaman $(k+1)! + 2, (k+1)! + 3, \ldots, (k+1)! + (k+1)$ sayıları k ardışık tam sayılardır ve her $2 \leq i \leq k+1$ için, $i|[(k+1)! + i]$ olduğundan $(k+1)! + i$ bir bileşik tam sayıdır.

Bu teorem asal sayıların $\mathbb{Z}^+$ da dağılımının düzensiz olduğunu gösterir.

2.36. Örnek.

$k = 3$ için $(3+1)!+2, (3+1)!+3, (3+1)!+4$

$$= 24+2, \quad 24+3, \quad 24+4$$

$$= 26, \quad 27, \quad 28$$

$k = 5$ için $(5+1)!+2, (5+1)!+3, (5+1)!+4, (5+1)!+5, (5+1)!+6$

$$= 722, 723, 724, 725, 726$$

2.37. Tanım. $x \in \mathbb{R}$ olmak üzere x ten büyük olmayan asal sayıların sayısı $\pi(x)$ ile gösterilir. Böylece $\pi(x) = |\{p: p \in \mathbb{P} \; ve \; p \leq x\}|$ tir.

Örneğin, $x < 2$ iken $\pi(x) = 0$ dır. Ayrıca $\pi(2) = 1$, $\pi(3) = 2$, $\pi(6) = 3$, $\pi(10) =$ 4 tür.

2.38. Teorem. (Asal Sayı Teoremi)

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1$$

dir.

n	$\pi(n)$	$\frac{\pi(n)}{n}$	$\frac{\pi(n)}{n}\log n$
10	4	0,400	0,921
100	25	0,250	1,151
500	95	0,190	1,181
1000	168	0,168	1,161
10000	1229	0,123	1,132
10^5	1592	0,096	1,105
10^6	78418	0,078	1,078
10^7	664579	0,066	1,064
10^8	5761455	0,058	1,068
10^9	50847534	0,051	1,057

Tablo 1.4 [4]

Tabloda görüldüğü gibi $\frac{\pi(x)}{x/\log x}$ kesrinde x değeri arttıkça bu kesrin değeri 1 e yaklaştığı görülmektedir.

2.39. Teorem. (Chebychef) Öyle $a, b \in \mathbb{R}^+$ vardır ki her $x \geq 2, x \in \mathbb{R}$ için

$$a\frac{x}{\log x} < \pi(x) < b\frac{x}{\log x}$$

tir.

2.40. Teorem. $\forall x \geq 2, x \in \mathbb{R}$ için $\prod_{p \leq x} p < 4^x$ tir.

2.41. Teorem. (Bertrand Postulatı) $\forall n > 1, n \in \mathbb{Z}$ için $n < p < 2n$ olacak biçimde bir $p \in \mathbb{P}$ vardır.

2.5. Asal Sayılarla İlgili Bazı Güncel Makaleler

Bu bölümde bu tezin bulgularının elde edilmesinde yararlı olan asal sayılarla ilgili bazı güncel makaleler ayrıntılı olarak incelenmiştir.

2.5.1. $2m$- asal çiftlerini elemek (Sieving $2m$-prime pairs [31])

Bu çalışmada Lampret, p bir asal sayı ve m bir pozitif tam sayı olmak üzere $(p, p + 2m)$ formundaki bir asallar çiftini $2m$-asal çifti olarak tanımlamış ve $2m$-asal çiftlerinin (özel olarak ikiz asal çiftlerinin) yeni bir karakterizasyonunu elde etmiştir. $m = 1$ için 2-asal çiftleri ikiz asallardır. $m = 2$ için 4-asal çiftleri kuzen asal çiftleri olarak bilinir: $(3,7), (7,11), (13,17), \ldots$ $m = 3$ için 6-asal çiftleri: $(5,11), (7,13), (11,17), \ldots$ $m = 4$ için 8-asal çiftleri: $(3,11), (5,13), (11,19), \ldots$ Böylece ikiz asal çiftlerini $2m$-asal çiftlerin özel bir durumu olarak düşünebiliriz ve ikiz asalların sonsuz çoklukta olduğu sanısı tüm $2m$-asal çiftleri için genelleştirilebilir.

Lampret çalışmasının ilk bölümünde verilen bir tam sayıya kadar olan ikiz asal çiftlerini bulduran temel bir metot sunmuştur. Bu metot aşağıdaki sonuçlara dayanır.

2.42. Lemma. p bir asal sayı olmak üzere eğer $p = 6j + 1$ veya $p = 6j - 1$ ise her $i \geq 1$ için $(6(pi + j) - 1, 6(pi + j) + 1)$ ve $(6(pi - j) - 1, 6(pi - j) + 1)$ ikiz asal çifti değildir.

2.43. Teorem. k pozitif bir tam sayı olmak üzere $(6k-1, 6k+1)$ ikiz asal çifti değildir ancak ve ancak $6j \pm 1$ formunda bir $p \leq \sqrt{6k+1}$ asalı ve $k = pi + j$ veya $k = pi - j$ olacak şekilde bir pozitif i tam sayısı mevcuttur.

Lampret metoduyla verilen bir tam sayıya kadar olan ikiz asal çiftlerini bulduran bir kalbur elde etmiştir. Lampret yukarıdaki sonuçları $2m$-asal çiftleri için genelleştirmiştir. Lampret'in sonucu, verilen bir tam sayıya kadar olan $2m$-asal çiftlerini (örneğin ikiz asal çiftlerini) bulduran temel bir metot sağlamaktadır. Bu metot ikiz asal kalburuna benzer olarak yapılır. Lampret, öncelikle 3 asalı dışındaki tüm $2m$-asal çiftlerini dört gruba ayırmıştır:

(i). $(6n-4)$-asal çiftleri: Birinci bileşeni 6 modülüne göre -1 ve ikinci bileşeni 1 e denk olan çiftlerdir, yani n ve k pozitif tam sayıları için $(6k-1, 6k+6n-5)$ formundaki asal çiftleri bu gruptadır.

(ii). $(6n-2)$-asal çiftleri: Birinci bileşeni 6 modülüne göre 1 ve ikinci bileşeni -1 e denk olan çiftlerdir, yani n ve k pozitif tam sayıları için $(6k+1, 6k+6n-1)$ formundaki asal çiftleri bu gruptadır.

(iii). Her iki bileşeni de 6 modülüne göre -1 e denk olan $6n$-asal çiftleri: n ve k pozitif tam sayıları için $(6k-1, 6k+6n-1)$ formundaki asal çiftleri bu gruptadır.

(iv). Her iki bileşeni de 6 modülüne göre 1 e denk olan $6n$-asal çiftleri: n ve k pozitif tam sayıları için $(6k+1, 6k+6n+1)$ formundaki asal çiftleri bu gruptadır.

Lampret, $2m$-asal çiftleri kalburu için aşağıdaki sonuçları vermiştir. 2.42. Lemma nın genellemesi olarak aşağıdaki lemmayı vermiştir.

2.44. Lemma. n bir pozitif tam sayı olmak üzere, $p = 6j-1$ asal ise her $i \geq 1$ için $(6(pi+j)-1, 6(pi+j)+6n-5)$ ve
$(6(pi-j-n+1)-1, 6(pi-j-n+1)+6n-5)$ çiftleri $(6n-4)$-asal çifti değildir.
$p = 6j+1$ asal ise her $i \geq 1$ için $(6(pi-j)-1, 6(pi-j)+6n-5)$ ve
$(6(pi+j-n+1)-1, 6(pi+j-n+1)+6n-5)$ çiftleri $(6n-4)$-asal çifti değildir.

2.45. Lemma. k bir pozitif tam sayı olmak üzere, $6k-1$ sayısı asal değilken i ve j pozitif tam sayıları için aşağıdaki denkliklerden biri sağlanır:

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

(ii). $p := 6j+1$ asaldır ve $k = pi - j$ dir.

Her iki durumda da her n pozitif tam sayısı için $p \leq \sqrt{6k-1}$ ve dolayısıyla $p \leq \sqrt{6k+6n-5}$ dir.

2.46. Lemma. k ve n pozitif tam sayılar olmak üzere, $6k+6n-5$ asal değilken i ve j pozitif tam sayıları için aşağıdaki denkliklerden biri sağlanır:

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

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

Her iki durumda da $p \leq \sqrt{6k+6n-5}$ dir.

2.47. Teorem. k ve n pozitif tam sayılar olmak üzere; $(6k-1, 6k+6n-5)$, $(6n-4)$-asal çifti değildir ancak ve ancak i ve j pozitif tam sayıları için aşağıdaki denkliklerden biri doğrudur:

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

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

Her iki durumda da $p \leq \sqrt{6k+6n-5}$ dir.

2.48. Teorem. k ve n pozitif tam sayılar olmak üzere; $(6k+1, 6k+6n-1)$, $(6n-2)$-asal çifti değildir ancak ve ancak i ve j pozitif tam sayıları için aşağıdaki denkliklerden biri doğrudur:

(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.

Her iki durumda da $p \leq \sqrt{6k+6n-1}$ dir.

2.49. Teorem. k ve n pozitif tam sayılar olmak üzere; $(6k-1, 6k+6n-1)$, $(6n)$-asal çifti değildir ancak ve ancak i ve j pozitif tam sayıları için aşağıdaki denkliklerden biri doğrudur:

(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.

Her iki durumda da $p \leq \sqrt{6k + 6n - 1}$ dir.

2.50. Teorem. k ve n pozitif tam sayılar olmak üzere; $(6k + 1, 6k + 6n + 1)$, $(6n)$-asal çifti değildir ancak ve ancak i ve j pozitif tam sayıları için aşağıdaki denkliklerden biri doğrudur:

(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.

Her iki durumda da $p \leq \sqrt{6k + 6n + 1}$ dir.

2.5.2. İkiz asallar üzerine bir not (A note on the twin primes [32])

1949'da Clement ikiz asallarla ilgili bir teorem ispatlamıştır. Bu makalede Ibrahima Gueye, Wilson ve Clement teoremlerini kullanarak, "$n + 2$ ve $n + 4$ sayıları asaldır ancak ve ancak $(n + 2)(n + 4) | n(n + 1)! - 2$ dir." sonucunu ispatlamıştır.

2.5.3. İkiz asallar üzerine açıklama (Remark on twin primes [33])

Clement'in ikiz asallarla ilgili teoremi, $n + 2$ ve $n + 4$ sayıları asaldır ancak ve ancak $(n + 2)(n + 4) | 4[(n + 1)! + 1] + n + 2$ dir. I.Gueye, $n + 2$ ve $n + 4$ sayıları asaldır ancak ve ancak $(n + 2)(n + 4) | n(n + 1)! - 2$ dir, sonucunu ispatlamıştır. Bu çalışmada J.Sandor, bu sonucun basit bir ispatını vermiştir.

BÖLÜM 3. ARAŞTIRMA BULGULARI

Bu bölümde, Bölüm 2'de ayrıntılı olarak incelenen ikiz asallarla ilgili makalelerin ışığında aşağıdaki problemlere yanıtlar verilmiştir:

Problem 1: Lampret'in çalışmasından esinlenerek Lampret'in ikiz asal çiftlerini bulduğu gibi Sophie Germain ve ilgili güvenli asal çiftlerini bulmak için bir kalbur elde edilebilir mi?

Problem 2: Clement'in ikiz asallarla ilgili Bölüm 2'de ifade edilen teoreminden ilham alınarak, Sophie German asallarının bir karakterizasyonu elde edilebilir mi?

3.1. Sophie Germain Asallarını Elemek

Bu kısımda Problem 1 ele alınmıştır. Lampret'in ikiz asallarla ilgili "Sieving $2m$-prime pairs" çalışmasından esinlenerek Sophie Germain ve ilgili güvenli asal çiftlerini bulmak için temel bir metot olarak bir elek elde edilecektir.

p asal iken $2p + 1$ de asal oluyorsa, p ye Sophie Germain asalı denir. Eğer p Sophie Germain asalı ise $2p + 1$ asalına güvenli asal denir. Sophie Germain, 1825'lerde, Sophie Germain asalları için Fermat'ın Son Teoremi'nin ilk durumunun doğru olduğunu göstermiştir. Yukarıda adı geçen çalışmasında, Lampret, m keyfi pozitif tam sayı olmak üzere $2m$-asal çiftlerini bulduran bir elek vermiştir. Lampret, bütün $2m$-asal çiftlerini dört gruba ayırmıştır. Bunlardan birisi, çiftin her iki bileşeni de mod 6 da -1 e kongrüent olan $6n$-asal çiftleridir. n ve k pozitif tam sayılar olmak üzere $6n$-asal çiftleri, $(6k - 1, 6k + 6n - 1)$ şeklindedir. Lampret, $(6k - 1, 6k + 6n - 1)$ formundaki $6n$-asal çiftlerinin bir karakterizasyonunu vermiştir.

Bu çalışmada, bir Sophie Germain asalı ve ilgili güvenli asal çifti *SG-S*-asal çifti olarak adlandırılacaktır.

3.1.1. Lampret'in sonucunu kullanarak *SG-S*-asal çiftlerini bulduran bir metot:

2 ve 3 dışındaki bütün asal sayılar, bir pozitif k tam sayısı için $6k-1$ ya da $6k+1$ formundadır. Eğer p asalı $6k+1$ formunda ise $2p+1$ asal olmadığından p bir Sophie Germain asalı değildir. Dolayısıyla $(6k+1, 12k+3)$ *SG-S*-asal çifti değildir. Böylece, *SG-S*-asal çiftleri bir pozitif k tam sayısı için $(6k-1, 12k-1)$ formundadır. Böylece $(12k-1)-(6k-1)=6k$ olduğundan *SG-S*-asal çiftleri Lampret'in $2m$-asal çiftleri sonucuna dönüşür, burada bir pozitif k tam sayısı için $2m=6k$ dır.

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 çiftlerini bulduran metot aşağıdaki gibidir.

1. $k = 1,2,\ldots,\left\lceil\frac{z}{6}\right\rceil$ tam sayıları listelenir.
2. $3 < p \leq \sqrt{z}$ olacak şekilde asallar bulunur.
3. Bulunan her bir $3 < p \leq \sqrt{z}$ asalları için;

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

Listede kalan her k tam sayısı, $(6k-1, 12k-1)$ *SG-S*-asal çiftlerini verir.

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

(i). $p = 5 = 6.1-1$ olduğundan $j=1$ dir ve dolayısıyla $k=5i+1$ ve $k=\frac{5i+1}{2}$ tam sayıları listeden atılır. Bu durumda listeden atılanlar $3, 6, 8, 11, 13, 16, 18, 21, 23, 26, 28, 31, 33, 36, 38, 41$ tam sayılarıdır.

(ii). $p = 7 = 6.1 + 1$ olduğundan $j = 1$ dir ve dolayısıyla $k = 7i - 1$ ve $k = \frac{7i-1}{2}$ tam sayıları listeden atılır. Bu durumda listeden atılanlar $3, 6, 10, 13, 17, 20, 24, 27, 31, 34, 38, 41$ tam sayılarıdır.

(iii). $p = 11 = 6.2 - 1$ olduğundan $j = 2$ dir ve dolayısıyla $k = 11i + 2$ ve $k = \frac{11i+2}{2}$ tam sayıları listeden atılır. Bu durumda listeden atılanlar $12, 13, 23, 24, 34, 35$ tam sayılarıdır.

(iv). $p = 13 = 6.2 + 1$ olduğundan $j = 2$ dir ve dolayısıyla $k = 13i - 2$ ve $k = \frac{13i-2}{2}$ tam sayıları listeden atılır. Bu durumda listeden atılanlar $11, 12, 24, 25, 37, 38$ tam sayılarıdır.

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 2.1

Listede kalan her k tam sayısı 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), (191,383), (233,467), (239,479).

3.2. Sophie Germain Asallarının Bir Karakterizasyonu

Bu kısımda Problem 2 ele alınmıştır. Clement'in ikiz asallarla ilgili kongrüansına benzer olarak Sophie German asallarının bir karakterizasyonu elde edilebilir.

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

İspat. Wilson teoremini kullanarak, $p \in \mathbb{P} \Leftrightarrow (p - 1)! \equiv -1\ mod(p)$

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

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

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

dir. Aksine, $(p+1)^2[(p-1)!]^2 \equiv 1\, mod(p)$ ve $p \notin \mathbb{P}$ olsun. Böylece $1 < t < p$ olacak şekilde p nin t tam sayı böleni vardır. Diğer yandan, eğer $(p+1)^2[(p-1)!]^2 \equiv 1\, mod(p)$ ise $[(p-1)!]^2 \equiv 1\, mod(p)$ dir. Bundan dolayı $[(p-1)!]^2 \equiv 1\, mod(t)$ dir. t tam sayısı aynı zamanda $[(p-1)!]^2$ nin bir böleni olduğundan bu bir çelişkidir. O halde p asal sayıdır.

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

İspat. Wilson teoremini kullanarak, $2p+1 \in \mathbb{P} \Leftrightarrow (2p)! \equiv -1\, mod(2p+1)$ dir. Böylece

$$2p+1 \in \mathbb{P} \Leftrightarrow (2p)(2p-1)\dots(2p-p)(2p-p-1)! \equiv -1\, mod(2p+1)$$
$$\Leftrightarrow (-1)(-2)\dots(-p-1)(p-1)! \equiv -1\, mod(2p+1)$$
$$\Leftrightarrow (-1)^{p+1}.(p+1)!\,(p-1)! \equiv -1\, mod(2p+1)$$
$$\Leftrightarrow (p+1)!\,(p-1)! \equiv -1\, mod(2p+1)$$
$$\Leftrightarrow (p+1).p.(p-1)!\,(p-1)! \equiv -1\, mod(2p+1)$$
$$\Leftrightarrow (p+1).p.[(p-1)!]^2 \equiv -1\, mod(2p+1)$$
$$\Leftrightarrow (p+1).(p+p+1-p-1).[(p-1)!]^2 \equiv -1\, mod(2p+1)$$
$$\Leftrightarrow (p+1).(-p-1).[(p-1)!]^2 \equiv -1\, mod(2p+1)$$
$$\Leftrightarrow -[(p+1)]^2.[(p-1)!]^2 \equiv -1\, mod(2p+1)$$
$$\Leftrightarrow [(p+1)]^2.[(p-1)!]^2 \equiv 1\, mod(2p+1)$$

dir.

3.4. Lemma. $p > 2$ bir sayı olsun. Bu takdirde $(p+1)^2.[(p-1)!]^2 \equiv 1\, mod(2p+1)$ ise $2p+1$ 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 t tam sayı böleni vardır. Diğer yandan 3.3 Lemma. nın ispatı ile

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

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

3.5. Teorem. $p > 2$, p Sophie Germain asalıdır. $\Leftrightarrow (p+1)^2.[(p-1)!]^2 \equiv 1\ mod\big(p(2p+1)\big)$ dir.

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

Bu bölümdeki bilgiler Baştan ve Akın'ın [34] numaralı kaynakta gösterilmiş olan çalışmasında yayınlanmıştır.

BÖLÜM 4. TARTIŞMA VE SONUÇ

Bu tezde, çeşitli formdaki asal sayılar araştırılmış ve özellikle Sophie Germain asalları ile ilgili bazı sonuçlar elde edilmiştir. Ayrıca bilinen en eski asal sayı test algoritması olan Eratosthenes kalburu başta olmak üzere asal sayıları bulmada kullanılan bir takım yöntemler incelenmiştir. Asal sayıların dağılımı hakkında genel bilgiler verilmiştir.

Bu tez çalışmasında, bulgularımıza ilham veren bazı güncel makalelerin sonuçlarına yer verilmiştir. Bu makaleler ışığında üretilen problemlere çözümler getirilmiştir. SG-S-asal çiftlerini bulduran bir elek önerilerek 250 ye kadar olan SG-S-asal çiftlerini elde etmek için bu eleğin kullanıldığı bir örnek verilmiştir. Ayrıca, bu tezde Sophie Germain asallarının kongrüanslarla elde edilmiş bir karakterizasyonu yer almaktadır.

Bu tez çalışması, asal sayılarla ilgili bundan sonra yapılacak bazı çalışmalara kaynak teşkil edebilir. Bu tezin bir bölümünde değinilen asal sayı test algoritmaları daha ayrıntılı ve daha geniş bir çerçevede ele alınarak hangi testin hangi çeşit asalı bulmada daha kullanışlı olduğu araştırma konusu olarak önerilebilir. Bu tür bir çalışma özellikle Sophie Germain asalları için yapılabilir.

Bu tez çalışmasındaki bulgular, 27- 29 Haziran 2018 tarihinde Ordu Üniversitesi'nde düzenlenen ICMME-2018 konferansında bildiri olarak sunulmuş olup Turkish Journal of Mathematics and Computer Science dergisinde konferans bildirisi olarak yayınlanmıştır.

KAYNAKLAR

[1] Asar, A. O., Arıkan, A., Sayılar Teorisi, Ankara: Gazi Kitapevi, 2012.

[2] Şenay, H., Sayılar Teorisi Dersleri, Konya: Dizgi Ofset Matbaacılık, 2007.

[3] Çallıalp P. D. F., Sayıların Teorisi, İstanbul: Birsen Yayınevi, 2009.

[4] Ribenboim, P., The Little Book Of Bigger Primes, 2.Edition, New York: Springer-Verlag, 2004.

[5] Sierpinski, W., Elemantary Theory of Numbers, Editor: A. Schinzel, Warszawa: Polish Scientific Publishers, 1988.

[6] https://mathcrypto.wordpress.com/2016/10/30/pepins-primality-test/. Erişim Tarihi: 31.03.2019.

[7] Dubner, H., Large Sophie Germain Primes, Mathematics Of Computation, Cilt 65, No. 213, Pp. 393-396, 1996.

[8] Crandall, R., Dilcher, K., Pomerance, C., A Search For Wieferich And Wilson Primes, Cilt 66, No. 217, 1997.

[9] Clement, P.A., Congruences for sets of primes, American Mathematical Monthly, Cilt 56, Pp. 23-25, 1949.

[10] Sondow, J., Ramanujan Primes and Bertrand's Postulate The American Mathematical Monthly, Cilt 116, No. 7, Pp. 630-635, 2009.

[11] http://www.fermatsearch.org/news.html. Erişim Tarihi: 29.01.2019.

[12] https://primes.utm.edu/mersenne/. Erişim Tarihi: 26.02.2019.

[13] https://www.mersenne.org/. Erişim Tarihi: 29.03.2019.

[14] http://mathworld.wolfram.com/SophieGermainPrime.html. Erişim Tarihi: 02.02.

2019.

[15] https://prime-numbers.info/article/sophie-germain-primes. Erişim Tarihi: 15.03. 2019.

[16] https://www.muhendisbeyinler.net/fermatin-son-teoremi/. Erişim Tarihi: 31.03. 2019.

[17] http://sitn.hms.harvard.edu/flash/2017/2-x-prime-1-200-year-old-story-sophie-germain-21st-century-legacy/. Erişim Tarihi: 02.02.2019.

[18] https://primes.utm.edu/glossary/page.php?sort=WieferichPrime. Erişim Tarihi: 28.02.2019.

[19] http://mathworld.wolfram.com/WilsonPrime.html. erişim tarihi: 27.02.2019.

[20] http://mathworld.wolfram.com/GeneralizedFermatNumber.html. Erişim Tarihi: 27.02.2019.

[21] https://primes.utm.edu/glossary/page.php?sort=Cullens. Erişim Tarihi: 02.02. 2019.

[22] https://primes.utm.edu/top20/page.php?id=1#records. Erişim Tarihi: 30.03. 2019.

[23] Yerlikaya, T., Kara, O., Kriptolojide Kullanilan Asal Sayi Test Algoritmalari, Trakya University Journal Of Engineering Sciences, Cilt 18, No. 1, Pp. 85-94, 2017 .

[24] http://mathworld.wolfram.com/Lucas-LehmerTest.html. Erişim Tarihi: 31.03. 2019.

[25] Menezes, A. J., Oorschot, P. C. V., Vanstone, S. A., Handbook Of Applied Cryptography, Crc Press, 1996.

[26] Boucher, T. F., On Cyclotomic Primality Tests, Knoxville: A Thesis Presented For The Master Of Science Degree The University Of Tennessee, 2011.

[27] Ding, T., Primalitytesting, University Of Manchester School Of Computer Science Project Report , Manchester, 2016.

[28] https://kconrad.math.uconn.edu/blurbs/ugradnumthy/solovaystrassen.pdf. Erişim Tarihi: 31.03.2019.

[29] Bandyopadhyay, S., Primality Testing A Journey From Fermat To Aks,

Chennai: Chennai Mathematical Institute, 2017.

[30] https://kconrad.math.uconn.edu/blurbs/ugradnumthy/millerrabin.pdf. Erişim Tarihi: 31.03.2019.

[31] Lampret, S., Sieving $2m$-Prime Pairs, Notes On Number Theory And Discrete Mathematics, Cilt 20, No. 3, P. 54–60, 2014.

[32] Gueye, I., A Note On The Twin Primes, South Asian Journal Of Mathematics, Cilt 2, No. 2, Pp. 159-161, 2012.

[33] Sándor, J., Remark On Twin Primes, Notes On Number Theory And Discrete Mathematics , Cilt 20, No. 3, P. 29–30 , 2014.

[34] Baştan, R., Akın, C., Notes On Sophie Germain Primes. In International Conference On Mathematics And Mathematics Education (ICMME 2018), Turkish Journal Of Mathematics And Computer Science, No.10, P.18–21, 2018.

ÖZGEÇMİŞ

Recep Baştan 1989 yılında Trabzon'un Vakfıkebir ilçesinde doğdu. İlk, orta ve lise eğitimini Vakfıkebir'de tamamladı. 2006 yılında Vakfıkebir Lisesi'nden mezun oldu. 2011 yılında başladığı Gaziosmanpaşa Üniversitesi Matematik Bölümü'nü 2015 yılında bitirdi. 2016 yılında Giresun Üniversitesi Matematik Anabilim Dalı'nda yüksek lisans eğitimine başladı.