ANKARA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

POLİNOM ZAMANLI BİR ASALLIK ALGORİTMASI

Süleyman Serkan ÖZÇİM

MATEMATİK ANABİLİM DALI

ANKARA
2018

TEZ ONAYI

Süleyman Serkan ÖZÇİM tarafından hazırlanan "**POLİNOM ZAMANLI BİR ASALLIK ALGORİTMASI**" adlı tez çalışması 10/10/2018 tarihinde aşağıdaki jüri tarafından oy birliği ile Ankara Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Danışman : Doç. Dr. Murat ŞAHİN
Ankara Üniversitesi Matematik Anabilim Dalı

Jüri Üyeleri :

Başkan : Prof. Dr. Sait HALICIOĞLU
Ankara Üniversitesi Matematik Anabilim Dalı

Üye : Doç. Dr. Murat ŞAHİN
Ankara Üniversitesi Matematik Anabilim Dalı

Üye : Doç. Dr. Ebru SOLAK
Orta Doğu Teknik Üniversitesi Matematik Anabilim Dalı

Yukarıdaki sonucu onaylarım.

Prof. Dr. Atila YETİŞEMİYEN
Enstitü Müdürü

ETİK

Ankara Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırladığım bu tez içindeki bütün bilgilerin doğru ve tam olduğunu, bilgilerin üretilmesi aşamasında bilimsel etiğe uygun davrandığımı, yararlandığım bütün kaynakları atıf yaparak belirttiğimi beyan ederim.

10/10/2018

Süleyman Serkan ÖZÇİM

ÖZET

Yüksek Lisans Tezi

POLİNOM ZAMANLI BİR ASALLIK ALGORİTMASI

Süleyman Serkan ÖZÇİM

Ankara Üniversitesi
Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı

Danışman: Doç. Dr. Murat ŞAHİN

Bir n pozitif tamsayısının 1 ve kendisinden başka pozitif böleni yoksa bu sayıya asal sayı denir. Asal sayıların sonsuz çoklukta olduğu ve her pozitif tam sayının asal sayıların çarpımı şeklinde tek türlü yazıldığı Euclid tarafından ispatlanmıştır. Ayrıca bir n pozitif tamsayısının asal olup olmadığını anlamak için çok eski çağlardan bu yana birçok yöntem geliştirilmiştir ve bu konu sayılar teorisinin temel problemlerinden birisidir. Bu tez altı bölümden oluşmaktadır. Giriş bölümünde Antik Yunan'dan (M.Ö. 300) Hindistan'a (2004) uzanan süreçte bir sayının asal olup olmadığını anlamak için ortaya çıkartılan algoritmalardan bahsedilmiştir ve tezin amacı açıklanmıştır. İkinci bölümde tez boyunca kullanılacak temel bilgiler verilmiştir. Tezin üçüncü bölümünde Lucas tarafından bulunan n-1 testine yer verilmiş ve Lucas'ın fikri açıklanmıştır (Özetle: Öyle büyük bir grup inşa et ki n asal olsun). Dördüncü bölümde ise Lucas dizileri yardımıyla elde edilen n+1 testinden bahsedilmiş ve özel olarak sadece Mersenne sayılarının asallığını belirleyen Lucas-Lehmer testi anlatılmıştır. Beşinci bölümde Lenstra tarafından bulunan sonlu cisimlerde asallık testi verilmiştir. Son bölümde ise diğer asallık algoritmalarının arkasındaki fikir geliştirilerek elde edilen, Agrawal, Kayal ve Saxena tarafından bulunan deterministik ve polinom zamanlı bir algoritma AKS verilmiştir.

Ekim 2018, 47 sayfa
Anahtar Kelimeler: Asal sayılar, deterministik algoritma, polinom zamanlı algoritma, asallık testleri, AKS

ABSTRACT

Master Thesis

A POLYNOMIAL TIME PRIMALITY ALGORITHM

Süleyman Serkan ÖZÇİM

Ankara University
Graduate School of Natural and Applied Sciences
Department of Mathematics

Supervisor: Doç. Dr. Murat ŞAHİN

A Positive integer is called prime if it has no positive factor except 1 and itself. There are infinitely many primes and any positive integer can be written uniquely as a product of primes. Euclid proved these two theorems. To determine whether n is a prime or a composite number many algorithms developed over the years and this subject became one of the main problems of the number theory. This thesis consist of six chapters. In the first chapter, the aim of the thesis is explained and the introduction mentioned some algorithms from Ancient Greek (B. C. 300) to India (2004). In the second chapter some basic concepts are given that will be used later. In the third chapter, Lucas's the n-1 test explained the idea of Lucas (build up a group so large that n must be prime). In the fourth section, there is an algorithm known as n+1 test which includes Lucas sequences and is useful for Mersenne numbers. The fifth section is for finite field primality test which found by Lenstra. In the last section, showed deterministic and polynomial time primality algorithm AKS which is obtained from the idea that behind the other primality tests.

October 2018, 47 pages

Key Words: Prime numbers, deterministic algorithm, polynomial time algorithm, primality tests, AKS

TEŞEKKÜR

Çalışmamı yönlendirip ilgi ve desteğini esirgemeyen danışman hocam sayın Doç. Dr. Murat ŞAHİN'e (Ankara Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı) en derin duygularımla teşekkür ederim.

Süleyman Serkan ÖZÇİM
Ankara, Ekim 2018

İÇİNDEKİLER

SİMGELER DİZİNİ

O	Algoritmanın en kötü durum karmaşıklığı
$< A >$	A kümesinin ürettiği alt grup
$o(a)$	a elemanının mertebesi
φ	Euler φ fonksiyonu
$\|G\|$	G grubunun mertebesi
$\left(\frac{a}{n}\right)$	a ve n için Jacobi sembolü
M_k	k. Mersenne sayısı
$\mathbb{Z}^+$	Pozitif tamsayılar kümesi
$R[x]$	R halkası üzerinde kurulan polinomlar halkası
R/I	R halkasının I idealine göre bölüm halkası
$U(R)$	R halkasının tersinir elemanlarının kümesi
$\mathbb{Z}$	Tamsayılar kümesi
$\mathbb{Z}_n$	mod n bağıntısına göre denklik sınıflarının kümesi
$\mathbb{Z}_n^*$	$U(\mathbb{Z}_n)$ kümesinin çarpma işlemi ile oluşturduğu grup
$\prod_{i=0}^{k} f(x)^i$	$f(x)^i$ polinomlarının çarpımları

1. GİRİŞ

Eğer 1'den büyük bir n tamsayısının 1 ve n den başka pozitif böleni yoksa n'ye bir asal sayı denir. Asal sayılar, antik Yunan uygarlıklarından günümüze kadar üzerinde çok fazla araştırma yapılan bir konu olmuştur. Euclid M.Ö 300'de sonsuz çoklukta asal sayı olduğunu ve her pozitif tam sayının asal sayıların çarpımı şeklinde tek türlü yazıldığını göstermiştir. Bu sebeple pozitif tam sayıların özelliklerini anlamak için asal sayıların anlaşılması gerekmektedir. Örneğin pozitif bir tamsayının asal olup olmadığı sorusu asırlardır üzerinde çalışılan bir sorudur ve günümüzde sayılar teorisinin temel problemlerinden birisidir. Tanımdan yola çıkılırsa bir n pozitif tamsayısının asal olup olmadığını anlamak için 1 ile n arasındaki sayılara bölünüp bölünmediğine bakılması gerekir. Aslında asal olmayan bir sayının karekökünden küçük veya eşit bir asal böleni vardır. Çünkü; eğer asal olmayan bir n sayısının tüm $p_1, p_2, ..., p_k$ asal bölenleri $\sqrt{n}$ değerinden büyük olsaydı $p_1p_2...p_k > \sqrt{n}\sqrt{n}...\sqrt{n} > n$ olurdu. Yani asal olmayan bir sayının tüm asal bölenleri $\sqrt{n}$ değerinden büyük olamaz. Dolayısıyla bir sayının asal olup olmadığını belirlemek için $\lfloor\sqrt{n}\rfloor$ değerine kadar bir böleninin olup olmadığına bakmak gerekir. (Pomerance ve Crandall 2005). Örneğin $2^{127} - 1$ sayısının asallığını anlamak için yaklaşık olarak 10^{19} bölme işlemi yapılması gerekir. Saniyede 10^{10} işlem yapabilen bir bilgisayarla dahi bu sayının asal olduğunun anlaşılması kabaca 30 yıl sürmektedir.

Asal sayılar günümüzde kriptografi alanında da çokça kullanılmaktadır. Örneğin RSA şifreleme algoritması çok büyük iki asal sayıya ihtiyaç duymaktadır. Dolayısıyla bir sayının asallığının belirlenmesi için hızlı testler bulmak kriptografi için de büyük önem arzetmektedir.

Fermat tarafından 1640 yılında asallık testlerinin temelini oluşturacak bir teorem bulunmuştur.
(Fermat) Eğer n asal ve $(a, n) = 1$ olacak şekilde $a \in \mathbb{Z}^+$ ise

$$a^{n-1} \equiv 1 \pmod{n}.$$

Ancak Fermat teoreminin tersi doğru değildir. Çünkü $n = 561$ ve $a = 2$ seçilirse $2^{560} \equiv 1 \pmod{561}$ olmaktadır fakat $561 = 3 \cdot 11 \cdot 17$ olduğundan 561 asal değildir. Dolayısıyla Fermat teoreminin tersi bir asallık testi olarak kullanıldığında deterministik olmamaktadır. Lucas 1876'da Fermat teoremine bazı şartlar getirerek deterministik fakat polinom zamanlı olmayan bir asallık algoritması oluşturmuştur. Örneğin $2^{2^k} + 1$ formundaki özel sayılar için Lucas testi etkili bir asallık testidir. Sonrasında Miller ve Rabin tarafından Lucas'ın teoremi geliştirilmiş ve Genelleştirilmiş Riemann Hipotezi (GRH) doğru kabul edilerek deterministik ve polinom zamanlı bir asallık algoritması bulunmuştur (Pomerance 2010).

Daha sonra Lucas ve Lehmer tarafından yalnızca Mersenne sayıları olarak bilinen $M_k = 2^k - 1$ formundaki özel sayılar için kullanılabilen bir asallık testi bulunmuştur. Şu ana dek bilinen en büyük asal sayı bir Mersenne asalıdır ve $2^{77,232,917} - 1$ şeklinde yazılır. 23 milyon basamağı bulunan bu sayının asallığını anlamak Lucas-Lehmer asallık testi kullanılarak yalnızca 6 gün sürmüştür (www.mersenne.org, 2018).

Lenstra, Adleman vd. tarafından 1984 yılında sonlu cisimler kullanılarak deterministik fakat polinom zamanlı olmayan bir asallık algoritması geliştirilmiştir. Bu algoritmanın karmaşıklığı $O((logn)^{cloglogn})$ dir (Pomerance 2010).

Yıllar süren araştırmalardaki hedef genel sayılar için kullanılabilen, her hangi bir koşula (hipoteze) bağlı olmayan, deterministik ve polinom zamanlı bir asallık algoritmasının bulunmasıdır. Euclid'ten bu yana süren çalışmalar amacına Hindistan'da ulaşmıştır. İlk olarak 2004 yılında Agrawal, Kayal ve Saxena tarafından geliştirilen bu algoritma AKS asallık algoritması olarak bilinmektedir. Deterministiktir ve karmaşıklığı $O(log^{7,5}n)$.

Bu tezin 2. bölümünde tez boyunca kullanılacak bazı tanımlardan bahsedilecektir. Sonrasında Lucas asallık algoritması 3. bölümde, Lucas Lehmer asallık algoritması 4. bölümde, sonlu cisimlerde asallık algoritması 5. bölümde ve son olarak AKS asallık algoritması 6. bölümde incelenmiştir.

2. KURAMSAL TEMELLER

Bu bölümde tez boyunca kullanılacak olan temel tanımlar ve teoremler verilmektedir.

2.1 Temel Tanımlar

Tanım 2.1.1 (Grup) G boştan farklı bir küme olsun. G kümesi üzerinde tanımlanan bir $*$ işlemi eğer

(1) Her $a, b, c \in G$ için $a * (b * c) = (a * b) * c$,

(2) her $a \in G$ için $a * e = e * a$ olacak şekilde $e \in G$ vardır,

(3) her $a \in G$ için $a * b = b * a = e$ olacak şekilde $b \in G$ vardır,

şartlarını sağlıyorsa $(G, *)$ ikilisine bir grup denir. Kısaca G olarak gösterilebilir (Roman 2006).

Tanım 2.1.2 $(G, *)$ bir grup olsun. Eğer her $a, b \in G$ için $a * b = b * a$ oluyorsa G ye değişmeli (abelyen) grup denir (Roman 2006).

Tanım 2.1.3 (Grubun Mertebesi) Bir G grubu sonlu sayıda elemana sahipse (kardinalitesi sonlu) o zaman G'ye sonlu grup, aksi halde sonsuz grup adı verilir. Grubun kardinalitesine grubun mertebesi denir ve $|G|$ ile gösterilir (Roman 2006).

Tanım 2.1.4 $(G, *)$ bir grup olsun. Eğer G kümesinin boştan farklı bir A alt kümesi $*$ işlemine göre bir grup oluşturuyorsa $(A, *)$ grubuna $(G, *)$ grubunun bir altgrubu denir ve $A \leq G$ ile gösterilir (Roman 2006).

Teorem 2.1.1 G değişmeli bir grup ve $\emptyset \neq A \subseteq G$ olsun. Bu durumda,

$$\langle A \rangle = \{a_1^{r_1} a_2^{r_2} \dots a_n^{r_n} \mid \text{her } 1 \leq i \leq n \text{ için } r_i \in \mathbb{Z}\}$$

kümesi G grubunun işlemine göre bir gruptur ve bu gruba G'nin A tarafından üretilen altgrubu denir (Roman 2006).

Ayrıca $A = \{a_1, a_2, \dots, a_n\}$ olmak üzere $G = \langle A \rangle$ ise $G = \langle a_1, a_2, \dots, a_n \rangle$ şeklinde gösterilir ve $a_1, a_2, \dots, a_n$ elemanlarına G nin üreteçleri denir.

Tanım 2.1.5 (Devirli Grup) G bir grup ve $a \in G$ olsun. $H := \{a^n \mid n \in \mathbb{Z}\}$ altgrubuna G'nin a tarafından üretilen devirli altgrubu denir ve $\langle a \rangle$ ile gösterilir. Özel olarak $G = \langle a \rangle$ olacak şekilde $a \in G$ varsa G'ye a tarafından üretilen devirli grup ve a'ya da G grubunun bir üreteci denir (Roman 2006).

Örnek 2.1.1 $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$ kümesi bilinen çarpma işlemi ile bir gruptur. $2 \in \mathbb{Z}_5^*$ için $\langle 2 \rangle = \mathbb{Z}_5^*$ olduğundan 2 bu grubun üretecidir ve $|2| = 4$ olur.

Tanım 2.1.6 (Grupta bir elemanın mertebesi) G bir grup ve $a \in G$ olsun. Eğer $\langle a \rangle$ sonlu bir grup ise $< a >$ grubunun eleman sayısına a nın mertebesi denir $|a|$ veya $o(a)$ ile gösterilir. Eğer $\langle a \rangle$ sonsuz bir grup ise a nın mertebesi sonsuzdur denir (Roman 2006).

Teorem 2.1.2 (Lagrange Teoremi) G sonlu bir grup ve $H \leq G$ olsun. Bu durumda H grubunun mertebesi G grubunun mertebesini böler. Özel olarak $a \in G$ ise a elemanının mertebesi G grubunun mertebesini böler (Roman 2006).

Teorem 2.1.3 Mertebesi asal olan her grup devirlidir (Roman 2006).

Tanım 2.1.7 (Halka) $(R,+)$ değişmeli bir grup ve R üzerinde '$\cdot$' (çarpma) işlemi tanımlı ve eğer

(1) Her $a,b,c \in R$ için $a \cdot (b \cdot c) = (a \cdot b) \cdot c$,

(2) her $a,b,c \in R$ için $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$,

şartlarını sağlıyorsa $(R,+,\ \cdot\ )$ üçlüsüne bir halka denir (Roman 2006).

Bu tezde $(R,+,\ \cdot\ )$ yerine kısaca "R halkası" ifadesi kullanılacaktır.

Tanım 2.1.8 R bir halka olsun. Her $x \in R$ için $x \cdot e = e \cdot x = x$ olacak şekilde bir $e \in R$ varsa e ye R halkasının birimi denir ve R ye birimli halka adı verilir (Roman 2006).

$(R,+,\ \cdot\ )$ halkasının $+$ işlemine göre birim elemanı 0_R ve $\cdot$ işlemine göre birim elemanı 1_R ile gösterilir.

Tanım 2.1.9 R bir halka olsun. Her $x,y \in R$ için $x \cdot y = y \cdot x$ ise R ye değişmeli halka adı verilir (Roman 2006).

Tanım 2.1.10 R bir halka ve R nin boştan farklı bir H alt kümesi R'nin işlemlerine göre halka oluyorsa H'ye R'nin althalkası denir (Roman 2006).

Tanım 2.1.11 R bir halka ve R nin boştan farklı bir alt kümesi I olsun. Eğer

(1) her $a,b \in I$ için $a-b \in I$,

(2) $a \in R$ ve $b \in I$ için $ab, ba \in I$

oluyorsa I'ya R'nin bir ideali denir (Roman 2006).

Tanım 2.1.12 R birimli, değişmeli bir halka ve $1_R \neq 0_R$ olsun. Eğer

$$x \cdot y = 0_R \text{ şartını sağlayan her } x, y \in R \text{ için } x = 0_R \text{ veya } y = 0_R$$

oluyorsa R'ye bir tamlık bölgesi denir (Roman 2006).

Tanım 2.1.13 (Cisim) R bir tamlık bölgesi olsun. Eğer $a \neq 0_R$ olan her $a \in R$ için $a \cdot b = b \cdot a = 1_R$ olacak şekilde $b \in R$ varsa R'ye bir cisim denir (Roman 2006).

Örnek 2.1.2 n pozitif bir tamsayı olsun. $\mathbb{Z}$ üzerinde

$$a \equiv b \pmod{n} \text{ gerek ve yeter şart } n|a-b$$

şeklinde tanımlanan bağıntı bir denklik bağıntısıdır ve bu denklik bağıntısına göre bir $a \in \mathbb{Z}$'nin denklik sınıfı

$$\bar{a} = \{b \in \mathbb{Z} \mid b \equiv a \pmod{n}\}$$

şeklinde tanımlanır. Bu denklik sınıflarının oluşturduğu küme $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \cdots, \overline{n-1}\}$ ile ifade edilir. Bu küme üzerinde $\bar{a} + \bar{b} = \overline{a+b}$ ve $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$ şeklinde tanımlanan $+, \cdot$ işlemlerine göre

$(\mathbb{Z}_n, +)$ bir grup ve $(\mathbb{Z}_n, +, \cdot)$ bir halkadır.

Eğer n asal sayı ise $(\mathbb{Z}_n, +, \cdot)$ bir cisimdir.

Teorem 2.1.4 $\mathbb{Z}_n$ kümesi üzerinde tanımlanan '$\cdot$' (çarpma) işlemine göre tersi olan elemanlarından oluşan küme $\mathbb{U}(\mathbb{Z}_n) = \{a \in \mathbb{Z}_n \mid \ (a, n) = 1\ \}$ dir. Bu küme çarpma işlemi ile bir gruptur (Roman 2006).

Teorem 2.1.4'te bahsedilen $\mathbb{U}(\mathbb{Z}_n)$ kümesinin '$\cdot$' işlemi ile oluşturduğu grup tez boyunca kısaca $\mathbb{Z}_n^*$ olarak ifade edilecektir.

Tanım 2.1.14 (Euler φ Fonksiyonu) n bir tamsayı olmak üzere φ fonksiyonu

$$\varphi(n) := |\{a \in \mathbb{Z}^+ \mid a < n,\ (a,n) = 1\}|$$

şeklinde tanımlanır (Roman 2006).

Bu tanımla $\varphi(n) \leq n-1$ olduğu kolaylıkla görülebilir. Ayrıca $\mathbb{Z}_n^*$ grubunun mertebesi Euler φ fonksiyonunun tanımından anlaşılacağı üzere $\varphi(n)$ dir.

Teorem 2.1.5 (Euler) Eğer $a, n \in \mathbb{Z}$ ve $(a,n) = 1$ ise

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

dir (Roman 2006).

Tanım 2.1.15 (Algoritma) Bir takım verilerle yola çıkarak ve sonlu sayıda aşamadan geçerek belli bir problemi çözme imkanı veren çok kesin komutlar topluluğuna algoritma denir (Nabiyev 2016).

Tanım 2.1.16 Algoritmik karmaşıklık bir problemi çözmek için oluşturulan algoritmanın ihtiyaç duyduğu kaynak ve süre miktarıdır. Karmaşıklık algoritmanın yürütüleceği sistem veya makinadan bağımsız şekilde de elde edilebilir dolayısıyla algoritma karmaşıklığı sistemden bağımsız düşünüldüğünde algoritmanın yürüteceği işlem sayısı olarak ifade edilir (Nabiyev 2016).

Bir problemin karmaşıklığı o problemi çözmek için uygulanabilecek olan tüm algoritmaların (henüz bilinmeyenler dahil) karmaşıklıklarının en küçüğüdür.

Tanım 2.1.17 (O Notasyonu) Eğer $n \geq n_0$ olacak şekildeki her n sabiti için $f(n) \leq cg(n)$ olacak şekilde c ve n_0 sabitleri bulunabiliyorsa $f(n) = O(g(n))$ olarak gösterilir (Nabiyev 2016).

Algoritmanın çalışma zamanının üst sınırı olan, en kötü durumdaki zamanın belirlenmesinde büyük O notasyonu kullanılır. Bu notasyon ilk defa 1984 yılında P. Bachmann tarafından kullanılmıştır (Nabiyev 2016). Ayrıca algoritmik karmaşıklığı belirlemek için θ notasyonu ortalama çalışma zamanını ifade etmek için ve Ω notasyonu ise en iyi çalışma zamanını ifade etmek için kullanılır.

Örnek 2.1.3 Bir algoritmanın sonuçlanması için yapılması gereken işlem sayısı en çok $f(n) = 3n^2 + 8n + 9$ olarak hesaplanmış olsun. Bu durumda $n_0 = 9$ ve $c = 4$ seçilirse her $n \geq 9$ için $3n^2 + 8n + 9 \leq 4n^2$ olmaktadır. Dolayısıyla bu algoritmanın karmaşıklığı $O(n^2)$ olarak ifade edilir. Örneğin bir n sayısının asal olup olmadığını 1 ile $\lfloor\sqrt{n}\rfloor$ arasındaki tamsayılara bölerek bulmaya çalışan algoritmanın karmaşıklığı $O(\sqrt{n})$ dir.

3. n-1 TESTİ

Fermat teoremi bir asallık testi olarak kullanılmaya çalışıldığında bazı sayıların testi geçtiği ancak asal olmadığı bilinmektedir. Peki Fermat teoremini tersine çevirmenin ve bir asallık testi elde etmenin bir yolu var mıdır? Bunu mümkün kılan bir yol Lucas tarafından 1876 yılında verilmiştir.

3.1 Lucas Teoremi ve Pepin Testi

Lemma 3.1.1 $a \in \mathbb{Z}_n^*$ için $o(a) = r$ olsun. Eğer $a^k \equiv 1 \pmod{n}$ ise $r|k$ dır.

Teorem 3.1.1 (Lucas) $a, n \in \mathbb{Z}$ birer tamsayı ve $n > 1$ olacak şekilde

$$\begin{aligned} &(i)\ a^{n-1} \equiv 1 \pmod{n}, \\ &(ii)\ q|n-1 \text{ olacak şekildeki her } q \text{ asalı için } a^{(n-1)/q} \not\equiv 1 \pmod{n} \end{aligned} \tag{3.1}$$

şartları sağlansın. Bu durumda n asaldır (Pomerance ve Crandall 2005).

İspat 3.1.1 a'nın $\mathbb{Z}_n^*$ grubundaki mertebesi r olsun. $r = 1$ olsa $a \equiv 1 \pmod{n}$ olur ancak bu durumda teoremin (ii) hipotezi sağlanmayacağından $r \neq 1$ dir. Lemma 3.1.1 ve (i) denkliğinden anlaşılacağı üzere $r|n-1$ dir. Bu r'nin aslında $n-1$ olduğu gösterilecektir.

$$n - 1 = q_1^{b_1} q_2^{b_2} \cdots q_t^{b_t} \quad \text{her } b_i \in \mathbb{Z}^+$$

şeklinde çarpanlarına ayrılsın ve kabul edilsin ki $r \neq n-1$. Bu durumda $n-1$'i bölen ancak r'yi bölmeyen en az bir $q_i^{b_i}$ sayısı vardır dolayısıyla bir m tamsayısı için $n - 1/q_i = rm$ dir. Bu durumda $a^{(n-1)/q_i} = a^{rm} = (a^r)^m \equiv 1 \pmod{n}$ elde edilir. Ancak bu durum teoremin (ii) şartı ile çelişir. Yani $r = n-1$ dir. Dolayısıyla a elemanının mertebesi $n-1$ olmaktadır. Bu durumda Euler teoremi ve Lemma 3.1.1

gereği $r = n - 1 | \varphi(n)$ dir. Yani $n - 1 \leq \varphi(n)$ elde edilir. Euler φ fonksiyonu hatırlandığında bu ifadeden n ile arasında asal sayıların sayısının $n - 1$ olduğu anlaşılır. Bu n'nin asal olması anlamına gelmektedir. □

Lucas'ın bu teoremi bir çok asallık testine temel oluşturan bir teoremdir. Aslında burada $(a, n) = 1$ olacak şekilde bir a sayısının $\mathbb{Z}_n^*$ grubunun bir alt grubunu ürettiği düşünülmektedir ve bu grubun mertebesi n'nin asallığını belirlemekte büyük öneme sahiptir. Yani $(a, n) = 1$ olacak şekilde bir a sayısının $\mathbb{Z}_n^*$'da ürettiği alt grubun mertebesi $n - 1$ olursa n asal olmak zorunda kalmaktadır. Teoremin altında yatan fikir, *"Öyle büyük bir grup inşa et ki n asal olmak zorunda kalsın"*, şeklinde ifade edilebilir (Pomerance 2010).

Bu teorem anlaşılması kolay bir asallık testidir. Ancak yukarıda ifade edilenler Fermat teoreminin tersi gibi düşünülse de cevaplanması gereken bazı sorular vardır.
(1) Eğer n asal ise şartları sağlayan bir a sayısı var mıdır?
(2) Eğer şartları sağlayan bir a varsa bulmanın bir yolu var mıdır?
(3) Teoremin (ii) şartındaki $(n - 1)$'in q asal bölenleri nasıl bulunabilir?

1. soruda n asal sayı ise $\mathbb{Z}_n^*$ grubunun devirli grup olup olmadığı sorulmaktadır. Çünkü böyle bir a'nın varlığı, mertebesi grubun mertebesine eşit olan bir elemanın varlığı anlamına gelmektedir. Yani bu a elemanı $\mathbb{Z}_n^*$ grubunun üretecidir aynı zamanda a'ya (mod n) için primitif kök denmektedir. Gauss primitif kök teoremi gereğince n asal olursa $\mathbb{Z}_n^*$ devirli bir gruptur dolayısıyla şartları sağlayan a sayısı vardır (Shanks 1993).

2. soruda primitif kökün nasıl bulunacağı ve bunun için elverişli bir algoritmanın olup olmadığı sorulmaktadır. $a = 2$ ile başlayarak ve Genelleştirilmiş Riemann Hipotezi (GRH) doğru kabul edilirse hızlı bir algoritma (polinom zamanlı) ile primitif kök bulunabildiği ispatlanmıştır (Shoup 1992).

3. soruda ise eğer bir a varsa Lucas hipotezlerinden (ii)'nin sağlanması için $n - 1$'in

çarpanlarına ayrılması gerekmektedir. İşte bu soru her sayı için cevaplaması zor bir sorudur ancak bazı özel değerler için kolay olabilmektedir. Örneğin Fermat sayıları olarak bilinen $n = 2^{2^k} + 1$ formundaki sayılar için $n - 1 = 2^{2^k}$ şeklinde yazılabildiğinden kolayca çarpanlarına ayrılabilmektedir bu yüzden bu özel sayılar için Lucas testi kullanılabilir Aşağıdaki örnek Pepin tarafından bulunmuştur ve Fermat sayılarının asallığını test etmektedir.

Örnek 3.1.1 Eğer $k \geq 0$ ise bu durumda $n = 2^{2^k} + 1$ sayısı asaldır ancak ve ancak $3^{(n-1)/2} \equiv -1 \pmod{n}$ (Pomerance 2010). Aşağıda bu örnek Legendre Sembolü ve Euler kriteri yardımıyla ispatlanmıştır.

Öncelikle $3^{(n-1)/2} \equiv -1 \pmod{n}$ olarak kabul edilsin. Bu durumda n sayısının asal olduğunun gösterilmesi gerekir. Bunun için Lucas teoreminden yararlanılabilir. $n - 1 = 2^{2^k}$ olduğundan bu sayının bir tane asal böleni vardır ve o da 2'dir. Lucas teoremindeki a değeri 3 seçilirse kabulümüz gereği $3^{(n-1)/2} \equiv -1 \pmod{n}$ olduğundan $q|n-1$ olacak şekildeki her q asalı için $a^{(n-1)/q} \not\equiv 1 \pmod{n}$ şartı sağlanmış olur. Ayrıca yine kabulden $3^{n-1} \equiv 1 \pmod{n}$ elde edilir, böylece Lucas teoreminin şartları gereği n asaldır.

Karşıt olarak n asal olsun. Bu durumda da $3^{(n-1)/2} \equiv -1 \pmod{n}$ olduğu gösterilmelidir. İspatın bu bölümü için Legendre sembolü ve Euler kriteri kullanılacaktır ve hatırlatma olması için aşağıda verilmiştir.

Tanım 3.1.1 (Legendre Sembolü) n tek asal sayı ve a bir tamsayı olmak üzere Legendre sembolü aşağıdaki şekilde tanımlanır (Pomerance ve Crandall 2005).

$$\left(\frac{a}{n}\right) := \begin{cases} 1 & , a \not\equiv 0 \pmod{n} \text{ ve } a \pmod{n}\text{'de bir tam kare} \\ -1 & , a \pmod{n}\text{'de bir tam kare değil} \\ 0 & , a \equiv 0 \pmod{n} \end{cases}$$

Lemma 3.1.2 (Euler Kriteri) n asal ve $(a, n) = 1$ ise $\left(\frac{a}{n}\right) = a^{(n-1)/2} \pmod{n}$ dir

(Pomerance ve Crandall 2005).

Ayrıca Legendre sembolünün kullanılacak özellikleri aşağıda verilmiştir,

$$\left(\frac{-1}{n}\right) = \begin{cases} 1 & , n \equiv 1 \pmod 4 \\ -1 & , n \equiv -1 \pmod 4 \end{cases} \tag{3.2}$$

$$\left(\frac{-3}{n}\right) = \begin{cases} 1 & n \equiv 1 \pmod 3 \\ -1 & n \equiv 2 \pmod 3 \end{cases} \tag{3.3}$$

Hatırlatmalardan sonra ispat aşağıdaki şekilde yapılmaktadır.

Öncelikle dikkat edilirse $n - 1 = 2^k$ çift olduğundan $2^{2^k} \equiv 1 \pmod 3$. Burada denkliğin her iki tarafına 1 eklenirse,

$$n = 2^{2^k} + 1 \equiv 2 \pmod 3$$

elde edilir. Ayrıca

$$n = 2^{2^k} + 1 \equiv 1 \pmod 4$$

elde edilir. Burada (3.2) ve (3.3) özellikleri kullanılırsa

$$\left(\frac{3}{n}\right) = \left(\frac{-1}{n}\right)\left(\frac{-3}{n}\right) = 1 \cdot (-1) = -1$$

bulunur. n asal olduğundan Euler kriteri gereği $\left(\frac{3}{n}\right) = 3^{(n-1)/2} \pmod n = -1 \pmod n$ olduğu görülür. Böylece n asal ise $3^{(n-1)/2} \equiv -1 \pmod n$ elde edilmiş olur. □

Lucas teoremi asallık testi olarak kullanıldığında en zor adım çok büyük n sayıları için $n-1$'in tüm asal çarpanlarının bulunmasıdır. Peki burada tüm çarpanların değil de, çarpanlardan bir bölümünün bilinmesi kullanılabilir mi? Bir sonraki bölümde bu soru incelenecektir.

3.2 Parçalı Çarpanlara Ayırma

Özel olarak F pozitif tamsayısının tüm asal çarpanları bilinsin ve

$$n-1 = FR \text{ olacak şekilde bir } R \in \mathbb{Z}^+ \text{ vardır} \tag{3.4}$$

şartı sağlansın. Eğer F, n'e bağlı olarak yeterince büyükse bu durum Lucas teoreminden daha genel bir asallık kriteri olarak kullanılabilir (Pomerance ve Crandall 2005). F'nin yeterince büyük olmasının ne anlama geldiği gösterilmeden önce F ile n'nin asal çarpanları arasındaki ilişkiyi açıklayan teorem aşağıda verilmiştir.

Teorem 3.2.1 n sayısı için (3.4) sağlansın ve a için,

$$\begin{aligned} &a^{n-1} \equiv 1 \pmod{n} \text{ ve} \\ &q|F \text{ olacak şekildeki her } q \text{ asalı için } (a^{(n-1)/q} - 1, n) = 1 \end{aligned} \tag{3.5}$$

olsun. Bu durumda n'nin her asal böleni $1 \pmod{F}$'e denktir (Pomerance ve Crandall 2005).

İspat 3.2.1 $n-1 = FR$ ve a tamsayısı için (3.5) sağlansın. Ayrıca p n'nin herhangi bir asal böleni olsun. Bu durumda,

$$\begin{aligned} a^{n-1} \equiv 1 \pmod{n} &\Rightarrow a^{n-1} \equiv 1 \pmod{p} \\ &\Rightarrow (a^R)^{(n-1)/R} \equiv 1 \pmod{p} \end{aligned}$$

elde edilir. Bu demektir ki a^R'nin $\mathbb{Z}_p^*$ grubundaki mertebesi $(n-1)/R = F$'nin bir bölenidir. Şimdi aslında bu mertebenin F olduğunu gösterilecektir. Her $q|F$ asalı için $(a^{(n-1)/q} - 1, n) = 1$ olduğundan $(a^{(n-1)/q} - 1, p) = 1$ elde edilir. Öyleyse yine her $q|F$ için,

$$\begin{aligned} a^{(n-1)/q} - 1 \not\equiv 0 \pmod{p} &\Rightarrow a^{(n-1)/q} \not\equiv 1 \pmod{p} \\ &\Rightarrow (a^R)^{(n-1)/Rq} \not\equiv 1 \pmod{p} \\ &\Rightarrow (a^R)^{F/q} \not\equiv 1 \pmod{p} \end{aligned}$$

elde edilir. Bu yüzden a^R'nin mertebesi F'nin aşikar olmayan bir böleni değildir. Yani bu mertebe F olur. Sonuç olarak Lagrange teoremi gereği a^R'nin $\mathbb{Z}_p^*$ grubundaki mertebesi yani F sayısı $\mathbb{Z}_p^*$ grubunun mertebesini böler. Dolayısıyla

$$\begin{aligned} F|p-1 &\Rightarrow Fy = p-1 \text{ olacak şekilde y tamsayısı vardır.} \\ &\Rightarrow p = Fy+1. \\ &\Rightarrow p \equiv 1 \pmod{F} \end{aligned}$$

elde edilir ve ispat biter. □

Hatırlayınız ki F eğer yeterince büyük seçilirse n'nin asallığı için bir kriter bulunabileceği söylenmişti. Aşağıdaki teorem ile F değerinin yeterince büyük olmasının ne anlama geldiği gösterilmiştir.

Teorem 3.2.2 Kabul edelim ki F'nin tüm asal çarpanları bilinsin ve $n-1 = FR$ olarak yazılsın eğer bir a için,

(i) $a^{n-1} \equiv 1 \pmod{n}$,

(ii) $q|F$ olacak şekildeki her q asalı için $(a^{(n-1)/q} - 1, n) = 1$

şartları sağlanır ve $F \geq \sqrt{n}$ olursa, n asaldır (Pomerance ve Crandall 2005).

İspat 3.2.2 Kabul edilsin ki p n'nin en küçük asal bölenidir. Teorem 3.2.1 gereği

$$p \equiv 1 \pmod{F} \text{ ise o zaman } p = Fx+1 \text{ olacak şekilde } x \in \mathbb{Z} \text{ vardır.}$$

Dolayısıyla $p > F$ olur. Ancak bu durumda $p > F \geq \sqrt{n}$ bulunur. Yani n sayısının en küçük asal böleni $\sqrt{n}$ değerinden büyüktür dolayısıyla n asal olmak zorunda kalır. □

Bu teorem ile birlikte Lucas'ın fikri pekiştirilmiş oldu. Özetle bu teorem sonucunda anlaşıldı ki $\mathbb{Z}_n^*$ grubunda bir elemanın mertebesi eğer $\sqrt{n}$ değerinden büyük ve $n-1$

değerini bölüyorsa bu durum n'nin asal olmasını gerektirmektedir. Fakat dikkat edilirse hem Lucas teoremi hem de Teorem 3.2.2 çarpanlara ayırma gibi zor bir problemi çözmeyi gerektirmektedir. Teorem 3.2.2, her ne kadar makul bir bölen bulmanın yeterli olduğunu gösterse de bu F değerini her zaman kolay bir şekilde elde etmek mümkün müdür? Bu sorunun cevabı her zaman "evet" değildir ancak bazı özel sayılar için bulunması kolay olabilir. Aşağıda Denomme ve Savin (2008) tarafından bulunmuş olan ve teoremin kolayca uygulanabildiği özel sayılara örnek verilmiştir.

Örnek 3.2.1 Kabul edelim ki l pozitif tamsayı ve $n_l = 2^{2^l} - 2^{2^{l-1}} + 1$ şeklinde yazılsın. Bu özel sayılar için F değeri

$$F_l = 2^{2^{l-1}}$$

olarak seçilebilir. Bunu göstermek için öncelikle F_l'nin çarpanlarına ayrılabildiği, $n_l - 1$ sayısını böldüğü ve $F_l > \sqrt{n_l}$ olduğu gösterilecektir. F_l sayısının tek asal çarpanının 2 olduğu görülmektedir. Bu yüzden F_l kolayca çarpanlarına ayrılabilmektedir.

Ayrıca $F_l = 2^{2^{l-1}}$ eşitliğinin her iki tarafı $2^{2^{l-1}} - 1$ ile çarpılırsa

$$\begin{aligned}(2^{2^{l-1}} - 1)F_l &= 2^{2^{l-1}}(2^{2^{l-1}} - 1) \\ &= 2^{2^l} - 2^{2^{l-1}} \\ &= 2^{2^l} - 2^{2^{l-1}} + 1 - 1 \\ &= n_l - 1\end{aligned}$$

elde edilir yani $F_l | n_l - 1$'dir.

Yine $F_l = 2^{2^{l-1}}$ eşitliğinde her iki tarafın karesi alınırsa

$$\begin{aligned}(F_l)^2 &= (2^{2^{l-1}})^2 \\ &= 2^{2^l} \\ &> 2^{2^l} - 2^{2^{l-1}} + 1 \\ &= n_l\end{aligned}$$

bulunur. Bu demektir ki $F_l^2 > n_l \Rightarrow F_l > \sqrt{n_l}$. Buraya kadar F_l sayısının $n_l - 1$'i böldüğü ve $\sqrt{n_l}$ değerinden büyük olduğu gösterilmiştir. Şimdi ise teoremin uygulanabileceği bir a değerinin belirlenmesi gerekmektedir. Bunun için $a_l = 7 \pmod{n_l}$ deneyelim. Kabul edelim ki $l \geq 2$ olsun, bu durumda $n_l \equiv 1 \pmod 4$ olup Jacobi sembolleri için kuadratik resiprositi kuralı (Crandall ve Pomerance 2005) gereği

$$\left(\frac{n_l}{7}\right) = \left(\frac{7}{n_l}\right)$$

dir. Ayrıca

$$n_l \equiv \begin{cases} 3 \pmod 7 & ; l \text{ tek ise} \\ 6 \pmod 7 & ; l \text{ çift ise} \end{cases}$$

olduğu görülür. Burada 3 ve 6 (mod 7) için tam kare (kuadratik rezidü) olmadıklarından $\left(\frac{n_l}{7}\right) = -1$ olur. Yani $l \geq 2$ için $\left(\frac{n_l}{7}\right) = \left(\frac{7}{n_l}\right) = -1$ dir.
Bu şartlar altında $l \geq 2$ için $n_l = 2^{2^l} - 2^{2^{l-1}} + 1$ sayısının asal olması için gerek ve yeter şart

$$7^{(n_l-1)/2} \equiv -1 \pmod{n_l} \tag{3.6}$$

olmasıdır.
($:\Rightarrow$) Eğer n_l asal olursa Euler kriterinden $\left(\frac{7}{n_l}\right) = 7^{(n_l-1)/2} \pmod{n_l}$ olur ayrıca $\left(\frac{7}{n_l}\right) = -1$ olduğundan $7^{(n_l-1)/2} \equiv -1 \pmod{n_l}$ denkliği sağlanmaktadır.
($\Leftarrow:$) Eğer (3.6) sağlanırsa n_l tek sayı olduğundan,

$$7^{n_l-1} \equiv 1 \pmod{n_l} \text{ ve } (7^{(n_l-1)/2} - 1, n_l) = 1$$

elde edilir, dikkat edilirse bu şartlar Teorem 3.2.2'de $a_l = 7 \pmod{n_l}$ ve $F_l = 2^{2^{l-1}}$ seçildiğinde elde edilen şartlardır yani n_l asal olur. □

Teorem 3.2.2'de bahsedilen F değeri bazı şartlar altında daha da küçük seçilebilmektedir. Aşağıda bu seçimleri gösteren iki teorem verilmiştir.

Teorem 3.2.3 (Brillhart, Lehmer ve Selfridge) Daha önce bahsedilen (2.4) ve (2.5) şartları sağlansın ve $n^{1/3} \leq F < n^{1/2}$ olsun. Ayrıca $c_1, c_2 \in [0, F-1]$ tamsayıları

için $n = c_2F^2 + c_1F + 1$ şeklinde yazıldığını göz önüne alırsak n'nin asal olması için gerek ve yeter şart $c_1^2 - 4c_2$ sayısının bir tamkare olmamasıdır (Pomerance ve Crandall 2005).

Teoremde bahsedilen n değerinin F tabanındaki gösterimini her zaman bulmak mümkün müdür? Bu mümkündür çünkü $n \equiv 1 \pmod{F}$ dir ve buradan n'nin F tabanındaki yazımında birler basamağının 1 olduğu anlaşılır. Yani teoremde ifade edildiği gibi F tabanında $c_1, c_2 \in [0, F-1]$ olacak şekilde $c_2F^2 + c_1F + 1$ şeklinde yazılabilirdir. Ayrıca yine teoremde bahsedilen $c_1^2 - 4c_2$ değerinin tamkare olup olmadığına bakmak için aşağıdaki algoritmadan yararlanılabilir.

Algoritma 1 Karekök değerini bulmak

Bu algoritma bir N pozitif tamsayısı için $\lfloor\sqrt{N}\rfloor$ sayını bulmaktadır.

1. **[Başlangıç]**

   B(N):= N pozitif tamsayısının ikilik tabanda yazılışındaki bitlerin sayısı;

   $u := 2^{\lceil B(N)/2 \rceil}$;

2. **[Newton İterasyonu]**

   $y := \lfloor (u + \lfloor N/u \rfloor)/2 \rfloor$;

   Eğer $(y \geq u)\{$

   sonuç u;

   $\}$

   $u = y$;

   [Newton İterasyonu] adımına dön;

Burada bir sayının tam kare olup olmadığını anlamak için algoritmada u elde edildikten sonra $u^2 = N$ olup olmadığına bakılması gerekir. Sıradaki teorem F değerinin daha da küçük seçilebilmesini sağlamaktadır.

Teorem 3.2.4 (Konyagin ve Pomerance) Kabul edelim ki $n \geq 214$, (2.4) ve (2.5) şartları sağlansın ve $n^{3/10} \leq F < n^{1/3}$ olsun. Ayrıca n sayısının F tabanındaki açılımı $c_3F^3 + c_2F^2 + c_1F + 1$ ve $c_4 = c_3F + c_2$ olarak ifade edilsin. Bu durumda n'nin

asal olması için gerek ve yeter şart aşağıdaki şartların sağlanmasıdır (Pomerance 2005).

(1) $(c_1 + tF)^2 + 4t - 4c_4$ sayısı $t \in [0, 5]$ için tam kare değildir.

(2) $v < F^2/\sqrt{n}$ olacak şekildeki en büyük v için $\frac{u}{v}$'nin sürekli kesir ayrışımı $\frac{c_1}{F}$'e yakınsasın. Eğer $d = \lfloor c_4 v/F + 1/2 \rfloor$ olarak seçilirse $vx^3 + (uF - C_1 v)x^2 + (c_4 v - dF + u)x - d \in \mathbb{Z}[x]$ polinomunun $aF + 1$ değeri n'nin aşikar olmayan bir böleni olacak şekilde bir a böleni yoktur.

4. n+1 TESTİ

Bir sayının asallığını ispatlamak için bir önceki bölümde incelenen testlerin esas zorluğu çarpanlara ayırma problemidir. Bazı özel n değerleri için $n-1$'i çarpanlarına ayırmak önceki bölümde görüldüğü gibi kolaydır. Bazen de $n+1$ değerini çarpanlarına ayırmak kolaydır. Örneğin Mersenne sayıları olarak bilinen 2^p-1 şeklinde yazılan sayılar gibi. Peki bu bilgi bir asallık testinde kullanılabilir mi? Bu bölümde Lucas dizilerinden elde edilen ve Mersenne sayılarının asallığını bulmak için kullanılan Lucas Lehmer asallık testi anlatılacaktır.

4.1 Lucas Dizileri

Bu bölümde Lucas dizilerinden elde edilen $n+1$ testini göstermeden önce Lucas dizilerinin tanımı ve bazı asallık şartlarından bahsedilecektir.

Tanım 4.1.1 (Lucas Dizileri) $a, b \in \mathbb{Z}$ ve

$$U_0 = 0, \quad U_1 = 1 \text{ olsun, } k \geq 2 \; U_k(a,b) = aU_{k-1} - bU_{k-2},$$
$$V_0 = 2, \quad V_1 = a \text{ olsun, } k \geq 2 \; V_k(a,b) = aV_{k-1} - bV_{k-2}$$

olarak tanımlanan dizilere Lucas dizileri denir.

Bu diziler için yineleme bağıntısı $U_k = aU_{k-1} - bU_{k-2}$ dir. Dolayısıyla karakteristik polinomu $f(x) = x^2 - ax + b$ şeklindedir ve $\Delta = a^2 - 4b$ dir. Ayrıca Lucas dizileri bu polinom için aşağıdaki gibi de ifade edilebilir (Crandall ve Pomerance 2005).

$$\begin{aligned} U_k &= \frac{x^k - (a-x)^k}{x-(a-x)} \pmod{f(x)} \\ V_k &= x^k + (a-x)^k \pmod{f(x)} \end{aligned} \tag{4.1}$$

Burada (mod $f(x)$) ifadesi $\mathbb{Z}[x]$ halkasındaki polinomların $f(x)$ polinomuna bölümünden kalanlarının bulunması anlamına gelmektedir. Yani U_k ve V_k dizilerinin elemanları $\mathbb{Z}[x]/(f(x))$ bölüm halkasının elemanlarıdır.

Tanım 4.1.2 Lucas dizilerinin (4.1)'deki tanımı dikkate alındığında $(n, 2b\Delta) = 1$ olan bir n pozitif tamsayısı için $U_r \equiv 0 \pmod{n}$ denkliğini sağlayan en küçük r pozitif tamsayısı $r_f(n)$ ile gösterilir.

Tanım 4.1.3 (Bölünebilir Dizi) Eğer bir a_n dizisi için $k|j$ iken $a_k|a_j$ oluyorsa bu diziye bölünebilir dizi denir.

Şimdi bu özelliğin Lucas dizileri için sağlandığı gösterilecektir. Kolaylıkla görülebilir ki $i|j$ ise $im = j$ olacak şekilde $m \in \mathbb{Z}$ vardır. Bu durumda,

$$\begin{aligned} U_j &= \frac{x^{im} - (a-x)^{im}}{x - (a-x)} \pmod{f(x)} \\ &= \frac{(x^i - (a-x)^i)((x^{i(m-1)})(a-x)^{i.0} + \cdots + (x)^{i.0}(a-x)^{i(m-1)})}{x - (a-x)} \pmod{f(x)} \\ &= U_i\ ((x^{i(m-1)})(a-x)^{i.0} + \cdots + (x)^{i.0}(a-x)^{i(m-1)}) (\mathrm{mod}\ f(x)) \\ &\Rightarrow U_i | U_j. \end{aligned}$$

□

Lemma 4.1.1 Eğer $(n, 2b\Delta) = 1$ ise $U_j \equiv 0 \pmod{n}$ olması için gerek ve yeter şart $j \equiv 0 \pmod{r_f(n)}$ yani $r_f(n)|j$ olmasıdır (Pomerance ve Crandall 2005).

Ayrıca (U_n) Lucas dizisi için n sayısı asal olduğunda sağlanan bir özellik aşağıdaki lemma ile verilmiştir.

Lemma 4.1.2 Eğer p asal ve (4.1)'deki f ve Δ için $(n, 2b\Delta) = 1$ ise $U_{p-\frac{\Delta}{p}} \equiv 0 \pmod{p}$ dir (Pomerance ve Crandall 2005).

Önceki iki lemmanın sonucu olarak aşağıdaki teorem verilebilir.

Teorem 4.1.1 Eğer n asal ve (4.1)'deki f ve Δ için $n \nmid 2b\Delta$ olursa $r_f(p)|p - \left(\frac{\Delta}{n}\right)$ dir.

4.2 n+1 Asallık Testi

Lucas dizileri kullanılarak Teorem 3.2.2'ye benzer şekilde bir asallık testi oluşturmak mümkündür. Aşağıda U_n dizisi kullanılarak elde edilen bir asallık kriteri verilmiştir. Bu kritere $n+1$ asallık testi adı verilmiştir.

Teorem 4.2.1 f ve Δ değerleri (4.1) deki gibi alınsın ve n pozitif tamsayısı için $(n, 2b) = 1$, $\left(\frac{\Delta}{n}\right) = -1$ olsun. Eğer $F|n+1$ ve

$$U_{n+1} \equiv 0 \pmod{n}, \quad \text{her } q|F \text{ asalı için } (U_{(n+1)/q}, n) = 1 \tag{4.2}$$

oluyorsa n'nin her p asal böleni için $p \equiv \left(\frac{\Delta}{p}\right) \pmod{F}$ olur. Özel olarak $F > \sqrt{n}+1$ ve (4.2) sağlanırsa n asaldır (Pomerance ve Crandall 2005).

Benzer şekilde V dizisi kullanılarak da bir asallık kriteri elde edilir.

Teorem 4.2.2 f ve Δ değerleri (4.1) deki gibi alınsın ve n pozitif tamsayısı için $(n, 2b) = 1$, $\left(\frac{\Delta}{n}\right) = -1$ olsun. Eğer F, $n+1$'in çift bir böleni ve

$$V_{F/2} \equiv 0 \pmod{n}, \quad \text{her } q|F \text{ tek asalı için } (V_{F/2q}, n) = 1 \tag{4.3}$$

oluyorsa n'nin her p asal böleni için $p \equiv \left(\frac{\Delta}{p}\right) \pmod{F}$ olur. Özel olarak $F > \sqrt{n}+1$ ve (4.3) sağlanırsa n asaldır (Pomerance ve Crandall 2005).

Bahsedilen $n+1$ testi özel olarak Mersenne sayıları için çok uygun ve hızlıdır. Aşağıda Mersenne sayıları için bu testin neden uygun ve hızlı bir test olduğunu

açıklayan teorem verilmiştir. Bu teoreme Lucas Lehmer Asallık Testi (LLT) denmektedir. İlk kez Lucas (1856) tarafından bulunan bu test sonrasında yine Lucas (1878) ve Lehmer (1930) tarafından geliştirilmiştir (Pomerance 2005).

Teorem 4.2.3 (Lucas-Lehmer Asallık Testi(LLT)) Bir (v_k) dizisini $k = 0, 1, 2, ...$ için $v_0 = 4$ ve $v_{k+1} = v_k^2 - 2$ olacak şekilde tanımlansın. p asal ve tek sayı olsun. Bu durumda $M_p = 2^p - 1$ sayısının asal olması için gerek ve yeter şart

$$v_{p-2} \equiv 0 \pmod{M_p}$$

olmasıdır (Pomerance ve Crandall 2005).

İspat 4.2.1 ($:\Leftarrow$) Önce $v_{p-2} \equiv 0 \pmod{M_p}$ olduğunu kabul edip M_p değerinin asal olduğu gösterilecektir. Bunun için Teorem 4.2.2'ye uygun $f(x)$ ve F değerleri belirlenmesi gerekmektedir. $f(x) = x^2 - 4x + 1$ olsun bu durumda $\Delta = 12$ olur. Şimdi $\left(\frac{\Delta}{M_p}\right)$ değeri hesaplanacaktır. p tek sayı olduğundan

$$M_p = 2^p - 1 \equiv (-1)^p - 1 \equiv (-1) - 1 \equiv 1 \pmod{3}$$

olur. Yani M_p ve 3 aralarında asaldır, kuadratik resiprosity kuralı gereği $\left(\frac{3}{M_p}\right) = -1$ elde edilir. Ayrıca

$$\left(\frac{4}{M_p}\right) = \left(\frac{2}{M_p}\right)^2$$

olduğundan bu değer ya 0 ya da 1 dir. Ancak $M_p \equiv 3 \pmod{4}$ olup $M_p = 4k + 3$ olacak şekilde bir k tamsayısı vardır. Bu nedenle M_p ve 4 sayılarının ortak böleni yoktur yani sonuç 0 çıkamaz ve $\left(\frac{4}{M_p}\right) = 1$ elde edilir. Böylece $\left(\frac{\Delta}{M_p}\right) = \left(\frac{3}{M_p}\right)\left(\frac{4}{M_p}\right) = (-1) \cdot 1 = -1$ bulunur. Eğer $F = 2^{p-1} = (M_p + 1)/2$ seçilirse F'nin asal böleni yalnızca 2 olduğu için (4.3) şartları $V_{2^{p-2}} \equiv 0 \pmod{M_p}$ şeklinde tek şarta dönüşür. Burada $f(x) = x^2 - 4x + 1$ ve $V_k = x^k + (a - x)^k \pmod{f(x)}$ olduğunu hatırlarsak $V_1 = a = 4 = v_0$ olur. Ayrıca $x(4 - x) \equiv 1 \pmod{f(x)}$ olduğundan,

$$V_{2m} \equiv x^{2m} + (4 - x)^{2m} = (x^m + (4 - x)^m)^2 - 2x^m(4 - x)^m \equiv V_m^2 - 2 \pmod{f(x)}$$

elde edilir. Böylece

$$\begin{aligned} V_{2^k} = V_{2.2^{k-1}} = V_{2^{k-1}}^2 - 2 &\equiv (V_{2^{k-2}}^2 - 2)^2 - 2 \\ &\equiv \cdots \\ &\equiv (((V_{2^0}^2 - 2)^2 - 2)^2 \cdots)^2 - 2 (\text{mod } f(x)) \end{aligned}$$

elde edilir. $V_1 = v_0$ olduğundan $V_{2^k} = v_k^2$ dir. Böylece sağlanması gereken (4.3) şartı,

$$V_{2^{p-2}} = v_{p-2} \equiv 0 \ (\text{mod } M_p)$$

şeklinde elde edilir. Ayrıca $p \geq 3$ olduğundan $F - 1 = 2^{p-1} - 1 > \sqrt{2^p} > \sqrt{2^p - 1}$ olduğu elde edilir yani $F > \sqrt{M_p} + 1$ dir. Sonuç olarak $F > \sqrt{n} + 1$ sağlanmış olur. Böylece kabuller Teorem 4.2.2 deki tüm şartları sağladı bu nedenle Teorem 4.2.2 gereği M_p sayısı asal oldu.

($:\Rightarrow$) Şimdi $M = M_p$ sayısı asal olsun. İspatın ilk kısmında gösterilmişti ki $\left(\frac{\Delta}{M}\right) = -1$ dir. Bu durumda Δ değeri (mod M) de tamkare değildir (Pomerance ve Crandall 2005). Yani $f(x) = x^2 - 4x + 1$ polinomunun $\mathbb{Z}_M$ halkasında sıfırı yoktur dolayısıyla bu halkada indirgenemezdir. Bu yüzden $f(x)$ polinomunun sıfırlarını $\mathbb{Z}_M$ halkasına katarak

$$\mathbb{Z}[x]/(f(x), M) := \{i + jx \mid i, j \in \mathbb{Z}\ , 0 \leq i, j \leq M - 1\}$$

şeklinde tanımlanan bölüm halkası elde edilebilir. Bu halkanın elemanları, katsayıları $\mathbb{Z}_M$ halkasından olan polinomların $f(x)$ polinomuna bölümünden elde edilen kalan sınıflarıdır. Bu halkadaki toplama işlemi (mod M) de yapılmakta ve çarpma işlemi $x^2 = 4x - 1$ eşitliği dikkate alınarak yine (mod M) de yapılmaktadır. Yani,

$$\begin{aligned} i_3 &= i_1 + i_2 \ (\text{mod } M), & j_3 &= j_1 + j_2 \ (\text{mod } M) \\ i_4 &= i_1 i_2 - j_1 j_2 \ (\text{mod } M), & j_4 &= i_1 j_2 + i_2 j_1 + 4 j_1 j_2 \ (\text{mod } M) \end{aligned}$$

olacak şekilde i_3, i_4, j_3, j_4 değerleri için toplama ve çarpma işlemleri;

$$\begin{aligned} (i_1 + j_1 x) + (i_2 + j_2 x) &= i_3 + j_3 x \\ (i_1 + j_1 x)(i_2 + j_2 x) &= i_4 + j_4 x \end{aligned}$$

şeklinde tanımlanır. Ayrıca daha önce belirtildiği gibi $f(x)$ indirgenemez olduğu için $\mathbb{Z}[x]/(f(x), M)$ halkası bir cisimdir ve M^2 elemanlı $\mathbb{F}_{M^2}$ cismine izomorftur. Burada $\mathbb{Z}_M$ alt halkası da $j = 0$ olacak şekilde $i + jx$ kalan sınıfları olarak düşünülebilir.
Bu $\mathbb{F}_{M^2}$ cisminde $\sigma(v) := v^M$ şeklinde bir fonksiyon tanımlansın. Bu fonksiyon aşağıdaki özellikleri sağlamaktadır (Frobenius otomorfizması).

$$\begin{aligned}\sigma(v+k) &= \sigma(v) + \sigma(k),\\ \sigma(vk) &= \sigma(v)\sigma(k),\\ \sigma(v) &= v \text{ olur ancak ve ancak } v \in \mathbb{Z}_M\end{aligned}$$

Hatırlayınız ki $f(x)$ polinomunun $\mathbb{Z}_M$ halkasında kökü olmadığı için $\mathbb{F}_{M^2}$ halkasını $f(x)$ polinomuna kök bulmak için oluşturulmuştu. Bu halka içindeki hangi kalan sınıflarının kök olduğuna bakılırsa

$$f(4-x) = (4-x)^2 - 4(4-x) + 1 \equiv x^2 - 4x + 1 \equiv 0 \pmod{f(x), M} \text{ ve}$$
$$f(x) = x^2 - 4x + 1 \equiv 0 \pmod{f(x), M}$$

olmaktadır. Yani bu kökler x ve $4 - x$ olur. Ayrıca $x^2 - 4x + 1 = 0$ eşitliğinin her iki tarafına σ fonksiyonu uygulanırsa,

$$\sigma(x^2 - 4x + 1) = \sigma(0)$$
$$\sigma(x)^2 - 4\sigma(x) + 1 = 0.$$

Böylece σ fonksiyonunun kökleri birbirine eşlediği anlaşılır. Yani x bir kök ise $\sigma(x)$ başka bir köktür. Polinomun yalnızca iki kökü olduğundan $x^M \equiv 4 - x \pmod{f(x), M}$ olur. Burada $(x-1)^{M+1}$ değeri iki farklı yoldan hesaplanabilir. Önce kullanılacak özellikler ifade edilecektir. M asal olduğundan $0 < i < M$ olacak şekildeki her i değeri için $M|\binom{M}{i}$ dir. Bu yüzden $(x-1)^M \equiv x^M - 1 \pmod{M}$ elde edilir. Bu denklikler kullanılarak

$$\begin{aligned}(x-1)^{M+1} = (x-1)(x-1)^M &\equiv (x-1)(x^M - 1)\\ &\equiv (x-1)(3-x)\\ &\equiv 3x - x^2 - 3 + x\\ &\equiv 4x - (4x-1) - 3\\ &\equiv -2 \pmod{f(x), M} \qquad (4.4)\end{aligned}$$

şeklinde bulunur. Sonra ikinci hesaplama için kullanılacak özellikler verilsin. M değeri asal ve $-1 \pmod 8$ olduğundan $\left(\frac{2}{M}\right) = 1$ dir. Euler kriteri gereği $2^{(M-1)/2} \equiv \left(\frac{2}{M}\right) = 1 \pmod M$ olarak bulunur. Ayrıca $(x-1)^2 = x^2-2x+1 \equiv (4x-1)-2x+1 \equiv 2x \pmod{f(x), M}$ dir. Sonuç olarak bu denklikler kullanıldığında,

$$\begin{aligned}(x-1)^{M+1} \equiv (2x)^{(M+1)/2} &= 2 \cdot 2^{(M-1)/2} x^{(M+1)/2} \\ &\equiv 2x^{(M+1)/2} \pmod{(f(x), M)} \end{aligned} \tag{4.5}$$

elde edilir. Bulunan (4.4) ve (4.5) birbirine eşitlenirse,

$$\begin{aligned} 2x^{(M+1)/2} \equiv -2 \pmod{f(x), M} \;&\Rightarrow\; x^{(M+1)/2} \equiv -1 \pmod{f(x), M} \\ &\Rightarrow\; x^{2^{p-1}} \equiv -1 \pmod{f(x), M} \end{aligned}$$

bulunur. Ayrıca burada $\sigma(x) = x^M \equiv 4-x \pmod{f(x), M}$ olduğu hatırlanır ve son bulunan denkliğin her iki tarafına σ fonksiyonu uygulanırsa,

$$\begin{aligned} \sigma(x^{2^{p-1}}) \equiv \sigma(-1) \pmod{f(x), M} \;&\Rightarrow (x^M)^{2^{p-1}} \equiv -1 \pmod{f(x), M} \\ &\Rightarrow (4-x)^{2^{p-1}} \equiv -1 \pmod{f(x), M} \end{aligned}$$

bulunur. Yani $x^{2^{p-1}} \equiv (4-x)^{2^{p-1}} \pmod{f(x), M}$. Bu yüzden,

$$U_{2^{p-1}} = \frac{x^{2^{p-1}} - (4-x)^{2^{p-1}}}{x-(4-x)} \equiv 0 \pmod{f(x), M}$$

dir. Lucas dizisi için $U_{2^{p-1}} = U_{2^{p-2}} V_{2^{p-2}}$ şartı sağlanmaktadır (Lehmer 1975) ve elde edildi ki $U_{2^{p-1}} \equiv 0$ dır. Yani ya $U_{2^{p-2}} \equiv 0 \pmod{f(x), M}$ ya da $V_{2^{p-2}} \equiv 0 \pmod{f(x), M}$ olmalıdır. Eğer $U_{2^{p-2}} \equiv 0 \pmod{f(x), M}$ olsa $x^{2^{p-2}} \equiv (4-x)^{2^{p-2}} \pmod{f(x), M}$ olacağından,

$$-1 \equiv x^{2^{p-1}} \equiv x^{2^{p-2}}(4-x)^{2^{p-2}} \equiv (x(4-x))^{2^{p-2}} \equiv 1^{2^{p-2}} \equiv 1 \pmod{f(x), M}$$

çelişkisi elde edilir. Bu yüzden $V_{2^{p-2}} \equiv 0 \pmod{f(x), M}$ dir. Ayrıca teoremin ilk kısmında ispatlanmıştı ki $V_{2^{p-2}} = v_{p-2}$ dir. Yani $v_{p-2} \equiv 0 \pmod M$ olur. Böylece ispat tamamlanır. □

Aşağıda Lucas Lehmer Asallık Testinin algoritması verilmiştir.

Algoritma 2 Lucas Lehmer Asallık Testi (LLT)

Bu algoritma p tek asal sayısı için $n = 2^p - 1$ değerinin asal olup olmadığını göstermektedir.

1. **[Başlangıç]**

   $u := 4$;

   $m := 1$;

2. **[Lucas-Lehmer Dizisini Hesapla]**

   $(m \leq p-2)$ olduğu sürece

   {

   $u = (u^2 - 2) \mod (n)$

   m=m+1

   };

3. **[Kalan Kontrolü]**

   Eğer $(u = 0)$ ise n asaldır.

   n asal değildir;

4.3 n+1 Testi İçin Geliştirmeler ve $n^2 - 1$ Testi

Bu bölümde, bir önceki bölümde gösterilen $n+1$ testindeki F değerinin daha küçük seçilebilmesini sağlayan geliştirmelerden bahsedilecektir.

Teorem 4.3.1 Lucas dizilerini belirleyen f, Δ ve n sayısı için $(n, 2b) = 1$ olacak şekilde $\left(\frac{\Delta}{n}\right) = -1$ olsun. Ayrıca $F > n^{1/3} + 1$ olacak şekilde $n + 1 = FR$,

$$U_{n+1} \equiv 0 \pmod{n}, \quad \text{her } q|F \text{ asalı için } (U_{(n+1)/q}, n) = 1$$

ve R sayısı F tabanında $0 \leq c_i \leq F - 1$ olacak şekildeki c_i'ler için $R = c_1 F + c_0$ şeklinde yazılsın. Bu durumda n sayısının asal olması için gerek ve yeter şart

$x^2 + c_0x - c_1$ ve $x^2 + (c_0 - F)x - c_1 - 1$ polinomlarının pozitif tamsayı köklerinin olmamasıdır (Pomerance ve Crandall 2005).

Ayrıca $n + 1$ testi eğer $F \geq n^{3/10}$ seçilebilirse daha da geliştirilebilir.

Teorem 4.3.2 $n \geq 214$ ve Teorem 4.2.1'in hipotezleri sağlansın yalnızca farklı olarak $n^{1/3} + 1 \geq F \geq n^{3/10}n^{1/3} + 1$ ve $n + 1$'in F tabanındaki yazımı $c_4 = c_3F + c_2$ olacak şekilde $c_3F^3 + c_2F^2 + c_1F$ olsun. Bu durumda n'nin asal olması için gerek ve yeter şart aşağıdaki ifadelerin sağlanmasıdır (Pomerance ve Crandall 2005).

(1) $-5 \leq t \leq 5$ olacak şekildeki her t için $(c_1 + tF)^2 - 4t + 4c_4$ ifadesi tamkare değildir.

(2) $v < F^2/\sqrt{n}$ olacak şekildeki en büyük v için $\frac{u}{v}$'nin sürekli kesir ayrışımı $\frac{c_1}{F}$'e yakınsasın ve $d = \lfloor c_4v/F + 1/2 \rfloor$ için $vx^3 - (uF - c_1v)x^2 - (c_4v - dF + u)x + d$ polinomunun $aF + 1$ değeri n'nin aşikar olmayan bir böleni olacak şekilde bir a böleni yoktur ve $vx^3 + (uF - c_1v)x^2 - (c_4v + dF + u)x + d$ polinomunun $bf - 1$ değeri n'nin aşikar olmayan bir böleni olacak şekilde bir b böleni yoktur.

Sıradaki teorem $n^2 - 1$ in bölenlerini kullanarak n'nin asallığının belirlenmesinin mümkün olduğunu göstermektedir.

Teorem 4.3.3 (Billhart, Lehmer ve Selfridge) n pozitif bir tamsayı olsun ve aşağıdaki şartlar sağlansın.

$F_1|n - 1$ ve $a^{n-1} \equiv 1 \pmod{n}$, $q|F_1$ olacak şekildeki her q asalı için $(a^{n-1} - 1, n) = 1$, $F_2|n + 1$ ve $f(x) = x^2 - ax + b, \Delta = a^2 - 4b$ için U_n Lucas dizisi ifade edilip $\left(\frac{\Delta}{n}\right) = 1$ ve $(n, 2b) = 1$.

Yukarıda geçen F_1 ve F_2 değerlerinin en küçük ortak katı F olsun. Bu durumda n sayısının her asal böleni $1 \pmod{F}$ ya da $n \pmod{F}$ değerlerinden birisine denktir

(Pomerance ve Crandall 2005). Özel olarak eğer $n \pmod F$ n'nin aşikar olmayan bir böleni değil ve $F > \sqrt{n}$ ise n asaldır.

Burada F_1 ve F_2 için eğer ikisi de çift sayı ise $F = \frac{1}{2}F_1F_2$ diğer durumlarda $(F_1, F_2) = 1$ olacağından $F = F_1F_2$ olarak elde edilir.

İspat 4.3.1 p, n'nin bir asal böleni olsun. Bu durumda Teorem 3.2.1 gereği $p \equiv 1 \pmod{F_1}$ dir. Benzer şekilde Teorem 4.2.1 gereği $p \equiv \left(\frac{\Delta}{p}\right) \pmod{F_2}$ dir. Yani $\left(\frac{\Delta}{p}\right) = 1$ ise,

$$p \equiv 1 \pmod{F_1} \text{ ve } p \equiv 1 \pmod{F_2} \Rightarrow p \equiv 1 \pmod{F}$$

ve $\left(\frac{\Delta}{p}\right) = -1$ ise

$$p \equiv 1 \pmod{F_1},\ p \equiv -1 \pmod{F_2} \text{ ve } n \equiv 1 \pmod{F_1}, n \equiv -1 \pmod{F_2}$$
$$\Rightarrow p \equiv n \pmod{F}$$

elde edilir. Yani $p|n$ olacak şekildeki p asal sayısı $1 \pmod F$ ya da $n \pmod F$'e denktir. □

5. SONLU CİSİMLERDE ASALLIK TESTİ

Bu bölümde Lenstra tarafından bulunan ve I pozitif tamsayısı için $n^I - 1$'in çarpanları bilinen bir böleni bulunduğunda n'nin asallığını belirleyen bir yöntemden bahsedilecektir.

5.1 Polinom Halkaları ile Asallık Testi

Teste geçmeden önce polinomlar halkası ve sonlu cisimler ile ilgili bazı hatırlatmalar yapılacaktır. Eğer $n > 1$ olacak şekilde bir tamsayı ise $\mathbb{Z}_n[x]$ halkasının elemanları aşağıdaki gibi gösterilmektedir.

$$Z_n[x] := \{a_0 + a_1x + a_2x^2 + \cdots \mid \text{her } a_i \in \mathbb{Z}_n\}$$

Bu halkada toplama ve çarpma işlemleri (mod n) de yapılmaktadır. $\mathbb{Z}_n[x]$'in boştan farklı bir I altkümesi eğer

$$\text{her } f, g \in I \text{ için } f - g \in I$$
$$\text{her } f \in I, \text{ her } g \in \mathbb{Z}_[x] \text{ için } fg, gf \ \in I$$

şartlarını sağlıyorsa I'ya $\mathbb{Z}_n[x]$ halkasının bir ideali denmektedir. Örneğin $f, g \in \mathbb{Z}_n[x]$ ise $a \in \mathbb{Z}_n[x]$ olacak şekildeki tüm af'lerin oluşturduğu küme $I = \{af \mid a \in \mathbb{Z}_n[x]\}$ bir idealdir. Gerçekten de her $a, b \in \mathbb{Z}_n[x]$ için $a - b \in \mathbb{Z}_n[x]$ olduğundan $af - bf = (a - b)f \in I$ dir. $\mathbb{Z}_n[x]$ çarpmaya göre değişme özelliğini sağladığından ve her $a, g \in \mathbb{Z}_n[x]$ için $ag \in \mathbb{Z}_n[x]$ olduğundan $afg = (ag)f \in I$ olur. Aynı şekilde $a, b \in \mathbb{Z}_n[x]$ için $af + bg$ de bir idealdır. Eğer $\mathbb{Z}_n[x]$ halkasının bir I ideali için $I = u\mathbb{Z}_n[x] = \{uf \mid f \in \mathbb{Z}_n[x]\}$ olacak şekilde bir $u \in \mathbb{Z}_n[x]$ varsa bu ideale tek üreteçli ideal denir ve $I =< u >$ ile gösterilir. Ayrıca birimli ve değişmeli bir halkada bir ideal halkanın birimini içeriyorsa bu ideal halkanın kendisidir, böylece $< 1 >$ ideali yani birimin ürettiği ideal halkaya eşittir. Örnek olarak verilen af ve $af + bg$ ideallerinin birincisi tek üreteçli ve f elemanı tarafından üretilmektedir.

İkincisinin ise f ve g'nin seçimine göre tek üreteçli olduğu ve olmadığı durumlar vardır. Örneğin $n = 15$, $f(x) = 3x + 1$, $g(x) = x^2 + 4x$ olsun. Bu durumda $f^2 - 9g = 1$ olduğu için $a = f(x)$ ve $b = 9$ seçilirse $af + bg$ ideali birimi içermektedir. Böylece bu polinomlar tarafından üretilen ideal $\mathbb{Z}_{15}[x]$ halkasına eşittir dolayısıyla tek üreteçlidir ve üreteci halkanın birimidir.

Tanım 5.1.1 Eğer $f, g \in \mathbb{Z}_n[x]$ ve ürettikleri ideal $\mathbb{Z}_n[x]$ halkasına eşitse bu polinomlara aralarında asal polinomlar denir. Bir diğer deyişle $af + bg = 1$ olacak şekilde $a, b \in \mathbb{Z}_n[x]$ vardır (Pomerance ve Crandall 2005).

Aşağıdaki algoritma Euclid bölme algoritmasının farklı bir versiyonu olarak düşünülebilir. Bu algoritma ya n sayısının aşikar olmayan çarpanlarını ya da g, f polinomları tarafından üretilen idealin monik (başkatsayısı bir olan) üretecini bulmaktadır.

Algoritma 3 İdealin Üretecini Bulmak

$n \geq 2$ ve $f, g \in \mathbb{Z}_n[x]$ ve g monik olsun. Bu algoritma ya n sayısının çarpanlarını ya da $h = (f, g)$ olacak şekilde monik bir $h \in \mathbb{Z}_n[x]$ bulmaktadır. (f ve g polinomlarının ürettiği ideal aynı zamanda h'nin ürettiği ideale eşittir.) Kabul edilsin ki $f = 0$ veya $f \leq \deg(g)$.

1. [**Sıfır Polinom Kontrolü**]

   Eğer $(f = 0)$ ise return g;

2. [**Euclid Adımı**]

   c sayısını f polinomunun başkatsayısının değerine eşitle;

   $c^* = c^{-1} \pmod{n}$ olacak şekilde c^* değerini Euclid algoritmasını kullanarak bul, eğer Euclid algoritması n'nin bölenlerini üretirse sonuç olarak onları ver ve algoritmadan çık;

   $f = c^* f \pmod{n}$;

   $r := g \pmod{f}$

   $(f, g) = (r, f)$;

   Sıfır Polinom Kontrolü Adımına git;

Teorem 5.1.1 Kabul edelim ki n, I, F pozitif tamsayı, $n > 1$ ve $F|n^I - 1$ olsun. Ayrıca $f, g \in \mathbb{Z}_n[x]$ için aşağıdaki şartlar sağlansın,

(1) $g^{n^I-1} - 1 \equiv 0 \pmod{f}$,

(2) $q|F$ olacak şekildeki her q asal sayısı için $(g^{(n^I-1)/q} - 1, f) = 1$,

(3) $g, g^n, g^{n^2}, \cdots, g^{n^{I-1}}$'ler ile yazılan her elementer simetrik polinom $\pmod{f}$ altında $\mathbb{Z}_n$'in bir elemanıdır.

Bu durumda n'nin her p asal böleni için $0 \leq j \leq I-1$ olacak şekilde bir j tamsayısı vardır öyle ki $p \equiv n^j \pmod{F}$'dir (Pomerance ve Crandall 2005).

Bu teoremin neden bir asallık şartı olarak düşünülebileceğini şöyle açıklanabilir. Eğer yukarıdaki teoremin şartları sağlanır ve $j = 0, 1, 2, \cdots, I-1$ için $n^j \pmod{F}$ değerlerinin her biri 1 ya da n ye eşitse bu n sayısının 1 ve kendisinden başka böleninin olmadığı anlamına gelmektedir yani n asaldır.

İspat 5.1.1 p sayısı, n'nin bir asal böleni olsun. Bu durumda $p \equiv n^j \pmod{F}$ olduğunun gösterilmesi gerekir. Öncelikle $\bar{f} := f \pmod{p}$ polinomunu düşünülürse bu polinom $\mathbb{Z}_p[x]$ halkasının bir elemanı olmaktadır. $\bar{f}_1$ polinomu ise $\bar{f}$'nin $\mathbb{Z}_p[x]$ halkasındaki indirgenemez çarpanı olsun. Bu yüzden $K := \mathbb{Z}_p[x]/(\bar{f}_1)$, $\mathbb{Z}_p$'nin bir sonlu cisim genişlemesidir. Bu cisim içinde g polinomunun değeri $\bar{g}$ ile gösterilsin. Yani $\bar{g} := g \ (mod\ \bar{f}_1, p)$. Bu durumda teoremin (1) ve (2) şartları $\bar{g}$ için tekrar ifade edilirse

(1) $\bar{g}^{n^I-1} = 1$

ve

$$
\begin{aligned}
&q|F \text{ olacak şekildeki her } q \text{ asalı için } (g^{(n^I-1)/q}-1, f) = 1 \\
&\Rightarrow (g^{(n^I-1)/q}-1)h + fk = 1 \text{ olacak şekilde } h, k \in \mathbb{Z}_n[x] \text{ vardır} \\
&\Rightarrow (g^{(n^I-1)/q}-1)h \equiv 1 \pmod{\bar{f}_1, p} \qquad\qquad (\bar{f}_1|\bar{f}) \\
&\Rightarrow g^{(n^I-1)/q} - 1 \not\equiv 0 \pmod{\bar{f}_1, p} \\
&\Rightarrow g^{(n^I-1)/q} \not\equiv 1 \pmod{\bar{f}_1, p} \\
&\Rightarrow \bar{g}^{(n^I-1)/q} \neq 1
\end{aligned}
$$

olduğundan,

(2) $q|F$ olacak şekildeki her q asal sayısı için $\bar{g}^{(n^I-1)/q} \neq 1$

olmaktadır. Bu nedenle $\bar{g}$'nin K^* (K cisminin çarpma işlemi altında oluşturduğu grup) grubundaki mertebesi F'nin bir pozitif katı ($tF, t > 0$) olmaktadır (Teorem 3.2.1'in ispatına benzer şekilde). Ayrıca teoremdeki (3) şartı $g, g^n, g^{n^2}, \cdots, g^{n^{I-1}}$'ları değişken olarak kabul eden I adet elementer simetrik polinomun (mod f) altında $\mathbb{Z}_n$'in elemanı olduğunu söylemektedir. Bunun ne anlama geldiği aşağıda kısaca açıklanmıştır. Bu değerler için elementer simetrik polinomlar,

$$
\begin{aligned}
&e_0(g, g^n, g^{n^2}, \cdots, g^{n^{I-1}}) = 1 \\
&e_1(g, g^n, g^{n^2}, \cdots, g^{n^{I-1}}) = g + g^n + g^{n^2} + \cdots + g^{n^{I-1}} \\
&e_2(g, g^n, g^{n^2}, \cdots, g^{n^{I-1}}) = gg^n + gg^{n^2} + \cdots + g^{n^2}g^{n^3} + \cdots + g^{n^{I-2}}g^{n^{I-1}} \\
&e_3(g, g^n, g^{n^2}, \cdots, g^{n^{I-1}}) = \sum_{0 \le j < k < l \le I} g^{n^j} g^{n^k} g^{n^l} \\
&\cdots \\
&e_I(g, g^n, g^{n^2}, \cdots, g^{n^{I-1}}) = gg^n g^{n^2} \cdots g^{n^{I-1}}
\end{aligned}
$$

şeklinde elde edilebilir. (3) şartı aslında bu polinomların hepsinin (mod $\bar{f}_1, p$) altında $\mathbb{Z}_p$'nin elemanı olduğunu söylemektedir. Yani yukarıdaki çarpımlar sabitlere karşılık gelmektedir. Aşağıda tanımlanan polinom dikkatle incelenirse,

$$h(T) := (T - \bar{g}) \cdots (T - \bar{g}^{n^I-1}) \in K[T]$$

katsayılarının yukarıda tanımlanan elementer simetrik polinomlar olduğu görülebilir. Yani özetle (3) şartı $h(T)$ polinomunun tüm katsayılarının $\mathbb{Z}_p$'nin elemanı olduğunu ve dolayısıyla $h(T) \in \mathbb{Z}_p[T]$ olduğunu ifade etmektedir. $\mathbb{Z}_p[T]$ halkasındaki bir polinom için eğer α kök ise α^p'de aynı polinomun köküdür. Bu yüzden $\bar{g}$, $h(T)$ polinomunun kökü olduğu için $\bar{g}^p$ de $h(T)$ polinomunun köküdür. Yani $h(\bar{g}^p) = 0$ dır. Ayrıca yukarıda görüldüğü gibi $h(T)$ polinomunun tüm kökleri $\bar{g}, \bar{g}^n, \cdots, \bar{g}^{n^I-1}$ elemanlarıdır. Bu yüzden $j \in [0, I-1]$ olacak şekilde bir j tamsayısı için $\bar{g}^p = \bar{g}^{n^j}$ dir. Sonuç olarak $\bar{g}$ elemanının mertebesi F'nin katı olduğu için $p \equiv n^j \pmod{tF}$ dolayısıyla $p \equiv n^j \pmod{F}$ olmaktadır. □

Bu teorem sonucunda ortaya şu sorular çıkmaktadır:
Eğer n asalsa teoremi sağlayan f, g var mıdır?
Eğer varsa bunları bulmak kolay mıdır?
Teoremde geçen (1), (2), (3) şartları hızlı şekilde kontrol edilebilir mi?

İlk sorulan soru kolay bir sorudur çünkü eğer n asalsa derecesi I olan her $f(x) \in \mathbb{Z}_n[x]$ indirgenemez polinomu ve f'nin katı olmayan her $g(x) \in \mathbb{Z}_n[x]$ polinomu için (1) ve (3) şartları sağlanmaktadır. Gerçektende eğer f indirgenemez ve derecesi I ise $K = \mathbb{Z}_n[x]/(f)$ halkası n^I mertebeli bir sonlu cisim olmaktadır. Bu durumda (1) şartı yalnızca Lagrange teoreminin (grubun elemanı grubun mertebesi defa kendisi ile çarpılırsa birim elde edilir.) K^* grubu için uygulaması olmaktadır. (3) şartının sağlanması için K cismi üzerinde tanımlanan Galois grubu dikkate alınmalıdır. Bu Galois grubu $Gal(K/\mathbb{Z}_n)$, elemanın n^j kuvvetini alan (frobenius otomorfizması) fonksiyonlar tarafından üretilmektedir. Yani $Gal(K/\mathbb{Z}_n)$ grubu $j \in [0, I-1]$ için $\sigma_j : K \to K$, $\sigma_j(\alpha) = \alpha^{n^j}$ olacak şekildeki I adet fonksiyonun bileşke işlemi ile oluşturduğu bir gruptur. Galois grubundaki fonksiyonlar yalnızca alt cisimdeki elemanları kendilerine götürürler (Pomerance ve Crandall 2005). Buradaki I adet σ_j fonksiyonunun her biri $g, g^n, \cdots, g^{n^{I-1}}$ lerin elementer simetrik polinomlarını kendilerine eşitler (Pomerance ve Crandall 2005). Bu nedenle elementer simetrik polinomlar $\mathbb{Z}_n$ cisminin elemanı olmaktadırlar. Teoremin (2) şartı f'nin katı olmayan her g için sağlanmamaktadır. Ancak K^* grubu devirli olduğundan ve her devirli

grubun üreteci (2) şartını sağladığından g'nin aynı zamanda K^* grubunun üreteci olarak seçilmesi gerekir. K^* grubunun $\varphi(n^I-1)$ tane üreteci bulunmaktadır. Bu yüzden derecesi I'dan küçük olacak şekilde rastgele seçilen bir $g \neq 0$ polinomunun üreteç olma olasılığı $\varphi(n^I-1)/(n^I-1)$ kadardır. Yani (2) şartını sağlayan g'yi bulmak zor bir işlem değildir. Ayrıca derecesi I olan ve $\mathbb{Z}_n[x]$'de indirgenemez olan bir f polinomu bulmakta çok zor değildir. Rastgele seçilen bir I dereceli polinomun indirgenemez olma olasılığı yaklaşık olarak $1/I$ kadardır.

Bu bölümün sonunda teorem 5.1.1 kullanılarak oluşturulan bir asallık algoritması verilmiştir. Bu algoritmaya sonlu cisimler asallık testi de denmektedir. Ancak bu algoritmanın uygulanabilmesi için başında da belirtildiği gibi uygun F ve I değerleri belirlenmeli. Peki bu değerler $F|n^I-1$, $F \geq \sqrt{n}$ olacak şekilde nasıl belirlenebilir? Hatırlayınız ki F değerinin tüm çarpanlarının bilinmesi gerekiyordu. Aşağıda F değerinin nasıl bulunacağını gösteren bir örnek verilmiştir.

Örnek 5.1.1 Eğer, k pozitif tamsayı olmak üzere $q = p^k$, $(n,q) = 1$ ve $\varphi(q)|I$ oluyorsa $q|n^I-1$ dir. Bu durum Euler teoremi kullanılarak kolaylıkla ispatlanabilir. $(n,q) = 1$ olduğundan $n^{\varphi(q)} \equiv 1 \pmod{q} \Rightarrow n^{\varphi(q)} - 1 \equiv 0 \pmod{q}$ elde edilir ayrıca $\varphi(q)|I$ olduğu için $n^I - 1 \equiv 0 \pmod{q}$ olur. Yani $n^I - 1 = qt$ olacak şekilde bir t tamsayısı vardır. Bu da $q|n^I-1$ olduğunu gösterir. Ayrıca eğer q 2'nin bir kuvveti ve 4'ten büyük ise $\frac{1}{2}\varphi(q)|I$ şartı yeterlidir. Örneğin $I = 12$ seçersek $\varphi(q)|I$ olan q değerleri $q_1 = 2^3$, $q_2 = 3^2$, $q_3 = 5$, $q_4 = 7$, $q_5 = 13$ elde edilir. Bu değerlerin her biri I değerini böldüğünden çarpımları yani $q_1 \cdot q_2 \cdot q_3 \cdot q_4 \cdot q_5 = 65520|n^I - 1$ dır. Bu nedenle $F = 65520$ olarak elde edilir.

Ancak yukarıdaki yöntem ile F aramanın gerektirdiği işlem sayısı nasıl bir değere bağlıdır? Kısaca bu algoritmanın karmaşıklığı nedir? Bu sorunun cevabı $O(logn)^{cloglogn}$ (Pomerance ve Crandall 2005). Bu değer incelendiğinde n arttıkça $logloglogn$ değeri sonsuza gitmektedir. Yani algoritmanın karmaşıklığı bir polinom olarak ifade edilememiştir. Bu nedenle algoritma polinom zamanlı değildir.

Algoritma 4 Sonlu Cisimlerde Asallık Testi

n, I, F pozitif tamsayıları verilsin, $F|n^I-1$, $F \geq \sqrt{n}$ şartları sağlansın ve F değerinin tüm asal çarpanları bilinsin. Bu algoritma sonuç olarak n'nin asal olup olmadığını göstermektedir.

1. [I **dereceli indirgenemez polinom**]

   Derecesi I olan monik bir $f(x) \in \mathbb{Z}_n[x]$ polinomunu rastgele seç. Bu polinom indirgenebilir ise başka bir polinom seç. (Burada eğer n asalsa indirgenemez bir $f(x)$ polinomu mutlaka bulunacaktır ya da n'nin bölenlerini bulacaktır.) Rastgele seçilen polinom indirgenemez olasıya kadar veya n'nin bir çarpanını bulasıya kadar devam et;

2. [**Primitif Elemanın Bulunması**]

   Rastgele, $\deg g < I$ olan monik bir $g(x) \in \mathbb{Z}_n[x]$ elemanı seç;

   Eğer $(1 \not\equiv g^{n^I-1} \pmod f)$ ise n asal değildir;

   $q|F$ oldukça {

   Algoritma (3) ile $(g^{n^{(I-1)/q}} - 1, f)$ değerini hesapla eğer n'nin çarpanları bulunursa n asal değildir;

   Eğer $((g^{n^{(I-1)/q}} - 1, f) \neq 1)$ ise [Primitif Elemanın Bulunması] adımına git;

   }

3. [**Simetrik Polinom Kontrolü**]

   $(T-g)(T-g^n)\cdots(T-g^{n^{I-1}}) = T^I + c_{I-1}T^{I-1} + \cdots + c_0 \in \mathbb{Z}_n[x,T]/(f(x))$ polinomunu oluştur;

   $j \in [0, I-1]$ oldukça {

   eğer $(c_j > 0)$ ise n asal değildir;

   }

4. [**Bölen Arama**]

   $j \in [0, I-1]$ oldukça {

   Eğer $n^j \pmod f$ n'nin aşikar olmayan bir böleni ise n asaldır;

   }

   n asal değildir;

6. AKS ASALLIK TESTİ

Bu bölüme kadar incelenen her testte bazı zorluklar bulunmaktadır. Örneğin $n-1$ testi büyük bir bölen bulmayı gerektirmektedir. Aynı şekilde $n+1$ testi için de yine büyük bir bölen bulmak gereklidir. Sonlu cisimlerde asallık testi uygulanırken de polinomların belirlenmesi aşamasında rastgelelik kullanılmaktadır ve bu algoritma polinom zamanlı değildir. Teorik olarak incelendiğinde bir asallık testi için iki durum çok önem arzetmektedir. Bunlar deterministiklik ve polinom zamanlılıktır. Bunlardan ilki deterministik olma, yani algoritmanın her aşamasının ve sonuçlarının kesinlik içermesi anlamına gelir. Polinom zamanlılık ise algoritmanın karmaşıklığının girdi olarak verilen değerin bit sayısına bağlı bir polinom tarafından sınırlanmasıdır. Yani tezde daha önceki bölümlerde bahsedilen testlerin hepsi, rastgelelik içerdiğinden veya karmaşıklıkları bir polinom tarafından sınırlanamadığından istenen deterministik ve polinom zamanlı olma şartlarını sağlamamaktadırlar. Antik Yunan'da başlayan asallık serüveni Hindistan'da 3 bilgisayar mühendisi tarafından sonuca ulaştırılmıştır.

Manindra Agrawal, Neeraj Kayal ve Nitin Saxena 2004 yılında hem deterministik hem de polinom zamanlı bir asallık algoritması bulduklarını duyurmuşlardır. Bu test AKS testi olarak bilinmektedir.

6.1 Birimin Kökleri ile Asallık Testi

Lemma 6.1.1 Eğer n asal sayı ise her $g(x) \in \mathbb{Z}[x]$ için,

$$g(x)^n \equiv g(x^n) \pmod{n},$$

denkliği sağlanmaktadır (Pomerance 2005).

Özel olarak Lemma 6.1.1'de $a \in \mathbb{Z}$ olacak şekilde $g(x) = x + a$ seçilirse,

$$(x + a)^n \equiv x^n + a \pmod{n} \tag{6.1}$$

elde edilir. Eğer $n \geq 2$ ve $(a, n) = 1$ olacak şekilde bir a tamsayısı için (6.1) sağlanırsa n asaldır. Yani (6.1) özelliği asallık için gerek ve yeter şart oluşturmaktadır. Ancak burada $a = 1$ olduğu durumda bile (6.1) denkliğini kontrol etmek için hızlı bir yöntem bilinmemektedir. Bakılırsa denkliğin sol tarafında oldukça fazla terim bulunmakta ve bu terimlerin her birinin kontrol edilmesi çok işlem gerektirmektedir. Eğer keyfi monik bir $f(x) \in \mathbb{Z}[x]$ polinomu seçilirse (6.1) denkliği,

$$(x + a)^n \equiv x^n + a \pmod{f(x), n} \tag{6.2}$$

olduğunu ifade etmektedir (Pomerance 2005). Bu yüzden eğer n asalsa her a tamsayısı ve monik $f(x) \in \mathbb{Z}[x]$ için (6.2) denkliği sağlanmaktadır. Ayrıca polinomun derecesi çok büyük olmadığı sürece (6.2) denkliği (6.1) e göre daha hızlı kontrol edilebilmektedir. Örnek olarak $a = 2$ ve $f(x) = x - 1$ alınırsa;

$$(x + 2)^n \equiv x^n + 2 \pmod{x - 1, n} \Rightarrow 3^n \equiv 3 \pmod{n}$$

elde edilmektedir. Bu denklik Fermat teoreminin $a = 3$ seçilmiş halidir. Bilindiği üzere bu denkliği sağlayan ancak asal olmayan sayılar bulunmaktadır. Örneğin $91^3 \equiv 1 (\text{mod } 3)$ olur ancak $91 = 13 \cdot 7$ şeklinde çarpanlarına ayrılan bir sayıdır. Sonuç olarak burada (6.2) denkliğinin asallık için gerek ve yeter şart olmadığı görülmektedir. Yani denklik (mod $f(x)$)'e taşınarak hız kazanıldı ama asallık kriteri $x - 1$ polinomu ile sağlanamadı. Ancak (6.2) denkliği ile bir genelleştirme sağlanmıştır dolayısıyla farklı polinomlar seçilebilir. Örneğin bazı küçük r değerleri için $x^r - 1$. Eğer n sayısı asal ise (6.2) denkliği sağlanmaktadır ancak asal olmayan bazı n değerleri için de denkliği sağlayan a ve r değerleri bulunabilmektedir (Agrawal vd. 2004). Agrawal, Kayal ve Saxena özel seçilmiş bir r değeri için belirli sayıda a değeri ile (6.2) denkliği sağlanırsa n'nin asal olduğunu göstermişlerdir (Agrawal vd. 2004). Burada a'ların sayısı ve özel r değeri $\log n$ cinsinden bir polinom tarafından sınırlanmıştır. Dolayısıyla AKS algoritması hem deterministik hem de polinom zamanlı bir algoritmadır. Algoritmaya temel oluşturan teorem aşağıda verilmiştir.

Teorem 6.1.1 (Agrawal,Kayal,Saxena) $n \geq 2$, $r > 0$, $(n, r) = 1$, n'nin $\mathbb{Z}_r^*$ grubundaki mertebesi $\lg^2 n$ değerinden büyük ve $0 \leq a \leq \sqrt{\varphi(r)} \lg n$ olacak şekilde her a tamsayısı için,

$$(x + a)^n \equiv x^n + a \pmod{x^r - 1, n} \tag{6.3}$$

denkliği sağlansın. Eğer $p > \sqrt{\varphi(r)} \lg n$ ve $p|n$ olacak şekilde bir p asalı varsa $n = p^m$ olacak şekilde bir $m \in \mathbb{Z}$ vardır. Özel olarak eğer n'nin $[1, \sqrt{\varphi(r)} \lg n]$ aralığında asal böleni yoksa ve n tam kuvvet değilse n asaldır.

Teoremde geçen $\lg n$ ifadesi $log_2 n$ olarak tanımlanmıştır.

İspat 6.1.1 n asal olmasın ve $p > \sqrt{\varphi(r)} \lg n$ olacak şekilde p asal bölenine sahip olsun. Gösterilecektir ki bir m pozitif tamsayısı için $n = p^m$ dir. Bunun için öncelikle

$$G := \{g(x) \in \mathbb{Z}_p[x] \mid g(x)^n \equiv g(x^n) \pmod{x^r - 1}\}$$

kümesi tanımlansın. Kabul gereği $\sqrt{\varphi(r)} \lg n < p$ olduğundan her $a \in [0, \sqrt{\varphi(r)} \lg n]$ için $a < p$ dir dolayısıyla her bir $x + a$ polinomu $\mathbb{Z}_p[x]$'in elemanıdır. Ayrıca (6.3) denkliğinden

$$(x + a)^n \equiv x^n + a \pmod{x^r - 1, n} \Rightarrow (x + a)^n \equiv x^n + a \pmod{x^r - 1, p}$$

elde edilir. Bu nedenle $0 \leq a \leq \sqrt{\varphi(r)} \lg n$ olacak şekildeki her a tamsayısı için $x + a \in G$ dir. G kümesi çarpma işlemine göre kapalıdır. Gerçekten de her $g(x), h(x) \in G$ için $g(x)^n \equiv g(x^n) \pmod{x^r - 1}$ ve $h(x)^n \equiv h(x^n) \pmod{x^r - 1}$ olduğundan

$$(g(x)h(x))^n = g(x)^n h(x)^n \equiv g(x^n)h(x^n) \pmod{x^r - 1}$$

olmaktadır. G kümesi çarpma işlemine göre kapalı olduğundan ϵ_a'lar negatif olmayan tamsayılar olmak üzere

$$\prod_{0 \leq a \leq \sqrt{\varphi(r)} \lg n} (x + a)^{\epsilon_a}$$

çarpımından elde edilen polinomlar da G kümesinin elemanıdır. Ayrıca $\sqrt{\varphi(r)}\lg n < p$ olduğundan bu polinomlar $\mathbb{Z}_p[x]$'de ayrık ve sıfırdan farklıdırlar. Çünkü $\mathbb{Z}_p$ cisim olduğundan $\mathbb{Z}_p[x]$ öklit bölgesi dolayısıyla tek türlü çarpanlarına ayrılabilir bir bölgedir. Özetle G kümesinin oldukça fazla elemanı vardır. Aynı zamanda G kümesi $\mathbb{Z}_p[x]$ halkasındaki polinomların x^r-1'e bölümünden elde edilen kalan sınıflarının bir birleşimidir. Yani, eğer $g_1(x) \in G$ ve $g_2(x) \in \mathbb{Z}_p[x]$ için $g_2(x) \equiv g_1(x) \pmod{x^r-1}$ ise $g_2(x) \in G$ dir. Bunu göstermek gerekirse

$$g_2(x) \equiv g_1(x) \pmod{x^r-1}$$

denkliğinde x yerine x^n yazılarak,

$$g_2(x^n) \equiv g_1(x^n) \pmod{x^{nr}-1}$$

elde edilir. Kolaylıkla görülebilir ki $x^r-1 | x^{nr}-1$ dir. Bu nedenle son denklik $(\mathrm{mod}\ x^r-1)$ için de sağlanmış olur. Yani

$$g_2(x)^n \equiv g_1(x)^n \equiv g_1(x^n) \equiv g_2(x^n) \pmod{x^r-1}$$

elde edilip $g_2(x) \in G$ olmuş olur. Buraya kadar yapılanlar özetlenirse;

• G kümesi çarpma işlemi altında kapalı dolayısıyla her $a \in [0, \sqrt{\varphi(r)}\lg n]$ için $x+a$ ve çarpımlarından elde edilen polinomlar G'nin elemanı ve G kümesi $\mathbb{Z}_p[x]$ halkasındaki polinomların x^r-1'e bölümünden elde edilen kalan sınıflarının bir birleşimidir.

G kümesindeki denkliği sağlayan değerler bir küme ile ifade edilirse bu küme

$$J := \{j \in \mathbb{Z}^+ \mid \text{ her } g(x) \in G \text{ için } g(x)^j \equiv g(x^j) \pmod{x^r-1}\}$$

olarak bulunur. G kümesinin tanımından anlaşıldığı üzere $n \in J$ ve aşikar olarak $1 \in J$ dir. Ayrıca her $g(x) \in \mathbb{Z}_p[x]$ polinomu için $g(x)^p = g(x^p)$ olduğundan $p \in J$ dir. Gösterilsin ki J çarpma işlemi altında kapalıdır. Eğer $j_1, j_2 \in J$ ve $g(x) \in G$ alınırsa G çarpma işlemine göre kapalı olduğundan $g(x)^{j_1} \in G$ dir. Ayrıca $g(x)^{j_1} \equiv g(x^{j_1})\ (\mathrm{mod}\ \ x^r-1)$ olduğundan bir önceki paragraftan anlaşılacağı üzere $g(x^{j_1}) \in G$

elde edilir. Böylece $j_2 \in J$ olduğundan,

$$g(x)^{j_1 j_2} \equiv g(x^{j_1})^{j_2} \equiv g((x^{j_2})^{j_1}) = g(x^{j_1 j_2}) \pmod{x^r - 1}$$

elde edilip $j_1, j_2 \in J$ dir. Yani J kümesi çarpma işlemi altında kapalıdır. Buraya kadar yapılanlar özetlenirse;

• J kümesi $1, p$ ve n sayılarını içeriyor ayrıca çarpma işlemine göre kapalıdır.

K ile $x^r - 1$ polinomunun tüm köklerini içeren en küçük cisim ifade edilsin. Yani K cismi $\mathbb{F}_p$ cismi üzerinde $x^r - 1$ polinomunun parçalanış cismi olsun. Dolayısıyla karakteristiği p ve birimin r derecedem köklerini içeren en küçük cisimdir. Özel olarak $\zeta \in K$ 1'in r dereceden bir primitif kökü olsun. Ayrıca ζ'yı kök kabul eden minimal polinom $h(x) \in \mathbb{F}_p[x]$ polinomu olsun. Bu nedenle $h(x)$, $x^r - 1$'in indirgenemez bir bölenidir. Böylece $K = \mathbb{F}_p[\zeta] \cong \mathbb{F}_p[x]/(h(x))$ olur. Burada $\deg h = k$ olarak kabul edilsin.

$$\sigma \ : \ \mathbb{Z}_p[x]/(x^r - 1) \to K = \mathbb{F}_p(\zeta) \cong \mathbb{F}_p[x]/(h(x))$$
$$\bar{x} \mapsto \zeta$$

şeklinde tanımlanan σ bir halka homomorfizmasıdır. G kümesinin bu homomorfizma altındaki görüntüsü aşağıdaki küme ile tanımlansın.

$$\overline{G} := \{\gamma \in K \mid g(x) \in G \text{ için } g(\zeta) = \gamma\}$$

Eğer $j \in J$ ve $g(x) \in G$ ise $\sigma(g(x)) = g(\zeta)$ olduğundan;

$$\begin{aligned} g(\zeta)^j = \sigma(g(x))^j &= \sigma(g(x))\sigma(g(x)) \cdots \sigma(g(x)) \\ &= \sigma(g(x)^j) \\ &= \sigma(g(x^j)) \\ &= g(\zeta^j) \end{aligned}$$

elde edilir. $(n, r) = 1$ olduğundan $(p, r) = 1$ olmaktadır. Dolayısıyla n ve p tarafından üretilen $< n, p >= \{n^a p^b \pmod{r} \mid a, b \in \mathbb{Z}^+\}$ grubu $\mathbb{Z}_r^*$ grubunun bir alt grubudur Bu alt grubun mertebesi d olsun yani $(| < n, p > | = d)$. G kümesinin

elemanlarından derecesi d'den küçük olan polinomların kümesi aşağıdaki şekilde gösterilsin.

$$G_d := \{g(x) \in G \mid g(x) = 0 \text{ veya } \deg g(x) < d\}$$

$\mathbb{Z}_r^*$ grubunun mertebesi $\varphi(r)$ olduğundan $r > \varphi(r) \geq d$ dir. Dolayısıyla G_d'nin elemanları $(\bmod\ x^r - 1)$'de farklıdırlar. Şimdi tanımlanan σ homomorfizmasının G_d üzerine kısıtlandığında birebir olduğu gösterilecektir. $g_1(x), g_2(x) \in G_d$ ve $g_1(\zeta) = g_2(\zeta)$ olsun. Eğer $a, b \geq 0$ için $j = n^a p^b$ ise $j \in J$ dir. Çünkü J çarpmaya göre kapalıdır. Bu yüzden;

$$g_1(\zeta^j) = g_1(\zeta)^j = g_2(\zeta)^j = g_2(\zeta^j)$$

olur. Burada n, p'nin $\mathbb{Z}^*$'da ürettiği grubun mertebesi d olduğu için d farklı j $(\bmod\ r)$ değeri elde edilir. Dolayısıyla eşitlik d farklı j $(\bmod\ r)$ değeri için sağlanmaktadır. Aynı zamanda ζ 1'in primitif kökü olduğundan farklı j $(\bmod\ r)$'ler için ζ^j farklı sonuçlar verecektir. Yani d farklı j değeri için $g_1(\zeta^j) - g_2(\zeta^j) = 0$ dır. Bu demektir ki $g_1(x) - g_2(x)$ polinomunun K cismi içinde en az d kökü vardır. Ancak $g_1(x) - g_2(x)$ polinomu G_d kümesinin elemanı olduğu için derecesi d'den küçüktür. Bu nedenle mecburen $g_1(x) = g_2(x)$ dir. Yani homomorfizma G_d'ye kısıtlandığında birebirdir. Şimdiye kadar yapılanlar özetlenirse;

• G_d'nin farklı polinomları $\overline{G}$'nin farklı elemanlarına karşılık gelmektedir.

Bu durum $\epsilon_a \in 0, 1$ olacak şekildeki aşağıdaki polinomlar için düşünüldüğünde,

$$g(x) = 0 \text{ veya } g(x) = \prod_{0 \leq a \leq \sqrt{d} \lg n} (x + a)^{\epsilon_a}$$

$d \leq \varphi(r)$ olduğu için çarpımdan elde edilen her $g(x)$ polinomu, G'nin elemanı olur. Ayrıca;

$$\begin{aligned} d > \lg^2 n &\Rightarrow \sqrt{d} > \lg n \\ &\Rightarrow d > \sqrt{d} \lg n \end{aligned}$$

elde edilir. Bu nedenle ϵ_a'ların hepsi birden 1 olmadığı sürece her $g(x)$, G_d'nin elemanı olmaktadır. Bu sebeple G_d'nin eleman sayısı

$$1 + (2^{\lfloor \sqrt{d} \lg n \rfloor + 1} - 1) > 2^{\sqrt{d} \lg n} = n^{\sqrt{d}}$$

olarak bulunur. Sonuç olarak,

$$\#\bar{G} \geq \#G_d > n^{\sqrt{d}}$$

dir. Daha önce belirtildiği gibi $K \cong \mathbb{F}_p[x]/(h(x))$ ve $h(x) \in \mathbb{F}_p[x]$ derecesi k olan indirgenemez bir polinomdur. Yani $K \cong \mathbb{F}_{p^k}$ dır. Bu nedenle eğer, j, j_0 pozitif tamsayılar olmak üzere $j \equiv j_0 \pmod{p^k - 1}$ ve $\beta \in K$ ise $\beta^j = \beta^{j_0}$.

$$J' := \{j \in \mathbb{Z}^+ \mid j_0 \in J \text{ için } j \equiv j_0 \pmod{p^k - 1}\}$$

kümesi oluşturulsun. Eğer $j_0 \in J$ için $j \equiv j_0 \pmod{p^k - 1}$ ve $g(x) \in G$ olursa,

$$g(\zeta)^j = g(\zeta)^{j_0} = g(\zeta^{j_0}) = g(\zeta^j)$$

dir. J çarpma işlemi altında kapalı olduğundan J''da öyledir. Ayrıca $np^{k-1} \equiv n/p \pmod{p^k - 1}$ olduğundan $n/p \in J'$ elde edilir. Buraya kadar yapılanlar özetlenirse

• J' çarpma işlemi altında kapalıdır. $1, n/p$ ve p sayıları J' kümesinin elemanlarıdır. Ayrıca her $j \in J'$ ve $g(x) \in G$ için $g(\zeta)^j = g(\zeta^j)$ dir.

$a, b \in [0, \sqrt{d}]$ olacak şekilde $p^a(n/p)^b$ tamsayıları düşünüldüğünde, burada d dğerinden daha fazla sayıda birbirinden farklı (a, b) sıralı ikilisi vardır. Ancak p ve n/p $\mathbb{Z}_r^*$ 'ın d mertebeli alt grubunun ($< n, p >$) elemanlarıdır. Bu yüzden 2 tane birbirinden farklı (a_1, b_1), (a_2, b_2) sıralı ikilileri vardır öyle ki $p^{a_1}(n/p)^{b_1} \equiv p^{a_2}(n/p)^{b_2} \pmod{r}$ dir. Kolaylık olması bakımından $j_1 := p^{a_1}(n/p)^{b_1}$ ve $j_2 := p^{a_2}(n/p)^{b_2}$ olarak gösterilsin. Bu gösterim ile $j_1 \equiv j_2 \pmod{r}$ olup $\zeta^{j_1} = \zeta^{j_2}$ dir. Ayrıca $j_1, j_2 \in J'$ olduğundan her $g(x) \in G$ için,

$$g(\zeta)^{j_1} = g(\zeta^{j_1}) = g(\zeta^{j_2}) = g(\zeta)^{j_2}$$

elde edilir. Dolayısıyla her $\gamma \in \overline{G}$ için $\gamma^{j_1} = \gamma^{j_2}$. Daha önce gösterilmişti ki $\overline{G}$'nin $n^{\sqrt{d}}$'den daha fazla elemanı vardır. Ayrıca $j_1, j_2 \leq p^{\sqrt{d}}(n/p)^{\sqrt{d}} \leq n^{\sqrt{d}}$ olduğundan $x^{j_1} - x^{j_2}$ polinomunun derecesi en fazla $\sqrt{d}$ dir. Sonuç olarak, bu polinomun K cismi içinde derecesinden fazla kökü bulunmaktadır bu yüzden $x^{j_1} - x^{j_2} = 0$ olur. Bu nedenle $j_1 = j_2$ dir. Yani

$$p^{a_1}(n/p)^{b_1} = p^{a_2}(n/p)^{b_2} \Rightarrow n^{b_1-b_2} = p^{b_1-b_2+a_2-a_1}$$

elde edilir. (a_1, b_1), (a_2, b_2) farklı sıralı ikililer olduklarından $b_1 \neq b_2$ dir. Sonuç olarak tamsayılar tek türlü çarpanlara ayrılabildiğinden,

$$n \in \mathbb{Z}^+ \text{ olacak şekilde } n = p^m$$

elde edilir ve ispat tamamlanır. □

Aşağıda AKS teoreminin asallık testine çevrilmiş hali algoritma olarak verilmiştir.

Algoritma 5 AKS Asallık Testi

Bu algoritma verilen bir n pozitif tamsayısının asal olup olmadığını belirlemektedir.

1. [**Kuvvet Testi**]

   Eğer $a, b \in \mathbb{Z}^+$ ve $b \neq 1$ olacak şekilde $n = a^b$ ise n asal değildir;

2. [r **Değerinin Belirlenmesi**]

   n sayısının $\mathbb{Z}_r^*$ grubundaki mertebesini $\lg^2 n$ değerinden büyük yapan r pozitif tamsayısını bul;

   Eğer n'nin $[2, \sqrt{\varphi(r)}\lg n]$ aralığında bir asal böleni varsa n asal değildir;

3. [**Kongrüans Kontrolü**]

   $a \in [0, \sqrt{\varphi(r)}\lg n]$ oldukça {

   Eğer $(x+a)^n \not\equiv x^n + a \pmod{x^r - 1, n}$ ise n asal değildir;

   }

   n asaldır;

Algoritma Teorem 6.1.1 gereği deterministiktir. Ayrıca aşağıdaki teorem gereği polinom zamanlı olmaktadır.

Teorem 6.1.2 Verilen bir n değerinin asal olup olmadığını belirleyen AKS asallık algoritmasının karmaşıklığı $O(log^{15/2}n)$ dir (Agrawal vd. 2004). Dolayısıyla algoritma polinom zamanlıdır.

7. TARTIŞMA VE SONUÇ

Asallık testleri bir çok gelişmeden sonra deterministik ve polinom zamanlı olma özelliğine AKS testi ile ulaşmıştır. Fermat teoremi asallık testine çevrildiğinde deterministik değildir. Lucas testi özel sayılar için kullanışlı ancak karmaşıklığı polinom zamanlı değildir. Sonlu cisimlerde asallık testi ise yine polinom zamanlı bir algoritma değildir. Tez boyunca incelenen diğer algoritmalarda da benzer durumlar vardır. Son olarak 6. bölümde AKS algoritmasının bu durumların nasıl üstesinden geldiği anlatılmıştır. Teorik olarak AKS algoritması uzun yıllardır ulaşmaya çalışılan hedefe ulaşmıştır. Bunun yanında pratikte kullanılması için AKS algoritmasının karmaşıklığının düşürülmesi yönünde çalışmalar yapılmaktadır. AKS algoritmasının en çok işlem gerektiren adımı 3. adımdır. Bu nedenle r ve a değerlerinin belirlenmesinde yapılacak geliştirmeler karmaşıklığın daha küçük değerlere indirilmesini sağlayacaktır. Bazı örneklerine kaynaklardan ulaşılabilir (Pomerance ve Crandall 2005).

KAYNAKLAR

Anonymous. 2018. Web Sitesi: https://www.mersenne.org, Erişim Tarihi 15.09.2018.

Agrawal, M., Kayal, N. and Saxena, N. 2004. PRİMES is in P. Ann. of Math, 160, pp.781-793.

Brillhart, J., Lehmer, D. H. and Selfridge, J. L. 1975. New primality criteria and factorization of $2^m \pm 1$. Mathematics of Computation 29(130), 620-647.

Crandall, R. and Pomerance, C. 2005. Prime Numbers A Computational Perspective Second Edition. Springer, 170-205, New York.

Denomme, R. and Savin, G. 2008. Elliptic curve primality test for Fermat and related primes. J. Number Theory 128, 2398-2412.

Lenstra, H. 1985. Jr. Galois theory and primality testing. In orders and their applications. Lecture Notes in Mathematics vol. 1142, Springer-Verlag, 168-189.

Pomerance, C. 2010. Primality Testing: Variations on A Theme of Lucas. Congressus Numerantium, 201, 301-312.

Pomerance, C. and Konyagin, S. 1997. On primes recognizable in deterministic polynomial time. In The Mathematics of Paul Erdös, I,volume 13 of Algorithm and Combinatorics, Springer-Verlag, 176-198. New York.

Roman, S. 2006. Field Theory. Springer, 326, New York.

Shoup, V. 1992. Searching for primitive roots in finite fields. Mathematics of Computation, 58(197), 369-380.

Shanks, D. 1993. Solved and Unsolved Problems in Number Theory 4th ed. Chelsea, 61-62, New York.

Williams, H. C. 1998. Edouard Lucas and primality testing. Canadian Math. Soc. Monographs 22. New York.

ÖZGEÇMİŞ

Adı Soyadı : Süleyman Serkan ÖZÇİM

Doğum Yeri : İzmir/Konak

Doğum Tarihi : 11/08/1990

Medeni Hali : Bekar

Yabancı Dili : İngilizce

Eğitim Durumu (Kurum ve Yıl)

Lise : Gaziemir Süper Lisesi (2008)

Lisans : Dumlupınar Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümü (2012)

Yüksek Lisans : Ankara Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı (Şubat 2013-Ekim 2018)

Çalıştığı Kurum/Kurumlar ve Yıl

Kütahya Final Dershanesi (2011-2013)

Ankara Karacan Dershanesi (2014-2015)

Nazime Özlem Özel Öğretim Kurumları (2015-2018)

Nette Kurs Online Eğitim Kurumları (2018-…)