T.C.
VAN YÜZÜNCÜ YIL ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI

ASAL SAYI TEST ALGORİTMALARI VE KRİPTOLOJİDEKİ UYGULAMALARI ÜZERİNE

YÜKSEK LİSANS TEZİ

HAZIRLAYAN: Erol AĞÇAKAYA
DANIŞMAN: Dr. Öğr. Üyesi Turgut HANOYMAK

VAN-2020

T.C.
VAN YÜZÜNCÜ YIL ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI

ASAL SAYI TEST ALGORİTMALARI VE KRİPTOLOJİDEKİ UYGULAMALARI ÜZERİNE

YÜKSEK LİSANS TEZİ

HAZIRLAYAN: Erol AĞÇAKAYA

VAN-2020

KABUL VE ONAY SAYFASI

Matematik Anabilim Dalı'nda Dr. Öğr. Üyesi Turgut HANOYMAK danışmanlığında, Erol Ağçakaya tarafından sunulan "**Asal Sayı Test Algoritmaları ve Kriptolojideki Uygulamaları Üzerine**" isimli bu çalışma Lisansüstü Eğitim ve Öğretim Yönetmeliği'nin ilgili hükümleri gereğince 03/01/2020 tarihinde aşağıdaki jüri tarafından **oy birliği** / ~~oy çokluğu~~ ile başarılı bulunmuş ve yüksek lisans tezi olarak kabul edilmiştir.

Başkan: Doç. Dr. İsmail Hakkı DENİZLER

Üye: Dr. Öğr. Üyesi Turgut HANOYMAK

Üye: Dr. Öğr. Üyesi Sait TAŞ

Fen Bilimleri Enstitüsü Yönetim Kurulu'nun 07/02/2020 tarih ve 2020/9-I sayılı kararı ile onaylanmıştır.

İmza

.....

Enstitü Müdürü

T.C. ŞENSOY Müdürü

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını bildiririm.

Erol AĞÇAKAYA

ÖZET

ASAL SAYI TEST ALGORİTMALARI VE KRİPTOLOJİDEKİ UYGULAMALARI ÜZERİNE

AĞÇAKAYA, Erol
Yüksek Lisans Tezi, Matematik Anabilim Dalı
Tez Danışmanı: Dr. Öğr. Üyesi. Turgut HANOYMAK
Şubat 2020, 59 Sayfa

Bu tez çalışması beş ana bölümden oluşmaktadır. Birinci bölümde asal sayı testleri hakkında günümüze kadar olan çalışmalar ile ilgili bilgi verilmiş ve asal sayı testlerinin önemi vurgulanmıştır. İkinci bölümde asal sayı test algoritmaları hakkında kaynak taraması yapılmıştır. Üçüncü bölümde çalışmamız boyunca kullanabileceğimiz bilgiler ve asal sayılarla ilgili temel özellikler ile kuadratik rezidülerle ilgili temel tanım ve teoremlere yer verilmiştir. Bu bilgiler özellikle Slovay-Strassen testinin uygulanması için gereklidir. Dördüncü bölümde Fermat, Euler, Miller-Rabin ve Slovay-Strassen olasılıksal (probabilistic) ve AKS kesin (deterministic) asallık testlerine geniş yer verilmiş ve bazı açık anahtarlı şifreleme algoritmalarından kısaca bahsedilip somut örnekler verilmiştir. Son bölümde ise tezin değerlendirildiği tartışma ve sonuç kısmına yer verilmiştir.

Anahtar kelimeler: Asal sayılar, Kesin asallık testi, Kuadratik rezidüler, Olasılıksal asallık testleri, Rabin Kriptosistemi, RSA Kriptosistemi.

ABSTRACT

ON PRIME NUMBER TEST ALGORITHMS AND APPLICATIONS IN CRYPTOLOGY

AĞÇAKAYA, Erol
M. Sc. Thesis., Mathematics
Asst. Prof. Dr. Turgut HANOYMAK
February 2020, 59 Pages

This thesis consists of five chapters. In the first chapter, some information about the prime number test algorithms is given and the importance of prime numbers in cryptography is introduced. In the second chapter, the studies in the literature about probabilistic and deterministic primality test algorithms are given. In the third chapter, the fundamental definitions and properties about primes and quadratic residues used in the following chapters are given. These are necessary especially for the application of Slovay-Strassen probabilistic primality test. In the fourth chapter; Fermat, Euler, Miller-Rabin and Slovay-Strassen probabilistic primality tests and AKS deterministic primality test are mentioned in details, also some public key encryption schemes are briefly mentioned with concrete examples. Finally, the last chapter consists of discussion and conclusion which is an evalution of the thesis.

Keywords: Prime numbers, Deterministic primality tests, Quadratic residues, Probabilistic primality tests, Rabin Cryptosystem, RSA Cryptosystem.

ÖN SÖZ

Bu tez çalışmasında, her türlü ilgi ve yardımlarını esirgemeyen danışmanım Sayın Dr. Öğr. Üyesi Turgut HANOYMAK'a teşekkür ederim. Ayrıca abim Nevzat AĞÇAKAYA ve Dr. Atilla BEKTAŞ'a yardımlarından dolayı teşekkürlerimi sunarım.

2020

Erol AĞÇAKAYA

İÇİNDEKİLER

Sayfa

Sayfa

ŞEKİLLER LİSTESİ

Şekiller **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış bazı simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler	**Açıklama**
AKS	Agrawal-Kayal-Saxena
ERH	Genelleştirilmiş Riemann Hipotezi
$\boldsymbol{O}$	Büyük O Notasyonu
$\boldsymbol{QR}$	Kuadratik rezidü
$\boldsymbol{QNR}$	Kuadratik olmayan rezidü
$\mathbb{Z}$	Tamsayılar kümesi
$\mathbb{Z}^+$	Pozitif tamsayılar kümesi
$\mathbb{N}$	Doğal sayılar kümesi

1. GİRİŞ

Günümüzde bilginin güvenli bir şekilde iletilmesi için şifreleme çok önemli hale gelmiştir. Şifreleme işlemi, simetrik ve asimetrik şifreleme olmak üzere ikiye ayrılır. Simetrik şifrelemede sadece tek bir gizli anahtar vardır. Şifrenin çözülmesi için mesajlaşan iki kişinin de bu anahtarı bilmesi gerekmektedir. Asimetrik şifrelemede anahtar açıktır ve bu anahtar kişinin kendi anahtarını kullanarak mesajı çözme olanağını sağlar. Bu yöntemin kırılması oldukça zordur. Bu zorluk asal sayıları çarpanlarına ayırma problemine dayanıyor. Bu nedenle önemli veriler şifrelenirken asimetrik şifreleme tercih edilir. Asimetrik şifrelemenin temeli asal sayılara dayanmaktadır. Şifrelemenin güçlü olması için yeteri kadar büyüklükte asal sayı bulabilmek önem arz eder. Küçük sayıların asal olup olmadığını kısa sürede anlayabiliriz fakat büyük sayıların asal olup olmadığını anlamak çok uzun sürmektedir. Bunun için de asallık testlerine başvurulmaktadır. Asallık testleri sayesinde çok büyük sayıların asal olup olmadığı anlaşılabilmektedir.

Kriptografik uygulamalarda "anahtar" olarak kullanılmak üzere çok büyük / çok uzun asal sayılara ihtiyaç duyulmaktadır. Her devirde bilim adamlarının ilgisini çeken asal sayılar, günümüzde güvenlik algoritmaları ve açık anahtarlı şifreleme gibi önemli uygulamaların temelini oluşturmaktadır. Bu nedenle asal sayılar üzerinde hem teorik hem uygulamalı olarak yoğun olarak çalışmalar yapılmaktadır.

Bu tez çalışması, kriptolojide güvenliği sağlamak için kullanılan asimetrik şifrelemelerde, anahtar olarak kullanılan sayıların (ki bu sayılar oldukça büyük sayılardır) asal mı bileşik sayı mı olduğunu bulabilmek için çeşitli asal sayı test algoritmalarını konu almaktadır. Bu test algoritmaları oldukça fazladır. Fakat bu tezde oldukça yaygın olarak kullanılan olasılıksal (probabalistic) asallık testleri olan Fermat, Euler, Miller-Rabin, Slovay-Strassen ve kesin (deterministic) testi olan AKS üzerinde ayrıntılı bir şekilde çalışılmıştır. Ayrıca yaygın olarak kullanılan açık anahtarlı RSA ve Rabin kriptosistemleri ve uygulamaları hakkında bilgi ve örneklere yer verilmiştir.

Yapılan literatür taramalarında bu konu hakkında yeterli düzeyde çalışmanın olmaması ve Türkçe yayınlanmış kaynak yetersizliğinden dolayı bu tezin bu alanda yapılacak olan çalışmalara katkı sunması amaçlanmaktadır.

2. KAYNAK BİLDİRİŞLERİ

Asal sayılar genel olarak matematikte ve özellikle de sayılar teorisinde önemli bir yere sahiptir. Asal sayıların farklı özelliklerini incelemek büyük ilgi çekmektedir. Bu yüzden çeşitli asal sayı test algoritmaları geliştirilmiştir. Bu tür verimli testler pratikte de faydalıdır. Öyle ki, çok sayıda şifreleme protokolünün büyük asal sayılara ihtiyacı vardır. PRIMES'in tüm asal sayılar kümesini gösterdiğini düşünelim. Asal sayıların tanımlanması, zaten n sayısının PRIMES'te olup olmadığını belirlemenin bir yolunu verir: n'yi her sayı ile bölmeyi deneyelim. Eğer $\sqrt{n}$'den küçük hiçbir m asalı, n'yi bölmüyorsa n asaldır aksi takdirde n bileşiktir. Bu test eski Yunanlılardan bu yana biliniyordu. Bununla birlikte, test yetersizdir: n'nin asal olup olmadığını belirlemek için $\Omega(\sqrt{n})$ adım sayısı kullanılır. Verimli bir test veren özellik Fermat'ın Küçük Teoremi'dir. Bununla birlikte, birçok bileşik n aynı zamanda bazılarını (örneğin, Carmichael sayıları durumunda) başarısız olduğu için doğru bir test değildir (Carmichael, 1910).

Bununla birlikte, Fermat'ın Küçük Teoremi, birçok verimli asallık testinin temeli olmuştur. 1975 yılında Miller, Fermat'ın Küçük Teoremi'ne dayanan bir özellik kullanarak, Genelleştirilmiş Riemann Hipotezi'ni (ERH) belirleyen deterministik bir polinom-zaman algoritması için bir özellik kullanmıştır (Miller, 1976).

Solovay ve Strassen, 1974'te asal bir n ve her pozitif a tamsayısı için $\left(\frac{a}{n}\right) = a^{\frac{n-1}{2}} (mod\ n)$ (Jacobi sembolüdür) özelliğini kullanarak farklı bir rastgele polinom-zaman algoritması elde etmiştir. Bu algoritmalar da ERH altında deterministik hale getirilebilir. O zamandan beri, birçok farklı özelliğe dayanan birincillik testi için bir dizi rastgele polinom-zaman algoritması önerilmiştir (Solovay ve Strassen, 1977).

1983 yılında, Adleman, Pomerance ve Rumely, $(logn)^{O(log\ log\ log\ n)}$ süresinde çalışan (üstel için gerekli olan tüm önceki deterministik algoritmalar) asallık için deterministik bir algoritma vererek büyük bir atılım gerçekleştirmiştir. Algoritmaları, bir anlamda Miller'in fikrinin genelleşmesiydi ve daha yüksek karşılıklılık yasaları kullanıyordu. 1986'da Goldwasser ve Kilian, neredeyse tüm girdilerde (yaygın olarak inanılan bir hipotez altındaki tüm girdiler) beklenen tüm polinom zamanında çalışan (o zamana kadar, hepsi ilkel olarak) üretilen eliptik eğrilere dayanan rasgele bir algoritma

önerdiler (Goldwasser ve Kilian, 1986). Atkin de benzer bir algoritma geliştirmiştir (Atkin, 1986).

Adleman ve Huang tüm girdilerde beklenen polinom-zamanda çalışan rastgele bir algoritma elde etmek için Goldwasser-Kilian algoritmasını değiştirdiler (Adleman ve Huang, 1992).

Asallık testi için ortak yaklaşımlar arasında bulunan olasılıksal Miller-Rabin test yöntemi (Rabin, 1980), Solovay-Strassen test yöntemi (Solovay ve Strassen, 1977) ve deterministik test yöntemi Agrawal, Kayal ve Saxena (Agrawal, Kayal ve Saxena, 2004**)** oldukça önemli asal sayı test algoritmaları geliştirilmiştir.

Ağustos 2004'te, M. Agrawal ve meslektaşları, bir sayının polinom zamanıyla başlayıp başlamayacağını belirlemek için belirleyici bir algoritma duyurdular (Agrawal ve ark. 2004). Hiç kimse daha önce polinom-zamanda çalışan deterministik bir algoritma üretememişti (polinom zamanında çalıştığı bilinen olasılıksal algoritmalar olmasına rağmen). Bu test, Agrawal-Kayal-Saxena birincilliği testi, siklotomik AKS testi veya AKS asallık testi olarak bilinir.

Agrawal ve arkadaşlarının 2004'teki orijinal algoritmasının karmaşıklığı $O\ (ln^{12+\varepsilon}\ p)$ idi. Fakat o zamandan beri genel tamsayılar için (Pomerance, 2005), $O(ln^{6+e}\ p)$ veya $O(ln^{4+e}\ p)$ belli tamsayılar için veya algoritmanın belirsiz bir sonuç vermesi için sonsuz bir şansla gerçekleşmesi gerekiyordu.

AKS testi polinom süresi sırasında ortaya çıkardığı genel sorunlar taşıma ve depolama karmaşıklığı açısından o kadar büyük ki, pratikte uygulanması mümkün değildir. Bernstein ve Jin Zhengping diğer algoritmalara kıyasla muazzam gelişmelere yol açtılar. Bu arada, onlar asallık testinin pratik uygulamalar için daha da geliştirilmesi gerektiğini söylediler. Mevcut AKS algoritmalarının hiçbiri pratikte güvenlik uygulamaları için faydalı değildir. Çünkü algoritma bütünlüğü olmadan elde edilemez muazzam bilgi işlem ve depolama giderlerine neden olmaktadır (Bernstein, 2007).

3. MATERYAL VE YÖNTEM

Tez boyunca cebirsel yapılarla ilgili kullanılan temel tanım ve teoremler, aksi belirtilmedikçe (Gilbert, 2009)'ten alınmıştır.

3.1. Kongrüanslar

$n \in \mathbb{Z}^+$ ve $a, b \in \mathbb{Z}$ olmak üzere $n|a-b$ ise a, b' ye kongrüenttir ve $a \equiv b \; mod \; n$ şeklinde yazılır.

$a \equiv b \; mod \; n \Leftrightarrow n|a-b \Leftrightarrow a-b = nk \, , k \in \mathbb{Z} \Leftrightarrow a = b + nk$ ifadesi yazılabilir.

Teorem 3.1.1. n pozitif tamsayı ve $a, b, c \in \mathbb{Z}$ olsun. Aşağıdaki önermeler doğrudur.

i) $a \equiv a \; mod \; n$ (yansıma özelliği)

ii) $a \equiv b \; mod \; n \Rightarrow b \equiv a \; mod \; n$ (simetri özelliği)

iii) $a \equiv b \; mod \; n, \; b \equiv c \; mod \; n \Rightarrow a \equiv c \; mod \; n$ (geçişme özelliği)

İspat.

i) $n|(a-a) = 0 \Rightarrow n|0$

ii) $a \equiv b \; mod \; m \Rightarrow n|(a-b) \Rightarrow n|-(a-b) \Rightarrow n|(b-a) \Rightarrow b \equiv a \; mod \; n$

iii) $a \equiv b \; mod \; n \Rightarrow n|(a-b)$, $a - b = nk_1$

$b \equiv c \; mod \; n \Rightarrow n|(b-c)$, $b - c = nk_2 \quad k_1, k_2 \in Z$

$a - c = (k_1 + k_2)$, $k_1 + k_2 = k_3$ alınırsa, buradan $a - c = nk_3 \Rightarrow n|(a - c) \Rightarrow a \equiv c \; mod \; n$ olur.

Teorem 3.1.2. $a \equiv b \; mod \; m$ ve $c \equiv d \; mod \; m$ ise

i) $a + c \equiv b + d \; (mod \; m)$

ii) $a - c \equiv b - d \; (mod \; m)$

iii) $ac \equiv bd \; (mod \; m)$

İspat. $a = b + q.m$ ve $c = d + k.m$ alınırsa,

i) $a + c = b + d + (q + k)m \; \Rightarrow a + c \equiv b + d \; (mod \; m)$

ii) $a - c = b - d + (q - k)m \; \Rightarrow a - c \equiv b - d \; (mod \; m)$

iii) $ac = bd + bkm + dqm + qkm^2$

$$ac = bd + (bk + dq + qkm)m$$

$$ac = bd\ (mod\ m)$$

Teorem 3.1.3. $a, b \in Z$ ve $k, m \in \mathbb{Z}^+$ olsun. Bu durumda,

$a \equiv b\ mod\ m\ \Rightarrow a^k \equiv b^k\ (mod\ m)$ dir.

İspat. $a \equiv b\ mod\ m \Rightarrow m|a - b$ dir. Bu durumda,

$a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \cdots + ab^{k-2} + b^{k-1})$ ifadesi yazılabilir. Buradan,

$m|a^k - b^k \Rightarrow a^k \equiv b^k\ mod\ m$ olur.

Teorem 3.1.4. a, b, c birer tamsayı n, pozitif tamsayı ve $(c, m) = d$ olmak üzere,

$$ca \equiv cb\ (mod\ m) \Rightarrow a \equiv b\ \left(mod\ \frac{m}{d}\right)$$

İspat. $ca \equiv cb(modm) \Rightarrow m|ca - cb$ dir. Buradan,

$ca - cb = qm,\ (q \in Z)$ yazılabilir. Buradan,

$(c, m) = d \Rightarrow d/c\ , d/m$ olur. Her iki taraf d ile bölünürse,

$$\frac{c}{d}(a - b) = \frac{m}{d}q \Rightarrow \frac{m}{d}|\frac{c}{d}(a - b)$$

$$\left(\frac{c}{d}, \frac{m}{d}\right) = 1 \Rightarrow \frac{\frac{m}{d}}{a - b} \Rightarrow a \equiv b\left(mod\frac{m}{d}\right)$$

olur.

Tanım 3.1.1. x bilinmeyen tamsayı olmak üzere,

$ax \equiv b\ mod\ m$ biçimindeki bir kongrüansa bir lineer (birinci dereceden) kongrüans denir. Burada a ve b bilinen tamsayıdır.

Teorem 3.1.5. $(a, m) = 1$ ise $ax \equiv b\ mod\ m$ kongruansının bir tek çözümü vardır.

İspat. Önce kongrüansın bir çözüme sahip olduğunu gösterelim.

$ax \equiv b\ mod\ m$ kongrüansının her iki tarafını $a^{\varphi(m)-1}$ ile çarpalım.

$$a^{\varphi(m)-1}ax \equiv ba^{\varphi(m)-1}\ mod\ m$$

olur.

$a^{\varphi(m)} \equiv 1\ mod\ m$ olduğundan $ax \equiv b\ mod\ m$ kongrüansının çözümü,

$$x \equiv ba^{\varphi(m)-1}\ mod\ m$$

olarak bulunur.

Kabul edelim ki kongrüansın x_1 ve x_2 gibi farklı iki çözümü olsun. Bu takdirde,

$ax_1 \equiv b\ mod\ m$ ve $ax_2 \equiv b\ mod\ m$ dir. Bu iki kongrüans taraf tarafa çıkarılırsa

$$a(x_1 - x_2) \equiv 0\ mod\ m$$

bulunur.

$(a, m) = 1$ olduğundan,

$x_1 - x_2 \equiv 0\ mod\ m \Rightarrow x_1 \equiv x_2\ mod\ m$ bulunur. Bu da x_1 ile x_2 nin aynı denklik sınıfında olduğunu gösterir.

3.2. Grup Kavramı

G boş olmayan bir küme ve $(*)$ da G üzerinde tanımlı bir ikili işlem olsun. Eğer aşağıdaki şartlar sağlanıyorsa (G,$*$) cebirsel yapısına bir grup denir.

1) Her $a, b \in G$ için $a * b \in G$ dir (kapalılık özelliği).

2) Her $a, b, c \in G$ için $(a * b) * c = a * (b * c)$ dir (birleşme özelliği).

3) Her $a \in G$ için $a * e = e * a = a$ olacak şekilde bir $e \in G$ vardır (birim eleman özelliği).

4) Her $a \in G$ için $a * b = b * a = e$ olacak şekilde bir $b \in G$ vardır (ters eleman özelliği).

Burada (3)'teki e elemanına grubun birim (etkisiz) elemanı denir. Ayrıca (4)'teki b elemanına a'nın tersi denir ve genelde $b = a^{-1}$ ile gösterilir.

5) Her $a, b \in G$ için $a * b = b * a$ ise (değişme özelliği), bu gruba Abelyen (değişmeli) grup denir.

Tanım 3.2.1. G bir grup, $a \in G$ olsun. $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ kümesine a tarafından üretilen grup denir. (Toplamsal notasyonda $\langle a \rangle = \{na : n \in \mathbb{Z}\}$). Burada a elemanına $\langle a \rangle$ grubunun üreteci denir. Eğer $G = \langle a \rangle$ olacak şekilde bir $a \in G$ varsa G'ye devirli grup denir.

Tanım 3.2.2. Bir G grubunun elemanlarının sayısına (eğer G sonlu ise) G nin mertebesi denir ve $|G|$ ile gösterilir. Eğer G sonsuz bir küme ise $|G| = \infty$ ile gösterilir.

Tanım 3.2.3.G bir grup ve $\emptyset \neq H \subseteq G$ olsun. Eğer H kümesi G'de tanımlanan grup işlemi ile bir grup oluyorsa H'ye G'nin bir altgrubu denir ve $H \leq G$ ile gösterilir.

Teorem 3.2.1. G bir grup $\emptyset \neq L \subseteq G$ olsun.

(a) L nin, G'nin bir alt grubu olması için gerek ve yeter şart her $a, b \in L$ için $ab^{-1} \in$ L olmasıdır.

(b) L sonlu ise L'nin alt grup olması için gerek ve yeter şart her $a, b \in L$ için $ab \in L$ olmasıdır.

İspat.(a) L bir alt grup ve $a, b \in L$ olsun. Bu durumda $b^{-1} \in L$'dir, çünkü L, bir gruptur. L, kapalı ve $a, b \in L$ olduğundan ab^{-1} 'dir. Şimdi L'nin boş olmayan bir alt küme olduğunu ve her $a, b \in L$ için ab^{-1} olduğunu kabul edelim. $b = a$ alırsak

$aa^{-1} = e \in L$ elde edilir. Şimdi de $a = e$ alalım, her $b \in L$ için, $b^{-1} \in L$ elde edilir. $a, b \in L$ olsun. $b^{-1} \in L$ olup $a(b^{-1})^{-1} = ab \in L$ elde edilir, yani L kapalıdır. Birleşme özelliği G'de olduğundan L'de de vardır. Sonuç olarak L bir alt gruptur.

İspat.(b) L bir alt grup olsun. L kapalı olduğundan her $a, b \in L$ için $ab \in L$ olduğu kolayca görülür. Şimdi L'nin boş olmayan sonlu ve kapalı bir altküme olduğunu kabul edelim. G'de birleşme özelliği olduğundan L'de birleşmelidir. $L = \{a_1, a_2, a_3 \ldots, a_n\}$, n elemanlı bir alt küme ve $a_k \in L$ olsun. Şimdi $a_1a_k, a_2a_k, \ldots, a_na_k$ elemanlarını göz önüne alalım. L kapalı olduğundan bu elemanların hepsi L'nin elemanlarıdır. Bu elemanlar birbirinden farklıdır. Çünkü, eğer bir $i \neq j$ için $a_ia_k = a_ja_k$ olsaydı sağdan kısaltma kuralı gereğince $a_i = a_j$ olurdu. $i \neq j$ olup bu mümkün

değildir. O halde $L = \{a_1a_k, a_2a_k, \ldots, a_na_k\}$ dir. $a_k \in L$ olup en az bir $1 \leq i \leq n$ için $a_k = a_ia_k$ olmalıdır. Yani $a_i = e$ olur ve $e \in L$'dir. Şimdi de, en az bir $1 \leq j \leq n$ için $a_i = a_ja_k$ olmalıdır. O zaman $(a_k)^{-1} = a_j$ bulunur. k, keyfi olduğundan, L'deki her elemanın tersi vardır. Dolayısıyla L bir alt gruptur.

Tanım 3.2.4. (Euler fonksiyonu) n bir pozitif tamsayı, $1 \leq a \leq n$ ve $(n, a) = 1$ olan a tamsayılarının sayısı $\varphi(n)$ ile gösterilir ve Euler Fonksiyonu olarak adlandırılır.

Euler Fonksiyonunun özellikleri şöyledir:

1) Eğer p asal sayı ise $\varphi(p) = p - 1 = p.\left(1 - \frac{1}{p}\right)$.

2) p asal sayı ve $a \in \mathbb{N}$ ise

$$\varphi(p^a) = p^a - p^{a-1} = p^a\left(1 - \frac{1}{p}\right).$$

3) $(m, n) = 1$ ise

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

$$m = p_1^{a_1}p_2^{a_2} \ldots p_k^{a_k}$$

$$\varphi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_k}\right)$$

Teorem 3.2.2. (Çin kalan teoremi) $m_1, m_2, \ldots, m_n \epsilon \mathbb{Z}^+$ ve her $i \neq j$ için $(m_i, m_j) = 1$ olsun ve $a_1, a_2, \ldots, a_n$ keyfi pozitif tamsayıları için,

$$x \equiv a_1 \, mod \, m_1$$

$$x \equiv a_2 \, mod \, m_2$$

.

.

.

$x \equiv a_n \, mod \, m_n$ kongrüans sisteminin tamsayılarda x_0 gibi bir çözümü vardır ve $m_1, m_2, \ldots, m_n$ modülüne göre $\overline{x_0}$ denklik sınıfı sisteminin çözüm kümesi olur.

İspat. $m_r' = m_1m_2 \ldots m_{r-1}m_{r+1} \ldots m_n$ olsun. Buna göre $r = 1,2, \ldots, n$ için $(m_r', m_r) = 1$ olduğundan, $(a, b) = 1$.

$1 = m_r'u_r' + m_r u_r$ olacak şekilde $u_r', u_r \in \mathbb{Z}$ vardır.

$$k_1 = m_1'u_1'a_1$$

$$k_2 = m_2'u_2'a_2$$

.

.

.

$$k_n = m_n'u_n'a_n$$

alalım. Ayrıca $x_0 = k_1 + k_2 + \cdots + k_n$ olsun.

$$k_r - a_r = m_r'u_r'a_r - a_r = (m_r'u_r' - 1)a_r = m_r(-u_r)a_r$$

$$x_0 - a_r = k_1 + k_2 + \cdots + k_n - a_r$$

$$= (k_r - a_r) + k_1 + k_2 + \cdots + k_{r-1} + k_{r+1} + \cdots + k_n$$

$$\Rightarrow \ x_0 - a_r \in m_r\mathbb{Z} \Rightarrow m_k \,|(x_0 - a_r)$$

$\Rightarrow \ x_0 \equiv a_r \ mod \ m_r, \ (r = 1, 2, \dots, n)$ o halde x_0 bu sistemin bir çözümü olur (Kılıç ve Sert, 2012).

3.3. $\mathbb{Z}_n^*$ Grubu

$\mathbb{Z}_n^* = \{\bar{a} \in \mathbb{Z}_n \mid (a, n) = 1\}$; yani, $\mathbb{Z}_n^*$, $\{\bar{1}, \bar{2}, \dots, \overline{n-1}\}$ şeklinde de yazılabilir. Grup notasyonu çarpımsal $mod\ n$'dir. Yani, $ab = [ab \ mod \ n]$ dir. $\mathbb{Z}_n^*$, bu özelliği açısından bir değişmeli gruptur.

(Bu çalışma boyunca her $[a] = \bar{a} \in \mathbb{Z}_n^*$ kümesinin elemanları a şeklinde gösterilecektir).

$\mathbb{Z}_n^*$ grubunun üretecinin özellikleri

i) $\mathbb{Z}_n^*$ devirli bir gruptur ancak ve ancak $n = 2, 4, \ p^k$ veya $2p^k, \ p > 2$ bir asal ve $k \geq 1$. Özel olarak, eğer p asal ise $\mathbb{Z}_p^*$ devirlidir.

ii) Eğer α, $\mathbb{Z}_n^*$ 'ın bir üreteci ise $\mathbb{Z}_n^* = \{ \ a^i \ mod n \mid 0 \leq i \ \leq \varphi(n) - 1 \ \}$'dir.

iii) Kabul edelim ki α, $\mathbb{Z}_n^*$ 'ın bir üreteci olsun. Bu durumda $b = \alpha^i \, mod n$ de $\mathbb{Z}_n^*$ 'ın bir üretecidir, ancak ve ancak $\big(i,\ \varphi(n)\big) = 1$ ayrıca Z_n^* devirli ise üreteç sayısı $\varphi\big(\varphi(n)\big)$ dir.

Örnek 3.3.1. $\mathbb{Z}_{25}^*$ devirli bir gruptur. Çünkü (i) gereği , $p^k = 5^2$ şartı sağlanıyor.

$$\varphi(25) = \varphi(5^2) = 5^2 - 5 = 20$$

$$\mathbb{Z}_{25}^* = \{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24\}$$

$\alpha, \mathbb{Z}_{25}^*$'ın bir üreteci olsun o halde $\mathbb{Z}_{25}^* = \langle\alpha\rangle$ yazılabilir.

2, $\mathbb{Z}_{25}^*$'ın bir üretecidir ve $\mathbb{Z}_{25}^* = \langle 2\rangle$ şöyle ki;

$2^1 = 2, 2^2 = 4, 2^3 = 8\,,\ 2^4 = 16,\ 2^5 = 7,\ 2^6 = 14, 2^7 = 3, 2^8 = 6,\ 2^9 = 12, 2^{10} = 24, 2^{11} = 23, 2^{12} = 21, 2^{13} = 17, 2^{14} = 9, 2^{15} = 18, 2^{16} = 11, 2^{17} = 22, 2^{18} = 19, 2^{19} = 13, 2^{20} = 1.$

$\mathbb{Z}_{25}^* = \langle 2\rangle = \langle 2^i\rangle$. Ancak ve ancak $\big(i, \varphi(25)\big) = 1$'dir.

$i = 1, 3, 7, 9, 11, 13, 17, 19$ ve $\varphi\big(\varphi(25)\big) = 8$ olmak üzere,

$\langle 2^i\rangle = \langle 2^1\rangle = \langle 2^3\rangle = \langle 2^7\rangle = \langle 2^9\rangle = \langle 2^{11}\rangle = \langle 2^{13}\rangle = \langle 2^{17}\rangle = \langle 2^{19}\rangle$'dir. Böylece toplam 8 tane üreteç vardır. Bunlar; $\langle 2\rangle = \langle 8\rangle = \langle 3\rangle = \langle 12\rangle = \langle 23\rangle = \langle 17\rangle = \langle 22\rangle = \langle 13\rangle$'tür.

Örnek 3.3.2. $\mathbb{Z}_{21}^*$ grubu devirliği değildir. Çünkü (i)'deki şartlar sağlanmaz.

Örnek 3.3.3. $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$. Bu elemanların herbiri 7 ile aralarında asaldır. Herhangi iki elemanın çarpımı yine $mod\ n$'dedir.

Mesela 2.3= $6\ mod\ 7,\quad 3.5 = 1\ mod\ 7,\ 2.5 = 3\ mod\ 7.$

Çarpımsal tersi için de şu örnekleri verebiliriz:

$3.5 = 1\ mod\ 7$ olmalıdır. Burada 3'ün çarpımsal tersi 5'tir veya $4.2 = 1\ mod\ 7$'dir. 2'nin çarpımsal tersi 4'tür.

3.4. Halka

Tanım 3.4.1. H, boş olmayan bir küme $\oplus$ ve $\odot$, H üstünde tanımlı iki ikili işlem olsun. Aşağıdaki koşullar sağlanırsa $(\oplus, \odot, H)$ üçlüsüne bir halka adı verilir;

1) $(H, \oplus)$ değişmeli bir gruptur.

2) $\odot$ işlemi, H üstünde birleşmelidir.

3) H da $\odot$ işleminin, $\oplus$ işlemi üzerine sağdan ve soldan dağılma özelliği vardır.

Tanım 3.4.2. Bir halka için çarpma işlemi değişmeli ise halkaya değişmeli halka, benzer şekilde çarpma işleminin birim elemanı varsa halkaya birimli halka denir.

Tanım 3.4.3. $(\oplus,\odot,H)$ bir halka olsun. , $\emptyset \neq S \subseteq H$ olmak üzere $(\oplus,\odot,S)$'da bir halka yapısına sahip ise S ye H'nin bir alt halkası denir.

Önerme 3.4.1. $(\oplus,\ \odot,\ H)$ bir halka ve $S \subseteq H, H$ nın boş olmayan bir alt kümesi olmak üzere $(S,\ \oplus,\ \odot)$ nın, $(H,\ \oplus,\ \odot)$ halkasının bir alt halkası olması için gerek ve yeter şart , $\forall\, x, y \in S$ için $x \oplus (-y) \in S$, $x \odot y \in S$ olmasıdır.

Tanım 3.4.4. H bir halka ve $a, b \in H$ olsun. $a \neq 0$ ve $b \neq 0$ iken $ab = 0$ oluyorsa a ya sıfırın bir sol böleni, b ye ise sıfırın bir sağ böleni adı verilir. Eğer H halkası değişmeli bir halka ise o takdirde a ve b nin her ikisine birden sıfırın bölenleri veya sıfır bölenler denir.

3.5. Cisim

Tanım 3.5.1. H birimli bir halka olmak üzere H'nin sıfırdan farklı her elemanının H da bir çarpımsal tersi varsa H ya bir yarı-cisim denir.

Tanım 3.5.2. H, birimli bir halka olsun. H'nin bir x elemanının H'de çarpımsal tersi mevcut ise bu elemana terslenebilir bir eleman denir. Eğer H'nin sıfırdan farklı her elemanı terslenebiliyorsa H'ye bir yarı-cisim ve eğer bir yarı-cisim değişmeli ise bu yarı-cisme bir cisim denir.

Önerme 3.5.1. $(F,\ \oplus,\ \odot)$ bir cisim ve $S \subseteq H$, H'nin boş olmayan bir alt kümesi olmak üzere $(F,\ \oplus,\ \odot)$'nın, $(F,\ \oplus,\ \odot)$ cisminin bir alt cismi olması için gerek ve yeter şartlar,

1) $\forall\, x, y \in S$ için $x \oplus (-y) \in S$, $x \odot y \in S$

2) $\forall\, x \in S - \{0\}$ için $x^{-1} \in S$ olmasıdır. (Erdoğan ve Yılmaz, 2008).

3.6. Eratosthenes Kalburu

Eratosthenes Kalburu iki sayı arasındaki asal sayıları bulmak için oldukça kullanışlı ve basit bir yöntemdir. Şekil 3.1.'de görüldüğü gibi, 1'e asal sayı olmadığı için çarpı işareti konur. 2, bir asal sayı olduğu için daire içine alınır, daha sonra 2'nin tüm katlarına çarpı işareti atılır. 3 ve 5 de daire içine alınır ve katlarına çarpı işareti atılır. 100'e kadar olan tüm sayılara bu işlemi uygularsak, 100'e kadar olan asal sayıları buluruz ve uygulama bu şekilde devam edip gider. Bu yönteme Eratosthenes'in Kalburu denir.

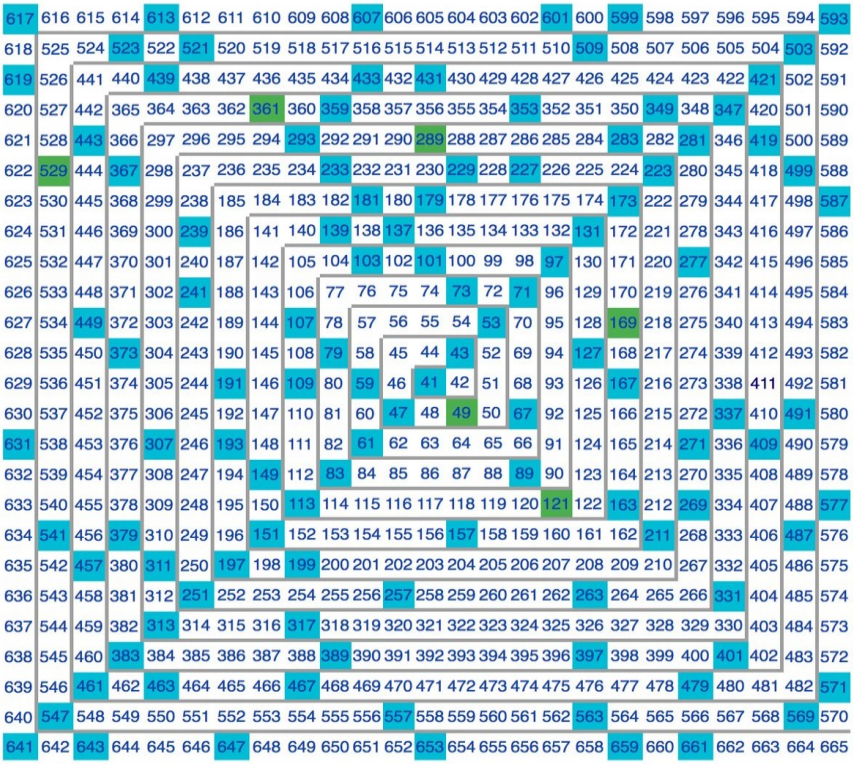
Şekil 3.1. Eratosthenes Kalburu.

3.7. Asal Sayı Spiralleri

3.7.1. Ulam asal sayı spirali

Ulam asal sayı spirali, 1963 yılında Polonyalı matematikçi Stanislaw Ulam tarafından bulunmuş olan, asal sayıların grafiksel gösterimidir. Ulam, bilimsel bir toplantıya katılmak üzereyken, can sıkıntısından kareli kağıt üzerine pozitif doğal sayıları (merkezde 1'den başlamak üzere) spiral şeklinde yazarken keşfetmiştir. Bu sistemi önce spirali doğal sayılarla oluşturmuş, daha sonra asal sayıları işaretlemiş, ve şaşkınlık içinde

farketmiş ki işaretlenmiş sayılar köşegenli yapılar oluşturuyor. Burada köşegenli yapılar ve doğrusal çizgiler daha belirgin olarak Şekil 3.2.'de gösterilmiştir.

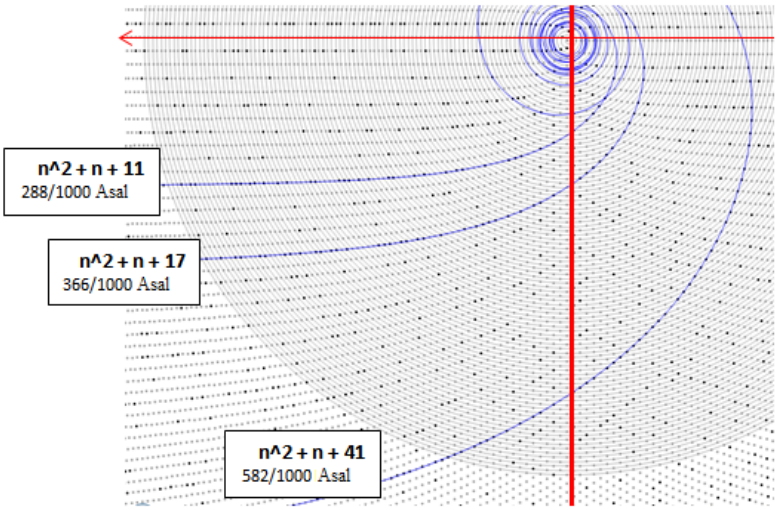


Şekil 3.2. Ulam Asal Sayı Spirali (Anonim-1, 2020).

3.7.2. Sacks asal sayı spirali

Bu spiral, 1994 yılında yazılım mühendisi Robert Sacks tarafından Ulam Spiralinin farklı bir çeşidi olarak keşfedilen, asal sayıların grafiksel gösterimidir. Ulam Spirali'nden birkaç konuda farklılık gösterir: Stanislaw Ulam tarafından kullanılan kare spirali yerine Arşimet Spirali üzerine inşa edilmiştir, Ulam Spiralinden farklı olarak merkeze "0" yazılır.

Sonuçta elde edilen görüntü Şekil 3.3.'teki gibidir.



Şekil 3.3. Sacks Asal Sayı Spirali (Anonim-2, 2020).

3.8. Asal Sayı Çeşitleri

3.8.1. Fermat asalları

$F_n = 2^{2^n} + 1$, $(n \in \mathbb{N})$ şeklinde yazılan sayılara Fermat sayıları denir. Fermat bu şekilde yazılan tüm sayıların asal olduğunu sanıyordu (Ribenboim, 1996).

$$F_o = 3$$

$$F_1 = 5$$

$$F_2 = 17$$

$$F_3 = 257$$

$$F_4 = 65537$$

Fermat, bütün Fermat sayılarının asal olduklarını ispatlamaya çalıştı ama başaramadı. Çünkü sanısı doğru değildi. F_5 asal değildir. $F_5 = 641 \times 6700417$'dir. Buradan, $a = 2^n$ biçiminde yazılabilse bile, $2^a + 1$ asal olmayabilir. Lucas, F_6'nın asal olmadığını ispatladı. 1880'de, Landry, $F_6 = 274177 \times 67280421310721$ eşitliğini buldu. F_7 ve F_8'de asal değiller. W. Keller, 1980'de F_{9448}'in asal olmadığını gösterdi. Bu

sayı $19 \times 2^{9450} + 1$'e bölünür. 1984'de yine W. Keller, F_{23471}'in asal olmadığını ispatladı. Bu sayının 10^{7000}'den fazla basamağı vardır ve $5 \times 2^{23473} + 1$'e tam bölünür.

Teorem 3.8.1.1. (Fermat'ın Küçük Teoremi) $n \in \mathbb{N}$ ve p asal sayı olsun. Bu durumda p, $n^p - n$ sayısını böler. Dolayısıyla eğer p, n'yi bölmüyorsa, $n^{p-1} - 1$'i böler (Singh, 1998).

3.8.2. Palindromik asallar

Soldan ve sağdan okunuşları aynı olan sayılara palindrom sayılar ve bu şekilde yazılan asal sayılara da palindrom asal sayılar denir. Bazı palindromik asal sayılar şunlardır; $2, 3, 5, 7, 11, 101, 131, 151, 181, 191, 313, 353, 373, 383, 727, 757, 787, \ldots$

Bilinen en büyük palindromik asal sayı $10^{474500} + 999 \times 10^{237249} + 1$ olup, 474501 basamaklı sayıdır.

3.8.3. Genelleştirilmiş Fermat asalları

$a^{2^n} + 1$ şeklinde olan asallardır. Bu sayının asal olabilmesi için a bir çift sayı olmak zorundadır. $919444^{1048576} + 1$ asal sayısı bilinen en büyük Genelleştirilmiş Fermat asal sayısıdır ve 6253210 basamaklıdır.

3.8.4. Sophie Germain asalları

p ve $2p + 1$ sayılarının ikisi birden asal sayı ise p asal sayılarına Sophie Germain asalı denir. Örneğin; $2, 3, 5, 7, 11, 23, 29, 41, 53, 83, 89, 113, 131,$ gibi sayılar örnek verilebilir (Takashi, 2000).

3.8.5. Faktöriyel asallar

$n! \mp 1$ şeklindeki sayılara Faktöriyel asallar denir. $147855! - 1$ asal sayısı, 711177 basamaklı en büyük faktöriyel asal sayısıdır.

3.8.6. Cullen asalları

$n \times 2^n + 1$ şeklindeki asallara Cullen asal sayıları denir. Bilinen en büyük Cullen asalı $6679881 \times 2^{6679881} + 1$ sayısı olup, 2108052 basamaklıdır.

$n \times b^n + 1$ şeklindeki asallara da Genelleştirilmiş Cullen asalları denir. Bilinen en büyük G. Cullen asalı; $1323365 \times 116^{1323365} + 1$ sayısı olup, 2732038 basamaklıdır (Marques, 2014).

3.8.7. Mersenne asalları

n, bir asal sayı olmak üzere; $2^n - 1$ sayısı da eğer asal sayı ise bu tip sayılara Mersenne sayıları denir. Eski çağlardan beri matematikçiler n asal sayı olmak şartıyla $2^n - 1$ asal sayılarını modellemeye çalıştılar (Berlekamp, 1984; Gilles, 1964; Robinson, 1954).

Günümüzde gelişmiş bilgisayarlarla Mersenne asal sayıları bulunmaya devam ediliyor. Kısaca GIMPS diye adlandırılan projeyle birçok gönüllü gün geçtikçe yeni Mersenne asal sayı bulmaya devam ediyor. Şu an bulunan en büyük Mersenne asalı, $2^{77.232.917} - 1$ olan ve 23.249.425 basamaklı sayıdır.

3.9. Kuadratik Rezidüler

Kuadratik rezidülerle ilgili tüm tanım ve teoremler, (Menezes ve ark, 2001; Katz ve ark., 2008) referanslı kaynaklardan derlenmiştir.

3.9.1. Asal Modüle Göre Kuadratik Rezidüler

Bir G grubu verildiğinde, bir eleman $y \in G$, eğer $x^2 = y$ ile bir $x \in G$ varsa, bir kuadratik rezidüdür. Bu durumda, x'i y'nin karekökü olarak adlandırırız. Bir abelyan grubunda, ikinci dereceden kalanlar kümesi bir alt grup oluşturur. Buradan $x^2 = y \bmod p$ olan bir x varsa, y nin bir kuadratik rezidü olduğu sonucuna varırız.

Teorem 3.9.1.1. $p > 2$ asal olsun. Her kuadratik rezidünün iki kökü vardır.

İspat. $y \in \mathbb{Z}_p$; bir kuadratik rezidü olmak üzere bir $x \in \mathbb{Z}_p$ vardır, öyle ki $x^2 = y \bmod p$ dir. Açıkça, $(-x)^2 = x^2 = y \bmod p$ dir. Ayrıca, $-x \neq x \bmod p$'dir. Eğer $-x = x \bmod p$ ise $2x = 0 \bmod p$ olur. Buradan $p|2x$ olur. p, asal olduğundan bu, $p|2$ ($p > 2$'den dolayı imkansız) veya $p|x$'in ($0 < x < p$'den dolayı imkansız) anlamına gelir. Yani $[x \bmod p]$ ve $[-x \bmod p]$, $\mathbb{Z}_p$'nin farklı elemanlarıdır ve y, en az iki kareköke sahiptir. $x \in \mathbb{Z}_p^*$; y'nin karekökü olmalıdır. Böylece, $x^2 = y = (x')^2 \bmod p$, ki bu $x^2 - (x')^2 = 0 \bmod p$ demektir. Sol taraftan çarpanlara ayırdığımız zaman, $(x - x')(x + x') = 0 \bmod p$ olur.

Böylece $p|(x - x')$ veya $p|(x + x')$ olur. İlk durumda $x' = x \bmod p$ ve ikinci durumda $x' = -x \bmod p$, y'nin aslında sadece $[\pm x \bmod p]$ karekköküne sahip olduğunu gösterir.

$sq_p: \mathbb{Z}_p^* \to \mathbb{Z}_p^*$; $sq_p(x) = [x \bmod p]$ olsun. Yukarıdaki önerme, $p > 2$'nin asal olduğu zaman sq_p'nin bire bir fonksiyon olduğunu göstermektedir. Buradan da $\mathbb{Z}_p^*$ 'nin elemanlarının yarısının kuadratik rezidülerden oluştuğunu görmüş oluruz. QR_p ile p modülüne göre kuadratik rezidü olanlar kümesini ve QNR_p ile de kuadratik rezidü olmayanlar kümesini belirtiriz. Bunu $p > 2$ asalları için gösterdik.

$$|QR_p| = |QNR_p| = \left|\frac{\mathbb{Z}_p^*}{2}\right| = \frac{p-1}{2}$$

Aşağıdaki gibi x'in $mod\ p$'ye göre Jacobi sembolü olan $\left(\frac{x}{p}\right)$'i tanımlayalım.

$p > 2$ asal ve $x \in \mathbb{Z}_p^*$ olmak üzere,

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{Eğer } x, mod\ p\text{'ye göre "kuadratik rezidü" ise} \\ -1 & \text{Eğer } x, mod\ p\text{'ye göre "kuadratik rezidü değil" ise} \\ 0 & \text{Eğer } x, p\text{'yi bölerse} \end{cases}$$

$\left(\frac{x}{p}\right) = \left([\frac{x \bmod p}{p}]\right)$ tanımlanarak, x'in herhangi bir üssü için doğal yolla genişletilebilir. Kuadratik rezidüleri $\mathbb{Z}_p^*$ cinsinden tanımlarsak; $p > 2$ asal, $\mathbb{Z}_p^*$; $p - 1$ mertebesinin devirli bir grubudur. g, $\mathbb{Z}_p^*$ 'nin bir üreteci olsun. Bu da şu anlama gelir:

$$\mathbb{Z}_p^* = \{g^0,\ g^1,\ g^2, \ldots g^{\frac{p-3}{2}},\ g^{\frac{p-1}{2}},\ g^{\frac{p+1}{2}}, \ldots, g^{p-2}\}$$

(burada p tek sayı, $(p-1)$'in çift sayı olduğunu hatırlayalım). Bu kümedeki her bir elemanın karesinin alınması ve üs içindeki $mod\,(p-1)$'in azaltılması, $\mathbb{Z}_p^*$ 'daki tüm kuadratik rezidülerin bir kümesini verir.

$$QR_p = \{g^0,\ g^2,\ g^4 \ldots, g^{p-3},\ g^0,\ g^2, \ldots,\ g^{p-3}\}$$

(Her kuadratik rezidünün bu kümede iki kez göründüğünü görmüş olduk). Kuadratik rezidülerin $\mathbb{Z}_p^*$ cinsinden olduğunu görüyoruz. Burada g^i ler $i \in \{o, \ldots, p-2\}$ olarak ifade edilir. Yukarıdaki yöntem, Jacobi sembolünü hesaplamak için basit bir yol gösterir ve böylece verilen bir elemanın $x \in \mathbb{Z}_p^*$ 'de kuadratik bir rezidü olup olmadığını hesaplamaya yarar.

Teorem 3.9.1.2. $p > 2$ bir asal olsun. Böylece, $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}\ mod\ p$'dir.

İspat. g, $\mathbb{Z}_p^*$ 'ın keyfi bir üreteci olsun. Eğer $x, mod\ p$ 'ye göre kuadratik rezidü ise bazı tamsayılar için $x = g^i$ şeklinde yazabiliriz (Burada i, pozitif çift tamsayı). Biz $i = 2j$ ve j de bir tam sayı olsun.

$x^{\frac{p-1}{2}} = \left(g^{2j}\right)^{\frac{p-1}{2}} = g^{(p-1)j} = (g^{p-1})^j = 1^j = 1\ mod\ p$'dir.

Böylece, $x^{\frac{p-1}{2}} = +1 = \left(\frac{x}{p}\right) mod\ p$ olur. Öte yandan, eğer x kuadratik rezidü değilse, o zaman bazı tek tamsayılar için $x = g^i$ olur. $i = 2j + 1$ yazılabilir. j, burada bir tamsayıdır.

$x^{\frac{p-1}{2}} = \left(g^{2j+1}\right)^{\frac{p-1}{2}} = \left(g^{2j}\right)^{\frac{p-1}{2}} . g^{\frac{p-1}{2}} = 1. g^{\frac{p-1}{2}} = g^{\frac{p-1}{2}} mod\ p$ olarak yazarsak, bu durumda,

$\left(g^{\frac{p-1}{2}}\right)^2 = g^{p-1} = 1\ mod\ p$ olarak yazılabilir.

Böylece, $g^{\frac{p-1}{2}} = \pm 1\ mod\ p$ dir. Çünkü $[\pm 1\ mod\ p]$, 1'in iki kareköküdür. g, bir üreteç olduğundan, böylece $(p-1)$ mertebesi ve $g^{\frac{p-1}{2}} \neq 1\ mod\ p$ olur. Buradan,

$x^{\frac{p-1}{2}} = -1 = \left(\frac{x}{P}\right)\ mod\ p$ olarak yazılabilir.

(Teorem 3.1.2.)'de verilen bir x elemanın $x \in \mathbb{Z}_p^*$ olup olmadığını test etmek için doğrudan bir polinom-zaman algoritması verir; buradan da bunun bir kuadratik rezidü olup olmadığı sonucu elde edilir.

Teorem 3.9.1.3. $p > 2$ bir asal olsun ve $x, y \in \mathbb{Z}_p^*$ olmak üzere, $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$ 'dir.

İspat. Önceki teoremi kullanarak,

$\left(\frac{xy}{p}\right) = (xy)^{\frac{p-1}{2}} = x^{\frac{p-1}{2}} y^{\frac{p-1}{2}} = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) \ mod\ p$ olur. Böylece,

$\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right) = \left(\frac{y}{p}\right) = \pm 1$ eşitliği sağlanır.

Sonuç 3.9.1.1. $p > 2$ asal olsun. $x, x' \in QR_p$ ve $y, y' \in QNR_p$ olmak üzere bu durumda,

1. $[xx' mod\ p] \in QR_p$

2. $[yy' mod\ p] \in QR_p$

3. $[xy\ mod\ p] \in QNR_p$ sonuçları yazılabilir.

3.9.1.1. Legendre Sembolü

Teorem 3.9.1.1.1. $p > 2$ bir asal sayı olmak üzere;

$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} (mod\ p), \qquad \left(\frac{a}{p}\right) = \begin{cases} 1, & a \in QR_p \\ -1, & a \in QNR_p \end{cases}$

İspat: $q, \mathbb{Z}_p^*$ 'da keyfi bir üreteç olsun. Eğer x bir kuadratik rezidü ise x'i , $x = q^i$ şeklinde gösterebiliriz (bazı i tamsayıları için).

i $= 2j$ olsun. (j tamsayı)

$$x^{\frac{p-1}{2}} = q^{\frac{(2j+1)(p-1)}{2}} = q^{j(p-1)} q^{\frac{p-1}{2}}$$

$q^{p-1} = 1\ mod\ p$, $q^{\frac{p-1}{2}}$ in 1'e eşit olup olmadığına bakalım şimdi.

$q^{\frac{p-1}{2}} = r$ olsun. Eşitliğin her tarafının karesini alırsak,

$q^{p-1} = r^2$ olur. ($q^{p-1} = 1$)

$1 = r^2$ ise, $r = 1$ veya $r = -1$ olur. Burada r, 1 mi -1 mi? q üreteç olduğundan $q^{p-1} = 1$ olduğu açıktır. Yani, eşitliği 1 yapan en küçük kuvvet,$(p-1)$ dir. $(p-1)/2$, $(p-1)$'ye göre daha küçük olduğundan, $q^{\frac{p-1}{2}}$, 1 olamaz. Dolayısıyla $q^{\frac{p-1}{2}} = -1$ olur.

Yani; $x^{\frac{p-1}{2}} = -1 \; mod \; p$ 'dir.

Tanım 3.9.1.1.1. (Legendre sembolünün özellikleri) $p > 2$ bir asal ve $a, b \in \mathbb{Z}$ olsun.

Legendre sembolü aşağıdaki özelliklere sahiptir:

i) $\left(\frac{a}{p}\right) = a^{(p-1)/2} \; mod \; p$ 'dir. $\left(\frac{1}{p}\right) = 1$ ve $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ buradan, eğer $p = 1 \; mod \; 4$ ise $-1 \in QR_p$ve eğer $p = 3 \; mod \; 4$ ise $-1 \in QRN_p$ dir.

ii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ dir. Buradan, eğer $a \in \mathbb{Z}_p^*$ ise $\left(\frac{a^2}{p}\right) = 1$ 'dir.

iii) $a = b \; mod \; p$ ise $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ 'dir.

iv) $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$ 'dir. Buradan eğer $p = 1 \; mod \; 8$, veya $p = 7 \; mod \; 8$ ve $p = 3 \; mod \; 8$ veya $p = 5 \; mod \; 8$ ise $\left(\frac{2}{p}\right) = -1$ dir.

v) q, p'den farklı asal olan bir tek sayı ise $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{(p-1)(q-1)/4}$ 'dir. Diğer bir deyişle $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$'dir. Hem p hem de $q, mod \; 4'$e göre $3'$e denk değilse bu durumda $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ dir.

3.9.2. Asal Olmayan (Kompozit) Modüle Göre Kuadratik Rezidüler

Şimdi dikkatimizi $\mathbb{Z}_n^*$ grubundaki kuadratik rezidülere çeviriyoruz. Eğer önceki bölümün sonuçlarını çin kalan teoremi ile birlikte kullanılırsa $y \leftrightarrow (y_p, y_q)$ ile tanımlı $\mathbb{Z}_n^* \simeq \mathbb{Z}_p^* \times \mathbb{Z}_q^*$ izomorfizması ve çin kalan teoremi yardımıyla verilen bir tamsayının $mod \; n'$ye göre kuadratik rezidü olup olmadığı kolayca bulunur (burada $n = pq$). Buradan, $y_p = [y \; mod \; p]$ ve $y_q = [y \; mod \; q]$ alınabilir.

Teorem 3.9.2.1. p, q farklı iki asal ve $n = pq$ olsun. $y \leftrightarrow (y_p, y_q)$ ile tanımlı $\mathbb{Z}_n^* \simeq \mathbb{Z}_p^* \times \mathbb{Z}_q^*$ izomorfizmasını ele alalım. Bu durumda, y'nin $mod\ n$'ye göre bir kuadratik rezidü olması için gerek ve yeter şart $y \in \mathbb{Z}_n^*$ 'ın $mod\ p$'ye ve $mod\ q$'ya göre kuadratik rezidü olmasıdır.

İspat. Eğer $y, mod\ n$'ye göre bir kuadratik rezidü ise, tanım gereği, $x \in \mathbb{Z}_n^*$ var, öyle ki $x^2 = y\ mod\ n$ olsun. $x \leftrightarrow (x_p, x_q)$ yazılabilir. Buradan,

$(y_p, y_q) \leftrightarrow y = x^2 \leftrightarrow (x_p \leftrightarrow x_q)^2 = (x_p^2\ mod\ p, x_q^2\ mod\ q)$, burada $(x_p, x_q)^2$ basitçe $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$ grubundaki elemanın karesidir.

$y_p = x_p^2\ mod\ p\ ve\ y_q = x_q^2\ mod\ q$ ve y_p, y_q'nun kuadratik rezidüler olduğu (uygun mod'a göre) gösterilmiştir, aksine, $y \leftrightarrow (y_p, y_q)$ ve y_p, y_q sırasıyla $mod\ p$ ve $mod\ q$'ya göre kuadratik rezidülerdir. Buna göre $x_p \in \mathbb{Z}_p^*$ ve $x_q \in \mathbb{Z}_q^*$ vardır. $x \in \mathbb{Z}_n^*$ ve $x \leftrightarrow (x_p, x_q)$ şeklinde olsun. x'in $y\ mod\ n$'nin bir karekökü olduğunu gösterir.

Her kuadratik rezidü $y \in \mathbb{Z}_n^*$ dört kareköke sahiptir. Bunu görmek için $y \leftrightarrow (y_p, y_q)\ mod\ n$ için bir kuadratik rezidü olsun ve (x_p, x_q) sırasıyla y_p ve $y_q mod\ p$ ve $mod\ q$'nun karekökleri olsun. Böylece, y'nin dört karekökü, $\mathbb{Z}_n^*$'dedir. Bunlar;

$(x_p, x_q), (-x_p, x_q), (x_p, -x_q)$, $(-x_p, -x_q)$ elemanlarıdır. Bunlardan bir tanesi y'nin kareköküdür.

$$(x_p, x_q)^2 = 0\left(\left[(\pm x_p)^2 mod\ p\right], \left[(\pm x_q)^2 mod\ q\right]\right)$$
$$= \left(\left[(x_p)^2 mod\ p\right], \left[(x_q)^2 mod\ q\right]\right)$$
$$= (y_p, y_q) \leftrightarrow y$$

(burada , $(.,.)^2$ gösterimi, $\mathbb{Z}_p\ x\ \mathbb{Z}_q$ grubundaki kareleri ifade eder). Çin kalan teoremi, dört elemanın varlığını gösterir. Bunlardan her biri $\mathbb{Z}_n^*$ 'nin farklı elemanlarına karşılık gelir. Çünkü x_p ve $-x_p,\ mod\ p$ ye göre , x_q ve $-x_q,\ mod\ q$ ya göre farklıdır.

Örnek 3.9.2.1. $\mathbb{Z}_{91}^*$ grubunu ele alalım (çin kalan teoremi gereği). 2'nin karesi 4 ve 4, $\mathbb{Z}_{91}^*$ 'in elemanı olduğundan 2 bir köktür. Bu kökler dört tanedir. Bunlar, (2, 2), (2, -2), (-2, 2), (-2, -2)'dir. Şimdi bu kökleri $(mod\ 7)$ ve $(mod\ 13)$'e göre yazalım.

$$([2\ mod\ 7], [2\ mod\ 13]) = (2, 2) \leftrightarrow 2$$

$$([2\ mod\ 7], [-2\ mod\ 13]) = (2, 11) \leftrightarrow 37$$

$$([-2\ mod\ 7], [2\ mod\ 13]) = (5, 2) \leftrightarrow 54$$

$$([-2\ mod\ 7], [-2\ mod\ 13]) = (5, 11) \leftrightarrow 89$$

$$2^2 = 37^2 = 54^2 = 89^2 \equiv 4\ mod\ 91$$

$QR_n, mod\ n$ 'ye göre kuadratik rezidüler kümesini göstersin. $mod\ n$'nin dörtte bir fonksiyonu kare olduğu için $\mathbb{Z}_n^*$ 'nin elemanlarının tam olarak 1/4'ünün kuadratik rezidüler olduğunu hemen görüyoruz. Alternatif olarak, $y \in \mathbb{Z}_n^*$ 'in sadece y_p, y_q kuadratik rezidüleri olması durumunda kuadratik bir rezidü olması nedeniyle QR_n ve $QR_p\ x\ QR_q$ arasında bire bir eşleşme olduğunu görebiliriz. Böylece, kuadratik rezidülerin $mod\ n$ ye göre oranı,

$$\frac{|QR_n|}{\mathbb{Z}_n^*} = \frac{|QR_p|.|QR_q|}{|\mathbb{Z}_n^*|} = \frac{\frac{p-1}{2}.\frac{q-1}{2}}{(p-1).(q-1)} = \frac{1}{4}$$

şeklinde olur.

3.9.2.1. Jakobi sembolü

Jakobi sembolü, bileşik n sayısı ve herhangi bir a tamsayısı verildiğinde, $\mathbb{Z}$'de $x^2 \equiv a\ mod\ n$'de çözümünün olup olmadığını kontrol etmeye yarar.

$$\left(\frac{x}{n}\right) = \begin{cases} 1 & \text{Eğer } x, mod\ n\text{'ye göre "kuadratik rezidü" ise} \\ -1 & \text{Eğer } x, mod\ n\text{'ye göre "kuadratik rezidü değil" ise} \\ 0 & \text{Eğer } x, n\text{'yi bölerse} \end{cases}$$

Teorem.3.9.2.1.1. $q > 2$ olan bir asal olsun ve $a, mod\ q$'ya göre bir kuadratik rezidü ise bu durumda $\left(\frac{a}{q}\right) = 1$'dir.

İspat. $q = q_1 q_2 \cdots q_n$ olsun; burada her q_i teksayı olan bir asaldır. a'nın $mod\ q$'ya göre bir kuadratik rezidü olduğunu düşünelim. Bu durumda $(a,q) = 1\ ve\ x^2 = a\ mod\ q$ çözümleri vardır.

Önce, $q_i\,|q, i = 1,\ldots n$ için $(a,q_i) = 1$ ve $x^2 = a\ (mod\ q_i)$ yazalım. Buradan, her $i = 1,2,\ldots,n\ için\ \left(\frac{a}{q_i}\right) = 1$'dir. Bu yüzden,

$\left(\frac{a}{q}\right) = \left(\frac{a}{q_1}\right)\left(\frac{a}{q_2}\right)\ldots\left(\frac{a}{q_n}\right) = 1.1\ldots 1 = 1$'dir.

Örnek 3.9.2.1.1. $\mathbb{Z}_{21}^*$'de kuadratik rezidü olan ve kuadratik rezidü olmayan elemanları bulalım.

$a \in \mathbb{Z}_{21}^*$	1	2	4	5	8	10	11	13	16	17	19	20
$a^2\ mod\ n$	1	4	16	4	1	16	16	1	4	16	4	1
$\left(\frac{a}{3}\right)$	1	-1	1	-1	-1	1	-1	1	1	-1	1	-1
$\left(\frac{a}{7}\right)$	1	1	1	-1	1	-1	1	-1	1	-1	-1	-1
$\left(\frac{a}{21}\right)$	1	-1	1	1	-1	-1	-1	-1	1	1	-1	1

Görüldüğü üzere sadece $\{1, 4, 16\}$ elemanları kuadratik rezidüdür.

Teorem 3.9.2.1.2. q ve q' tek pozitif sayılar olsun ve varsayalım ki $(pp', qq') = 1$ olsun. Bu durumda,

(1) $\left(\frac{p}{q}\right)\left(\frac{p}{q'}\right) = \left(\frac{p}{qq'}\right)$

(2) $\left(\frac{p}{q}\right)\left(\frac{p'}{q}\right) = \left(\frac{pp'}{q}\right)$

(3) $\left(\frac{p^2}{q}\right) = \left(\frac{p}{q^2}\right) = 1$

(4) $\left(\frac{p^2p'}{q^2q'}\right) = \left(\frac{p'}{q'}\right)$

(5) Eğer $p = p'\ mod\ q$ ise $\left(\frac{p}{q}\right) = \left(\frac{p'}{q}\right)$

İspat.(1). q ve q' sayılarını tek asal sayıların çarpımı olarak yazalım.

$q = q_1 q_2 \dots q_m$ve $q' = q_1' q_2' \dots q_n'$ Bu durumda,

$$\left(\frac{p}{q}\right)\left(\frac{p}{q'}\right) = \left(\left(\frac{p}{q_1}\right)\left(\frac{p}{q_2}\right)\dots\left(\frac{p}{q_m}\right)\right)\left(\left(\frac{p}{q_1'}\right)\left(\frac{p}{q_2'}\right)\dots\left(\frac{p}{q_m'}\right)\right) = \left(\frac{p}{qq'}\right)$$

İspat.(2). q'yu tek asal sayıların çarpımı şeklinde yazalım.

$q = q_1 q_2 \dots q_m$ Böylece,

$$\left(\frac{p}{q}\right)\left(\frac{p'}{q}\right) = \left(\left(\frac{p}{q_1}\right)\left(\frac{p}{q_2}\right)\dots\left(\frac{p}{q_m}\right)\right)\left(\left(\frac{p'}{q_1}\right)\left(\frac{p'}{q_2}\right)\dots\left(\frac{p'}{q_m}\right)\right)$$

$$= \left(\left(\frac{p}{q_1}\right)\left(\frac{p'}{q_1}\right)\right)\left(\left(\frac{p}{q_2}\right)\left(\frac{p'}{q_2}\right)\right)\dots\left(\left(\frac{p}{q_m}\right)\left(\frac{p'}{q_m}\right)\right)$$

$$= \left(\left(\frac{pp'}{q_1}\right)\left(\frac{pp'}{q_2}\right)\dots\left(\frac{pp'}{q_m}\right)\right) = \left(\frac{pp'}{q}\right)$$

İspat.(3). q'yu tek asal sayıların çarpımı şeklinde yazalım.

$$q = q_1 q_2 \dots q_m$$

Eğer q_k, tek sayı olan bir asal ise $\left(\frac{p^2}{q_k}\right) = 1$ olur (Legendre sembolü gereği). Buradan,

$$\left(\frac{p^2}{q}\right) = \left(\frac{p^2}{q_1}\right)\left(\frac{p^2}{q_2}\right)\dots\left(\frac{p^2}{q_m}\right) = 1.1 \dots 1 = 1$$

bulunur. Daha sonra eğer q_k, asal olan bir tek sayı ise, şu sonuca varırız.

$$\left(\frac{p}{q_k}\right)\left(\frac{p}{q_k}\right) = (\pm 1)^2 = 1$$

$$\left(\frac{p}{q^2}\right) = \left(\frac{p}{q_1}\right)\left(\frac{p}{q_1}\right)\left(\frac{p}{q_2}\right)\left(\frac{p}{q_2}\right)\dots\left(\frac{p}{q_m}\right)\left(\frac{p}{q_m}\right) = 1.1 \dots 1 = 1$$

İspat.(4). $\left(\frac{p^2p'}{q^2q'}\right) = \left(\frac{p^2}{q^2q'}\right)\left(\frac{p'}{q^2q'}\right) = \left(\frac{p'}{q^2q'}\right) = \left(\frac{p'}{q^2}\right)\left(\frac{p'}{q'}\right) = \left(\frac{p'}{q'}\right)$

İspat.(5). q'yu tek asal sayıların çarpımı şeklinde yazalım.

$$q = q_1 q_2 \dots q_m$$

$p = p' mod\ q$ ve her $k = 1,2, \dots, m$ için $p = p' mod\ q_k$ dır. Bu yüzden,

$\left(\frac{p}{q_k}\right) = \left(\frac{p'}{q_k}\right)$ olur (Legendre sembolü gereği). Buradan,

$$\left(\frac{p}{q}\right) = \left(\frac{p}{q_1}\right)\left(\frac{p}{q_2}\right)\dots\left(\frac{p}{q_m}\right) = \left(\frac{p'}{q_1}\right)\left(\frac{p'}{q_2}\right)\dots\left(\frac{p'}{q_m}\right) = \left(\frac{p'}{q}\right)$$

bulunur.

Teorem 3.9.2.1.3. $q > 2$ asal sayı olsun. Bu durumda,

$\left(\frac{-1}{q}\right) = (-1)^{(q-1)/2'}$dir.

İspat. q'yu tek asal sayıların çarpımı şeklinde yazalım.

$q = q_1 q_2 \dots q_m$ buradan,

$\left(\frac{-1}{q}\right) = \left(\frac{-1}{q_1}\right)\left(\frac{-1}{q_2}\right)\dots\left(\frac{-1}{q_n}\right)$ (Legendre sembolleri).

$\left(\frac{-1}{q_k}\right) = (-1)^{(q_k-1)/2}$dir. Her $k = 1.2 \dots n$ için,

$\left(\frac{-1}{q}\right) = (-1)^{(q_1-1)/2}(-1)^{(q_2-1)/2} \dots (-1)^{(q_n-1)/2} = (-1)^S$ Buradan,

$S = \sum_{k=1}^{n} \frac{q_k-1}{2}$alınabilir. Buna göre,

$$S = \sum_{k=1}^{n} \frac{q_k - 1}{2} = \frac{\prod_{k=1}^{n} q_k - 1}{2} = \frac{q-1}{2} \ (mod\ 2)$$

$\left(\frac{-1}{q}\right) = (-1)^{(q-1)/2}$ bulunur.

Teorem 3.9.2.1.4. p pozitif tek sayı olsun. Buna göre,

$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$ dir.

İspat. p'yi tek asal sayıların çarpımı şeklinde yazalım.

$$p = p_1 p_2 \dots p_n$$

$\left(\frac{2}{p}\right) = \left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right)\dots\left(\frac{2}{p_n}\right)$ (Legendre sembolü gereği).

Her $k = 1,2, \dots, n$ için $\left(\frac{2}{p_k}\right) = (-1)^{(p_k^2-1)/8}$ dir. Böylece,

$\left(\frac{2}{p}\right) = (-1)^{(p_1^2-1)/8}(-1)^{(p_2^2-1)/8} \ldots (-1)^{(p_n^2-1)/8} = (-1)^S$ dir. Buradan,

$S = \sum_{k=1}^{n} \frac{(p_k^2-1)}{8}$ yazılabilir.

$S = \sum_{k=1}^{n} \frac{(p_k^2-1)}{8} = \frac{\prod_{k=1}^{n}(p_k^2-1)}{8} = \frac{p^2-1}{8}(mod2)$. Böylece ,

$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$ elde edilir.

Örnek 3.9.2.1.2.

$$\left(\frac{41}{675}\right) = \left(\frac{41}{3^3 5^2}\right) = \left(\frac{41}{3.5}\right) = \left(\frac{41}{3}\right)\left(\frac{41}{5}\right) = \left(\frac{2}{3}\right)\left(\frac{1}{5}\right) = (-1).1 = -1$$

4. BULGULAR VE TARTIŞMA

Bu bölümde, asal sayı teoreminden önce bir algoritmanın çalışma süresi ve işlem sayısı ile ilgili birkaç tanımın yapılmasında fayda görülmektedir.

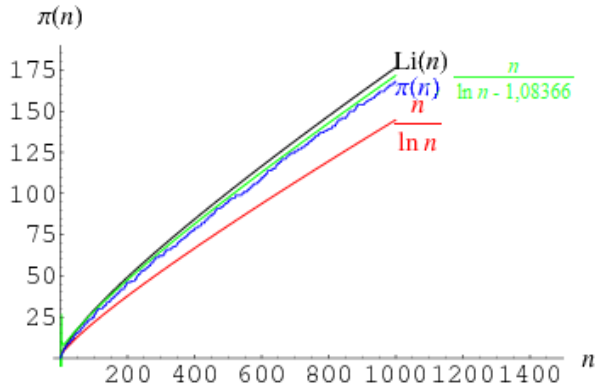
Tanım 4.1. Bir girdi üzerinde bir algoritmanın çalışma süresi, toplam hesaplanan işlem sayısıdır.

Tanım 4.2. Bir algoritmanın en kötü durumda çalışma süresi, herhangi bir girdi için çalışma süresinin bir üst sınırıdır.

Tanım 4.3. Asimptotik üst sınır $\forall\, n \geq 0$ için $0 \leq f(n) \leq c.g(n)$ pozitif bir c sabiti ve $n_0 \in \mathbb{Z}^+$varsa $f(n) = O(g(n))$ dir.

Tanım 4.4. En kötü çalışma süresi, $O(n^k)$ olan algoritmaya polinom zamanlı algoritma denir. Burada n girdi uzunluğu ve k sabittir. Bu şekildeki algoritmalar, iyi veya etkin algoritmalar olarak da bilinmektedir (Menezes ve ark., 2001).

Teorem 4.1. (Asal sayı teoremi) Asal sayı teoremi, asal sayma fonksiyonu $\pi(n)$ için asimptotik bir form verir. Bu form, bir n değerinden küçük olan sayıları sayar. Büyük n için,



Şekil 4.1. Asal Sayı Dağılımı (Anonim-3, 2020).

$$\pi(n) \sim \frac{n}{\ln n + B}$$

ile $B = -1.08366$ (burada B bazen Legendre sabiti olarak adlandırılır). Bu ifade yalnızca ilk terimde doğru olan bir formüldür.

$$\frac{n}{\ln n + B}\sin\frac{n}{\ln n} - B\frac{n}{(\ln n)^2} + B^2\frac{n}{(\ln n)^3} + \cdots$$

(Nagell, 1951; Wagon, 1991; Havil, 2017).

$\pi(n) \sim \frac{n}{\ln n}$ (Gauss önermesi)

Gauss daha sonra tahminini geliştirdi ve $\pi(n) \sim Li(n)$ ifadesini yazdı. Burada,

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

logaritmik integraldir. Gauss, 1849 yılında Encke'ye yazdığı bir mektupta bahsettiği bu sonucu yayınlamadı. Daha sonra 1863'te yayınlandı (Havil, 2017). $Li\,(n)$, sonsuzlukla ilgili asimptotik serilere sahiptir.

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

ve ilk üç terimi almanın tek başına $n \,/\, \ln(n)$'den daha iyi bir tahmin olduğu gösterilmiştir (Derbyshire, 2004).

(1) ifadesi genellikle "asal sayı teoremi" olarak bilinir ve bağımsız olarak Hadamard (1896) tarafından ispatlanmıştır. $n \leq 1000$ için yukarıda bir $\pi\,(n)$ (alt eğri) ve $Li\,(n)$ grafiği gösterilmiştir.

Asal sayı teoremi küçük n için kontrol edildi ve her zaman $\pi\,(n) < Li\,(n)$ eşitsizliğinin doğru olduğu anlaşıldı. Bu varsayım, Littlewood, (1916) tarafından eşitsizliğin yeterince büyük n için sonsuza doğru tersine döndüğü ispatlandığında çürütülmüştü (Ball ve Coxeter 1987; Havil, 2017).

Skewes daha sonra, $\pi\,(n) - Li\,(n) = 0$ 'ın ilk geçişinin, şimdi Skewes sayısı olarak bilinen bir sayı olan $10^{10^{10^{34}}}$ öncesi gerçekleştiğini gösterdi (Havil, 2017). Geçiş için üst sınır daha sonra 10^{371} 'e düşürülmüştür. Lehman, 1966'da 1166 veya 1167 ondalık basamaklı sayılar için en az 10^{500} geri dönüşün gerçekleştiğini ispatladı.

Chebyshev oranına sınır koydu.

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

ve büyük n sayıları için eşitsizliğinin doğru olduğunu gösterdi (Nagell, 1951; Landau, 1974; Hardy ve Wright, 1979; Rubinstein ve Sarnak, 1994; Hardy, 1999; Derbyshire, 2004).

$0.89\ Li(n) < \pi(n) < 1.11\ Li(n)$ eşitsizliği yazılabilir. Burada, $Li\ (x)$ logaritmik integraldir. Buradan,

$0.922 < \frac{\pi(n)}{\frac{n}{\ln n}} < 1.105$ eşitsizliği yazılabilir (Havil, 2017). Buradan,

$\lim_{n\to\infty} \frac{\pi(n)}{\frac{n}{\ln n}} = 1$'dir (Havil, 2017; Derbyshire, 2004). 1850'de Chebyshev'in $\pi(n)$'nin $n\ /\ ln$'den farklı olamayacağını gösterdiğini ve yaklaşık %10'dan daha fazla farklılıklar gösterdiğini ve bu nedenle sadece yeterince büyük n sayıları için doğru olduğunu göstermiştir.

Hadamard, 1896'daki asal sayı teoremini, Riemann zeta fonksiyonunun derin özelliklerine ihtiyaç duymadığı şekilde sıfırlamadığını göstererek ispatladı (Smith, 1994; Hardy, 1999). Wiener, 1959'da bu belirsiz ifadenin kelimenin tam anlamıyla yorumlanmasını sağladı (Hardy, 1999). Bu ispat, Landau (1990) tarafından basitleştirildi.

Erdős (1949) ve Selberg (1949) (Ball ve Coxeter, 1987; Havil, 2017) tarafından temel bir ispat bulundu (Hoffman, 1998; Derbyshire, 2004). Asal sayı teoreminin temel ispatlarının sürümleri, Nagell'in (1951) ve Hardy ve Wright'ın (1979) son bölümünde görünür.

Hadamard'ın ispatı basit trigonometrik eşitsizliğe dayanır.

$$3 + 4\cos\theta + \cos 2\theta = 2(1 + \cos\theta)^2 \geq 0$$

(Hardy, 1999; Havil, 2017).

$$\pi(x) = Li(x) + O\left(\frac{x}{\ln x} e^{-a\sqrt{\ln x}}\right)$$

Bazı a sabitleri için (Knuth, 1998), burada $O\ (x)$, asimptotik gösterimdir. 1901'de Koch, Riemann hipotezinin doğru olması durumunda,

$\pi(x) = Li(x) + O\left(\sqrt{x}\ln x\right)$ ifadesinin doğru olduğunu gösterdi.

Buradan aşağıdaki ifade de yazılabilir:

$\pi(x) = Li(x) + O\left(x^{1/2+\varepsilon}\right)$ (Derbyshire, 2004). Buradaki hata terimi daha sonra,

$\pi(x) = Li(x) + O\left(xe^{\left(\frac{A(\ln X)^{3/5}}{(\ln\ln x)^{1/5}}\right)}\right)$ şeklinde ifade edilebilir (Walfisz, 1963; Riesel, 1994; Knuth, 1998; Derbyshire, 2004). Ingham, Ramanujan'ın formülünü kullanarak asal sayı teoremini ispatladı.

$$\sum_{n=1}^{\infty} \frac{\sigma_a(n)\sigma_b(n)}{n^s} = \frac{\zeta(s)\zeta(s-a)\zeta(s-b)\zeta(s-a-b)}{\zeta(2s-a-b)}$$

$\sigma_a(n)$, bölen işlevidir (Hardy, 1999).

Riemann, asal sayma fonksiyonunu,

$\pi(n) \to Li(n) - \frac{1}{2}Li\left(n^{1/2}\right)$ dir. Burada $n < 10^7$ için $Li\,(n)$'den daha iyi bir yaklaşımdır. Riemann (1859)'da ayrıca Riemann işlevini önerdi.

$$R(x) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} Li\left(x^{1/n}\right)$$

μ, Möbius işlevidir (Wagon, 1991). Küçük n için daha iyi bir yaklaşım ($n < 10^9$ için 10 kat faktörü ile) Gram serisidir.

$$\lim_{x\to\infty} \frac{\theta(x)}{x} = 1$$

veya

$$\lim_{x\to\infty} \frac{\psi(x)}{x} = 1$$

$\theta(x)$ ve $\psi(x)$ Chebyshev'in çalıştığı yerlerdir. Chebyshev, bu ifadelerin tek olası sınırının 1 olduğunu, ancak sınırın varlığını ispatlayamadığını gösterdi (Hardy, 1999).

$|Li(x) - \pi(x)| \leq c\sqrt{x}\ln x$ (Ingham, 1990; Landau, 1974; Ball ve Coxeter, 1987; Hardy, 1999). Riemann hipotezi varsayımından elde edilen bazı sınırlamalar,

$$\pi(x) = Li(x) + O\left[xe^{-(\ln x)^{1/2}/15}\right]$$

$\pi(x) = Li(x) + O\left[xe^{-0.009(\ln x)^{3/5}/(\ln\ln x)^{1/5}}\right]$ şeklindedir.

4.1. Fermat Testi

Teorem 4.1.1. (Fermat Teoremi) $p, p|\ a$ sağlamayan bir asal sayı olsun. Bu durumda,

$a^{p-1} \equiv 1\ mod\ p$'dir.

İspat. a sayısının, $a, 2a, 3a, \ldots, (p-1)a$ gibi ilk $(p-1)$ katından oluşan sayı takımını göz önüne alalım. Bu sayılar, $mod\ p$'ye göre birbirleri ile kongrü 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 $a, 2a, 3a, \ldots, (p-1)a$ sayı takımı, belirli bir sırada alındığında, $mod\ p$'ye göre 1,2,3, …, $(p-1)$ sayı takımına kongrü olur, yani $a, 2a, 3a, \ldots, (p-1)a \equiv$ 1,2,3, …, $(p-1)\ (mod\ p)$, böylece $a^{p-1}(p-1)! \equiv (p-1)!\ (mod\ p)$, p, $(p-1)!$ 'i bölmediğinden $a^{p-1} \equiv 1(mod\ p)$ elde edilir. p bir asal sayı ve a bir tamsayı olmak üzere, $a^p = a\ (mod\ p)$ dir. Ayrıca a ve p'nin en büyük ortak böleni 1 ise, $a^{p-1} = 1\ mod\ p$'dir.

Örnek 4.1.1. $(a, 17) = 1$ olacak şekilde $a = 3$ sayısını alalım ve 17 sayısına Fermat teoremini uygulayalım.

$3^{16} = 1\ mod\ 17$'dir. Bu durumda 17 sayısı Fermat testine göre asal sayıdır. Fermat teoremine göre eğer n asal ise n ile aralarında asal olan herhangi bir a sayısı için, $a^{n-1} \equiv 1\ mod\ n$ denkliği sağlanır. Fakat bunun tersi her zaman doğru değildir. Bu denkliği sağlayıp da asal olmayan sayılar bulunabilir.

Tanım 4.1.1. (Fermat yalancı asalı) n, bileşik (kompozit) tek tamsayı olsun. n ile aralarında asal bir a tamsayısı için $a^{n-1} \equiv 1\ mod\ n$ denkliği sağlanıyorsa, bu n sayısına a tabanına göre bir Fermat yalancı asalı denir.

Örnek 4.1.2. $n = 91$ sayısı ve $a = 3$ tabanını ele alalım. Bu durumda,

$$3^{90} = 1\ mod\ 91$$

denkliği elde edilir. O halde 91 sayısı 3 tabanına göre yalancı asaldır. Fakat 91 sayısı, 2 tabanına yalancı bir asal değildir. Çünkü,

$$2^{90} = 64\ mod\ 91$$

dir.

Tanım 4.1.2. (Fermat şahidi) n, bileşik (kompozit) tek tamsayı olsun. n ile aralalarında asal bir a tamsayısı için $a^{n-1} \neq 1\ mod\ n$ denkliği sağlanıyorsa, bu a sayısına n'nin bileşikliği (kompozitliği) için bir Fermat şahidi denir.

Tanım 4.1.3. (Carmichael sayıları) $(a, n) = 1$ ile tüm pozitif tamsayılar için $a^{n-1} \equiv 1\ (mod\ n)$ eşitliğini sağlayan bir kompozit n tamsayısı olsun. Bu n tamsayısına Carmichael sayısı denir. Yirminci yüzyılın başlarında bu sayılar üzerinde çalışan Robert Carmichael'dan sonra Carmichael sayısı veya mutlak bir yalancı asal olarak adlandırılır. Tahmin edilebileceği gibi, Carmichael sayıları çok azdır. 10^6 'nın altında 43, 10^{15} sayısının altında 105,212 Carmichael sayısı vardır. Richard Pinch, 10^{16}'nın altında 246.683 Carmichael sayısı olduğunu tespit etmiştir. 10^{16}'nın altında 279.238.341.033.925 tane asal sayı vardır. Bu nedenle bir sayının Carmichael sayısı olma ihtimali milyarda birden daha azdır (Dorsey, 1999).

Örnek 4.1.3. $n = 91$ sayısı ve $a = 2$ tabanını ele alalım. Bu durumda,

$$2^{90} = 64\ mod\ 91$$

olduğundan, 2 tabanı, 91 sayısının kompozitliğine bir Fermat şahididir.

Örnek 4.1.4 $2^{9699690} = 0100618 \neq 1\ mod\ 9699691$ ve 9699691'in asal olmadığını biliyoruz. Daha dramatik bir örnek verelim.

$$n = 72769523494671107612633.$$

Buradan,

$2^{n-1} = 1382973387568859937483 \neq 1\ mod\ n$ 'dir. Buradan n'nin bileşik sayı olduğunu görüyoruz. n'nin en küçük çarpanı bir trilyondan daha büyük olduğundan, her

bir asalı bir trilyondan daha az deneyerek, bileşikliği test etmek oldukça zaman alacaktır. Fermat testi Carmichael sayılarını test ederken başarısız olmaktadır (Mollin, 2002).

Örnek 4.1.5. 561 Carmichael sayısını Fermat testinden geçirelim.

$561 = 3.11.17$, $(a,n) = 1$, $a^{n-1} = 1\ mod\ n$ olmak üzere; $(a, 561) = 1$

$$a^{560} = 1\ mod\ 561$$

n'in asal mı yoksa bileşik mi olduğunu test etmek için, rasgele bir a seçilir ve bir $a^{n-1} \equiv mod\ n$ hesaplanır.

i) Eğer $a^{n-1} = 1\ (mod\ n)$ ise olası bir asal sayıyı belirtir ve isteğe bağlı olarak test birkaç kez daha tekrarlanır.

ii) Eğer $a^{n-1} \neq 1(mod\ n)$ ise n, bileşiktir ve durur.

Teorem 4.1.2. (Wilson) Eğer p asal sayı ise p, $(p-1)! + 1$ 'i böler. Yani, $(p-1)! \equiv -1\ mod\ p$ 'dir.

İspat. $p = 2$ için denkliğin sağlandığı açıktır. $p > 2$ kabul edersek p bir tek sayı olur. $x^{p-1} - 1 = 0\ mod\ p$ polinom denkliğinin çözümleri, (Fermat teoreminden dolayı) $x = 1, 2, 3, \ldots, p-1$'dir. O halde, her bir kök polinomun çarpanı olacağından;

$x^{p-1} - 1 = (x-1)(x-2)\ldots(x-(p-1))\ (mod\ p)$ olur. Şimdi bu özdeşlikte, $x = 0$ yazarsak, sağ tarafta çift sayıda çarpan olduğundan; $(p-1)! = -1\ (mod\ p)$ elde edilir.

4.2. Euler Testi

n tek olan bir asal ise, bir tamsayının $mod\ n$'de en fazla iki karekökü olabileceğini biliyoruz, özellikle, 1'in kareköklerı ± 1'dir.

Eğer bir $a \neq 0\ mod\ n$ ise $a^{\frac{(n-1)}{2}}$, $a^{n-1} = 1\ mod\ n$'nin kareköküdür, yani $a^{\frac{(n-1)}{2}} = \pm 1\ mod\ n$ 'dir.

Eğer $a^{\frac{(n-1)}{2}} \neq \pm 1\ mod\ n$ bazı a'lar için $a \neq 0\ mod\ n$ oluyorsa o zaman n bileşiktir.

$a \neq 0 \; mod \; n$ ile rastgele seçilen bir a için $a^{n-1} = 1 \; (mod \; n)$ değerini hesaplayalım.

i) Eğer bir $a^{\frac{(n-1)}{2}} \neq \pm 1 \; (mod \; n)$ ise n,olası bir asaldır. İsteğe bağlı olarak testi birkaç kez tekrarlayalım. Eğer n büyükse ve rastgele seçilmişse, n'nin asal olma olasılığı 1'e çok yakındır.

ii) Eğer bir $a^{\frac{(n-1)}{2}} \neq \pm 1 \; (mod \; n)$ ise n bileşiktir.

Tanım 4.2.1. (Euler yalancı asalı) n tek bileşik tamsayı ve $a \in [n, n-1]$ olsun. Eğer, $(a, n) = 1$ ve $a^{\frac{(n-1)}{2}} = \left(\frac{a}{n}\right) \; (mod \; n) \Rightarrow n$'ye a tabanına göre bir Euler yalancı asalı denir. Bu durumda a'ya da Euler yalancısı denir.

Tanım 4.2.2. (Euler şahidi) n tek bileşik tamsayı ve $a \in [n, n-1]$ olsun. Eğer, $(a, n) > 1$ ve $a^{\frac{(n-1)}{2}} \neq \left(\frac{a}{n}\right) \; (mod \; n) \Rightarrow a,$ tabanına n'nin bileşikliği için bir Euler şahidi denir (Pomerance, 1980; Selfridg, 1980; Wagstaff, 1980).

Örnek 4.2.1. $n = 91$ sayısı ve $a = 9$ tabanını ele alalım.

$9^{45} = 1 \; mod \; 91$ ve $\left(\frac{9}{91}\right) = 1$ dir. Bu durumda 91 sayısı, 9 tabanına göre bir euler yalancı asalıdır.

Örnek 4.2.2. $n = 1387$ ve $a = 2$ alalım.

$a^{(n-1)/2} = 2^{(n-1)/2} = 2^{693} = 512 \neq \pm 1 \; mod \; 1387$ 2, n için bir Euler şahididir fakat Fermat şahidi değildir. Çünkü $2^{n-1} = 1 \; mod \; n$'dir.

Euler, $\{1, \ldots, n-1\}$ 'deki n için şahit sayısı 1224'tür. Bu sayı o aralıktaki sayıların $\approx$ %88,2'sidir.

$n = 49141$ için aşağıdaki tablodan 5, bir Euler şahididir.

a	$a^{(n-1)/2} \; mod \; n$	$\left(\frac{a}{n}\right)$
2	-1	-1
3	1	1
4	1	1
5	8163	1

Euler, $\{1,\ldots,n-1\}$ kümesindeki n için şahit sayısı 36972'dir. Bu, bu aralıktaki sayıların yaklaşık $\%75{,}2$'sidir.

Euler testi, Fermat testinden daha güçlüdür. Fermat testi n'nin bileşik olduğunu tespit ederse, Euler testi de yapar. Ancak Euler testi, Fermat testi başarısız olsa bile n'nin bileşik olduğunu bulabilir. n, tek bir bileşik tam sayıysa, Euler testi için en az 4 kareköke sahiptir.

Böylece, $(a^{\frac{(n-1)}{2}} \equiv \beta\ (mod\ n)$ değerine sahip olabiliriz; burada $\beta \neq \pm 1$, 1'in kareköküdür. Daha sonra bir $a^{n-1} = 1\ (mod\ n)$ denkliği durumunda, Fermat Testi sayıyı muhtemel bir asal sayı olarak bildirir, ancak Euler testi (doğru şekilde) n'yi bileşik olarak bildirir.

Teorem 4.2.1. E kümesi n nin kompozitliğine şahitlik eden bir küme olsun. Bu durumda $\mathbb{Z}_n^*$'ın elemanlarının en az yarısı n'nin kompozitliğine şahitlik eder.

İspat. E, $\mathbb{Z}_n^*$ 'de şahit olmayanların kümesi olsun; yani bir $a \in E$ için $a^{n-1} = 1\ mod\ n$ anlamına gelir. Açıkça, $1 \in E$'dir. Eğer $a, b \in E$ ise o zaman $(ab)^{n-1} = a^{n-1} \cdot b^{n-1} = 1 \cdot 1 = 1\ mod\ n$'dir ve dolayısıyla $ab \in E$'dir. Bu durumda E'nin $\mathbb{Z}_n^*$'nin bir alt grubu olduğu sonucuna varıyoruz. (Varsayımla) en az bir şahit olduğu için, $E, \mathbb{Z}_n^*$'nin bir özalt grubudur. Daha sonra $\mathbb{Z}_n^*$ elemanlarının en azından yarısının E olmadığını (ve dolayısıyla şahit olduğunu) gösteren $|E| \leq |\mathbb{Z}_n^*|/2$ ifadesi yazılabilir. n birleşik sayı olsun. n'nin kompozit olduğuna dair bir şahit varsa, en azından $|\mathbb{Z}_n^*|/2$ şahit vardır. Algoritmanın herhangi bir yinelemesinde bir şahit veya $\mathbb{Z}_n^*$'de bulunmayan bir eleman bulma ihtimalimiz bu nedenle en az

$$\frac{\frac{|\mathbb{Z}_n^*|}{2} + \left((n-1) - |\mathbb{Z}_n^*|\right)}{n-1} = 1 - \frac{|\mathbb{Z}_n^*|/2}{(n-1)} \geq 1 - \frac{|\mathbb{Z}_n^*|/2}{|\mathbb{Z}_n^*|} = \frac{1}{2}$$

dir. Dolayısıyla algoritmanın yinelemelerin hiçbirinde şahit bulunamaması olasılığı (ve dolayısıyla algoritmanın yanlışlıkla 'asal' çıkma olasılığı") en fazla 2^{-t} 'dir (Katz ve ark., 2008).

Örnek 4.2.2. $2^{340} = 1\ mod\ 341$ olmasına rağmen 341 bileşik sayıdır.

$5^{560} = 1\ mod\ 561$ olmasına rağmen 561 bir Carmichael ya da bileşik sayıdır.

341 bileşik sayı olmasına rağmen $2^{170} = 1\ mod\ 341$'dir.

$5^{280} = 67 \neq \pm 1\ mod\ 561$ burada 561 bileşik sayıdır. Böylece 561 sayısı Euler testini geçmedi. Buradan 561'in 5 tabanına göre Euler testi için bileşikliğinin kesin olduğu sonucuna varılabilir ve burada 561, 5 tabanına göre bir Euler şahididir. Fakat 341 sayısı 2 tabanına göre Euler testini geçti. O halde 341, 2 tabanına göre bir Euler yalancı asalıdır.

1729 ve 2465 tamsayıları, mutlak Euler yalancı asalları (mutlak Fermat yalancı asalları, yani Carmichael sayıları ile benzerlik gösterir) olarak adlandırılır.

Bunlar, $(a, n) = 1$ olan her a için bir $a^{\frac{(n-1)}{2}} \neq \pm 1\ mod\ n$ olacak şekilde bileşik tek tam sayılardır.

4.3. Miller-Rabin Testi

Bir sayının asal olup olmadığını test etmek için kullanılan en yaygın yöntemlerden biri de Michael Rabin tarafından Gary Miller'ın fikirlerine dayanarak geliştirilen Miller-Rabin Asallık Testidir. Hata oranı oldukça düşüktür (Arnault, 1995).

Asallık testi algoritmaları olasılık temelli yöntem ve deterministik yöntem olarak sınıflandırılır. Olasılık tabanlı yöntem hızlıdır ancak yanlış karar verme olasılığı yüksektir. Deterministik yönteminin en büyük özelliği yanlış karar vermemesidir. Ancak test hızı o kadar düşük ki pratik uygulamalarda olasılık tabanlı yöntem kadar uygun değildir. Miller-Rabin algoritması, Fermat'ın Küçük Teoremi'ni kullanarak iyileştirmeler gerçekleştirir. Fermat'ın Küçük Teoremi'ne karekökü dahil eder (Rabin, 1980; Miller, 1976). Miller-Rabin asallık testinde, Fermat testinin karekök testi ile uygun bir şekilde birleştirilmesi sonucu bazen ¼ oranında yanlış karar verme olasılığı neticesinde güçlü yalancı asal kararlaştırılır. Testte birden fazla taban sayısının seçilmesi, bu yanlış karar verme olasılığını son derece düşük bir seviyeye çekebilir. Örneğin; testte 64 temel sayı seçmek $1 / (464)$ yanlış karar verme olasılığına neden olabilir. Testte, $n - 1$, m ve 2'lik tek sayıdaki eleman ile temsil edilir.

$$n - 1 = m.2^k$$

taban sayısı Fermat testi şeklinde yazılabilir. İfadeyi a tabanında yazarsak,

$$a^{n-1} = a^{m.2^k} = [a^m]^{2^k}$$

elde edilir. Dikkat edilmesi gereken $a^{n-1}\ mod\ n$ tek adımda değil, $k + 1$ adımda hesaplanır. Bu durum örnek alınarak her adımda karekök testi yapılabilir. Karekök testi başarısız olursa, "n" ifadesinin bileşik olduğu anlamı çıkar. Her adım doğruysa sadece Fermat testi değil, aynı zamanda tüm karekök testlerinin geçerliliğinden emin olabiliriz.

Fermat'ın teoreminden çok daha yüksek bir olasılıkla bu asallığı test etmeyi sağlayan basit bir uzantı vardır. Bu durum, iki gerçeğe dayanmaktadır:

1. Bir cisim üzerinde, $x^2 = 1$ karesel denkleminin iki çözümü vardır: 1 ve −1.

2. $mod\ n$ tamsayı olan $\mathbb{Z}_n$, n bir asal sayı olduğunda tam olarak bir cisim oluşturur. Miller-Rabin testi aşağıdaki gibi çalışır: n asallığı test etmek için bir tek sayı olsun.

1) $n - 1$, $m.2^s$ formunda bir sayı olsun (burada n tek sayı olduğundan $n - 1$ çift sayı olur ve 2 nin kuvvetlerini barındırır. s≥ 1).

2) $1 < a < n - 1$ olacak şekilde bir a taban sayısı seçilir ve aşağıdaki hesaplamalar yapılır:

$$(*) \qquad a^m mod n, (a^m)^2 mod n, \dots (a^m)^{2^s} mod\ n$$

Bu hesaplama tamamlanır. Şimdi de bu hesaplamaların sonucunu yorumlayalım:

$(a^m)^{2^s} = a^{n-1} = 1\ mod\ n$ (Fermat teoremi gereği), $(a, n) = 1$.

Not: Eğer $(a, n) > 1$ ise n asal sayı değildir. Bu nedenle sayılar dizisinin (*) ile bitmesi gerekir, aksi takdirde n asal değildir. (*) ile bittiğini varsayarak devam eden sayıyı düşünelim. Burada x sayısını arayacağız. Eğer n asal ise $\mathbb{Z}_n$, $x = -1$ veya 1 anlamına gelen bir cisimdir. Bu nedenle (*) her zaman 1 veya −1 ile devam etmelidir. Bu olursa sayının "muhtemelen" asal olduğu sonucuna varılır. Bu testin n'den küçük olan değerlerin en fazla 1/4'ü için yanlış cevap verdiği kanıtlanabilir. n bileşik sayı ise ve a tabanını kullanan yukarıdaki test "asal" çıktısını verirse, n, a tabanına güçlü bir yalancı asal denir. Uygulamada bu tür sayılar oldukça nadirdir (Koblitz, 1994).

Örnek 4.3.2. n = 972133929835994161 sayısını alalım ve $a = 2$ olsun. Bu durumda,

(n bir carmichael sayısı)

$$n-1=a^k.m=972133929835994160\ =2^4.60758370614749635.$$

$$2^{60758370614749635}\equiv 338214802923303483\equiv(mod972133929835994161)$$

$$2^{2.60758370614749635}\equiv 338214802923303483^2\equiv(mod972133929835994161)$$
$$\equiv 332176177406351611 8\equiv(mod972133929835994161)$$

$$2^{2^2 60758370614749635}\equiv 332176177406351611 8^2\equiv(mod972133929835994161)$$
$$\equiv 779803551049098051\equiv(mod972133929835994161)$$

$$2^{2^3.60758370614749635}\equiv 779803551049098051^2\equiv(mod972133929835994161)$$
$$\equiv 1$$

Bu sonuç n'nin bileşik sayı olduğunu gösterir.

Örnek 4.3.3. $n = 2857191047211793$ için bir $a = 1003$ kullanarak, bir Carmichael sayısı olmayan, bileşik olan bir tamsayı test edeceğiz.

$n - 1 = 2^4 \cdot 178574440450737$ ve $a = 1003$ olsun.

$$1003^{178574440450737}\equiv 1135781085623492\ (mod2857191047211793\ )$$

$$1003^{2.178574440450737}\equiv 1135781085623492\ ^2\ (mod\ 2857191047211793)$$
$$\equiv 84313648747407\ (mod2857191047211793\ )$$

$$1003^{2^2.178574440450737}\equiv 84313648747407\ ^2\ (mod\ 2857191047211793)$$
$$\equiv 2321094267189023\ (mod2857191047211793\ )$$

$$1003^{2^3 178574440450737}\equiv 2321094267189023^2\ (mod2857191047211793\ )$$
$$\equiv 978857874792606\ (mod2857191047211793)$$

Bu sonuca göre n bileşik bir sayıdır.

4.4. Solovay-Strassen Testi

Jacobi sembolünü ifade eden $\left(\frac{a}{n}\right)$ ve n asal ise bu ifadenin Legendre sembolüne eşdeğer olduğunu hatırlayalım. Solovay-Strassen testi aşağıdaki gerçeğe dayanmaktadır.

Tanım 4.4.1. (Euler kriteri) n asal olan tek sayı olsun. $(a,n)=1$ şartını sağlayan her a pozitif tamsayısı için $a^{(n-1)/2}=\left(\frac{a}{n}\right)(mod\ n)$'dir.

Böylece, p değerine sahipsek ve bunun asal olup olmadığını belirlemek istiyorsak, a'nın rastgele değerlerini kontrol edebilir ve yukarıdaki eşitliğin doğruluğundan emin olabiliriz. Eğer bu eşitlik doğru değilse, p'nin asal olmaması gerektiğini biliyoruz.

Teorem 4.4.1. (Solovay-Strassen). n tek bir bileşik pozitif tamsayı olsun. $\{2,\ldots,n-1\}$ için de bir tamsayı vardır. Öyle ki, $(a,n)=1$ ve $a^{(n-1)/2}\neq\left(\frac{a}{n}\right)\ mod\ n$'dir.

İspat. Tüm pozitif tamsayılar n'yi geçmeyecek ve n'yi göreceli olarak asal olarak kabul edersek, $a^{(n-1)/2}=\left(\frac{a}{n}\right)\ mod\ n$ olduğunu varsayalım. Eğer $(a,n)=1\ ise$ bu denkliğin her iki tarafının karesini alırsak, $a^{n-1}=\left(\frac{a}{n}\right)^2=(\pm1)^2=1\ mod\ n$ olduğunu görürüz. Dolayısıyla, n bir Carmichael sayısı olmalıdır. Bu nedenle, $n=q_1q_2\ldots q_r$ olduğunu biliyoruz ki burada $q_1,\ q_2\ldots,q_r$ farklı tek asal sayılardır.

Şimdi, $1\leq a\leq n$ ve $(a,n)=1$ olan tüm tamsayılar için bir $a^{(n-1)/2}=1\ mod\ n$ olduğunu gösterelim. a'nın (n) gibi bir tamsayı olduğunu varsayalım.

$a^{(n-1)/2}=-1\ mod\ n$ olduğunu söyleyebiliriz.

$1<b<n$ ve $(b,n)=1$ ve $b\equiv a\ (mod\ q_1),\ \ b\equiv 1\ (mod\ q_1q_2\ldots q_r)$ olan bir tamsayı bulmak için çin kalan teoremini kullanıyoruz.

Daha sonra $b^{(n-1)/2}=a^{(n-1)/2}=-1\ (mod\ q_1)$ ve $b^{(n-1)/2}=1\ (mod\ q_1q_2\ldots q_r)$ olduğunu gözlemledik. Son iki denklikten bu denkliklerle çelişen $b^{(n-1)/2}\neq\pm1\ mod\ n$ yani, $a^{(n-1)/2}=\left(\frac{a}{n}\right)(mod\ n)$ denkliği yazılabilir. Bu nedenle, $1\leq a\leq n$ ve $(a,n)=1$ olan her biri için bir $a^{(n-1)/2}=1\ mod\ n$ olmalıdır. Sonuç olarak, Euler yalancı asalı tanımından, $1\leq a\leq n$ ve $(a,n)=1$ için $a^{(n-1)/2}=\left(\frac{a}{n}\right)(mod\ n)$ olduğunu biliyoruz. Ancak, bu mümkün değildir. Bu nedenle, orijinal varsayım yanlıştır. $[2,n-1]$ aralığında $(a,n)=1$ ve $a^{(n-1)/2}\neq\left(\frac{a}{n}\right)(mod\ n)$ olacak şekilde en az bir tam sayı olmalıdır (Rosen, 1984).

Algoritma. Solovay-Strassen olasılıksal asallık testi

Solovay-Strassen (n, t)

GİRDİ: $n \geq 3$ tek bir tamsayı ve $t \geq 1$ güvenlik parametresi.

ÇIKTI: "asal mı?" sorusuna cevap: "asal" veya "bileşik".

1. 1'den t'ye kadar olanları yapmak için:

   1.1 $2 \leq a \leq n-2$ ve $(a, n) = 1$ olacak şekilde rasgele bir tamsayı seç.

   1.2 r'yi hesapla, $r = a^{(n-1)/2} \, (mod\ n)$.

   1.3 Eğer $r \neq 1$ ve $r \neq n-1$ ise "bileşik" cevabı dön.

   1.4 Jacobi sembolünü hesapla $s = \left(\frac{a}{n}\right)$.

   1.5 Eğer $r \neq s (mod\ n)$ ise "bileşik" cevabı dön.

2. "Asal" a geri dön.

(Bektaş, 2005).

n bir tek bileşik tamsayı olsun. Solovay-Strassen'in (n, t) n'nin "asal" olduğunu bildirme olasılığı $1/2^t$ 'den azdır. Modüler kuvvet alma için hızlı algoritmalar kullanan Solovay-Strassen olasılıksal asallık testi algoritmasının çalışma süresi $O(t.log3n)$'dir. Burada t bir rastgele sayı, a test ettiğimiz sayı ve n birincillik için test etmek istediğimiz değerdir. Algoritmanın başarısız olma olasılığı $1/2^t$ 'dir. Kriptografi amaçları için, 100 gibi yeterince büyük bir t değeri seçersek, algoritmanın başarısız olma şansı o kadar küçüktür ki, şifreleme uygulamalarında kullanılabilir.

4.5. AKS (Agrawal-Kayal-Saxena) Testi

Teorem 4.5.1. (Agrawal, Kayal ve Saxena) bir $a \in \mathbb{Z}$, $n \in \mathbb{N}, n \geq 2$ ve $(a, n) = 1$ olsun.

$(x + a)^n \equiv (x^n + a) \, mod\ n$ 'dir.

İspat. $0 < i < n$ için x^i 'nin yani $((x + a)^n - (x^n + a))$ katsayıları, $\binom{n}{i}a^{n-i}$dir. Varsayalım ki n bir asal sayı olsun. O zaman binomun katsayıları, $\binom{n}{i} \equiv 0\ (mod\ n)$ her $1 \leq i \leq n-1$ tarafından bölünebilir.

Fermat'ın Küçük Teoremi'ne $a^n \equiv a\ mod\ n$ ifadesi uygunluk gösterir. Şimdi n'nin kompozit (bileşik) olduğunu ve q'nun $q^k \nmid n$'nin bir asal çarpanı olduğunu varsayalım. Buradan, binomun katsayılarını;

$\binom{n}{q} = \frac{n!}{q!(n-q)!} = \frac{n.(n-1)\ldots(n-q+1)}{1.2\ldots q}$ şeklinde yazabiliriz. Paydanın $q^k \nmid n$ olduğunu biliyoruz ama q asaldır ve paydaki diğer sayıların hiçbirini bölmez. Ayrıca $q^k \nmid q!$ 'dur. Bu yüzden q'nun $\binom{n}{q}$ de mertebesi $k-1$ ve $q^k \nmid n\ q$ 'dur. $(a,n) = 1$, böylece $(a,q) = 1$ ve $q \nmid a^{n-q}$ 'dir. Dolayısıyla, x^q 'nun katsayısı $\binom{n}{q} a^{n-q} \neq 0\ (mod\ q^k)$ ve dolayısıyla $\binom{n}{q} a^{n-q} \neq 0\ mod\ n$ 'dir. Bunun anlamı $\mathbb{Z}_n$'de

$(x + a)^n \equiv (x^n + a) \neq 0$'dır (Agrawal, Kayal ve Saxena, 2004).

Örnek 4.5.1.

$n = 3$ ve $a = 2$ alalım. Teorem gereği;

$$(x + 2)^3 \equiv (x^3 + 2)\ mod\ 3$$

$$(x + 2)^3 \equiv x^3 + 6x^2 + 12x + 8$$

$\equiv (x^3 + 2)\ mod\ 3$'tür. Buradan $x^2\ ve\ x$'in katsayılarının $mod\ 3$'e göre 0 olduğunu ve sabit terimin de $mod\ 3$'e göre değerinin 2 olduğu sonucu ortaya çıkar. Burada n'nin yani 3'ün asal olduğunu gördük.

Şimdi de $n = 4\ ve\ a = 3$ alalım.

$(x + 3)^4 = (x^4 + 3)\ mod\ 4$ olup olmadığı kontrol edilir.

$$(x + 3)^4 \neq x^4 + 12x^3 + 54x^2 + 108x + 81$$

$$\neq x^4 + 2x^2 + 1\ mod\ 4$$

$$\neq x^4 + 3\ mod\ 4$$

Buradan da anlaşıldığı gibi 4 bir bileşik sayıdır.

Algoritma. AKS asallık testi

Şayet $a > 0$ ve $b > 1$ için $n = a^b$ eşitliği sağlanıyorsa, n sayısı asal değildir.

$or(n) > log2(n)$ denklemini sağlayan en küçük r değeri bulunur.

Şayet $1 < (a, n) < n$ denklemini sağlayan bir $a \leq r$ *değeri bulunabiliyorsa sayı asal değildir.*

Şayet n ≤ r ise n asal sayıdır.

a değeri 1'den $\lfloor \sqrt{\varphi(r)}\, log(n) \rfloor$ değerine kadar olan değerler için,

Şayet $(x + a)^n \neq x^n + a \ (mod\ x^r - 1, n)$ eşitsizliği sağlanıyorsa sayı asal değildir.

Yukarıdaki şartlardan geçerse, sayı asaldır.

(Anonim-4, 2020).

4.6. Testlerin Karşılaştırılması

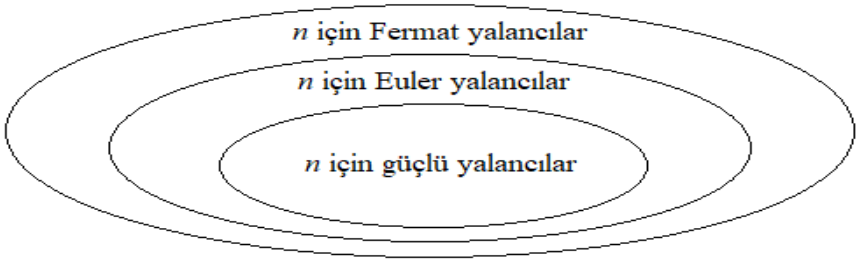
Aşağıdaki gerçek, Fermat yalancıları, Euler yalancıları ve güçlü yalancılar arasındaki ilişkileri açıklamaktadır. n, tek bir bileşik tamsayı olsun.

$i)$ a, n için bir Euler yalancısıysa, n için de bir Fermat yalancısıdır.

$ii)$ a, n için güçlü bir yalancıysa, n için de Euler yalancısıdır.

Örnek 4.6.1. (Fermat, Euler, güçlü yalancıları)

$n = 65$ bileşik tamsayısını ele alalım. Bu sayı için Fermat yalancıları $\{1, 8, 12, 14, 18, 21, 27, 31, 34, 38, 44, 47, 51, 53, 57, 64\}$'dir. Euler yalancıları ise $\{1, 8, 14, 18, 47, 51, 57, 64\}$ iken güçlü yalancılar $\{1, 8, 18, 47, 57, 64\}$'dir. Sabit bir bileşik n için, Şekil 4.2. incelenebilir.



Şekil 4.2. Testlerin Karşılaştırılması.

Miller-Rabin testi daha karmaşık görünse de, aslında, en kötüsü, modüler çarpımlar açısından Fermat'ın testiyle aynı miktarda hesaplama yapılmasını gerektirir. Bu nedenle Miller-Rabin testi, Fermat'ın tüm yönleriyle yaptığı testten daha iyidir. En kötüsü, Miller-Rabin $(n, 1)$ 'de tanımlanan hesaplamaların sırası, $a^{(n-1)/2}\ (mod\ n)$ 'nin eşdeğerini gerektirir. Aynı zamanda, Miller-Rabin'in $(n, 1)$ Solovay-Strassen'den $(n, 1)$ daha az hesaplama gerektirdiği durumda, ikincisi bir $a^{(n-1)/2}(mod\ n)$ ve muhtemelen başka bir Jacobi'nin hesaplanmasını gerektirir. Bu nedenle, Solovay-Strassen testi bir sayının asal olup olmadığını test etme sırasında Jacobi sembolünün kullanımı sırasında hata yapma olasılığı yüksektir. Bu yüzden bu test, hem hesaplama hem de kavramsal olarak daha karmaşıktır. Solovay Strassen testini (veya Fermat testini) Miller-Rabin testi üzerinde kullanmak için hiçbir neden yoktur. Bunun nedenleri aşağıda özetlenmiştir:

(i). Solovay-Strassen testi hesaplama açısından daha pahalıdır.

(ii). Solovay-Strassen testi, aynı zamanda Jacobi sembol hesaplamaları içerdiğinden daha zordur.

(iii). Solovay-Strassen için hata olasılığı $1/2^t$ ile yukarıda, Miller-Rabin için hata olasılığı $1/4^t$ ile sınırlandırılmıştır.

(iv). n için güçlü bir yalancı aynı zamanda n için bir Euler yalancısıdır. Bu nedenle, doğruluk açısından Miller-Rabin testi hiçbir zaman Solovay-Strassen testinden daha kötü değildir (Bektaş, 2005).

4.7. Bazı Açık Anahtarlı Kriptosistemler

Son zamanlarda, yasadışı veri erişiminden kaynaklanan büyük kayıplar nedeniyle, veri güvenliği kamu, özel ve savunma kuruluşları için önemli bir konu haline gelmiştir. Değerli verileri veya bilgileri yetkisiz erişime, yasa dışı değişikliklere ve çoğaltmaya karşı korumak için çeşitli şifreleme teknikleri kullanılır. Kriptografi, gizli kodla yazma bilimidir. İki temel kriptografik teknik türü vardır (Stinson, 2006). Simetrik ve asimetrik kriptografi. Simetrik şifrelemede, şifreleme ve şifre çözme için aynı anahtar kullanılır. Asimetrik şifrelemede, biri ortak anahtar olarak adlandırılan şifreleme için, diğeri özel anahtar olarak adlandırılan şifre çözme için iki farklı anahtar kullanılır (Paar ve Pelzl, 2010).

4.7.1. RSA Şifreleme Algoritması

RSA, açık anahtarlı bir şifreleme yöntemidir.1978 yılında Ron Rivest, Adi Shamir ve Leonard Adleman tarafından geliştirilmiştir (Rivest ve ark., 1978). Güvenirliği, verilen bileşik bir sayıyı çarpanlara ayırma zorluğuna dayanır. Açık anahtar ile şifrelenen mesaj, gizli anahtar ile aslına dönüştürülür (Stalling, 2006).

RSA, ilk uygulanabilir açık anahtarlı şifreleme sistemlerinden biri olarak bilinen ve güvenli veri iletimi için yaygın olarak kullanılan bir şifreleme sistemidir **(**Hoffstein, Pipher ve Silverman, 2008). Böyle bir şifreleme sisteminde, şifreleme anahtarı herkese açıktır ve gizli tutulan şifre çözme anahtarından farklıdır. RSA'da bu asimetri, iki büyük asal sayının çarpımını çarpanlarına ayırma zorluklarına dayanmaktadır (Gura, Patel, Wander, Eberle ve Shantz, 2004).

RSA'da asal çarpanlar gizli tutulmalıdır. Herkes bir mesajı şifrelemek için ortak anahtarı kullanabilir, ancak şu anda yayınlanan yöntemlerle, ortak anahtar yeterince büyükse, yalnızca asal çarpanları bilen biri mesajı uygun bir şekilde çözebilir. RSA şifrelemesini kırmak, RSA sorunu olarak bilinir. Çarpanlara ayırma problemi kadar zor olup olmadığı açık bir sorudur **(**Hoffstein, Pipher ve Silverman, 2008; Rivest, Shamir, Adleman, 1978).

4.7.1.1. RSA kriptosistemi için anahtar üretimi

Anahtar üretmek isteyen Erol şu yolları izler:

1. p ve q gibi farklı iki büyük asal sayı seçer.
2. $n = p.q$ değerini hesaplar.
3. $\varphi(n) = (p-1).(q-1)$ değerini hesaplar.
4. $1 < e < \varphi(n)$ ve $ebob\big(e, \varphi(n)\big) = 1$ olacak şekilde rastgele bir e sayısı seçer.
5. $e.d \equiv 1 \bmod (\varphi(n))$ denkliğini sağlayan d sayısını hesaplar.
6. Erol'un açık anahtarı (n, e); gizli anahtarı d'dir.

4.7.1.2. RSA kriptosistemi için şifreleme

m mesajını şifrelemek isteyen Turgut şu yolları izler:

1. Erol'un açık anahtarına ulaşır.
2. $c \equiv m^e \bmod n$ değerini hesaplar.
3. c şifre metnini Erol'a yollar.

4.7.1.3. RSA kriptosistemi için deşifreleme

Turgut'tan gelen şifre metni çözmek isteyen Erol, kendi özel anahtarını kullanarak $m \equiv c^d \bmod n$ değerini hesaplar ve metnin orijinaline ulaşır.

Algoritmanın doğruluğu: $m$mesajı için $(m^e)^d \equiv m \bmod n$ kongrüansı hesaplanırsa işlemlerin doğruluğu ispatlanmış olur.

$(m^e)^d \equiv m \bmod n$ yani $(m^e)^d \equiv m \bmod (pq)$'dir.

$(m^e)^d \equiv m \bmod p$ ve $(m^e)^d \equiv m \bmod q$ denkliklerine göre,

$(m^e)^d \equiv m \bmod (pq)$ denkliği kanıtlanmış olur.

Fermat Teoremi'nden $ebob(m, p) = 1$ olmak üzere $m^{p-1} \equiv 1 \bmod p$'dir.

$$e.d \equiv 1 \, mod \, \varphi(n).$$

$$e.d \equiv 1 \, mod \, ((p-1)(q-1))$$

$$e.d - 1 \equiv mod \, ((p-1)(q-1))$$

$$e.d - 1 \equiv k \, ((p-1)(q-1)), \; k \in \mathbb{Z}$$

$$(m^e)^{\mathrm{d}} = m^{ed-1}m = m^{k(p-1)(q-1)}m = (m^{p-1})^{k.(q-1)}m$$

$$m^{p-1} \equiv 1 \, mod \, p \text{ olduğundan}$$

$$1.m = m \, mod \, p$$

Dolayısı ile $(m^e)^{\mathrm{d}} \equiv m \, mod \, p$ denkliği de gösterildi. Benzer şekilde, $(m^e)^{\mathrm{d}} \equiv m \, mod \, q$ denkliğini de gösterebilir. Sonuç olarak $c^d \equiv (m^e)^{\mathrm{d}} \equiv m \, mod \, n$ denkliği gösterildi (Menezes ve ark., 2001).

Örnek 4.7.1.3.1.

Anahtar üretimi:

1. Erol, $p = 12611$ ve $q = 12589$ asal sayılarını seçer.
2. $n = 12611.12589 = 158759879$ değerini hesaplar.
3. $\varphi(n) = (p-1).(q-1) = 12610.12588 = 158734680$ değerini hesaplar.
4. $1 < e < \varphi(n)$ ve ebob $(e, \varphi(n)) = 1$ olacak şekilde $e = 7$ sayısını seçer.
5. $d \,.7 \equiv 1 \, mod \, (158759879)$ ise $d = 22676383$ değerini hesaplar.
6. Erol'un açık anahtarı $(158759879{,}7)$; gizli anahtarı (22676383)'tür.

Şifreleme:

1. Turgut, Erol'un açık anahtarına ulaşır.
2. $m = 874519$ düz metnini şifreler;

$$c \equiv m^e \, mod \, n$$

$c \equiv 874519^7 \, mod \, 158759879$ ise $c = 30608246$.

3. Turgut, $c = 30608246$ şifre metnini Erol'a yollar.

Deşifreleme:

Erol, Turgut'tan gelen şifre metni, gizli anahtarı aracılığıyla aşağıdaki işlemleri yaparak orijinaline dönüştürür.

$$m \equiv c^d \, mod \, n$$

$$30608246^{22676383} \, mod \, 158759879 = 874519.$$

4.7.2. Rabin Şifreleme Algoritması

Michael Rabin tarafından 1979 yılında bulunmuş bir asimetrik şifreleme türüdür. Bu tekniğin güvenirliği bileşik sayıları çarpanlara ayırma zorluğuna dayanır (Rabin, 1979).

RSA ortak anahtar şifrelemesi veya RSA dijital imza şemalarındaki genel üs ne kadar küçük olursa, şifreleme işlemi o kadar verimli olur. Michael O. Rabin böylece e = 2'yi seçerek bir şifreleme sistemi oluşturdu. Bu sistem Rabin kriptosistemi olarak adlandırılır. Fakat bu sistem RSA da olduğu kadar basit değildir (Rabin, 1978).

Modüler karekök problemi ile modülün çarpanlara ayrılması arasında denklik verildiğinde, bunu kriptografik uygulamalar için kullanmaya çalışmak doğaldır. Rabin bir açık anahtarlı şifreleme sistemi önerdi (Rabin, 1978).

4.7.2.1. Rabin kriptosistemi için anahtar üretimi

Anahtar üretmek isteyen Erol şu yolları izler:

1. p ve q gibi farklı iki büyük asal sayı seçer.
2. $n = pq$'yu hesaplar.
3. Erol'un açık anahtarı n; gizli anahtarları (p, q)'dur.

4.7.2.2. Rabin kriptosistemi için şifreleme

m mesajını şifrelemek isteyen Turgut şu yolları izler:

1. Erol'un açık anahtarına ulaşır.
2. $c \equiv m^2 \, mod \, n$ değerini hesaplar.
3. c şifre metnini Erol'a yollar.

4.7.2.3. Rabin kriptosistemi için deşifreleme

1. Turgut'tan gelen şifre metni çözmek isteyen Erol, kendi özel anahtarını kullanarak $m \equiv \sqrt{c} \bmod n$ değerini hesaplar.
2. $m^2 \equiv c \, mod \, n$ nin, $k^2 \equiv c \, mod \, p$ ve $k^2 \equiv c \, mod \, q$ gibi iki denk çözümü vardır. Buradan $m = c^{\frac{p+1}{4}} mod \, p$ ve $m = c^{\frac{q+1}{4}} mod \, q$'dur.

Sonuçta, dört kökü çin kalan teoremine göre hesaplar:

$$+mmod \, p$$

$$-m \, mod \, p$$

$$+m \, mod \, q$$

$$-m \, mod \, q$$

Bunlardan biri mesajdır (Galbraith, 2012).

Örnek 4.7.2.3.1.

Anahtar üretimi:

1. Erol, birbirinden farklı $p = 17827 \; ve \; q = 23879$ asal sayılarını seçer.
2. $n = 17827.23879 = 425690933$ değerine ulaşır.
3. $p \equiv 3 \, mod \, 4$, $q \equiv 3 \, mod \, 4$ olacak şekilde p ve q'yu seçtik. (p ve q'yu bu şekilde seçmemizin sebebi kök bulmada bize kolaylık sağlamasıdır).
4. Erol, $m = 119897888$ mesajını seçer ve $c = m^2 mod \, n = 343655015$ değerini hesaplar.

Şifreleme:

1. Turgut, Erol'un açık anahtarı olan 425690933 değerine ulaşır.

2. $m = 119897888$ mesajını seçer ve $c = m^2 \, mod \, n = 343655015$ değerini hesaplar. $c = 343655015$ değerini Erol'a yollar.

Deşifreleme:

$$c \equiv m^2 \, mod \, 425690933 = 343655015$$

$c^{\frac{p+1}{4}}, mod \, p$' ye göre ve $c^{\frac{q+1}{4}}, mod \, q'$ ya göre birer köktürler.

$x \equiv c^{\frac{p+1}{4}} mod \, p$ nin y_1 ve y_2 gibi farklı iki kökü vardır.

$y_1 \equiv c^{4457} mod \, 17827 = 6514, y_2 = 11313$

$x \equiv c^{\frac{q+1}{4}} mod q$'nun y_3 ve y_4 gibi farklı iki kökü vardır.

$y_3 \equiv c^{5970} mod \, 23879 = 22450, \; y_4 = 1429$ çin kalan teoremi gereğince 4 farklı denklem sistemi elde edilir. Şimdi bu denklem sistemlerini çözelim.

1. Denklem sistemini çözelim. Bu çözüme, m_1 diyelim.
   $x \equiv 6514 \, mod \, p$ ve $a_1 = 6514$ diyelim.
   $x \equiv 22450 \, mod \, q$ ve $a_2 = 22450$ diyelim.
   $(p, q) = 1$ buradan öklid algoritması gereği $1 = p.s + q.t$ yazılabilir. Burada $s, t \in \mathbb{Z}$'dir.

Şimdi bu eşitliği $mod \, p$'ye göre hesaplarsak buradan $1 = q.t$ bulunur ve $t = q^{-1} = 6719$ aynı şekilde $mod \, q$'ya göre hesaplarsak buradan, $s = p^{-1} = -9000$ bulunur.

$$m_1 = (a_1.t.q + a_2.s.p) \, mod \, n$$

$$m_1 = 6514.6719.23879 + 22450.(-9000).17827 = 305793045$$

2. Denklem sistemini çözelim. Bu çözüme,m_2 diyelim. Benzer şekilde,
   $x \equiv 6514 \, mod \, p$ ve $a_1 = 6514$ diyelim.
   $x \equiv 1429 \, mod \, q$ ve $a_2 = 1429$ diyelim.

$m_2 = (a_1.t.q + a_2.s.p) \, mod \, n.$

$$m_2 = 6514.6719.23879 + 1429.(-9000).17827 = 228833886$$

3. Denklem sistemini çözelim. Bu çözüme,m_3 diyelim. Benzer şekilde,

   $x \equiv 11313\ mod\ p$ ve $a_1 = 11313$ diyelim.

   $x \equiv 22450\ mod\ q$ ve $a_2 = 22450$ diyelim.

$$m_3 = (a_1.t.q + a_2.s.p)\ mod\ n$$

$m_3 = 11313.6719.23879 + 22450.(-9000).17827 = 96857047.$

4. Denklem sistemini çözelim. Bu çözüme , m_4 diyelim. Benzer şekilde,

   $x \equiv 11313\ mod\ p$ ve $a_1 = 11313$ diyelim.

   $x \equiv 1429\ mod\ q$ ve $a_2 = 1429$ diyelim.

$$m_4 = (a_1.t.q + a_2.s.p)\ mod\ n$$

$$m_4 = 11313.6719.23879 + 1429.(-9000).17827 = 119897888.$$

Görüldüğü gibi mesaj (m), m_1, m_2, m_3, m_4 köklerinden birine eşittir. Buradaki kök, m_4 tür.

5. SONUÇ

Geçmişten bugüne asal sayılar üzerine yapılan çalışmalar devam etmekte ve asal sayılar gizemini korumaya devam etmektedir. Küçük asal sayıları bulmak kolaydır fakat büyük asal sayıları bulmak için ufak asallara bölme işlemi gibi işlemler oldukça zaman almaktadır.

Daha kısa sürede asal sayı belirlemek için çeşitli asal sayı test algoritmaları geliştirilmiştir. Fakat bu testler sayının asal olduğunu kesin olarak ilan eden ve büyük bir ihtimalle asal olduğunu söyleyen testler olarak ikiye ayrılmıştır. Bu testler olasılıksal (probabilistic) ve kesin (deterministic) testler olarak adlandırılır. Bu tezde Fermat, Euler, Miller-Rabin ve Slovay-Strassen gibi oldukça sık kullanılan bir sayının olası asal olduğunu söyleyen testler ve bir sayının kesin olarak asal olduğunu söyleyen AKS testi hakkında geniş bilgiler ve örneklere yer verilmiştir. Ayrıca asimetrik kriptosistemlerden RSA kriptosistemi ve Rabin kriptosistemi hakkında bilgi verilmiş olup bunlar, örneklerle desteklenmiştir.

KAYNAKLAR

Adleman, L. M., Huang, M.-D. A., 1992. ***Primality Testing and Abelian Varieties Over Finite Felds***, Springer.

Agrawal, M., Kayal, N., Saxena, N., 2004. PRIMES is in P, ***Annals of Mathematics,* 160** (2): 781-793.

Anonim-1, 2020. ***https://www.quora.com/Re-Ulam-spiral-How-exactly-does-highlighting-the-prime-numbers-on-an-existing-plane-justify-renaming-the-entire-plane-after-the-person-that-made-that-single-observation***. Erişim tarihi: 04.02.2020.

Anonim-2, 2020. ***https://medium.com/cantors-paradise/unexpected-beauty-in-primes-b347fe0511b2***. Erişim tarihi. 04.02.2020.

Anonim-3, 2020. ***http://mathworld.wolfram.com/PrimeNumberTheorem.html***. Erişim tarihi. 04.02.2020.

Anonim-4, 2020. ***http://bilgisayarkavramlari.sadievrenseker.com/2011/04/13/aks-asallik-testi-aks-primality-test/.*** Erişim tarihi. 01.02.2020.

Arnault, F., 1995. Rabin-Miller Primality Test: Composite Numbers Which Pass It, ***Mathematics of Computation,* 64** (209): 355-361.

Atkin, A. O. L., 1986. Manuscript, ***Lecture Notes of a conference***, Boulder CO., 1986.

Ball, W. W. R., Coxeter, H. S. M., 1987. ***Mathematical Recreations and Essays,*** 13th ed. New York. Dover, 61.

Bektaş, A., 2005. ***Probabilistic Primality Tests***, Master's Graduate Project, METU.

Berlekamp, E., 2015. ***Algebraic Coding Theory,*** Revised Edition. World Scientific Publish. Co.

Bernstein, D. J., 2007. Proving primality in essentially quartic random time, ***Mathematics of Computation,* 76** (257): 389-403.

Carmichael, R. D., 1910. Note on a number theory function. ***Bull. Amer. Math. Soc.,* 16**: 232–238.

Derbyshire, J., 2004. The Prime Number Theorem. Ch. 3 in ***Prime Obsession****:* Bernhard Riemann and the Greatest Unsolved Problem in Mathematics. New York. Penguin, 32.

Dorsey, Z. S., 1999. Methods of Primality Testing, MIT ***Undergraduate Journal of Mathematics,*** 133.

Erdoğan, M., Yılmaz, G., 2008. Çözümlü Problemlerle ***Soyut Cebir ve Sayılar Teorisi***, Beykent Üniversitesi.

Erdős, P., 1949. Démonstration élémentaire du théorème sur la distribution des nombres premiers. ***Scriptum 1***, Centre Mathématique, Amsterdam.

Galbraith, S., 2012. ***Mathematics of Public Key Cryptography***. Cambridge University Press, New York.

Gilbert, L., Gilbert, J., 2009. ***Elements of Modern Algebra.***

Gilles, D., 1964. Three New Mersenne Primes and a Statistical Theory, ***Mathematics of Computation,* 18** (85): 93-97.

Goldwasser, S., Kilian, J., 1986. Almost all primes can be quickly certified. STOC' 86: ***Proceedings of Annual ACM Symposium on the Theory of Computing***. 316.

Gura, N., Patel, A., Wander, A., Eberle, H., Shantz, S. C., 2004. ***CHES 2004: Cryptographic Hardware and Embedded Systems***.

Hadamard, J., 1896. Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques ***Bull. Soc. Math.,*** **24**: 199-220.

Hardy, G. H., Littlewood, J. E., 1916. Contributions to the theory of the Riemann zeta-function and the theory of the distribution of primes. ***Acta Math.,*** **41**: 119-196.

Hardy, G. H. and Wright, E. M., 1979. Statement of the Prime Number Theorem. §1.8 in ***An Introduction to the Theory of Numbers,*** 5th ed. Oxford, England. Clarendon Press, 9.

Hardy, G. H., 1999. The Proof of the Prime Number Theorem and Second Approximation of the Proof. §2.5 and 2.6 in ***Ramanujan: Twelve Lectures on Subjects Suggested by His Life and Work,*** *3rd ed.* New York. Chelsea., 16, 27., and 28-33.

Havil, J., 2017. ***Gamma: Exploring Euler's Constant***. Princeton, NJ: Princeton University Press.

Hoffman, P., 1998. ***The Man Who Loved Only Numbers****: The Story of Paul Erdős and the Search for Mathematical Truth.* New York. Hyperion.

Hoffstein, J., Pipher, J., Silverman, J. H., 2008. ***An Introduction to Mathematical Cryptography***., Springer.

Ingham, A. E., 1990. ***The Distribution of Prime Numbers.*** London: Cambridge University Press, 83.

Katz, J., Lindel, Y., 2008. ***Introduction to Modern Cryptography***, Taylor and Francis Group.

Kılıç, A., Sert, V., 2012. ***Çin Kalan Teoremi***. Çanakkale Onsekiz Mart Üniversitesi.

Knuth, D. E., 1998. ***The Art of Computer Programming****, Third edition, Seminumerical Algorithms.* Addison-Wesley.

Koblitz, Neal., 1994. Graduate Texts in Mathematics: ***A Course in Number Theory and Cryptography***. Second Edition. Springer. New York.

Landau, E., 1974. ***Handbuch der Lehre von der Verteilung der Primzahlen****, 3rd edition.* Chelsea Pub.

Landau, E., 1990. ***Elementare Zahlentheorie****.* AMS Chelsea Publishing.

Lehman, R. S., 1966. On the Difference $\pi(x) - \mathrm{Li}(x)$. ***Acta Arith.,*** **11**: 397-410.

Marques, D., 2014. On Generalized Cullen and Woodall Numbers That are Also Fibonacci Numbers. **Journal of Integer Sequences. 17**.

Menezes, J.A., Vanstone, S.A., Van Oorschot, P.C., 2001. ***Handbook of Applied Cryptography***. CRC Press. 816.

Miller, G. L., 1976. Riemann's hypothesis and tests for primality. ***Journal of Computer and System Sciences.***, **13**: 300–317.

Mollin, A. R., 2002. ***RSA and Public-Key Cryptography***, Chapman and Hall/CRC, 1. Edition.

Nagell, T., 1951. The Prime Number Theorem. Ch. 8 ***in Introduction to Number Theory.*** New York. Wiley. 275.

Paar, C., Pelzl, J., 2010. ***Understanding Cryptography***, A Textbook for Students and Practitioners, Springer.

Pomerance, C., Crandall, R., 2005. ***Prime Numbers: A Computational Perspective,*** 2nd ed. New York. Springer-Verlag.

Pomerance, C., Selfridge, J. L., Wagstaff, S. S., 1980. The Pseudoprimes to $25 \cdot 10^9$ ***Mathematics of Computation,*** **35** (151): 1003-1026.

Rabin M O., 1980. Probabilistic algorithm for testing primality, ***Journal of Theory,*** **12** (1): 128-138.

Rabin, M.O., 1978. Digitalized signatures. ***Foundations of Secure Computation,*** eds. R. Lipton and R. De Millo. Academic Press, New York, 155–166.

Rabin, M.O., 1979. Digitalized signatures and public-key functions as intractable as factorization. MIT/LCS/TR-212, ***MIT Laboratory for Computer Science***, Cambridge.

Ribenboim, P., 1996. ***The New Book of Prime Number Records***. New York: Springer-Verlag.

Riemann, B., 1859. Über die Anzahl der Primzahlen unter einer gegebenen Grösse. ***Monatsberichte der Berliner Akademie***.

Riesel, H., 1994. The Remainder Term in the ***Prime Number Theorem. Prime Numbers and Computer Methods for Factorization,*** 2nd ed. Birkhäuser, Boston. 6.

Rivest, R. L., Shamir, A., Adleman, L., 1978. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. ***Communications of the ACM.,*** **21** (2): 120–126.

Robinson, R. M., 1954. Mersenne and Fermat Numbers. **Proc. Amer. Math. Soc., 5**, 842-846.

Rosen, K. H., 1984. ***Elementary Number Theory and Its Applications***, Addison-Wesley, publishing Company.

Rubinstein, M., Sarnak, P., 1994. Chebyshev's Bias. ***Experimental Mathematics,*** **3** (3): 173-197.

Selberg, A., 1949. An Elementary Proof of the Prime Number Theorem. ***Annals of Mathematics,*** **50** (2): 305-313.

Singh, S., 1998. ***Fermat's Enigma***: The Epic Quest to Solve the World's Greatest Mathematical Problem.

Smith, D. E., 1984. ***A Source Book in Mathematics.*** Dover publications.

Solovay, R., Strassen, V., 1977. A fast Monte-Carlo test for primality, ***SIAM Journal on Computing,*** **6** (1): 84–86.

Stalling, W., 2006. ***Cryptography and Network Security*** Principal and Practice. Pearson Publishing, Fifth Edition, USA.

Stinson, D. R., 2006. ***Cryptography: Theory and Practice*** Third edition. CRC Press.

Takashi, A., 2000. On Sophie Germain primes. **Tatra Mt. Math. Publ., 20**, 65-73.

Wagon, S., 1991. ***Mathematica in Action***. New York: W. H. Freeman and Company.

Walfisz, A., 1963. Ch. 5 in ***Weyl'sche Exponentialsummen in der neueren Zahlentheorie***. Berlin: Deutscher Verlag der Wissenschaften.

Wiener, N., 1959. §19 et seq. in ***The Fourier Integral and Certain of Its Applications***. Dover Pub.

ÖZ GEÇMİŞ

1988 yılında Van'da doğdu. İlk ve orta öğrenimini aynı şehirde tamamlayarak, 2005 yılında Van Yüzüncü Yıl Üniversitesi Matematik Bölümü'ne yerleşti. 2013 yılında ise aynı üniversitenin Matematik Anabilim Dalı'nda Yüksek Lisans programına başladı.

T.C
VAN YÜZÜNCÜ YIL ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
LİSANSÜSTÜ TEZ ORİJİNALLİK RAPORU

Tarih: 16/12/2019

Tez Başlığı / Konusu: Asal sayı Test Algoritmaları ve Kriptolojideki Uygulamaları Üzerine

Yukarıda başlığı konusu belirlenen tez çalışmamın Kapak sayfası, Giriş, Ana bölümler ve Sonuç bölümlerinden oluşan toplam 82 sayfalık kısmına ilişkin, 16/12/2019 tarihinde şahsım tarafından Turnitin intihal tespit programından aşağıda belirtilen filtreleme uygulanarak alınmış olan orijinallik raporuna göre, tezimin benzerlik oranı % 12 (oniki) dır.

Uygulanan filtreler aşağıda verilmiştir:

- Kabul ve onay sayfası hariç,
- Teşekkür hariç,
- İçindekiler hariç,
- Simge ve kısaltmalar hariç,
- Gereç ve yöntemler hariç,
- Kaynakça hariç,
- Alıntılar hariç,
- Tezden çıkan yayınlar hariç,
- 7 kelimeden daha az örtüşme içeren metin kısımları hariç (Limit inatch size to 7 words)

Van Yüzüncü Yıl Üniversitesi Lisansüstü Tez Orijinallik Raporu Alınması ve Kullanılmasına İlişkin Yönergeyi inceledim ve bu yönergede belirtilen azami benzerlik oranlarına göre tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini bilgilerinize arz ederim.

16.12.2019
Tarih ve İmza

Adı Soyadı: Erol AĞÇAKAYA

Öğrenci No:139102055

Anabilim Dalı: Matematik

Programı: Cebir ve Sayılar Teorisi

Statüsü: Y. Lisans ☒ Doktora ☐

DANIŞMAN ONAYI
UYGUNDUR

Dr. Öğr. Üyesi Turgut HANOYMAK

ENSTİTÜ ONAYI
UYGUNDUR

Prof. Dr. Osman ŞENSOY
Enstitü Müdürü