T.C.
YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ASAL SAYILAR VE DAĞILIMLARI

Metehan TURAN

YÜKSEK LISANS TEZİ
Matematik Mühendisliği Anabilim Dalı
Matematik Mühendisliği Programı

Danışman
Dr. Öğr. Üyesi Serkan ONAR

Temmuz, 2024

T.C.
YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ASAL SAYILAR VE DAĞILIMLARI

Metehan TURAN tarafından hazırlanan tez çalışması 11.07.2024 tarihinde aşağıdaki jüri tarafından Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Matematik Mühendisliği Anabilim Dalı Matematik Mühendisliği Programı **YÜKSEK LISANS TEZİ** olarak kabul edilmiştir.

Dr. Öğr. Üyesi Serkan ONAR
Yıldız Teknik Üniversitesi
Danışman

Jüri Üyeleri

Dr. Öğr. Üyesi Serkan ONAR, Danışman
Yıldız Teknik Üniversitesi _____

Prof. Dr. İbrahim EMİROĞLU, Üye
Yıldız Teknik Üniversitesi _____

Dr. Öğr. Üyesi Elif KAYA, Üye
İstanbul Sabahattin Zaim Üniversitesi _____

Danışmanım Dr. Öğr. Üyesi Serkan ONAR sorumluluğunda tarafımca hazırlanan Asal Sayılar ve Dağılımları başlıklı çalışmada veri toplama ve veri kullanımında gerekli yasal izinleri aldığımı, diğer kaynaklardan aldığım bilgileri ana metin ve referanslarda eksiksiz gösterdiğimi, araştırma verilerine ve sonuçlarına ilişkin çarpıtma ve/veya sahtecilik yapmadığımı, çalışmam süresince bilimsel araştırma ve etik ilkelerine uygun davrandığımı beyan ederim. Beyanımın aksinin ispatı halinde her türlü yasal sonucu kabul ederim.

Metehan TURAN

İmza

Sevgili Aileme,

TEŞEKKÜR

Öncelikle bu tezin teknik ve teorik detaylarının ötesinde, manevi destek ve rehberlikleriyle yanımda olan değerli danışmanım Dr. Öğr. Üyesi Serkan ONAR'a en içten teşekkürlerimi sunuyorum. Kendisinin samimiyeti, yardımseverliği ve içtenliği bu sürecin en değerli parçalarından biri olmuştur.

Bilime olan saygı ve değeri bana aşılayan annem ve babama da özel bir teşekkür borçluyum. Onların bilime verdikleri önem, bana sadece akademik bir anlayış katmakla kalmayıp, aynı zamanda yaşamın her alanında bir rehber olmuştur.

Son olarak, bu süreçte bana sonsuz sabır ve anlayış gösteren, her zaman yanımda duran ve bana inanan eşim Aybüke'ye ayrı bir teşekkür etmek istiyorum. Onun sevgisi ve motivasyonu her daim yaptığım işi anlamlı kılmıştır. Bir başarı elde ettiğimde bana gururla bakması, beni her zaman yeni başarılara teşvik etmiştir.

Metehan TURAN

İÇİNDEKİLER

SİMGE LİSTESİ

$\pi(n)$	Asal sayma fonksiyonu.
$\phi(n)$	Euler phi fonksiyonu.
O	Büyük "O" notasyonu.
o	Küçük "o" notasyonu.
$\mu(n)$	Möbius fonksiyonu.
$\zeta(s)$	Riemann zeta fonksiyonu.
li(n)	Logaritmik integral fonksiyonu.
$\Omega(n)$	n'nin kaç asal çarpanı olduğunu. verir.
$\omega(n)$	n'nin kaç farklı asal çarpanı olduğunu verir.
P_n	$\Omega(x) = n$ eşitliğini sağlayan x'lerin kümesi.
$\lfloor . \rfloor$	Basamak fonksiyonu.
$\log n$	n'nin doğal logaritması.

KISALTMA LİSTESİ

PRNG	Pseudo Random Number Generator
CSPRNG	Cryptographically Secure Pseudo Random Number Generator
LCG	Linear Congruential Generator
LSFR	Linear Feedback Shift Register
RNG	Random Number Generator
NIST	National Institute of Standarts and Technology
RH	Riemann Hipotezi

ŞEKİL LİSTESİ

ÖZET

Asal Sayılar ve Dağılımları

Metehan TURAN

Matematik Mühendisliği Anabilim Dalı
Yüksek Lisans Tezi

Danışman: Dr. Öğr. Üyesi Serkan ONAR

Bu çalışmada, asal sayıların doğal sayılar içindeki dağılımları hem teorik hem de pratik anlamda araştırılmıştır. Geniş bir literatür araştırması verilerek asal sayılarla ilgili çalışmaların geçmişten günümüze nasıl süreçlerden geçtiği incelenmiştir. Tarihsel süreçte elde edilen bu birikimin hem orijinal hem de farklı ispatları verilerek konseptin genişletilmesi hedeflenmiştir. Sonrasında keyfi aritmetik fonksiyonlar için analitik üst sınırlar bulabilen yeni bir yöntem üzerinde çalışılmış ve bu yöntem ile asal sayı teoreminin karmaşık analize girilmeden bir ispatı verilmiştir. Yine bu yöntem kullanılarak asal indisli dizi veya aritmetik seriler üzerinde nasıl yaklaşık toplam elde edilebileceğine dair bir araştırma yapılmıştır. Asal sayıların modüler uzaydaki tekdüze dağılımından yararlanılarak bir sözde rastgele sayı üreteci (PRNG) algoritması geliştirilmiştir. Her PRNG algoritması gibi, NIST SP 800-22 test süiti ile test edilerek istatistiksel anlamda başarılı olup olmadığı araştırılmıştır. Daha sonra asal sayıları, kompozit sayıların özel bir durumu olarak düşünen bir anlayışla, belirli bir büyüklükten küçük olan kompozit sayıların adedine dair analitik yaklaşımlar üzerinde çalışılmıştır. Sonrasında bu yöntem kullanılarak birçok ispatı bulunan asal sayıların sonsuzluğunun bir başka ispatı daha verilmiştir.

Anahtar Kelimeler: Asal sayılar, Sayılar kuramı, Kriptografi

YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ABSTRACT

Prime Numbers and Their Distribution

Metehan TURAN

Department of Mathematical Engineering
Master of Science Thesis

Supervisor: Dr. Öğr. Üyesi Serkan ONAR

In this study, the distribution of prime numbers among natural numbers has been investigated both theoretically and practically. A comprehensive literature review is provided to examine how studies on prime numbers have evolved from past to present. The aim is to expand the concept by presenting both original and different proofs of this accumulated knowledge throughout history. Subsequently, a new method capable of finding analytical upper bounds for arbitrary arithmetic functions has been developed, and using this method, a proof of the prime number theorem without delving into complex analysis has been presented. This method was also used to explore how approximate sums can be obtained on sequences or arithmetic series with prime indices. A pseudo-random number generator (PRNG) algorithm was developed by utilizing the uniform distribution of prime numbers in modular space. Like every PRNG algorithm, it was tested with the NIST SP 800-22 test suite to investigate its statistical success. Furthermore, analytical approaches to the number of composite numbers smaller than a certain size were studied, viewing prime numbers as a special case of composite numbers. Finally, using this method, another proof of the infinitude of prime numbers was provided, adding to the many existing proofs.

Keywords: Prime numbers, Number theory, Cryptography

YILDIZ TECHNICAL UNIVERSITY
GRADUATE SCHOOL OF SCIENCE AND ENGINEERING

1
GİRİŞ

1.1 Tezin Amacı

Bu çalışma, sayılar teorisi alanındaki Türkçe kaynak eksikliğini gidermeye ve tarihsel birikimden elde edilen ispat ve varsayımları çeşitli bakış açılarıyla zenginleştirmeye odaklanmaktadır. Bu doğrultuda, sadece tek bir konuyla sınırlı kalmayarak asal sayılar üzerine yapılan çalışmaların geneline yönelik kapsamlı bir kaynak oluşturulması hedeflenmiştir.

1.2 Tezin Hipotezi

p_i i'ninci asal sayıyı temsil etmek üzere tezin hipotezi aşağıdaki gibidir:

$\forall n, m \in \mathbb{Z}^+,\ \exists k \in \mathbb{N}$ öyle ki $(p_k, p_{k+1}, p_{k+2}, \ldots, p_{k+n-1}) \mod m$ sabit bir dizidir.

Yani her n pozitif tam sayısı için, m modülünde, ardışık asallar içerisinde, tekrar eden n uzunluğunda bir dizi vardır. Bunun daha genel versiyonu ise aşağıdaki gibidir:

$(a_i)_{i=1}^n, n$ uzunluğunda bir dizi olsun. O halde,

$$\forall n, m \in \mathbb{Z}^+,\ \exists k \in \mathbb{N} \text{ öyle ki } (p_i)_{i=k}^{k+n-1} = (a_i)_{i=1}^n \mod m$$

olur. Yani her n pozitif tam sayısı için m modülünde, ardışık asalları içerisinde, istenilen örüntüde bir dizi bulunabilir.

Bu tez çalışması, sunulan hipotezin kesin bir ispatını içermemektedir. Bu tür ispatların yıllar süren kapsamlı bir araştırma gerektirdiğini düşünüyoruz. Yine de bu varsayımlar çerçevesinde bir sözde rastgele sayı üreteci geliştirilecek ve güçlü istatistiksel yöntemlerle test edilerek hipotezin geçerliliği sorgulanacaktır.

1.3 Literatür Özeti

Bu bölümde Euclid'den günümüze asal sayılarla ilgili çalışmaların nasıl süreçlerden geçtiği yüzeysel olarak ele alınacaktır. Daha detaylı bir literatür taramasına tezin ikinci bölümünde yer verilmiştir.

Antik çağların matematiği, Euclid'in asal sayıların sonsuz olduğunu kanıtladığı çalışmalarıyla zenginleşmiştir. Bu temel teorem, matematik tarihinin en önemli buluşlarından biri olarak kabul edilir. Bu döneme ait bilinen bir diğer çalışma ise Eratosthenes'in asal sayıları ayırt etmek için geliştirdiği elektir. Ancak o dönemlere ait yazılı kaynakların sınırlı olması nedeniyle elimizde bu iki önemli çalışma dışında fazla bilgi bulunmamaktadır.

Orta Çağ'da Harezmi gibi İslam matematikçileri, cebirsel denklemler üzerine çalışmalarıyla tanınırken, asal sayılar üzerine de önemli gözlemler yapmışlardır. Bu dönem aynı zamanda Diophantus'un cebirsel denklemler üzerine yazdığı eserlerle de zenginleşmiş, bu çalışmalar sayılar teorisinin daha sonraki gelişimine önemli katkılar sağlamıştır.

Rönesans ve modern döneme gelindiğinde Fermat ve Mersenne gibi matematikçiler, asal sayılar üzerine kendi teoremlerini ortaya koyarak bu alandaki bilgi birikimini genişletmişlerdir [1]. Özellikle Fermat'ın teoremleri günümüzde halen kriptografi alanında kullanılmaktadır. Euler ise kendisinin matematikteki geniş ilgi alanları içinde asal sayılara özel bir önem vermiş ve bu sayıların özelliklerin anlaşılmasını kolaylaştırmıştır [2–4].

19. yüzyılın başlarında, Gauss, Legendre, Möbius, Chebyshev, Mertens ve Dirichlet gibi matematikçiler asal sayıların dağılımı ve özellikleri üzerine çalışmalar yaparak sayılar teorisine katkıda bulunmuşlardır. Gauss'un çalışmaları belirli bir büyüklükten küçük olan asal sayıların dağılımını anlamamıza büyük katkılar sağlamıştır [5]. Bu dönemde Dirichlet, aritmetik ilerlemelerde asal sayıların sonsuz olduğunu kanıtlayarak, asal sayılar teorisinde yeni bir dönem başlatmıştır [6]. Ayrıca Dirichlet'in çalışması bu tezin hipotezi olarak verdiğimiz varsayımın da temelini oluşturur. Möbius, toplam serileri üzerindeki ters çevirme formülü sırasında asal sayılarla yakından ilişkili olan μ fonksiyonunu bulmuştur. Möbius fonksiyonu olarak bilinen bu fonksiyon günümüzde halen ispatlarda sıkça kullanılan bir araçtır. Chebyshev, Bertrand varsayımı olarak bilinen, n ve $2n$ arasında mutlaka bir asal sayı bulunur problemini çözmüştür [7]. Bunu çözerken geliştirdiği matematiksel araçlar yine günümüzde halen araştırmacılar tarafından sıkça kullanılmaktadır. Mertens 1874 yılında birbiri ile ilişkili olan 3 teorem öne sürmüştür ki bu tez çalışmasında bunlardan biri kullanılarak Gauss'un ve

Legendre'nin öne sürdüğü asal sayı teoremi ispatlanacaktır [8].

Riemann, 19. yüzyılın ortalarında, asal sayıların dağılımı üzerine hipoteziyle bilim dünyasında büyük bir etki yaratmıştır. Riemann Hipotezi (RH) olarak bilinen bu hipotez, günümüzde halen çözülememiş bir problem olarak varlığını sürdürmektedir [9]. 20. yüzyıl matematikçileri Hardy ve Littlewood, Riemann'ın çalışmalarını temel alarak asal sayılar üzerindeki çalışmaları genişletmişlerdir [10]. 21. yüzyılda, Green ve Tao'nun aritmetik ilerlemelerde asal sayılar üzerine ortaya koyduğu sonuçlar, bu alanda önemli çalışmalardan biri olarak kabul edilir [11]. Bu teoreme göre asal sayılar dizisi üzerinde istenilen uzunlukta bir aritmetik ilerleme her zaman vardır. Green ve Tao'nun bu çalışması, tezimizde öne sürdüğümüz hipotezin zayıf bir versiyonu olarak düşünülebilir. Daha sonra Goldston, Pintz ve Yıldırım'ın yaptığı çalışma ikiz asallar varsayımınının ispatı için iyi bir adım olarak kabul edilir [12]. Yitang Zhang'ın bu çalışmayı geliştirerek ardışık asal sayılar arasındaki boşluklar üzerine yaptığı çalışmalar, bu uzun tarihsel yolculuğun en yeni meyvelerinden biridir. Zhang bu çalışmasında ardışık asallar arasındaki farkın sonsuz kez 70 milyondan küçük olabileceğini göstermiştir [13]. Maynard ise Zhang'ın çalışmalarını baz alarak yeni teknikler geliştirmiştir [14]. Bu çalışma, Polymath Project ismi verilen araştırmayla daha da geliştirilerek Zhang'ın 70 milyon olan üst sınırı 246'ya kadar düşürülmüştür [15].

Riemann'ın çalışmasından sonra, RH şartı altında birçok teorem öne sürülmüştür [16–20]. Günümüze yakın önemli çalışmalardan biri de Dudek'in 2015 yılında, Riemaan Hipotezine bağlı olarak asal sayma fonksiyonunu iyileştiren çalışmasıdır [21, 22]. RH'nin ispatlanması bütün bu varsayımları teoreme dönüştüreceğinden, bu hipotez matematik dünyasında önemli bir yere sahiptir. Bu yüzden Clay Matematik Enstitüsü tarafından bir milyon dolar ödüle layık görülmüştür. Bu tez çalışmasında RH ile ilgili çalışmalara yer vermedik. [23–25] kaynakları RH'nin tarihini, matematiksel alt yapısını ve ispatlandığında hangi sonuçların elde edilebileceğini detaylıca ele alır.

Bir sayının asal olup olmadığının test edilmesi, bilgisayar bilimlerinde ve kriptografide sıkça karşılaşılan problemlerden biridir. Bu algoritmaların çalışma süresi, kalitesiyle ters orantılı olarak kabul edilir. Bir algoritmanın girdi değerini n kabul edersek, eğer algoritmanın çalışma zamanının üst sınırları $O(n), O(n^2), O(n^k)$ şeklinde polinomlarla ifade edilebiliyorsa bunlara "polinom zamanda çalışan" veya kısaca "polinom zamanlı" algoritma denir. Eğer algoritmanın çalışma zamanı $O(e^n)$ şeklinde üstel bir fonksiyon ile sınırlanmışsa, bu algoritma "üstel zamanda çalışan" veya "polinom zamanlı olmayan" olarak adlandırılır. Stephen Cook ve Leonid Levin'in 1970'li yıllarda birbirinden

bağımsız yürüttüğü çalışmalar polinom ve üstel zamanda çözülebilen problemlerin sınıflandırılması konusunda bilgisayar bilimlerinin temel problemlerinden biri olan P vs NP probleminin temellerini oluşturmuştur [26, 27].

1976 yılında Miller, RH varsayımı altında bir sayının asal olup olmadığını test eden polinom zamanlı bir algoritma geliştirdi [20]. Daha sonra Rabin bunu RH'den bağımsız hale getirdi [28]. Ancak Rabin'in algoritması olasılıksal bir algoritmadır. Yani belirli güven aralıkları içinde doğru çalışır. Baillie–PSW algoritması da olasılıksal algoritmalara örnek olarak verilebilir [29]. Olasılıksal algoritmalar, genellikle kesinlikten ödün vererek, polinom zaman karmaşıklığında işlem yapabilme avantajına sahiptir. Deterministik algoritmalar ise kesin sonuçlar verdiklerinden genelde daha fazla algoritma adımları içerir. Ancak AKS algoritması asallık testi alanında, hem deterministik hem polinom zamanlı çalışan hem de herhangi bir hipoteze bağlı olmayan ilk algoritma olmuştur [30]. Bu algoritmaların yanında eliptik eğrilerin özelliklerini kullanan algoritmaların ilki Atkin'in 1986'da yayınladığı algoritmadır [31]. Eliptik eğri algoritmalarının karşılaştırılması için Ali Rıza'nın 2006 yılındaki çalışması incelenebilir [32].

Bir tam sayıyı asal çarpanlarına ayırma algoritmaları günümüzde halen polinom zamanda çözülememiştir. Bundan faydalanarak Rivest, Shamir ve Adleman, isimlerinin baş harfini oluşturan RSA algoritmasını geliştirerek modern şifrelemenin temellerini oluşturmuşlardır [33]. Eliptik eğri şifrelemesinin temellerini de Koblitz ve Miller oluşturmuştur [34, 35]. Bu algoritmalar günümüzde halen verileri şifreleyerek ağ trafiğinin güvenliğini sağlamaktadır.

1.4 Tanımlar, Notasyonlar ve Kavramlar

Bu bölümde, çalışmadaki ispatların daha iyi anlaşılabilmesi için bazı tanımlardan ve notasyonlardan bahsedilecektir. Bu notasyonlar için genel olarak Hardy ve Wright'ın 1938 yılında yayınladıkları ders kitabı temel alınmıştır [36].

Tanım 1.1. a, b ve c tam sayıları, $a = bc$ eşitliğini sağlıyorsa, $b|a$ ve $c|a$ yazılır. $b|a$, b a'yı kalansız böler anlamına gelir.

Tanım 1.2. a ve b tam sayıları için, $a = bc$ eşitliğini sağlayacak hiçbir c tam sayısı bulunmuyorsa, $b \nmid a$ yazılır.

Başka bir deyişle $a = b.c + r$ ifadesi ancak 0'dan farklı bir r ile sağlanabiliyorsa $b \nmid a$ yazılır. Bu, a'nın b'yi tam bölemediği anlamına gelir.

Tanım 1.3. $M \in \mathbb{R}$ ve $n \in \mathbb{R}$ olmak üzere, $|f(t)| < M.g(t)$ eşitsizliğini her

$t > n$ için sağlayan bir M pozitif tam sayısı varsa $f(t) = O(g(t))$ yazılır. "O" notasyonuna "büyük o" notasyonu denir.

O notasyonu çalışmamızda fonksiyonların üst sınırlarını belirlemek için sıkça kullanılacaktır. Aslında $f(t) = O(g(t))$ ifadesi $t \to \infty$ iken $f(t) \leq g(t)$ olarak düşünülebilir. Ancak bu karşılaştırma fonksiyonların kendisi için değil, sabit çarpanlardan arındırılmış halleri için geçerlidir.

Tanım 1.4. $f(x) \sim g(x)$ ise $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$ demektir. Burada f ile g fonksiyonları asimptotiktir denir.

Benzer şekilde bu tanım da $x \to \infty$ iken $f(x) \leq g(x)$ ve $g(x) \leq f(x)$ ifadelerinin birlikte sağlanması anlamına gelir ki bu da $f(x) = g(x)$ olmasını gerektirir. Tabii bu gerçek anlamda bir eşitlik değildir. Örneğin $f(x) = x^2 + x$ ve $g(x) = x^2$ ifadeleri arasındaki fark, x büyüdükçe büyür. Ancak oranları 1'e yaklaşır. Bu durumda $f(x) \sim g(x)$ yazılır. Ancak bu fonksiyonlar sonsuzda eşitlenmez. Bu kavrama "asimptotik eşitlik" adı verilir.

Tanım 1.5. $\Omega(n)$, n sayısının kaç asal çarpanı olduğunu ifade eder.

Örneğin $\Omega(12) = 3.2.2$ olduğundan ve burada 3 adet asal sayı olduğundan $\Omega(12) = 3$ olur. Bir n doğal sayısı $p_1^{a_1}.p_2^{a_2}...p_k^{a_k}$ şeklinde ifade edilirse $\Omega(n) = \sum a_i$ şeklinde hesaplanabilir.

Tanım 1.6. $\omega(n)$, n sayısının kaç farklı asal çarpanı olduğunu ifade eder.

Örneğin $\omega(12) = 3.2.2$ olduğundan ve burada 2 farklı asal sayı olduğundan $\omega(12) = 2$ olur. Bir n doğal sayısı $p_1^{a_1}.p_2^{a_2}...p_k^{a_k}$ şeklinde ifade edilirse $\omega(n) = k$ olur.

Tanım 1.7. $\pi(n)$, n pozitif tam sayısından küçük veya eşit, kaç adet asal sayı olduğunu simgeler.

Çalışma boyunca $\log x$ ifadesi, x'in doğal logaritmasını temsil edecektir.

1.4.1 Modüler Çarpımsal Ters

Lemma 1.1. *a ve b aralarında asal pozitif tam sayılar ise $a.x \equiv 1 \mod b$ olacak şekilde, $0 < x < b$ aralığında bir x tam sayısı vardır [37].*

İspat. $0 < x < b$ aralığında $a.x \equiv a.y \mod b$ olacak şekilde farklı x ve y tam sayıları olduğunu kabul edelim. O halde:

$$ax \equiv ay \mod b$$

$$ax = ay + bc$$

$$a(x - y) = bc$$

$$x - y = \frac{bc}{a}$$

$$x = \frac{b}{a}c + y.$$

Burada $\frac{b}{a}.c$ değerini tam sayı yapacak c değerlerini düşünürsek $a|c$ olmalıdır. Buradan da $c = a.k$ yazılabilir ($k \in \mathbb{Z}$). Bu denklemi yerine yazarsak:

$$x = b.k + y$$

olur. $k = 0$ olduğu durumda $x = y$'dir. x'in bundan sonraki en küçük değeri için $k = 1$ alınır, $x = b + y$ bulunur. O halde $0 < x < b$ aralığında $a.x \equiv a.y \mod b$ olacak şekilde farklı x ve y'ler yoktur. $a.x \equiv c \mod b$ denkliğini düşündüğümüzde, x'in bu aralıktaki farklı değerlerine karşılık c de farklı değerler alır. Güvercin yuvası ilkesine göre bu değerlerden biri 1 olmak zorundadır.

Örnek olarak 3'ün 7'ye göre modüler tersini bulmak istersek,

$$3.x \equiv 1 \mod 7$$

yazarız. Burada $x = 5$ denkliği sağlar. Ayrıca $k \in \mathbb{Z}$ olmak üzere $x = 5 + 7k$ eşitliğini sağlayan tüm x değerleri de bu denkliği sağlar. Bunlardan tümü aynı denklik sınıfında olduğundan doğru cevaptır. Ancak sadece $x = 5$ değeri $0 < x < 7$ aralığında kaldığından diğer hepsini temsilen 3'ün 7'ye göre modüler tersi olarak söylenir. ■

1.4.2 En Büyük Ortak Bölen

a ve b tam sayılarından en az biri 0'dan farklı ise, bu ikisini de tam bölen en büyük d tam sayısına a ve b'nin en büyük ortak böleni (EBOB) denir. İngilizcede $\gcd(a, b)$ olarak gösterilir.

Bununla ilgili bilinen en eski algoritma Euclid'in elementler kitabında yer alan algoritmadır. Algoritmanın temeli, bölme işlemi ve modüler aritmetik üzerine kuruludur.

Euclid'in algoritması, herhangi iki pozitif tamsayı a ve b (diyelim ki $a \geq b$) için EBOB'u ($\gcd(a, b)$) aşağıdaki adımları takip ederek bulur:

1. Eğer $b = 0$ ise, $\gcd(a, b) = a$'dır ve algoritma sonlanır.
2. Aksi takdirde, a'yı b'ye böleriz ve kalanı buluruz. $r = a \mod b$.
3. a'yı b ile ve b'yi r ile değiştiririz.
4. Adım 1'e geri dön.

Bu süreç, kalan r sıfır olduğunda sona erer. Bu noktada, b son sıfır olmayan r değeridir ve iki sayının EBOB'u olarak kabul edilir.

Örnek olarak, $\gcd(252, 198)$'i hesaplayalım:

$$\begin{aligned} 252 &\equiv 54 \mod 198 \\ 198 &\equiv 36 \mod 54 \\ 54 &\equiv 18 \mod 36 \\ 36 &\equiv 0 \mod 18. \end{aligned}$$

Bu örnekte, son sıfır olmayan kalan 18'dir. Dolayısıyla, $\gcd(252, 198) = 18$'dir.

Lemma 1.2. *Eğer a ve b'nin en büyük ortak böleni d ise, $ax + by = d$ denklemini sağlayan x ve y tam sayıları mutlaka vardır. Bu özelliğe "Bézout's lemma" denir [38].*

İspat. a ve b'nin en büyük ortak böleni d olduğuna göre, $a = d.f$ ve $b = d.g$ yazılır. Burada f ve g tam sayıları aralarında asal olmak zorundadır. Bu iki denklemi x ve y ile çarparsak;

$$a.x = d.f.x$$

$$b.y = d.g.y$$

bulunur. İki denklem taraf tarafa toplanırsa:

$$a.x + b.y = d(f.x + g.y)$$

olur. Şimdi $f.x + g.y$ ifadesi 1 olabiliyorsa ispat tamamlanmış olur:

$$f.x + g.y = 1$$

$$f.x = 1 - g.y$$

$$f.x \equiv 1 \mod g.$$

Son denklikteki x, f'nin g modunda modüler tersini ifade eder. Burada f ile g aralarında asal oldukları için Lemma 1.1'e göre böyle bir x kesinlikle vardır. Dolayısıyla $f.x + g.y = 1$ denklemini sağlayan x ve y tam sayıları mevcuttur. O halde $a.x + b.y = d$ olacak şekilde x ve y tam sayıları da vardır.

■

Tanım 1.8. a ve b tam sayıları için bu iki sayıyı ortak bölen tek pozitif tam sayı 1 ise, yani $\gcd(a, b) = 1$ ise, a ve b aralarında asaldır denir.

1.4.3 Bölünebilmenin Temel Özellikleri

$a = bc$ denklemini sağlayacak şekilde seçilen a,b ve c tam sayıları bu eşitliğin sonucu olarak aşağıdaki özellikleri sağlar. Bu kısımda yer alan ispatlar, tarafımızdan önerilen ve geliştirilen ispatlardır.

Sonuç 1.1. $\forall a \in \mathbb{Z}$ *için* $a|0$*'dır.*

İspat. Bu özellik, 0'ın her tam sayıya tam bölündüğünü söyler. Bölünebilmenin tanımını kullanırsak:

$$0 = a.c \tag{1.1}$$

olur. Eşitlik 1.1'de c tam sayısını 0 olarak seçtiğimizde $\forall a \in \mathbb{Z}$ için bu eşitlik sağlandığından bu özelliğin sağlandığını söyleyebiliriz.

■

Sonuç 1.2. $\forall a \in \mathbb{Z}$ *için* $1|a$ *ve* $a|a$*'dır.*

İspat. Yine bölünebilmenin tanımını kullanırsak:

$$a = 1.c \tag{1.2}$$

olur. Eşitlik 1.2'de a ne seçilirse seçilsin, $c = a$ olacak şekilde bir c tam sayısı seçildiğinde bu özellik de sağlanır. Benzer şekilde:

$$a = a.c \tag{1.3}$$

eşitliği incelenirse yine a ne seçilirse seçilsin $c = 1$ seçildiğinde bu eşitlik de sağlanacaktır. Dolayısıyla bu iki özellik de sağlanır. ■

Sonuç 1.3. $\forall a, b \in \mathbb{Z}$ *ve* $a|b$ *ise* $\forall c \in \mathbb{Z}$ *için* $a|b.c$ *olur.*

İspat. $c = 0$ için $a|0$ elde ederiz ki bunu zaten 1.1 ile göstermiştik. $a|b$ olduğuna göre $n \in \mathbb{Z}$ olacak şekilde $b = a.n$ denklemini sağlayan bir n tam sayısı vardır. Bu denklemin iki tarafı da 0'dan farklı bir c tam sayısı ile çarpılırsa,

$$b.c = a.n.c \tag{1.4}$$

elde edilir. Burada $n.c$ sayısını d olarak adlandırılırsa:

$$b.c = a.d \tag{1.5}$$

elde ederiz. O halde artık bölünebilme tanımına göre $a|b.c$ yazılabilir. ■

Sonuç 1.4. $\forall a, b, c \in \mathbb{Z}$ *olsun.* $a|b$ *ve* $b|c$ *ise* $a|c$ *olur.*

İspat. $a|b$ verildiğine göre $b = a.k$ yazılabilir ($k \in \mathbb{Z}$). $b|c$ verildiğine göre aynı şekilde $l \in \mathbb{Z}$ olacak şekilde $c = b.l$ yazılabilir. İkinci denklemde b yerine $a.k$ yazarsak:

$$c = a.k.l \tag{1.6}$$

olur. $k.l = d$ olacak şekilde bir d tam sayısı mutlaka var olduğuna göre $a|c$ yazılabilir. ■

Sonuç 1.5. *$\forall a, b \in \mathbb{Z}$ ve $b \neq 0$ için $a|b$ ise $|b| \geq |a|$ olur.*

İspat. $a|b$ verildiğine göre $b = a.c$ yazılabilir. $b \neq 0$ olduğundan a veya c'nin 0 olma şansları yoktur. Burada b negatif ise a veya c'den biri negatif diğeri pozitif olur. c'nin pozitif olduğu durumda, $c \geq 1$ yazılabilir. Eşitsizliğin her iki tarafını da pozitif bir sayı olan $-a$ ile çarparsak $-a.c \geq -a$ elde edilir, bu da $-b \geq -a$ olarak yazılabilir. a ve b negatif olduğundan $|a| = -a$ ve $|b| = -b$ eşitliklerini yerlerine yazarsak $|b| \geq |a|$ elde edilir.

b'nin negatif a'nın pozitif olduğu durumda c negatif olduğundan $c \leq -1$ olur. Yine eşitsizliği $-a$ ile genişletirsek $-a.c \geq a$ ve buradan yine $|b| \geq |a|$ yazılabilir.

Eğer b pozitifse a ve c negatif olabilir. Bu durumda $c \leq -1$ yazılıp a ile genişletirse $a.c \geq -a$ olur ve bu da yine $|b| \geq |a|$ olarak gösterilebilir. Son durumda bütün tam sayılar pozitifse benzer adımlarla $a.c > a$ ve buradan da $|b| \geq |a|$ elde edilir. ■

1.4.4 Asal Sayılar

Sözel olarak ifade etmek gerekirse; 1 ve kendisi olmak üzere yalnızca iki farklı pozitif böleni olan doğal sayılara asal sayı denir. Örneğin; 2,3,5,7,11 sayıları asal sayıdır. 4,6,8,9,10 sayıları ise asal sayı değildir. 20. yüzyılın önde gelen sayılar teorisi ders kitapları genel olarak aşağıdaki tanımı kullanmıştır [36, 37, 39].

Tanım 1.9. $a, p \in \mathbb{N}$ olmak üzere $D = \{a : 1 < a < p, a|p\}$ kümesinin hiç elemanı yoksa, p tam sayısına asal sayı denir. Bu tanıma göre 1 asal sayı değildir. Çünkü p'nin 1'den büyük olma şartı sağlanmamıştır.

Sonuç 1.6. *En küçük asal sayı 2'dir.*

İspat. p yerine 2 yazıldığında $D = \{a : 1 < a < 2, a|2\} =$ olur. O halde 2 asaldır. 1 asal olmadığına göre ve asal sayılar doğal sayıların alt kümesi olduğuna göre en küçük asal sayı 2'dir. ■

Aslında 2, diğer asal sayılardan farklı olarak $a|p$ şartına bakmaya gerek kalmaksızın asal oldu. Yani 2'nin asal sayı olmasının bölünebilme koşulu ile ilgisi yoktur. Sanki tanım "ilk asal sayı 2 olsun" gibi keyfi bir öneri ortaya atmış gibi duruyor. Belki de bu yüzden asal sayıları değerlendirirken 2'yi ayrı kategorize etmek gerekebilir. Belki de asal sayıları 3'ten veya n'den başlatan tanımlar genişletilmiş bir bakış açısı sunacağından konseptin anlaşılmasını kolaylaştırılabilir.

Tanım 1.10. 1'den büyük bir tam sayı asal değilse bu sayıya "bileşik" ya da "kompozit" sayı denir. Bir sayının asal ya da kompozit olduğunun belirlenmesi uygulama alanı oldukça geniş bir konudur. Literatürde birçok asallık testi algoritması bulunmaktadır. Bu algoritmaların geliştirilmesinde birçok matematikçi ve bilim insanı önemli katkılarda bulunmuştur. Antik Yunan döneminden beri asal sayılar üzerine çalışmalar yapılsa da, modern asallık testi algoritmalarının temeli Fermat, Euler ve Legendre gibi matematikçilerin çalışmalarına dayanır. 20. yüzyılda Rabin-Miller ve Solovay-Strassen gibi olasılıksal asallık testleri geliştirilmiş ve bu algoritmalar büyük asal sayıların test edilmesinde kullanılmıştır [20, 28, 40]. Bu algoritmalar bir tam sayının asal olup olmadığını belirli güven aralığı dahilinde söyler. Yani sonuçlar kesin değildir. Daha sonra 2000'lerde Agrawal-Kayal-Saxena (AKS) algoritması, asallık testinde köklü bir ilerleme sağlamış ve teorik olarak kesin sonuçlar üretebilen bir algoritma sunmuştur [30]. Bu isimler sadece birkaç örnek olup, asallık testi alanında birçok araştırmacı ve geliştirici bu algoritmaların evrimine katkı sağlamıştır. İleriki bölümlerde önerdiğimiz rastgele sayı üretecinin hızı ve kriptografik güvenliği için bu asallık testlerinin detaylı analizi gerekecektir.

Tanım 1.9 ve Tanım 1.10 incelendiğinde 1'in ne asal ne de kompozit olduğu görülür. Ancak 1'i asal sayı kabul eden birçok matematikçi vardır [41]. Genelde 1'in asal kabul edilmemesinin nedeninin aritmetiğin temel teoremini bozması olduğu düşünülür. Ancak daha iyi sebeplerimiz var. Her asal sayı, kendisinden sonra gelen katlarının kompozit olmasına neden olur. Örneğin 2 asal sayıdır ve 4,6,8,10 gibi tüm çift sayıların kompozit olmasının sebebidir. Ya da 3'ten sonra 6,9,12,15 sayıları da benzer şekilde 3'ün varlığı yüzünden kompozit olurlar. Bu yüzden 1 asal sayı olsaydı diğer bütün tam sayılar 1'in katı olacağından hepsi kompozit olurdu ki bu durumda çalışmayı burada bitirebilirdik. Yine aynı bakış açısıyla 1'in kompozit sayı olduğunu da söyleyemiyoruz çünkü her kompozit sayı en az 2 asal çarpandan oluşuyor. Ancak 1'in tek pozitif çarpanı kendisi olduğundan ve kendisi de asal olmadığından 1'i kompozit olarak da değerlendiremiyoruz. Bu yüzden modern dönemdeki asal sayı tanımlarının 1'i dışarıda bırakacak şekilde kurgulandığını söylemek yanlış olmaz.

Neredeyse Asal Kavramı

Neredeyse asal, veya ingilizce adıyla "almost prime", asal olmayan ancak asal olmaya yakın sayılar için kullanılır. k-neredeyse asal kavramı ise bir tam sayının neredeyse asal olma durumunu derecelendirir ve bunlardan oluşan küme genelde P_k ile gösterilir. Örneğin 2-neredeyse asal, $\Omega(n) = 2$ olan n tam sayılarını temsil

eder. 2-neredeyse asallar aynı zamanda yarı asal (semiprime) olarak bilinir. $\pi_k(n)$ ise n pozitif tam sayısından küçük veya eşit olan k-neredeyse asalların adedini verir. Aslında asal sayılar $k = 1$ durumunu temsil eder.

Bu bölümde asal sayılarla ilgili giriş tanımlarını yaptığımıza göre şimdi asal sayıların tarihten günümüze nasıl bir yoldan geçtiğini, hangi medeniyetlerin nasıl katkılar sağladığını, yakın tarihte asal sayılarla ilgili ne gelişmeler yaşandığını inceleyelim.

2
ASAL SAYILARIN TARİHİ

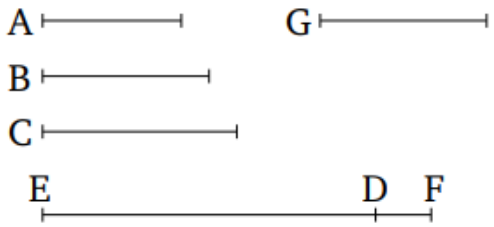
Çalışmamızda asal sayı tanımını ilk kimin veya hangi medeniyetin yaptığı ile ilgili somut bir bilgiye ulaşamadık. Zaten asal sayı tanımının bir kişi tarafından yapıldığını düşünmek yanıltıcı olabilir çünkü eski dönemlerde iletişim bugünkü kadar anlık değildi. Dolayısıyla birden fazla kişi birbirinden habersiz aynı tanımı yapmış olabilir. Yine de Antik Yunan döneminde bile asal sayılar üzerine düşünüldüğü ve bu sayılarla ilgili çalışmalar yapıldığı bilinmektedir. Ancak bu döneme ait yazılı kaynaklar sınırlı olduğundan asal sayı tanımının kim tarafından yapıldığı veya tam olarak ne zaman ortaya çıktığı konusunda kesin bir bilgi bulunmamaktadır. Bu, matematik tarihinde anonim bir mesele olarak kalmıştır.

M.Ö 300'ler civarında Euclid'in Stoikheia veya Türkçe ismi ile "Elemanlar" olarak bilinen eserinde asal sayılarla ilgili çok önemli çalışmalar yer almaktadır. Belki de birçoğunuz ilkokulda asal sayılarla tanıştıktan sonra kendine "Acaba kaç tane asal sayı var?", "Görünüşe göre asal sayılar gitgide seyreliyor, acaba bir yerde bitiyorlar mı?", "Bir yerden sonra bütün sayılar kendisinden küçük sayılara bölünüyor mu?", "Yoksa sonsuza kadar gidiyorlar mı?" gibi asal sayıların yapısı hakkında sorular sormuşsunuzdur. İşte Euclid, M.Ö 300'lü yıllarda bu soruları cevapsız bırakmamış ve asal sayıların sonsuz olduğunu ispatlamayı başarmıştır.

2.1 Asal Sayıların Sonsuzluğu ve Euclid'in İspatı

Euclid, Elemanlar adlı eserinin 9. kitabının 20. önermesinde asal sayıların sonsuz olduğunu gösteriyor. Aslında aşağıdaki ispat çoğu kaynakta bulunmasına rağmen Euclid'in orijinal ispatı değildir.

İspat. $p_1, p_2 ... p_n$ şeklinde n adet asal sayımız olsun. Eğer bu sayıları çarpıp sonuca 1 eklersek $p = p_1.p_2....p_n + 1$ elde ederiz. Bu sayı ya asaldır ya değildir. Eğer asal ise başta kabul ettiğimizden farklı bir asal sayı bulmuş oluruz ve bu yöntemle yeni asal sayılar elde edebiliriz. Eğer asal değilse o zaman bu sayının farklı asal



Şekil 2.1 Euclid'in Elemanları, Kit. 9, Önerme 20

çarpanları vardır çünkü p sayısı p_n'lerin hiçbirine tam bölünmez. O zaman asal sayıları n gibi bir sabit ile sınırlayamayız. Demek ki asal sayılar sonsuzdur. ■

Orijinal ispata gelecek olursak, Euclid'in ispatı biraz daha geometriktir. Ayrıca n adet değil 3 adet asal üzerinden yapılır.

İspat. A, B ve C asal uzunluklar olsun ve her biri ED uzunluğunu ölçebiliyor olsun (Euclid "ölçebiliyor" kelimesini "böleni olmak" anlamında kullanıyor). Ve ED uzunluğu A, B, C tarafından ölçülebilen en küçük uzunluk olsun (EKOK). Buna birim DF uzunluğu eklendiğinde artık A, B ve C uzunlukları EF uzunluğunu ölçemez. Burada EF ya asaldır ya da değildir. Eğer asal ise başta kabul ettiğimiz A, B ve C uzunluklarından daha fazla asal elde edebileceğimiz anlamına gelir. Eğer EF asal değilse o zaman G gibi bir uzunluk EF'yi ölçebilir. Burada iki ihtimal var. Acaba G uzunluğu A, B, C uzunluklarından farklı mı yoksa aynı mı? Eğer biri ile aynı ise, o zaman G hem ED uzunluğunu hem de EF uzunluğunu ölçebilir. Ancak bu mantıklı değildir. Çünkü ED'yi tam ölçüyorsa geriye bir birimlik DF uzunluğu kalır ve bunu ölçemez. O halde G uzunluğu A, B, C'den farklıdır. Bu da yine asal sayıların A, B, C ile sınırlanamayacağını gösterir. ■

Euclid'ten sonra Euler, Dirichlet, Goldbach, Erdös gibi matematikçiler de farklı ispatlar sunmuşlardır. Farklı bir bakış açıları sunduklarından hepsini değerli buluyoruz. O yüzden bu çalışmada ileriki bölümlerde bir ispat da biz sunacağız.

2.2 Aritmetiğin Temel Teoremi

Aritmetiğin temel teoreminin modern ispatını ilk olarak Gauss'un verdiği iddia edilir [42]. Bu doğrudur ancak yine Euclid döneminde bir bütün olarak olmasa bile Elements kitabının farklı önermelerinden çıkarımlarla bu teorem inşa edilebilir [43]. Bunun da dışında Kamal al-Din al-Farisi, Gauss'tan önce aritmetiğin temel teoremini inşa etmeyi başarmıştır [44].

Teorem 2.1. *Her pozitif $n > 1$ tam sayısı ya asaldır ya da asal sayıların kuvvetlerinin çarpımı olarak tek türlü yazılabilir:*

$$n = \prod_{i}^{k} p_i^{n_i}.$$

İspat. 1'den büyük n pozitif tamsayısı eğer asal ise n^1 şeklinde yazılır. Eğer asal değilse kendisinden küçük ve 1'den farklı a ve b tam sayı çarpanları vardır. Burada problem aslında iyi bir avantajla başa dönüyor:

$$1 < a \leq b < n.$$

Burada n sonlu bir tam sayı olduğundan 1 ile n arasında sonlu sayıda tam sayı vardır. Aynı çarpanlarına ayırma süreci a ve b üzerinden yürütüldüğünde 1'e doğru yaklaşan sonlu bir döngünün içerisinde olunur. Bu da n tam sayısının sonlu bir şekilde asal çarpanlara sahip olduğunu bize gösterir.

Ancak teorem bu asal çarpımın tek türlü olduğunu da söylüyor. Eğer tek türlü değilse o zaman p_i ve q_i'ler asal olmak üzere aşağıdaki eşitliğin geçerli olması gerekir:

$$p_1^{a_1}.p_2^{a_2}...p_k^{a_k} = q_1^{b_1}.q_2^{b_2}...q_l^{b_l}. \tag{2.1}$$

Burada her iki tarafı da q_1'e bölersek eşitliğin sol tarafındaki asal sayıların hiçbiri q_1 ile tam bölünmeyeceği için tam sayı olmayan bir rasyonel sayı olur. Ancak eşitliğin sağ tarafı tam sayı olarak kalır. Bu durumda böyle bir eşitliğin mümkün olamayacağı anlaşılır. Ancak belki de iki taraf da aynı asal sayılardan oluşuyor, fakat üsler farklıdır. Bu durumda da aşağıdaki eşitliği inceleriz:

$$p_1^{a_1}.p_2^{a_2}...p_k^{a_k} = p_1^{b_1}.p_2^{b_2}...p_k^{b_k}.$$

Burada da eşitliğin sağ tarafındaki tüm terimler sol tarafa atılırsa,

$$p_1^{a_1-b_1}.p_2^{a_2-b_2}...p_k^{a_k-b_k} = 1$$

elde edilir. Eşitliğin sol tarafındaki bazı $a_i - b_i$ terimleri negatif bazıları da pozitif

olabilir. Pozitif olanlara $p_i^{c_i}$' diyelim , negatif olanlara da $q_i^{-d_i}$ diyelim ve eşitliği tekrardan yazalım:

$$p_1^{c_1}.p_2^{c_2}...p_{k_0}^{c_{k_0}} = q_1^{b_1}.q_2^{b_2}...q_{k_0}^{b_{k_0}}.$$

Bu da Eşitlik 2.1 ile verilen problemin aynısıdır ve onun mümkün olmayacağını zaten göstermiştik. ■

2.3 Eratosthenes Süzgeci

Aynı dönemlerde adını mucidinden alan Eratosthenes Süzgeci [45], algoritması basit gibi görünse bile, günümüzde asal sayılarla ilgili hesaplama içeren algoritmaları hızlandırmak için kullanılıyor. Algoritma şu şekildedir: 2'den başlayarak, belirli bir N sayısına kadar olan tüm pozitif tam sayılar yazılır. En küçük henüz işaretlenmemiş sayı bulunur (ilk adımda bu 2 olur) ve asal sayı olarak işaretlenir. Bu asal sayının kendisi hariç katları (yani 4, 6, 8,...) listeden silinir. Bu silme işleminden sonra listenin başına dönüp işaretlenmemiş ilk sayı için aynı işlem tekrar edilir. Bu şekilde devam edildiğinde listede kalan sayılar asal sayılar olacaktır. Eratosthenes Süzgeci'nin standart bir uygulaması, n'den küçük asal sayılar bulunmak istendiğinde $O(n \log \log n)$ zaman karmaşıklığına sahiptir [46].

2.4 Pierre de Fermat

Antik Yunan döneminden Fermat'ya kadar, Diophantus, Harezmi gibi matematikçilerin kitaplarında asal sayılardan bahsedilmişse de bu dönemde spesifik olarak asal sayılarla ilgili çalışmaların sayısı çok azdır. Ancak Fermat ile başlayıp daha sonra Euler, Gauss ve Riemann ile devam edecek süreç, asal sayılara çok farklı bir bakış açısı kazandıracaktır. Asal sayılarla ilgili, "Fermat'nın Küçük Teoremi" olarak bilinen teoremi Fermat ortaya atmış ancak ispatlamamıştır [1].

Teorem 2.2. *p bir asal ve a, p'ye bölünemeyen bir tam sayı ise $a^{p-1} \equiv 1 \mod p$ olur. Veya başka şekilde yazacak olursak $a^p \equiv a \mod p$ olur.*

Yıllar sonra Euler, bu teoremin daha geniş bir versiyonunu yayınlayarak ispatlamıştır. Ancak henüz o kısma geçmeden burada basit bir ispat yapılabilir.

İspat. p asal olduğundan a ile aralarında asaldır. a, $2a$, $3a$ ... $(p-1)a$ sayılarını düşünelim. Yine Lemma 1.1'e göre bu sayıların p'ye bölümünden kalanlar 0 hariç

p'nin bütün kalan sınıflarını içerecektir. O halde bu sayılar çarpılırsa $a^{p-1}.(p-1)! \equiv 1 \mod p$ elde edilir. Aynı şekilde $(p-1)!$ de p'nin 0 hariç tüm kalanlarını içerdiğinden ve hepsi birbirinin modüler tersi olarak eşleşeceğinden $(p-1)! \equiv 1 \mod p$ olur. Buradan da basitçe $a^{p-1} \equiv 1 \mod p$ yazılabilir. ■

2.5 Leonhard Euler

Leonhard Euler, dünyanın gelmiş geçmiş en üretken matematikçilerinden biri olarak kabul edilir. Matematiğin bir çok alanında çalışmalar yapmıştır. Bu bölümde Euler'in sayılar teorisi ile ilgili çalışmalarına değineceğiz.

2.5.1 Eulerin Phi Fonksiyonu

İsimini yunancadaki ϕ harfinden alan bu $\phi(n)$ fonksiyonu, $1 \leq k \leq n$ aralığındaki $\gcd(k,n) = 1$ şartını sağlayan k değerlerinin adedini verir [3].

Sonuç 2.1. *Eğer n, 1'den büyük bir tam sayı ise ve asal çarpanları $p_1, p_2, ..., p_k$ şeklinde ise $\phi(n) = n.(1-\frac{1}{p_1}).(1-\frac{1}{p_2})...(1-\frac{1}{p_k})$ olur.*

İspat. Diyelim ki n'nin asal çarpanları $p_1 < p_2 < ... < p_k$ eşitsizliğini sağlasın. Ayrıca n'nin kalan sınıfları da $1, 2, ...n$ olsun. Bu durumda $n.(1-\frac{n}{p_1})$ ifadesi bu kalan sınıflarından p_1'in katı olmayanların adedini verir. Geriye kalanlardan da aynı şekilde $(1-\frac{1}{p_2})$ oranında p_2'nin katı olmayan kalan sınıfı vardır. Bu şekilde devam edildiğinde $\phi(n) = n.(1-\frac{1}{p_1}).(1-\frac{1}{p_2})...(1-\frac{1}{p_k})$ elde edilir. ■

2.5.1.1 ϕ Fonskiyonunun Özellikleri

Sonuç 2.2. *p bir asal sayı ise $\phi(p) = p-1$ olur.*

İspat. $\phi(n) = n.(1-\frac{1}{p_1}).(1-\frac{1}{p_2})...(1-\frac{1}{p_k})$ tanımını kullanırsak, p asal sayı olduğu durumda bu eşitlik $\phi(p) = p.(1-\frac{1}{p})$ şeklinde olur. Bu işlemin sonucu da $p-1$'e eşittir. ■

Sonuç 2.3. *n ve m aralarında asal tam sayılar ise, $\phi(n.m) = \phi(n).\phi(m)$ olur.*

İspat. n ve m aralarında asal ise, ortak çarpanları yoktur. O halde $n = p_1^{a_1}.p_2^{a_2}...p_k^{ak_1}$ ve $q_1^{b_1}.q_2^{b_2}...q_l^{b_l}$ olarak yazılabilir. Burada q_i ve p_i'lerin her biri farklı asal sayılardır. Yine tanımı kullanırsak:

$$\phi(n) = n.(1-\frac{1}{p_1}).(1-\frac{1}{p_2})...(1-\frac{1}{p_k})$$

$$\phi(m) = m.(1 - \frac{1}{q_1}).(1 - \frac{1}{q_2})...(1 - \frac{1}{q_l}).$$

Taraf tarafa çarparsak:

$$\phi(n).\phi(m) = m.n.(1 - \frac{1}{q_1}).(1 - \frac{1}{q_2})...(1 - \frac{1}{q_l}).(1 - \frac{1}{p_1}).(1 - \frac{1}{p_2})...(1 - \frac{1}{p_k}).$$

Sağ tarafa dikkatlice bakarsak, $m.n$ çarpımının bütün asal çarpanlarını içermektedir. Dolayısıyla $\phi(n).\phi(m) = \phi(n.m)$ olarak yazılabilir. ■

Sonuç 2.4. $\phi(p^k) = p^k - p^{k-1}$.

İspat. Tanımda yerine yazarsak, $\phi(p^k) = p^k.(1 - \frac{1}{p})$ elde edilir. Parantez dağıtılırsa $\phi(p^k) = p^k - p^{k-1}$ elde edilir. ■

Sonuç 2.5. *n pozitif tam sayısının pozitif bölenleri d_1, d_2, ... d_k ise $n = \phi(d_1) + \phi(d_2) + ... + \phi(d_k)$ olur.*

İspat. n'nin tüm pozitif kalanlarını (1,2,...,n) n'ye bölersek n adet kesir elde ederiz. Bu kesirlerin en sade hallerini düşünürsek, paydada d_1, d_2, ... d_k bölenlerinin hepsi yer alır. Bu kesirler en sade halde olduğundan pay ve paydalar aralarında asal olacaktır. Yani paydasında d_1 bulunan kesir sayısı, d_1 ile aralarında asal ve d_1'den küçük pozitif tam sayıların adedine eşittir. Bu da tanıma göre $\phi(d_1)$'dir. Benzer şekilde paydasında d_2 olan kesir sayısı $\phi(d_2)$ olur ve diğer hepsi için geçerlidir. Tüm kesir sayısı n olduğu için $n = \phi(d_1) + \phi(d_2) + ... + \phi(d_k)$ olur. ■

2.5.2 Euler Çarpımı

Euler; harmonik serilerin, indisleri asal sayılardan oluşan çarpım olarak ifade edilebileceğini göstererek sayılar teorisine önemli bir bakış açısı kazandırmıştır [4].

Teorem 2.3. $\zeta(s) = \prod_p \frac{1}{1-p^{-s}}$

Euler'in orijinal ispatı aşağıdaki gibidir.

İspat.

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \frac{1}{6^s} + \frac{1}{7^s}...$$

Her iki taraf da $\frac{1}{2^n}$ ile çarpılır:

$$\frac{1}{2^s}.\zeta(s) = \frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} + \frac{1}{8^s} + \frac{1}{10^s} + \frac{1}{12^s}...$$

Eşitliğin sağ tarafı zaten orijinal $\zeta(s)$ içinde var olan terimlerden oluşur. Yani eşitliğin her iki tarafını da $\zeta(s)$'den çıkarırsak:

$$\zeta(s) - \frac{1}{2^s}.\zeta(s) = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{9^s} + \frac{1}{11^s} + \frac{1}{13^s}...$$

$$\frac{2^s - 1}{2^s}.\zeta(s) = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{9^s} + \frac{1}{11^s} + \frac{1}{13^s}... \tag{2.2}$$

Benzer şekilde $\frac{1}{3^s}$ ile çarpılır:

$$\frac{2^s - 1}{2^s}.\frac{1}{3^s}.\zeta(s) = \frac{1}{3^s} + \frac{1}{9^s} + \frac{1}{15^s} + \frac{1}{21^s} + \frac{1}{27^s} + \frac{1}{33^s}...$$

Dikkat edilirse, bu ifadelerin hepsi 3'ün katı olup, 2'nin katı olmayan ifadelerdir. Eşitlik 2.2'den eşitliğin her iki tarafını da çıkarırsak:

$$\frac{2^s - 1}{2^s}.\frac{3^s - 1}{3^s}\zeta(s) = 1 + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{11^s} + \frac{1}{13^s} + \frac{1}{17^s} + \frac{1}{19^s}...$$

Bu şekilde devam edildiğinde sağ tarafta sadece 1 kalır. Sol tarafta ise $\frac{p^s-1}{p}$ terimlerinden oluşan çarpım kalır:

$$\prod_p \frac{p^s - 1}{p^s}\zeta(s) = 1$$

$$\zeta(s) = \prod_p (1 - \frac{1}{p^s})^{-1}$$

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}}$$

■

Aslında $\zeta(s)$, Dirichlet serilerinin özel bir durumundan ibarettir. Dirichlet serileri ise aşağıdaki gibidir:

$$\sum_{n=1}^{\infty} \frac{a(n)}{n^s}.$$

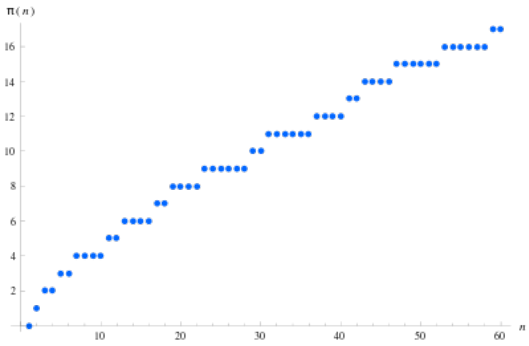
Burada eğer $a(n)$ çarpımsal bir fonksiyonsa, yani $a(m.n) = a(m).a(n)$ şeklinde yazılabiliyorsa, o zaman Euler çarpımı yine aşağıdaki şekilde geçerli olur:

$$\sum_{n=1}^{\infty} \frac{a(n)}{n^s} = \prod_{p} \frac{1}{1 - \frac{a(n)}{p^s}}.$$

Yukarıdaki son özellik Euler'in çalışması içerisinde yer almaz. Sonraki süreçte Euler'in çalışmalarının genişletilmesinin sonucu olarak ortaya çıkmıştır. Ayrıca bu seriler Dirichlet doğmadan önce de bilinen ve üzerinde çalışılan serilerdi. Bu serilerin Dirichlet serileri olarak anılması, Dirichlet'in 1837'deki çalışmasına dayanır.

2.6 Carl Friedrich Gauss ve Adrien-Marie Legendre

Euler'in bu çalışmalarının ardından asal sayıların dağılımıyla ilgili çalışmalar yapan Gauss ve Legendre, konuyla ilgilenen matematikçileri heyecanlandıracak sonuçlar elde etmiştir. Gauss ve Legendre, birbirinden bağımsız ve habersiz yürüttüğü çalışmalarda "Asal Sayma Fonksiyonu" ya da İngilizce ismiyle "Prime Counting Function" adı verilen ve bundan sonra $\pi(n)$ ile göstereceğimiz fonksiyonunu incelemiş ve analitik olarak ifade etmeye çalışmıştır. $\pi(n)$ fonksiyonu, çemberin çevresinin çapına oranı olan π sayısıyla tamamen alakasız, bir doğal sayı olan n'den küçük ve eşit olan asal sayıların adedini veren fonksiyondur.



Şekil 2.2 60'a kadar olan doğal sayılar için $\pi(n)$ fonksiyonu

Gauss, 1849 yılında Encke'ye yazdığı cevap mektubunda 1792 veya 1793 yıllarında asal sayıların yoğunluğuyla ilgilendiğini ve n'den küçük asal sayıları aşağıdaki integralle yaklaşık olarak ifade edebileceğini söyler [5].

$$\pi(n) \sim \int_0^n \frac{dt}{\log t}$$

Gauss'un bahsettiği 1792'li yıllara gittiğimizde, yaptığı çalışmalarda n'den küçük asal sayıları yaklaşık olarak $\frac{n}{\log(n)}$ olarak ifade ettiği görülüyor [47]. Rastgele dağılıyor gibi görünen asal sayıların aslında daha önce bildiğimiz iki basit fonksiyon olan n ve $\log(n)$ oranından oluşan bir eğriyi takip ettiklerini iddia eden Gauss bu isabetli öngörüsüne rağmen bu varsayımın ispatını vermemiştir. Hatta Gauss bu çalışmalarını yayınlamamıştır bile. Bu bilgileri onun el yazılarının ve mektuplaşmalarının derlemelerinden biliyoruz.

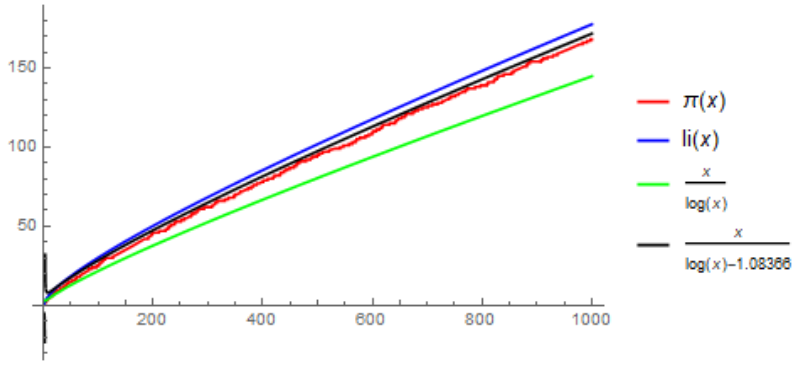
Legendre ise 1798'de yaptığı çalışmada n'den küçük asal sayıları aşağıdaki gibi ifade edebileceğini söylemiştir [48]:

$$\frac{n}{A.\log(n) + B}.$$

Daha sonra 1808'de yaptığı çalışmada buradaki A ve B sabitlerini sırasıyla 1 ve -1.08366 olarak belirledi [49]:

$$\frac{n}{\log(n) - 1.08366}.$$

Gauss, Echke'ye yazdığı mektupta Legendre'nin yaklaşımının küçük n değerleri için logaritmik integral fonksiyonundan iyi olduğunu, ancak büyüyen n değerleri için durumun tam tersine döneceğini söylüyor.



Şekil 2.3 $\pi(n)$, $\frac{n}{\log(n)}$, $\int \frac{dt}{\log(n)}$, $\frac{n}{\log(n)-1.08366}$ karşılaştırması

Gerçekten de büyük n değerleri için (yaklaşık 5 milyondan sonra) Gauss'un logaritmik integral fonksiyonunun daha yakın sonuçlar verdiği ortaya çıkmıştır [50].

Gauss ve Legendre'nin bu çalışmaları asal sayıların dağılımının anlaşılmasına büyük katkı sağlamıştır. Yine de bu yaklaşımlar onların döneminde varsayım olarak kalmıştır. Bu asimptotik yaklaşımların teoreme dönüşmesi 19. yüzyılın sonunda gerçekleşecektir.

2.7 August Ferdinand Möbius

1790-1868 yılları arasında yaşamış Alman matematikçi, sayılar teorisine "Möbius fonksiyonu", "Möbius dönüşümü", "Möbius ters çevirme formülü" konuları ile katkılar vermiştir.

2.7.1 Möbius Ters Çevirme Formülü

1832 yılında Möbius, yayınladığı makalede aritmetik fonksiyonların nasıl ters çevrileceğini gösterdi [51]. Bu ters çevirme işlemi/formülü zaman içerisinde "Möbius Inversion" olarak anıldı. Formüle geçersek, g ve f aritmetik fonksiyonlar olsun. O halde $g(n) = \sum_{d|n} f(d)$ olduğunda burada $f(n)$ de g'ye bağlı bir seri olarak ifade edilebilir:

$$f(n) = \sum_{d|n} \mu(d).g(\frac{n}{d}).$$

Burada $\mu(d)$ ise "Möbius fonksiyonu" olarak bilinir. Yani Möbius fonksiyonu bu ters çevirme işleminin ispatı sonucunda ortaya çıkmıştır.

2.7.2 Möbius Fonksiyonu

Parçalı fonksiyon olarak tanımlanmıştır. n pozitif bir tam sayı olmak üzere:

$$\mu(n) = \begin{cases} 1 & n \text{ tam kareye bölünmeyen ve çift sayıda asal çarpana sahip ise} \\ -1 & n \text{ tam kareye bölünmeyen ve tek sayıda asal çarpana sahip ise} \\ 0 & n \text{ tam kareye bölünüyorsa} \end{cases} \tag{2.3}$$

Burada "tam kareye bölünmeyen" ifadesi İngilizce literatürde "square-free" olarak geçer. Möbius fonksiyonu sayılar teorisinde oldukça kullanışlı bir fonksiyondur. Örneğin, Sonuç 2.5'de Möbius fonksiyonu kullanmadan yaptığımız ispatı şimdi Möbius ters çevirme formülünü kullanarak yapabiliriz.

İspat. n, k adet asal çarpana sahip olsun. $f(n) = \phi(d_1) + \phi(d_2) + ... + \phi(d_k)$ olduğunu varsayalım. Burada $f(n)$ fonksiyonunu bulmaya çalışıyoruz. Möbius ters çevirme formülünü kullanırsak:

$$\phi(n) = \sum_{d|n} \mu(d).f(\frac{n}{d}). \tag{2.4}$$

Aynı zamanda Tanım 2.1'e göre $\phi(n) = n.(1 - \frac{1}{p_1}).(1 - \frac{1}{p_2})...(1 - \frac{1}{p_k})$ olduğunu biliyoruz. Bu ifadeyi dağılma özelliğini kullanarak açarsak:

$$\phi(n) = n.(1 - (\frac{1}{p_1} + \frac{1}{p_2} + ... + \frac{1}{p_k}) + (\frac{1}{p_1.p_2} + \frac{1}{p_1.p_3} + \frac{1}{p_2.p_3} + ... + \frac{1}{p_{k-1}.p_k}) - ...$$

Yukarıdaki ifadeyi açıklayacak olursak, dikkat edilirse $\frac{1}{p_i}$ değerleri negatif, $\frac{1}{p_i.p_j}$ değerleri ise pozitif olmuştur. Bunun sebebi $\frac{1}{p_i}$ değerlerinin orijinal ifadede negatif durumda olmasıdır. Birbirleri ile çarpıldığında pozitife dönerler. Eğer tek sayıda $\frac{1}{p_i}$ değeri çarpım durumda olursa işareti negatif, çift sayıda olurlarsa işareti pozitif olacaktır. Bu da Möbius fonksiyonunun tanımına çok benzer. Burada n'yi dağıtırsak:

$$\phi(n) = n - (\frac{n}{p_1} + \frac{n}{p_2} + ... + \frac{n}{p_k}) + (\frac{n}{p_1.p_2} + \frac{n}{p_1.p_3} + \frac{n}{p_2.p_3} + ... + \frac{n}{p_{k-1}.p_k}) - ...$$

Şimdi n'nin bölenlerini düşünelim. Bunlardan bazıları p_i'ler olacaktır, bazıları $p_i.p_j$ şeklinde olacaktır. Bazıları ise $p_i^2.p_j$ şeklinde olabilir. Ancak yukarıdaki ifadede hiç $p_i^2.p_j$ şeklinde ifade yok. Aslında onları var olarak kabul edip çarpanlarını 0 olarak düşünebiliriz. O halde yukarıdaki ifadeyi tekrar yazacak olursak:

$$\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d}.$$

Bunu yukarıdaki Eşitlik 2.4'te belirtilen ters çevirme formülüne eşitlersek:

$$\phi(n) = \sum_{d|n} \mu(d).\frac{n}{d} = \sum_{d|n} \mu(d).f(\frac{n}{d}).$$

Buradan da $f(\frac{n}{d}) = \frac{n}{d}$ elde ederiz ki bu da f'nin sabit fonksiyon olduğu anlamına gelir. Baştaki denklemde yerine yazılırsa $f(n) = \phi(d_1) + \phi(d_2) + ... + \phi(d_k) = n$ elde edilir. ■

2.8 Peter Gustav Lejeune Dirichlet

Dirichlet, 19. yüzyıl matematiğine derinlemesine katkıda bulunmuş bir Alman matematikçidir ve sayılar teorisi alanında öncü bir figür olarak kabul edilir. Özellikle Dirichlet'in asal sayıların aritmetik ilerlemeler üzerindeki dağılımı hakkındaki teoremi, bu alanda çok önemli bir çalışmadır. Ayrıca, Dirichlet karakterleri ve Dirichlet birim teoremi gibi kavramlar, cebirsel sayılar teorisi ve analitik sayılar teorisinde önemli çalışmalar olarak kabul edilir. Bu yüzden Dirichlet'in çalışmaları sayılar teorisi ve diğer matematik alanlarında yeni araştırma yolları açmış ve onu sayılar teorisinin etkili figürlerinden biri yapmıştır.

2.8.1 Dirichlet'in Aritmetik İlerlemeler Teoremi

Bu teorem, Dirichlet'in 1837'de yayınladığı Almanca makalesinde ortaya çıkar [6]. Başlığın Türkçe'si zaten aşağıdaki teoremi birebir anlatır.

Teorem 2.4. *Aralarında asal herhangi iki a ve d pozitif tam sayıları için, $a + dn$ aritmetik ilerlemesinde sonsuz adet asal sayı bulunur.*

Örneğin, $3 + 4n$ aritmetik ilerlemesini düşünelim. $3, 7, 11, 15, 19, 23...$ diye uzayıp gider. Teorem, bu ve bunun gibi a ve d'nin aralarında asal olduğu her aritmetik ilerlemede sonsuz adet asal sayı bulabileceğimizi söyler. Aslında doğal sayılar da $1n + 0$ aritmetik ilerlemesi olarak düşünülebilir. Böyle düşünüldüğünde Dirichlet, Euclid'in sonsuz asal teoreminin, sadece doğal sayıların oluşturduğu aritmetik ilerleme için değil, a ve d'nin aralarında asal olduğu tüm aritmetik ilerlemeler için geçerli olduğunu göstermiştir.

2.9 Pafnuty Chebyshev

Chebyshev, Bertrand's postülatı olarak bilinen, $n < p < 2n$ olacak şekilde en az bir p asal sayısı olduğunu belirten varsayımı ispatlamıştır [7]. Bu süreçte $\theta(x)$ ve $\psi(x)$ olmak üzere iki fonksiyon tanımlamıştır ki bunlar ileride $\pi(x)$ fonksiyonu için alt ve üst sınırlar bulmak için matematikçiler tarafından sıkça kullanılmıştır.

$$\theta(x) = \sum_{p \leq x} \log p$$

$$\psi(x) = \sum_{n \leq x} \Lambda(n).$$

Burada Λ von Mangoldt fonksiyonu olarak bilinir ve aşağıdaki gibi tanımlanmıştır.

$$\Lambda(x) = \begin{cases} \log p & \text{eğer } k \in \mathbb{Z}^+ \text{ için } n = p^k \ (p \text{ asal}) \text{ ise} \\ 0 & \text{diğer durumlarda} \end{cases}$$

Bu fonksiyonun temel amacı, yukarıdaki Chebyshev fonksiyonları gibi asal sayıları içeren toplamları daha yönetilebilir formda ifade etmek ve asal sayılarla ilgili toplam fonksiyonlarının analitik olarak incelenmesini kolaylaştırmaktır.

2.10 Franz Mertens

Mertens, sayılar teorisi alanında üç kritik teorem geliştirdi ki bunlar genellikle Mertens üçlemesi olarak bilinir. Bu teoremler asal sayıların terslerinin toplamları ve logaritmalarının davranışları ile ilgilidir ve asal sayıların dağılımını anlamada önemli rol oynarlar [8].

2.10.1 Mertens'in Birinci Teoremi

Asal sayılar üzerinde koşan bir serinin yakınsaklığını vurgular ve aşağıdaki gibidir:

Teorem 2.5.

$$\left| \sum_{p \leq n} \frac{\log p}{p} - \log n \right| \leq 2.$$

2.10.2 Mertens'in İkinci Teoremi

Euler'in harmonik serinin asallar üzerindeki toplamının ıraksaklığını kanıtladığından önceki bölümlerde bahsetmiştik. Mertens buna daha iyi bir bakış açısı katarak bir üst sınır belirliyor.

Teorem 2.6. *M, bir sabit ve o küçük "o" notasyonu olmak üzere,*

$$\sum_{p \leq n} \frac{1}{p} - \log \log n = M + o(1)$$

eşitliği geçerlidir. $M \approx 0.2614972...$*'dir.*

Burada $n \to \infty$ iken $o(1) \to 0$ olur. Yani teorem $\sum_{p \leq n} \frac{1}{p}$ ile $\log \log n$ arasındaki farkın sonsuzda M'ye eşit olduğunu belirtir.

2.10.3 Mertens'in Üçüncü Teoremi

Bu teorem aslında ikinci teoremle yakından ilişkilidir.

Teorem 2.7. *γ Euler-Mascheroni sabiti olmak üzere,*

$$\lim_{n \to \infty} \log n \prod_{p \leq n} \left(1 - \frac{1}{p}\right) = e^{-\gamma}$$

eşitliği geçerlidir. $\gamma \approx 0.57721...$'dir

Burada $\prod_{p \leq n} \left(1 - \frac{1}{p}\right)$ ifadesi aslında n civarındaki bir tam sayının asal olma olasılığını verir. Çünkü n tam sayısının asal olabilmesi için kendisinden önceki asal sayılara bölünmemesi gerekir. Örneğin n tam sayısının 2'ye bölünmeme olasılığı $\frac{1}{2}$, 3'e bölünmeme olasılığı $\frac{2}{3}$'tür. Bunu genelleştirirsek n tam sayısının herhangi bir p asalına bölünmeme olasılığı $\frac{p-1}{p}$ veya $1 - \frac{1}{p}$ olarak ifade edilebilir. Hepsine birden bölünmeme olasılığı ise bunların çarpımıdır ki bu da bize yukarıdaki ifadeyi verir.

Mertens'in teoreminde $\log n$ terimini karşıya atarsak şunu elde ederiz:

$$\lim_{n \to \infty} \prod_{p \leq n} \left(1 - \frac{1}{p}\right) = \lim_{n \to \infty} \frac{1}{e^{\gamma} \log n}.$$

Her iki tarafın logariması alınırsa,

$$\lim_{n \to \infty} \sum_{p \leq n} \log \left(1 - \frac{1}{p}\right) = -\gamma - \log \log n.$$

olur. Burada $\log(1 - \frac{1}{p})$ ifadesini $\frac{1}{p} = 0$'da seriye açarsak,

$$\lim_{n \to \infty} -\sum_{p \leq n} \left(\frac{1}{p} + \frac{1}{2p^2} + \frac{1}{3p^3} + ...\right) = -\gamma - \log \log n.$$

Burada $\sum_{p \leq n} \left(\frac{1}{2p^2} + \frac{1}{3p^3} + ...\right)$ ifadesinin yakınsak olduğunu biliyoruz. Buna μ deyip eşitliğin sağ tarafına atarsak,

$$\lim_{n\to\infty} \sum_{p\leq n} \left(\frac{1}{p}\right) = \gamma - \mu + \log\log n$$

elde ederiz. Burada $\gamma - \mu$ ifadesi Mertens sabiti olan M'ye eşittir ve bu da Mertens'in ikinci teoremini verir.

2.11 Bernhard Riemann

Riemann'ın çalışmaları genelde kompleks analiz üzerinde yoğunlaşmıştır. Riemann'ın sayılar teorisi alanındaki tek yayınlanmış çalışması 1859 yılında yayınlanan, başlığı Türkçe'ye çevrildiğinde "Belirli bir büyüklüğün altındaki asal sayıların sayısı hakkında" anlamına gelen ve meşhur RH'nin ortaya atıldığı çalışmadır [9]. Riemann bu makalesinde, önce ζ fonksiyonun analitik devamını $\zeta(s)$ ile $\zeta(1-s)$ arasındaki ilişkiyi elde edecek şekilde yazmış ve sonra bu fonksiyon yardımıyla tıpkı Gauss gibi x'ten küçük olan asal sayıların sayısının davranışını araştırmıştır. Bunu yaparken π fonksiyonlarının toplamı şeklinde bir f fonksiyonu tanımlamıştır.

$$f(x) = \pi(x) + \frac{1}{2}\pi(x^{1/2}) + \frac{1}{3}\pi(x^{1/3}) + \frac{1}{4}\pi(x^{1/4}) + \frac{1}{5}\pi(x^{1/5}) + \frac{1}{6}\pi(x^{1/6}) + \dots$$

Riemann'ın yeni f fonksiyonu aslında asal sayıların üslerini de kısmi olarak asal kabul etmeye dayanır. Örneğin $9 = 3^2$ olduğundan yarı asal olarak kabul edilir. Ya da $27 = 3^3$ olduğundan 1/3 asal olarak kabul edilir. Riemann bu fonksiyonun analitik davranışını incelemiş ve aşağıdaki eşitliği elde etmiştir:

$$f(x) = \mathrm{li}(x) - \sum_{\alpha} \mathrm{li}(x^{1/2+\alpha i}) + \int_x^\infty \frac{dx}{x(x^2-1)\log x} + \log\zeta(0) \tag{2.5}$$

Bu eşitlikte, α değerleri $\zeta(s)$ fonksiyonunu 0 yapan reel olmayan s değerlerinin imajiner kısmıdır yani $a = \mathrm{Im}(s)$. Riemann bu s değerlerinin hepsinin reel kısmının 1/2 olduğunu varsaydığından yukarıdaki eşitlikte bunu x^s olarak göstermek yerine $x^{1/2+\alpha i}$ şeklinde göstermiştir. Riemann bu varsayımı ispatlamaya çalışmış ve birkaç başarısız denemeden sonra çalışmasının ana amacından sapmamak için hipotez olarak bırakmıştır. Bu hipotez daha sonra Riemann Hipotezi olarak anılacak ve yıllar boyu çözülememiş bir problem olarak kalacaktır.

Riemann burada Mobius ters çevirme formülünü uygulayarak $\pi(x)$ değerini f cinsinden elde ediyor.

$$\pi(x) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} f(x^{1/n})$$

$$\pi(x) = f(x) - \frac{1}{2}f(x^{1/2}) - \frac{1}{3}f(x^{1/3}) - \frac{1}{5}f(x^{1/5}) + \frac{1}{6}f(x^{1/6})...$$

Burada f yerine Eşitlik 2.5 ile verilen ifade yazılırsa,

$$\pi(x) = \text{li}(x) - \frac{1}{2}\text{li}(x^{1/2}) - \frac{1}{3}\text{li}(x^{1/3}) - \frac{1}{5}\text{li}(x^{1/5}) + \frac{1}{6}\text{li}(x^{1/6})... + o(\text{li}(x))$$

gibi bir ifade elde edilir. Bu da Riemann'ın çalışmanın sonunda elde ettiği sonuçtur. Ancak bu sonuç henüz ispatlanmamış bir hipoteze dayalıdır. Riemann'dan sonra da bu hipotezin çatısı altında birçok çalışma yapılmıştır. Eğer RH ispatlanırsa bütün bu çalışmalar teoreme dönüşeceğinden bu hipotez matematik dünyasında önemli bir yere sahiptir.

2.12 Jacques Hadamard ve Charles Jean de la Vallée Poussin

Birbirinden bağımsız olarak yürüttükleri çalışmalarda 1896 yılında $\pi(x) \sim li(x)$ ifadesini kanıtlamışlardır [52, 53]. İkisi de bunun yaparken ζ fonksiyonunun özelliklerinden ve kompleks analiz tekniklerinden yararlanmıştır. Bu ispatlar asal sayı teoreminin ilk kesin ispatları olarak kabul edilir. Bu ispatlardan sonra da birçok analitik ve elementer ispatlar sunulmuştur. Bu tez çalışmasında da Mertens'in teoremlerinden yararlanılarak asal sayı teoreminin farklı bir ispatı verilecektir.

2.13 G. H. Hardy ve John E. Littlewood

Hardy-Littlewood k-tuple varsayımları, özellikle asal sayıların dağılımındaki belirli tamsayı dizilerinin modelleri üzerine odaklanmaktadır. Bu varsayımlardan ilki, G. H. Hardy ve J. E. Littlewood tarafından 1923 yılında ortaya atılmış olup, belirli bir büyüklükten küçük asal k-tuple'ların asimptotik sıklığını ele alır.

Varsayım, pozitif çift tamsayılar olan $m_1, m_2, \ldots, m_k$ için, $p, p + m_1, p + m_2, \ldots, p + m_k$ şeklinde tanımlanan dizilerdeki sayıların herhangi bir asal sayıya göre tam kalan sınıfını oluşturmadığını ve $p, p+m_1, p+m_2, \ldots, p+m_k$ sayılarının

hepsinin asal olduğu durumları sayan $\pi_P(n)$ fonksiyonunun asimptotik davranışını ifade eder. Bu varsayıma göre, $\pi_P(n)$ fonksiyonu aşağıdaki formülle verilir:

$$\pi_P(n) \sim C_P \int_2^n \frac{dt}{(\log t)^{k+1}}.$$

Burada C_P sabiti, belirli asal sayılar üzerinden hesaplanan ve q asal sayısı için $m_1, m_2, \ldots, m_k$ sayılarının q modülü altında aldığı farklı kalan sayısına bağlı olan bir çarpım olarak ifade edilmiştir. C_P hesaplaması aşağıdaki formülle ifade edilir:

$$C_P = 2^k \prod_{q \text{ prime}, q \geq 3} \left(\frac{1 - \frac{w(q; m_1, m_2, \ldots, m_k)}{q}}{(1 - \frac{1}{q})^{k+1}} \right).$$

Burada $w(q; m_1, m_2, \ldots, m_k)$, $m_1, m_2, \ldots, m_k$ sayılarının q'ya bölündüğünde elde edilen farklı kalanların sayısını belirtir. Örneğin $P = 2$ durumu ikiz asallara karşılık gelir ve C_2 yaklaşık olarak $1.320323...$'dür. Bu varsayım, asal sayıların belirli diziler içindeki dağılımı için iyi bir araç olduğundan analitik sayılar teorisi alanında önemli bir yer tutar.

2.14 Green ve Tao

Green ve Tao'nun ana sonucu şu şekilde ifade edilmiştir [11] :

Teorem 2.8. *Asal sayılar kümesi, herhangi bir pozitif tam sayı k için, k-terimli aritmetik ilerlemeler içerir.*

Yani eğer $\mathbb{P}$ asal sayılar kümesini temsil ederse, herhangi bir $k \in \mathbb{N}$ için, $\mathbb{P}$ içinde ardışık olarak artan k adet asal sayıdan oluşan bir aritmetik dizi bulunur.

Green-Tao Teoremi, Szemerédi'nin Teoremi'nin bir genelleştirilmesi olarak görülebilir. Bu teorem herhangi bir yeterince yoğun alt kümenin, herhangi bir boyutta aritmetik ilerlemeler içereceğini söyler. Green ve Tao, asal sayılar arasında benzer düzenlilikler olduğunu göstermişlerdir.

2.15 Goldston, Pintz ve Yıldırım

Goldston, Pintz ve Yıldırım'ın çalışması, sayılar teorisinde önemli sonuçlar elde etmiştir. Asal sayı teoreminden, sayılar büyüdükçe asal sayılar arasındaki boşlukların arttığını biliyoruz. Hatta asal sayı teoremine göre n reel sayısı civarında

iki asal sayı arasındaki farkın yaklaşık olarak $\log n$ olduğunu da biliyoruz. Ancak yine de büyük n sayıları için bile ardışık iki asal sayı arasındaki farkın 2 olduğunu gözlemleyebiliyoruz. Örneğin aralarında 2 fark olan bilinen en büyük asallar $2996863034895.2^{1290000} \pm 1$ [54]. İkiz asallar varsayımı, bunun sonsuz kez tekrar edeceğini söylese de henüz kesin bir kanıta sahip değildir. Goldston, Pintz ve Yıldırım'ın çalışması ikiz asallar varsayımının zayıf bir formunu kanıtlar. p_n'nin, $n.$ asal sayıyı temsil ettiğini varsayarsak, matematiksel olarak bu teorem aşağıdaki gibi ifade edilir [12]:

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\log n} = 0. \tag{2.6}$$

Bu sonuç, $\inf p_{n+1} - p_n$ 'in sabitten küçük olduğu anlamına gelmese de $\log n$'den küçük olduğunu anlamına gelir. Yani n civarında asal sayılar arasındaki fark yaklaşık olarak $\log n$ olsa bile bu sadece beklenen değerdir. Ardışık asal sayılar arasındaki boşlukların sınırları üzerine yapılan bu ilerleme, birçok yeni araştırma konusunu da beraberinde getirdiğinden, bu çalışma sayılar teorisi alanında saygın bir çalışma olarak yer almaktadır.

2.16 Yitang Zhang

Yitang Zhang, 2013 yılında asal sayılar arasındaki boşluklar üzerine önemli bir sonuç elde etti [13]. Çalışmasında, ardışık asal sayılar arasındaki boşluğun sonsuz kez belirli bir sabit sayıdan küçük olduğunu kanıtladı.

Zhang'ın temel sonucu şu şekildedir:

Teorem 2.9. *Ardışık asal sayılar p_n ve p_{n+1} arasında sonsuz kez 70 milyondan küçük bir fark vardır. Yani,*

$$\liminf_{n\to\infty}(p_{n+1} - p_n) < 70.10^6. \tag{2.7}$$

Bu teorem, asal sayılar arasındaki boşlukların üst sınırının sabit bir sayı olduğunu ve bu boşluğun belirli bir değerden daha küçük olabileceğini gösterir. Zhang'ın bu sonucu, ikiz asal sayılar varsayımının ispatına yönelik önemli bir adım olarak kabul edilir.

Zhang'ın sonucu, sonraki araştırmalar için bir temel oluşturmuş ve asal sayı teorisinde yeni araştırma alanlarının açılmasına katkıda bulunmuştur. Bu sonuç Polymath Project gibi kolektif araştırma çabalarıyla daha da geliştirilmiş ve boşluk

246'ya kadar düşürülmüştür [55].

Elbette, asal sayılarla ilgili çalışmalar bu verilenlerle sınırlı değildir. Bu bölümde verilen çalışmalar asal sayılar hakkında dönüm noktaları olduğunu düşündüğümüz majör çalışmalardır.

3
ASAL SAYILAR ÜZERİNE ÇEŞİTLİ İNCELEMELER

Bu bölümde, önceki bölümde bahsettiğimiz çalışmalardan esinlenerek asal sayılarla ilgili kendi çalışmalarımıza ve sonuçlarımıza yer vereceğiz.

3.1 Aritmetik Fonksiyonların Analitik Temsili

Aritmetik fonksiyon tam sayılardan gerçel ya da karmaşık sayılara tanımlı fonksiyonlara denir. Yani α aritmetik fonksiyon ise, $\alpha : \mathbb{Z} \to \mathbb{C}$ olur.

Lemma 3.1. *α monoton artan aritmetik fonksiyon olsun ve β monoton azalan analitik fonksiyon olsun. O halde $\alpha(x)-\eta(x) = O(\eta'(x))$ üst sınırı için $\int \alpha(x)\beta(x)dx = \int \eta(x)\beta(x)dx$ eşitliğini sağlayan bir diferansiyellenebilir ve sürekli η fonksiyonu her zaman vardır.*

İspat. Diyelim ki $\alpha(x)\beta(x) = \lambda(x)$ ve $\eta(x)\beta(x) = \gamma(x)$. α'nın bir aritmetik fonksiyon olduğunu ve yalnızca tam sayılarda tanımlandığını biliyoruz. Ancak, analizimiz için, tanımını gerçel sayılara şu şekilde genişletiyoruz: herhangi bir gerçel sayı x için, $\alpha(x)$ şöyle tanımlanır: $\alpha(\lfloor x \rfloor)$, burada $\lfloor x \rfloor$, x'ten küçük veya ona eşit olan en büyük tam sayıyı ifade eden taban fonksiyonudur. Bu genişletme, α'nın gerçel sayılar boyunca tanımlanmasını sağlar ve yalnızca tam sayı değerlerinde sıçramalar gösterir. Zaten α'yı bu şekilde gerçel sayılara genişletmeden, $\int \lambda(x)\, dx$ integrali çok da anlamlı olmazdı.

$\gamma : \mathbb{R} \to \mathbb{R}$ fonksiyonu ve $i \in \mathbb{N}$ olmak üzere, γ_i aşağıdaki gibi sonsuz bir fonksiyon dizisi olarak tanımlansın:

$$\gamma(x) = \begin{cases} \gamma_1(x) & \text{için } x \in [a_0, a_1], \\ \gamma_2(x) & \text{için } x \in (a_1, a_2], \\ \vdots & \\ \gamma_i(x) & \text{için } x \in (a_{i-1}, a_i], \\ \vdots & \end{cases}$$

Burada aralıklar $[a_0, a_1], (a_1, a_2], \ldots, (a_{i-1}, a_i], \ldots$ artan fonksiyon α'nın sıçrama noktalarına göre belirlenir. Her γ_i kendi tanım kümesinde sürekli ve türevlenebilirdir. Uç noktalar a_i, α'nın atlama gösterdiği yerlerde, yani α'nın sürekli olmadığı noktalardan seçilir. Aynı şekilde, λ fonksiyonunu da bu şekilde temsil edebiliriz.

$$\lambda(x) = \begin{cases} \lambda_1(x) & \text{için } x \in [a_0, a_1], \\ \lambda_2(x) & \text{için } x \in (a_1, a_2], \\ \vdots & \\ \lambda_i(x) & \text{için } x \in (a_{i-1}, a_i], \\ \vdots & \end{cases}$$

γ fonksiyonunun tanımı bu şekilde belirledikten sonra tanımlı olduğu aralıkta sürekliliği ve türevlenebilirliği sağlamak belirli koşulları gerektirir. Özellikle, γ fonksiyonunun sürekli olması için, her a_i noktasında aşağıdaki gibi olması gerekir:

$$\gamma_i(a_i) = \gamma_{i+1}(a_i) = \frac{\lambda_i(a_i) + \lambda_{i+1}(a_i)}{2} = c. \tag{3.1}$$

Burada c değeri için $\lambda_i(a_i)$ ve $\lambda_{i+1}(a_i)$ noktalarının aritmetik ortasını seçtik. Aslında c değeri $\lambda_i(a_i)$ ve $\lambda_{i+1}(a_i)$ arasında herhangi bir değer olabilirdi. Ancak γ fonksiyonunun mümkün olduğunca λ'yı takip etmesini istediğimizden tam ortasından geçmesinin avantajlı olduğunu düşünüyoruz. Benzer şekilde, üst sınırı aşağıdaki gibi temsil edebiliriz:

$$\gamma_i(a_{i-1}) = \gamma_{i-1}(a_{i-1}) = \frac{\lambda_i(a_{i-1}) + \lambda_{i-1}(a_{i+1})}{2} = d. \tag{3.2}$$

Bu koşullar, α_i noktalarında, yani sıçrama noktalarında, γ fonksiyonunu sürekli hale getirir. Ayrıca, γ'nın türevlenebilirliğini garanti etmek için, bu noktalardaki

türevlerin de eşit olması gerekir, yani $\gamma_i'(a_i) = \gamma_{i+1}'(a_i)$. İşlemleri kolaylaştırmak için, bu türev değerlerini a_i noktalarında sıfır olarak belirleyebiliriz.

$$\gamma_i'(a_i) = \gamma_{i+1}'(a_i) = 0. \tag{3.3}$$

Bu seçim, eğimin tanım boyunca sürekli kalmasının yanında, türevlenebilirlik koşulunu da karşılar.

Son olarak, γ fonksiyonunu bu şekilde inşa etmenin en baştaki amacı, λ ile integrallerinin eşit olmasıydı. Yani $\int \lambda_i(x)\,dx = \int \gamma_i(x)\,dx$ eşitliği sağlanmalıdır. Kabul edelim ki $\int \gamma_i(x)dx = \Gamma_i(x)$. Böylece,

$$\Gamma_i(a_i) - \Gamma_i(a_{i-1}) = \int_{a_{i-1}}^{a_i} \lambda_i(x)dx = p \tag{3.4}$$

elde edilir. Bu dört kısıtlamayla birlikte, γ fonksiyonumuzu inşa etmeye hazırız. Eşitlik 3.3 ile verilen kısıtlamasını dikkate alarak, aşağıdaki denklemi yazabiliriz:

$$\gamma_i'(x) = c_1\,(x - a_i)\,(x - a_{i-1})\,(x - c_2)\,. \tag{3.5}$$

Burada türevlerin sıfıra eşit olduğu başka fonksiyonlar da seçilebilirdi. Seçilen fonksiyon, işlem kolaylığı sağlayan, çözüm için uygun olduğu düşündüğümüz herhangi bir fonksiyondur. Şimdi her iki tarafı da x'e göre integre edelim:

$$\gamma_i(x) = \frac{c_1}{4}x^4 - \frac{a_{i-1} + a_i + c_2}{3}x^3 + \frac{(a_{i-1} + a_i)c_2 + a_i a_{i-1}}{2}x^2 - a_i a_{i-1} c_2 x + k. \tag{3.6}$$

1. ve 2. kısıtlamaları kullanarak:

$$c = -\frac{a_{i-1}^2\left(a_{i-1}^2 + (-2a_i - 2c_2)\,a_{i-1} + 6c_2 b\right)c_1}{12} + k \tag{3.7}$$

$$d = \frac{a_i^2\left(-\frac{a_i^2}{2} + (a_{i-1} + c_2)\,b - 3c_2 a\right)c_1}{6} + k \tag{3.8}$$

3.7 ve 3.8 denklemlerini düşündüğümüzde, k ve c_2'yi bilinmeyenler olarak kabul

edersek, bu denklem sisteminin çözüm kümesi şu şekildedir:

$$c_2 = \frac{c_1 a^4 - 2c_1 a^3 a_i + 2c_1 a_i^3 a - c_1 a_i^4 + 12c - 12d}{2c_1 \left(a^3 - 3a^2 a_i + 3a_i^2 a - a_i^3\right)}, \tag{3.9}$$

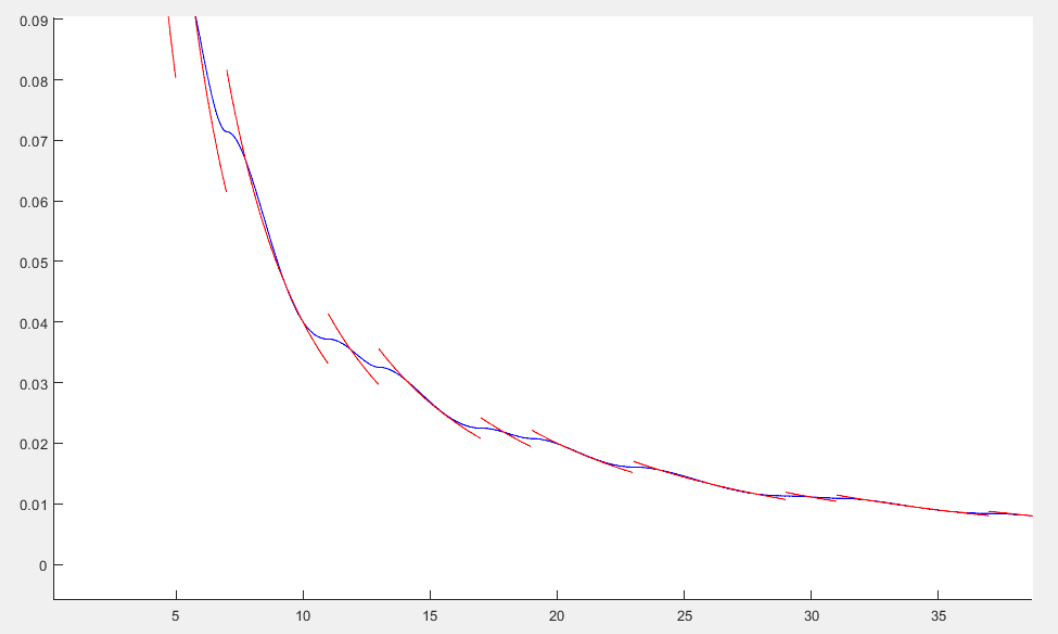
$$k = \frac{a_{i-1}^5 c_1 a_i^2 - 3a_{i-1}^4 c_1 a_i^3 + 3a_{i-1}^3 c_1 a_i^4 - a_{i-1}^2 c_1 a_i^5 + 4a_{i-1}^3 d - 12a_{i-1}^2 a_i d + 12a_{i-1}\, a_i^2 c - 4a_i^3 c}{4\left(a_{i-1}^3 - 3a_{i-1}^2 a_i + 3a_i^2 a_{i-1} - a_i^3\right)}. \tag{3.10}$$

Elde edilen denkleme 4. kısıtlamayı uyguladığımızda:

$$-\frac{\left(\left(a_{i-1} - a_i\right)^4 c_1 + 60c + 60d\right)\left(a_{i-1} - a_i\right)}{120} = p \tag{3.11}$$

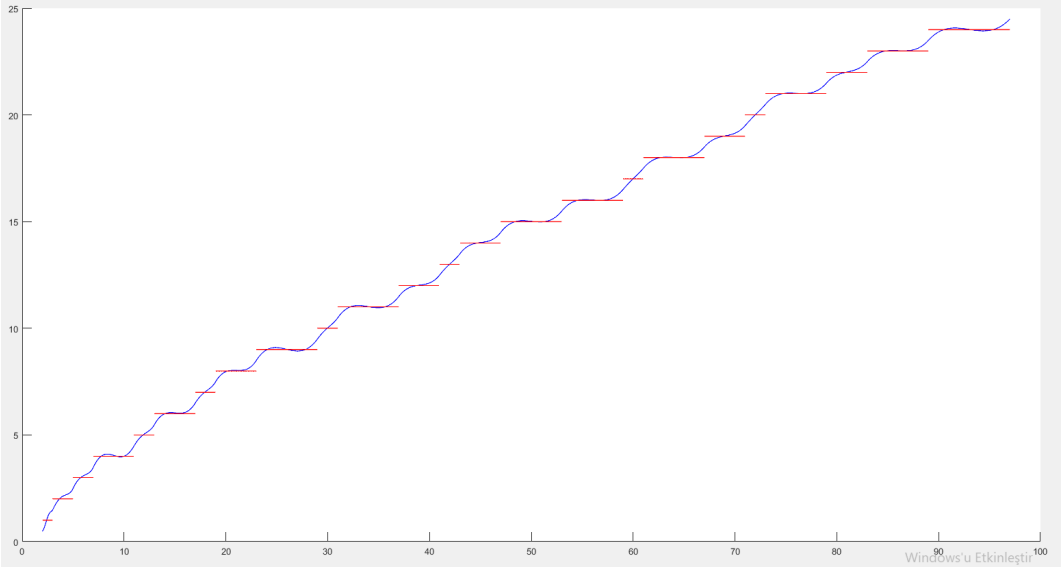
$$c_1 = \frac{60\left(\left(-c - d\right) a_{i-1} + \left(c + d\right) a_i - 2p\right)}{\left(a_{i-1} - a_i\right)^5}. \tag{3.12}$$

Şimdi tüm k, c_1 ve c_2 değerlerini biliyoruz ve bunlar dört kısıtımızı karşılıyor. Bunu takiben, artık $\gamma_i(x)$'i de biliyoruz. Böylece lemmanın ilk kısmını ispatladık. İkinci kısım için, $\alpha(x) - \eta(x) = O(\eta'(x))$ olduğunun ispatlanması gerekiyor. Ancak bu çalışmada bunun ispatını veremiyoruz. Yine de bu varsayımın aşağıdaki grafiklerle desteklendiği gözlemlenebilir.



Şekil 3.1 $\frac{\pi(x)}{x^2}$ ile asimptotik eğri

Kırmızı eğri γ fonksiyonu, mavi ise $\lambda(x) = \frac{\pi(x)}{x^2}$. Şekil 2'de başka bir örnek verilmiştir. Kırmızı çizgiler asal sayı sayma fonksiyonu $\pi(x)$'i, mavi çizgi ise bizim $\eta(x)$ yaklaşımımızı temsil eder.



Şekil 3.2 $\pi(x)$ ile asimptotik eğri

Şimdi bu Lemmayı kullanarak asal sayı teoreminin bir ispatı verilecektir.

3.2 Asal Sayı Teoreminin Bir İspatı

Asal sayı teoreminin bir çok ispatı bulunmaktadır [56–59]. Bu bölümde yeni bir ispat daha verilecektir.

Türevlenebilir bir $f(x)$ fonksiyonu için aşağıdaki ifadeyi ele alalım.

$$\sum_{p \leq n} f(p). \tag{3.13}$$

Buradaki asal sayı indislerinden oluşan seriyi doğal sayı indislerinden oluşan bir seriye çevirmek için χ_p adında bir karakteristik fonksiyon tanımlayalım:

$$\chi_p(x) = \begin{cases} 1 & \text{eğer } x \text{ asal ise,} \\ 0 & \text{değilse.} \end{cases}$$

Şimdi χ_p fonksiyonu yardımıyla 3.13 toplamının indislerini doğal sayılara çevirirsek,

$$\sum_{p\leq n} f(p) = \sum_{k\leq n} f(k).\chi_p(k)$$

elde edilir. Eşitliğin sağ tarafında Abel'in kısmi toplam formülünü uygularsak

$$\sum_{k\leq n} f(k).\chi_p(k) = \pi(n).f(n) - \int_0^n \pi(u)f'(u)du$$

bulunur. Burada Mertens'in teoremlerinden yararlanmak için $f(k)$'yı $\frac{1}{k}$ ile değiştireceğiz. Böylece,

$$\sum_{k\leq n} \frac{\chi_p(k)}{k} = \frac{\pi(n)}{n} + \int_0^n \frac{\pi(u)}{u^2}\, du$$

olur. Şimdi $\pi(n)$'nin türevlenebilir ve analitik karşılığı olan $\eta(n)$ yerleştirilir. Lemma 3.1'den hatırlayacağımız üzere integralin değeri değişmez:

$$\sum_{k\leq n} \frac{\chi_p(k)}{k} = \frac{\pi(n)}{n} + \int_0^n \frac{\eta(u)}{u^2} du.$$

Kısmi integrasyon kuralını uygulayarak, aşağıdaki eşitliği elde ederiz.

$$\sum_{k\leq n} \frac{\chi_p(k)}{k} = \frac{\pi(n)}{n} - \frac{\eta(n)}{n} + \int_0^n \frac{\eta'(u)}{u} du.$$

Lemma 3.1'in bir sonucu olarak, $\pi(n) - \eta(n) = O(\eta'(n))$ olduğunu biliyoruz. Bu nedenle, aşağıdaki eşitliği yazabiliriz:

$$\sum_{k\leq n} \frac{\chi_p(k)}{k} = O\left(\frac{\eta'(n)}{n}\right) + \int_0^n \frac{\eta'(u)}{u}\, du.$$

Eşitliğin sol tarafına Mertens'ın ikinci teoremini yerleştirirsek:

$$\log\log n + M + o(1) = O\left(\frac{\eta'(n)}{n}\right) + \int_0^n \frac{\eta'(u)}{u}\, du.$$

Şimdi n'nin sonsuza gitmesi durumunu düşünelim. Burada $o(1)$ ve $O\left(\frac{\eta'(n)}{n}\right)$

terimleri 0 olur.

$$\lim_{n\to\infty} \log\log n + M = \lim_{n\to\infty} \int \frac{\eta'(n)}{n}\, dn.$$

Her iki tarafın türevini alırsak sağ tarafa Leibniz kuralı uygulamamız gerekir. Leibniz kuralı belirli integralin türevini almak için kullanılır ve aşağıdaki gibidir.

$$\frac{d}{dn}\left(\int_{a(n)}^{b(n)} f(u,n)\, du\right) = f(b(n),n)\cdot b'(n) - f(a(n),n)\cdot a'(n) + \int_{a(n)}^{b(n)} \frac{\partial}{\partial n} f(u,n)\, du.$$

Burada $f(u,n) = \frac{\eta'(n)}{n}$, $a(n) = 0$, $b(n) = n$ olur ve yerlerine yazılırsa,

$$\frac{d}{dn}\left(\int_0^n \frac{\eta'(u)}{u}\, du\right) = \frac{\eta'(n)}{n}\cdot 1 - 0 + 0 = \frac{\eta'(n)}{n}$$

elde edilir. Bu durumda iki tarafın türevi alındığında,

$$\lim_{n\to\infty} \frac{1}{n\log n} = \lim_{n\to\infty} \frac{\eta'(n)}{n}$$

eşitliği elde edilir. Burada n'ler birbirini götürür ve aşağıdaki ifadeyi elde ederiz.

$$\frac{1}{\log n} \sim \eta'(n)$$

$$\int_0^n \frac{dx}{\log x} \sim \eta(n)$$

$$\int_0^n \frac{dx}{\log x} \sim \pi(n).$$

Bu da bize asal sayı teoremini verir.

■

3.3 Asal İndisli Dizilerde Toplama

Asal sayılarla ilgili problemlerden biri de terimleri asal sayıların fonksiyonlarından oluşan dizilerin toplamı ile ilgilidir. Örnek olarak aşağıdaki toplamı verebiliriz.

$$\sum_{p\leq n} \frac{1}{\log p} = \frac{1}{\log 2} + \frac{1}{\log 3} + \frac{1}{\log 5} + ...$$

Bu tarz toplamlar, asal sayıların dağılımları ile ilgili problemleri çözerken, araştırmacıların sıkça karşılaştıkları problemlerdir. Burada indislerimiz sadece doğal sayılardan oluşsaydı, basit integral tekniklerini kullanarak bir yaklaşım bulabilirdik. Ancak indislerimiz asal sayılardan oluştuğu için işler biraz daha karmaşık hale geliyor. Böyle durumlarda bir önceki bölümde kullandığımız Abel'in kısmi toplam formülü ve Lemma 3.1 kullanarak bir yaklaşım geliştireceğiz. Bu yaklaşımı doğrudan "yenilikçi" olarak değerlendirmek yanlış olur zira bu yaklaşımın temel fikirlerini Riemann oluşturmuştur. Stieltjes ise Riemann'ın fikirlerini geliştirerek kesikli fonksiyonların nasıl integral cinsinden sürekli hale getirileceğini göstermiştir [60]. Bizim yöntemimiz ise bir üst sınır oluşturarak daha hassas bir yaklaşım elde etmeye yöneliktir.

Sonuç 3.1. *$f(p)$ sınırlı analitik fonksiyon olmak üzere,*

$$\sum_{p\leq n} f(p) \sim \int_2^n f(t).d(\pi(t)).$$

Gerard, yukarıdaki ifadeyi 2022 yılında yaptığı bir çalışmada göstermiştir [61]. Biz bunun nasıl elde edileceğinden ve nasıl geliştirilebileceğinden bahsedeceğiz. Riemann-Stieltjes integrasyon yöntemi ile elde edilen bu sonucu daha sonra Abel kısmi toplam formülü ile ve bir önceki bölümde ispatladığımız Lemma 3.1 ile güncelleyeceğiz.

Buradaki yaklaşımımız bütün tam sayılardan sadece kompozit sayıları eleyerek asal toplamları elde etmek olacak. Bunun için her aralıkta o aralığa ait asal sayı yoğunluğunu bilmemiz önemlidir. $\pi(x)$ fonksiyonunu kullanarak bunu elde edebiliriz.

Herhangi bir r reel sayısı ve d reel mesafesi için, $(r-d, r)$ aralığındaki asal sayıları hesaplayalım. Örneğin $r = 1000$ ve $d = 10$ için 990 ve 1000 aralığındaki asalların sayısını elde edebiliriz. Bu sayıyı aradaki mesafe olan 10'a böldüğümüzde bu bölgenin asal sayı yoğunluğunu elde etmiş oluruz. $\pi(r) - \pi(r-d)$ ifadesi bize $(r-d, r)$ arasındaki asal sayıları verir. Bunu d mesafesine bölersek $\frac{\pi(r)-\pi(r-d)}{d}$ elde

ederiz ki bu da r civarında ve d genişliğindeki asal sayı yoğunluğunu ifade eder. Burada d sayısını 0'a götürerek bu yaklaşımı daha iyi hale getirebiliriz.

$$\lim_{d\to 0} \frac{\pi(r) - \pi(r-d)}{d}$$

Bu da aslında türevin tanımıdır ve bu değerin eşiti $\frac{d(\pi(r))}{dr}$'dir.

Elde edilen bu ifade r civarındaki asal yoğunluğunu temsil etmektedir. Örneğin 2 ile 10 arasındaki sayıların yaklaşık olarak yarısı asaldır. Yani bu ifadenin değeri bu civarlarda yaklaşık olarak $\frac{1}{2}$ olacaktır. Ancak daha büyük sayılar için aynı şeyi denediğimizde bu değerin azaldığını görürüz. O halde her bir sayıyı kendi asal yoğunluğu ile çarparak sadece asal toplamlar için bir yaklaşım elde edebiliriz. Bu da bizi aşağıdaki integrale götürür.

$$\sum_{p\leq n} f(p) \sim \int_2^n f(t).d(\pi(t)). \tag{3.14}$$

Bu tam bir ispat sayılmaz. Hatta bu tanım eksik sayılır. Çünkü $\pi(t)$ aritmetik olduğundan diferansiyellenebilir değildir. Şimdi gerçek bir ispatı Abel'in kısmi toplam formülü ve Lemma 3.1 ile verdiğimiz lemma yardımıyla yapacağız.

İspat. $\sum_{p\leq n} f(p)$ ifadesini Abel'in kısmi toplam formülü ile açacak olursak:

$$\sum_{k=0}^{n} \chi_p(k).f(k) = \pi(n).f(n) - \int_0^n \pi(u).f'(u)du.$$

Burada Lemma 3.1 kullanılarak eşitliğin sağ tarafındaki integralde, $\pi(u)$ yerine $\eta(u)$ yazılabilir.

$$\sum_{k=0}^{n} \chi_p(k).f(k) = \pi(n).f(n) - \int_0^n \eta(u).f'(u)du.$$

Şimdi kısmi integrasyon kuralı uygulanırsa:

$$\sum_{k=0}^{n} \chi_p(k).f(k) = \pi(n).f(n) - \left(\eta(n).f(n) - \eta(0).f(0) - \int_0^n \eta'(u).f(u)du\right)$$

elde edilir. $\eta(0).f(0)$ sabit olduğundan bunu N olarak ifade edersek,

$$\sum_{k=0}^{n} \chi_p(k).f(k) = f(n).(\pi(n) - \eta(n)) + \int_0^n \eta'(u).f(u)du + N.$$

Burada $\pi(n) \sim \eta(n)$ olduğundan $\lim_{n\to\infty} \pi(n) - \eta(n) = o(\eta(n))$ olur. O halde tüm ifadede n'nin sonsuza gittiği durumu düşünürsek:

$$\lim_{n\to\infty} \sum_{p\leq n} f(p) = \lim_{n\to\infty} \left(f(n).(\pi(n) - \eta(n)) + \int_0^n \eta'(u).f(u)dn + N \right)$$

$$\lim_{n\to\infty} \sum_{p\leq n} f(p) = f(n).o(\eta(n)) + \lim_{n\to\infty} \left(\int_0^n \eta'(u).f(u)du \right).$$

f'nin azalan olduğu durumlarda $n \to \infty$ için $f \to 0$ olacağından,

$$\sum_{p\leq n} f(p) \sim \int_0^n \eta'(u).f(u)du$$

yazılabilir.

■

elde edilir ve böylece ispat tamamlanır. Burada η fonksiyonu π fonksiyonunun asimptotik karşılığı olduğundan $\eta'(n)$ yerine asal sayı teoreminden elde edilen $\eta'(n) \sim \frac{1}{\log n}$ yazıldığında yaklaşık hesaplamalarla asal indisler üzerinden toplamlar elde edilebilir.

$$\sum_{p\leq n} f(p) \sim \int_0^n \frac{f(u)}{\log u} dn. \tag{3.15}$$

Asal sayılar 2'den başladığı için alt sınır 2 ile değiştirilebilir. Bu asimptotikliği bozmayacaktır. Şimdi 3.15 ile verilen ifadeyi kullanarak 1'den 10000'e kadar olan asal sayıları toplayacağımız bir örnek yapalım.

$$\sum_{p\leq 10000} p = 2 + 3 + 5 + 7 + ... + 9973 = 5736396. \tag{3.16}$$

Eşitlik 3.16 ile bulunan sonuç sayıların gerçek toplamıydı. Şimdi asimptotik yaklaşım ile bulmak için 3.15 özelliğini kullanırsak,

$$\sum_{p \leq 10000} p \sim \int_{2}^{10000} \frac{x}{\log x} dx$$

$$2 + 3 + 5 + 7 + ... + 9973 \approx 5762206.407538401$$

elde edilir. Bu şekilde örnekler çoğaltılabilir. Burada seçilecek olan η fonksiyonu bu yaklaşımın hassasiyetini belirleyecektir. Örneğin 2.3 ile verilen grafikte asal sayma fonksiyonunu yaklaşık olarak temsil eden fonksiyonları karşılaştırmıştık. Toplamın yapılacağı aralık için π fonksiyonunu en iyi temsil eden η fonksiyonu, en iyi yaklaşımı verecektir. Yani $\sum |\pi - \eta|$, o aralık için minimize edilmelidir.

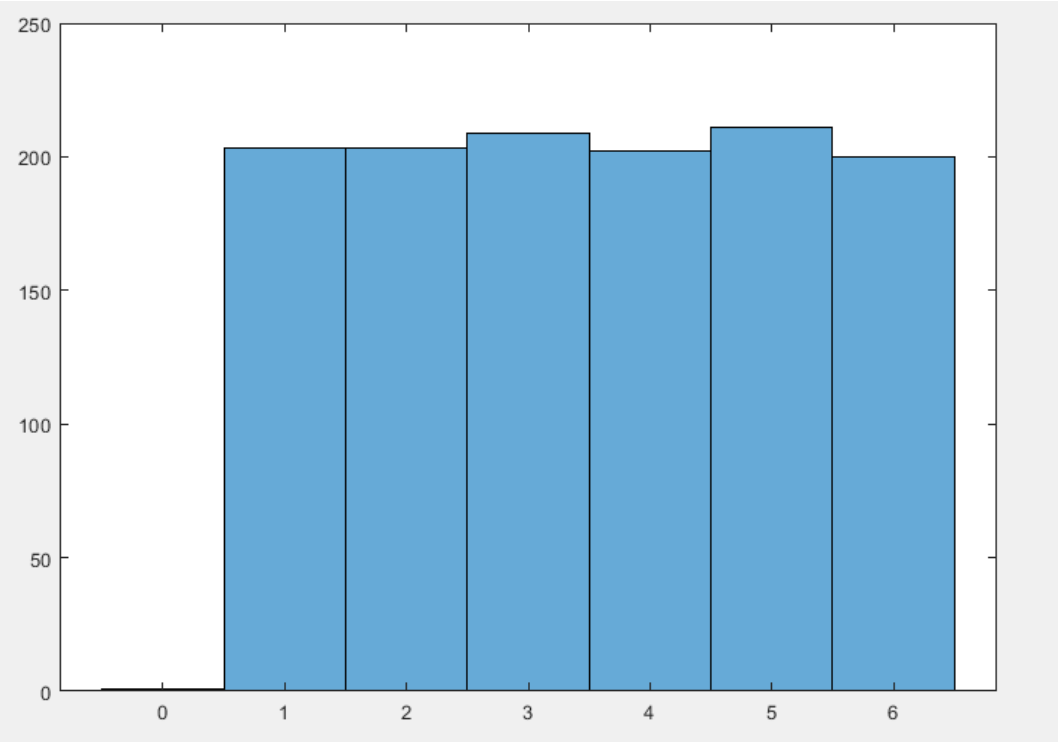
3.4 Asal sayılar ile PRNG algoritması

Tekdüze dağılım, olasılık teorisinde ve istatistikte önemli bir yere sahiptir. Bir aralıkta bulunan tüm değerlerin eşit olasılıkta gerçekleştiğini belirtir. Önceki bölümlerde Dirichlet'in asal sayıların aritmetik ilerlemeler hakkındaki teoreminden bahsetmiştik. Bu teorem aslında şu varsayımı da beraberinde getirir:

Sonuç 3.2. *n'den küçük asal sayıların bir a pozitif tam sayısına bölümünden kalan d tam sayıları tekdüze dağılım gösterir.*

Bu varsayım Vallée Poussin tarafından 1896 yılında teoreme dönüşmüştür [53].

Şekil 3.3 ile verilen histogram 10000'den küçük asal sayıların 7 ile bölümünden kalanların kaç kere tekrar ettiğini göstermektedir.



Şekil 3.3 10000'e kadar olan asal sayıların 7 modunda tekrar sayısı

Histogramda 10000'den küçük 1229 asal sayının 6 farklı kalan sınıfına yaklaşık olarak eşit dağıldığını ve her bir kalanın yaklaşık olarak 205 kere tekrar ettiğini gözlemleriz. Sayılar büyüdüğünde bu durum daha da belirgin hale gelmektedir.

Bu durum, asal sayıların $an + d$ formunda ortaya çıkışının rastgele olduğunu, istatistiksel yöntemlerle bir sonraki asal sayının hangi formda olacağının bir tahminini yapmanın anlamsız olduğuna işaret eder. Herhangi bir N doğal sayısına kadar ortaya çıkan $an+d$ formundaki asalların aslında sonrakileri etkilemediğini de gösterir. Örneğin yeterince büyük bir n'den sonra üst üste gelen 10 asal sayının 6'ya bölümünden kalanların 1 olması, sıradaki asal sayının 6'ya bölümünden kalanın 5 olma olasılığını artırmaz. Çünkü tekdüze dağılımın doğası bunu gerektirir. Bu, üst üste 5 kız doğuran bir annenin sıradaki çocuğunun erkek olma olasılığını etkilememesine benzetilebilir.

Bu bölümde, bu durumun avantaja çevrilerek kriptografide nasıl kullanılacağından bahsedilecektir.

Asal sayılar modüler bir uzayda gösterildiğinde, tekdüze olarak dağılmış gibi görünürler. Herhangi bir modüler tabanda asal sayıların bu sahte tekdüze dağılımı, sahte rastgele dizilerin oluşturulması için ilgi çekici bir potansiyel sunar. Bu tür diziler, simülasyonlar, kriptografik protokoller ve öngörülemez sonuçların kritik

olduğu algoritmalar için hayati önem taşır.

Bu asal sayıların sahte rastgele özelliğini kullanarak, yeni bir PRNG algoritması oluşturma yaklaşımını öneriyoruz. Yöntemimiz, asal sayıların modüler aritmetik özelliklerine dayanıyor. Bu sayede üretilen sözde rastgele sayıların tekdüzelik kriterini sağlamasını amaçlıyoruz. Bu, herhangi bir PRNG'nin etkinliğini değerlendirmek için anahtar bir metrik olan istatistiksel rastgeleliğe ulaşmak için kritik öneme sahiptir.

Yöntemimize geçmeden önce PRNG algoritmalarından ve türlerinden bahsetmekte fayda var. PRNG (Pseudo-Random Number Generator) sözde rastgele sayı üretecidir. Burada "sözde" kelimesi üretecin gerçekten rastgele sayılar üretmediğini, belirli bir algoritmayı takip ederek rastgele görünen sayılar ürettiğini betimler. Örneğin π sayısının basamakları, konuyla ilgili bilgisi olmayan birine gösterildiğinde aralarında bir ilişki bulamayacaktır. Ancak oradaki bütün rakamlar bir serinin 10 tabanında kalanlarını takip etmektedir. Bu yüzden gerçekten rastgele değillerdir ve bu sahte rastgeleliğe "pseudo" yani "sözde" rastgelelik denir.

Literatüdeki PRNG algoritmalarını temel olarak ikiye ayırmak mümkün: LCG (linear congruential generator) ve LFSR (linear feedback shift register). LCG algoritmalarının genel formu aşağıdaki gibidir.

$$x_{n+1} = ax_n + b \mod m.$$

Lineer bir denklemin m modunda kongrüansı olduğundan bunlara "Lineer kongrüansiyel üreteç" denir. Bilinen en iyi örneklerden biri Blum Blum Shub sahte rastgele sayı üreticisidir ([62]). Bu algoritma, güvenliğini iki büyük asal sayının çarpımına dayandırır ve böylece faktörizasyona dayalı saldırılara karşı dayanıklıdır. Ancak, bazen döngülere girebilmesi, kriptografik uygulamalarda kullanımında potansiyel bir dezavantaj oluşturmaktadır. Başka bir örnek olarak Lehmer rastgele sayı üreticini verebiliriz ([63]). Bu algoritma da rastgeleliği artırmak için asal bir modül kullanır. Basitliği ve asal sayıların özelliklerine dayanması, bizim önerdiğimiz PRNG yaklaşımı ile uyumludur. Ancak, bilinen bir dezavantajı, özellikle modül dikkatlice seçilmediğinde ürettiği dizilerin kısa periyotlara sahip olabilmesi ve bu durumun güçlü rastgelelik gerektiren uygulamalardaki etkinliğini zayıflatabilmesidir. Daha sonra Thomson ve Rotenberg, Lehmer üreticisini geliştirdiler [64, 65]. Aslında birçok LCG algoritması Lehmer algoritmasının türevlerini içerir.

Diğer bir tür ise LFSR algoritmalarıdır. Bu algoritmalar da genel olarak bit kaydırma ve bit işlem operatörlerini kullanarak karmaşıklık yaratmayı hedefler. Genel formu aşağıdaki gibidir.

$$x_{n+1} = x_n \oplus x_{n-k}.$$

Burada $\oplus$ xor operatörüdür.

Bunların birlikte kullanımı ise hibrit algoritmalar olarak adlandırılır. Avaroğlu ve arkadaşlarının 2014 yılında yaptığı çalışma hibrit algoritmalara örnek olarak gösterilebilir [66].

Önerdiğimiz algoritma LCG tarafına biraz daha yakın durmaktadır. Çünkü bu algoritmanın lineerliği, tam sayılar üzerinde olmaktan çok asal sayılar dizisi üzerindedir. Bunun yanında algoritmamız bir LCG algoritması ile birleştirildiği için hibrit olarak da kabul edilebilir.

3.4.1 Algoritma akışı

Bu bölümde önerdiğimiz PRNG algoritmasının akışını detaylı inceleyeceğiz.

Keyfi olarak seçilen doğrusal olmayan bir fonksiyon f için, doğrusal olmayan bir kongrüansal üretecin standart biçimi aşağıdaki gibi tanımlanır:

$$x_n = f(x_{n-1}) \mod m.$$

Algoritmamızda fonksiyon f aşağıdaki gibi tanımlanmıştır:

$$f(x_n) = \lfloor c_n \cdot x_n \rfloor_p.$$

Burada, c_n bir tam sayı dizisidir ve $\lfloor k \rfloor_p$ notasyonu, k'den küçük veya eşit olan en büyük asal sayıyı temsil eder, yani:

$$\lfloor k \rfloor_p = \max\{q \leq k \mid q \text{ asal sayıdır}\}.$$

c_n dizisi için güçlü bir periyoda sahip herhangi bir LCG kullanılabilir:

$$c_n = (a \cdot c_{n-1} + b) \mod m.$$

Böylece, önerilen sahte rastgele sayı üreteci nihayetinde şu şekilde olur:

$$x_n = \lfloor c_{n-1} \cdot x_{n-1} \rfloor_p \mod p$$
$$c_n = (a \cdot c_{n-1} + b) \mod m.$$

Burada, x_0 başlangıç değeri olarak belirlenir. Sayı p herhangi bir asal sayı olabilir, ancak rastgele bit üretimi isteniyorsa, $2^n + 1$ biçiminde seçilmesi önerilir. Diğer üreteçlerin aksine, $\lfloor c_{n-1} \cdot x_{n-1} \rfloor_p$ değeri garantili olarak asal sayı olacak ve hiçbir zaman p'ye tam olarak bölünmeyecektir. Sonuç olarak, $\lfloor c_{n-1} \cdot x_{n-1} \rfloor_p \bmod p$ işlemi, $[1, p-1]$ aralığında tam sayılar verir ve bu aralıkta $p-1$ adet tam sayı vardır. Bu nedenle, $p = 2^n + 1$ seçilirse, $p - 1 = 2^n$ olur ve bu ikili sisteme rahatça dönüştürülebilir.

Algorithm 1 Sözde Rastgele Sayı Üreteci

1: **Girdi:** x_0 başlangıç değeri, a, b, m sabitler , p asal sayı.
2: **Çıktı:** x_n rastgele sayı dizisi.
3: c_0 herhangi bir değer olarak belirle.
4: $x \leftarrow x_0$
5: $c \leftarrow c_0$
6: **while** true **do**
7: $\quad c \leftarrow (a \cdot c + b) \mod m$ ▷ c_n değerini günvelle
8: $\quad x \leftarrow \lfloor c \cdot x \rfloor_p \mod p$ ▷ Yeni x_n değerini oluştur
9: $\quad$ Çıktı x
10: **end while**

Bu algoritmanın güvenilirliği ve rastgeleliği, asal sayıların doğal sayılar içerisindeki öngörülemez karmaşıklığına dayanmaktadır. Her ne kadar bir sonraki veya önceki asal sayıyı bulmak için algoritmalar bulunsa da, kesin bir analitik fonksiyon mevcut değildir. Dolayısıyla oluşturulan sayılardan başlangıç değerini türetmeye çalışan bir saldırganın başvurabileceği tek yöntem kaba kuvvet algoritmalarını kullanmaktır.

Herhangi bir sahte rastgele sayı üreticisi (PRNG) algoritmasında olduğu gibi, başlangıç değerlerini, x_0 ve modül p'yi belirlemek çok önemlidir. Daha önce de belirtildiği gibi, p'nin $2^n + 1$ formunda seçilmesi rastgele bitler üretmek için önemlidir. Ancak, algoritma yalnızca belirli bir aralıkta rastgele sayılar üretmek için kullanılacaksa, p herhangi bir asal sayı olarak seçilebilir. Rastgele sayıların üretilmesi için p'nin asal olması gerekmediğini unutmamak önemlidir. Örneğin, $p = 6$ olarak seçilirse, üretilen sayılar sadece 1 ve 5 olur ve bunlar kolayca [0,1]

tam sayı aralığına eşlenebilir. p'nin asal olarak seçilmesi ise bu eşleme sürecinden bizi kurtarır ve algoritmanın daha hızlı çalışmasını sağlar.

Ayrıca, a, b ve m değerlerinin uzun periyotlu LCG oluşturacak şekilde seçilmesi gerekmektedir. Bunun için daha önce deneyimlenmiş özel sayılar kullanılabilir. Örneğin, $a = 1664525$, $b = 1013904223$ ve $m = 2^{32}$ olarak seçilebilir [67].

3.4.2 Algortimanın Test Edilmesi

Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), sahte rastgele sayı üreticilerinin rastgeleliğini değerlendirmek için özel olarak tasarlanmış kapsamlı bir istatistiksel testler dizisi sunmaktadır. Bu testler, üretilen dizilerin istatistiksel özelliklerini değerlendirmek için yaygın bir ölçüt olarak kabul edilmektedir ve kriptografik uygulamalar ile yüksek düzeyde rastgelelik gerektiren diğer alanlarda kullanılan PRNG'lerin doğrulanması için çok önemlidir.

NIST test dizisi, rastgeleliğin farklı yönlerini hedefleyen çeşitli testler içermektedir; bunlar arasında bitlerin frekansı, desenlerin dağılımı, korelasyonların varlığı ve matematiksel dönüşümlere verilen yanıt gibi unsurlar bulunmaktadır. PRNG'mizin çıktı dizilerini bu testlerden geçirerek, performansını bu boyutlar genelinde titizlikle değerlendiriyor ve hassas uygulamalar için zafiyet oluşturup oluşturmadığını araştırıyoruz.

Testlerin tanıtımını ve uygulanmasını takiben, NIST test dizisinden elde edilen sonuçları sunacak ve tartışacağız. Bu sonuçlar, önerilen PRNG algoritmasının bu standart testlerdeki performansına dayanarak güçlü ve potansiyel zayıf yönlerinin ayrıntılı bir analizini sağlayacaktır.

Algoritma, $x_0 = 42$, $p = 65537$, $a = 1664525$, $b = 1013904223$ ve $m = 2^{32}$ değerleri seçilerek 50.000 döngü için çalıştırıldı. Oluşturulan rastgele bitler, NIST SP 800-22 kullanılarak test edildi ve aşağıdaki tabloda gösterilen sonuçlar elde edildi.

P-VALUE	PROPORTION	STATISTICAL TEST
0.350485	12/12	Frequency
0.534146	12/12	BlockFrequency
0.122325	12/12	CumulativeSums
0.911413	12/12	CumulativeSums
0.911413	12/12	Runs
0.066882	12/12	LongestRun

P-VALUE	PROPORTION	STATISTICAL TEST
0.213309	12/12	Rank
0.213309	12/12	FFT
0.534146	12/12	NonOverlappingTemplate
0.213309	12/12	ApproximateEntropy
0.213309	12/12	LinearComplexity

Sonuçlar, algoritmanın istatistiksel karmaşıklığının yeterli olduğunu göstermektedir. Burada, p-değerinin 0.01'in üzerinde olması testin başarılı olduğu anlamına gelir. Testin başarıyla sonuçlanması PRNG'nin %99 güven düzeyinde gerçek rastgeleliğe yakın olduğunu gösterir. Ancak %1 olasılıkla test, kusursuz ve rastgeleliğe çok yakın bir PRNG'nin gerçekten rastgele olmadığını belirtebilir. Bu nedenle bu istatistiksel testlerde ortaya çıkabilecek anomaliler iyi analiz edilmelidir. Örneğin, 100 testten 1'inde p-değeri 0.01'in altında olabilir ve bu durum normal kabul edilmelidir. Bu durumda, PRNG başarılı olarak değerlendirilecektir.

Ancak bir PRNG algoritmasının kriptografik anlamda güvenli olması için (CSPRNG) istatistiksel testler yeterli değildir. Bitlerin bir kısmından yola çıkılarak x_0 ve p değerleri elde edilebilirse PRNG algoritması kriptografik anlamda güvenli sayılmaz. Tam da bu yüzden, bu karmaşıklığı artırabilmek için bunu güvenli sayılan bir LCG algoritması ile birleştirdik. Böylece algoritmanın hangi asal sayıya denk geleceği daha öngörülemez hale gelir. Bir PRNG algoritmasının CSPRNG olabilmesi için başka bir kriter ise algoritmanın çalışma zamanının herhangi bir anında, algoritmanın iç durumu (yani bizim örneğimizde x ve c değerleri) bir şekilde ele geçilirse bile, sonraki ve önceki bitler tekrardan oluşturulamamalıdır. Bizim PRNG algoritmamız bu kriteri sağlamamaktadır. Bunun sağlanması için dış kaynaklardan rastgele sayılarla algoritmanın iç durumu sürekli olarak güncellenmelidir. Burada Avaroğlu ve arkadaşlarının 2015 yılında yaptığı çalışma yol gösterici olacaktır [68].

Bu algoritmanın temel fonksiyonu $\lfloor . \rfloor_p$ fonksiyonudur. Burada herhangi bir n tam sayısından önceki ilk asal sayıyı hesaplamak n büyüdükçe yüksek maliyetli zaman karmaşıklığına yol açabilir. O nedenle burada AKS algoritması [30] gibi deterministik asallık testi algoritmaları yerine Miller-Rabin asallık testleri gibi olasılıksal testlere yönelmek avantajlı olacaktır [20, 28]. Sarıkaya'nın yaptığı 2019 yılındaki çalışma, implementasyon sırasında hangi testin kullanılacağına dair ışık tutabilecek bir çalışmadır [69].

Şunu da belirtmek gerekir ki, Miller-Rabin asallık testi, algoritmasının bir bölümünde asallık testi için rastgele sayı adayları seçer. Bu adaylar verilen sayının asallığını kontrol eden inputlar olarak düşünülebilir. Burada PRNG algoritmamızın deterministik yapısının bozulmaması için oradaki rastgele sayı seçiminde de deterministik bir algoritma kullanılmalıdır. Örneğin *millerrabin*(n) fonksiyonu n asal olsa bile algoritmanın çalışma prensibi gereğince bazı denemelerde n'yi kompozit olarak gösterebilir. Bu da PRNG'nin aynı girdilere karşı farklı çıktılar üretmesine neden olabilir.

3.5 Kompozit Sayıların Dağılımı

Aritmetiğin temel teoremine göre her pozitif tam sayının, asal sayılar ve onların üslerinin çarpımı şeklinde benzersiz bir biçimde yazılabildiğini biliyoruz.

$$m = p_1^{a_1} p_2^{a_2} ... p_n^{a_n}, m \in \mathbb{Z}^+.$$

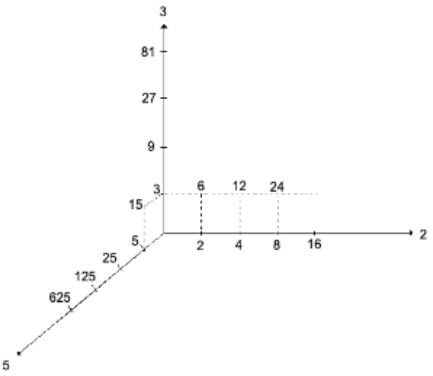
Burada p_n, n'inci asal sayıyı temsil etmektedir. Aslında sonsuz adet asal sayı olduğundan n sonsuza gider. O halde pozitif bir tam sayıyı sadece a_n'lerin bir fonksiyonu olarak göstermek yanlış olmaz.

$$m = m(a_1, a_2, a_3, ..., a_k, ...)$$

Örneğin tüm $a_n = 0$ için $m = 1$ olur. Ya da $a_1 = 1$ ve diğer a_n 'ler 0 ise $m = 2$ olur. Bu şekilde farklı a_n değerleri için m ve $\mathbb{Z}^+$ arasında birebir ve örten bir fonksiyon yazılabildiğine göre, eksenleri asal sayılar ve üslerinden oluşan sonsuz boyutlu bir koordinat sistemine tüm pozitif tam sayıları yerleştirebiliriz. Örneğin sadece 3 boyuttan oluşan bir örnek Şekil 3.4 ile verilmiştir.

Burada, pozitif tam sayıları bu koordinat sistemindeki pozisyonlarına göre gruplara ayıracağız. Bu gruplamada asal sayılar aslında sadece bu gruplardan biri olacaktır. Bu ayrım, asal sayılarla ilgili daha önce yapılmış çalışmalarla elde edilen birikimi de desteklemektedir. Bu gruplar, önceki bölümlerde bahsettiğimiz P_n kümesi ile karıştırılmamalıdır. Çünkü P_n kümesinin elemanları $\Omega(x) = n$ eşitliğini sağlayan x'lerden oluştur. Biz ise tam sayıları Ω notasyonuna göre değil, ω notasyonuna göre gruplara ayıracağız.

Geometride nokta boyutsuz olarak kabul edilir. Bu sistemde bütün asal eksenlerin kesiştiği tek nokta 1'dir. Bu yüzden 1 tek başına bir kategoride yer alacaktır. 1'in



Şekil 3.4 Asal sayı koordinat sistemi

ne asal ne de kompozit olması, onun bütün sayılardan ayrı bir kategoride yer alması gerektiğini de doğruluyor. Diğer bir kategori eksenlerin üzerindeki sayılardır. Bu sayılar, asal sayılar ve üslerinden oluşur. Bu yüzden asal sayılar ve üslerini de aynı kategoride ele alacağız.

Sonuç 3.3. *Eğer asal sayıların üslerini de asal kabul edersek ve asal sayma fonksiyonunu $\pi'(x)$ olarak değiştirecek olursak yine asimptotiklik bozulmayacaktır. $\pi(x) \sim \pi'(x)$ olur.*

İspat. Öncelikle aşağıdaki eşitlik ile başlayalım.

$$\pi'(x) = \pi(x) + \pi(\sqrt{x}) + \pi(\sqrt[3]{x}) + \pi(\sqrt[4]{x})...$$

Eğer $x \to \infty$ için $\sum_{n=2}^{\infty} \pi(x^{1/n}) = o(\pi(x))$ olduğunu gösterebilirsek ispat tamamlanacaktır. Burada her bir $\pi(x^{1/n})$ terimi yerine, asimptotik karşılığı olan $\frac{x^{1/n}}{\log x^{1/n}}$ yazılarak aşağıdaki ifade elde edilir.

$$\pi'(x) \sim \frac{x}{\log x} + \frac{2.\sqrt{x}}{\log x} + \frac{3.\sqrt[3]{x}}{\log x} + \frac{4.\sqrt[4]{x}}{\log x}...$$

Şimdi $A = \frac{2.\sqrt{x}}{\log x} + \frac{3.\sqrt[3]{x}}{\log x} + \frac{4.\sqrt[4]{x}}{\log x}...$ gibi bir kabul yapalım. Burada her terimin yerine daha büyük bir terim yazarak ifadeyi büyüteceğiz. Ancak öncelikle bu terimleri aşağıdaki gibi gruplara ayıralım.

$$A = \sum_{k=2}^{3} \frac{k.\sqrt[k]{x}}{\log x} + \sum_{k=4}^{7} \frac{k.\sqrt[k]{x}}{\log x} + \sum_{k=8}^{15} \frac{k.\sqrt[k]{x}}{\log x} + \sum_{k=16}^{31} \frac{k.\sqrt[k]{x}}{\log x} + ...$$

$$A = \sum_{j=1}^{\infty} \sum_{k=2^j}^{2^{j+1}-1} \frac{k.\sqrt[k]{x}}{\log x}$$

Yukarıdaki ifadede iç içe iki tane toplam sembolü var. İçteki toplam sembolünde $2^j \leq k$ eşitsizliği geçerlidir. Eğer $\frac{k.\sqrt[k]{x}}{\log x}$ ifadesinin yerine $\frac{2^j.\sqrt[2^j]{x}}{\log x}$ yazarsak, kökün derecesi küçüldüğünden, x sonsuza giderken bu ifade büyür. O zaman aşağıdaki eşitsizliği yazabiliriz.

$$A < \sum_{j=1}^{\infty} \sum_{k=2^j}^{2^{j+1}-1} \frac{2^j.\sqrt[2^j]{x}}{\log x}$$

Artık içteki toplamda k değişkeni olmadığından sabit olarak düşünüp toplayabiliriz.

$$A < \sum_{j=1}^{\infty} \frac{2^{2j}.\sqrt[2^j]{x}}{\log x}$$

Biliyoruz ki x sonsuza giderken aritmetik ortası geometrik ortasından büyük olur, yani $x/n > \sqrt[n]{x}$ olur. Bunu kullanarak,

$$A < \sum_{j=1}^{\infty} \frac{2^{2j}.\sqrt[2^j]{x}}{\log x} < \sum_{j=1}^{\infty} \frac{x}{2^j.\log x}$$

En sağdaki seri, geometrik seridir ve değeri $\frac{x}{\log x}$'e eşittir.

$$A < \sum_{j=1}^{\infty} \frac{2^{2j}.\sqrt[2^j]{x}}{\log x} < \frac{x}{\log x}$$

$$\frac{2.\sqrt{x}}{\log x} + \frac{3.\sqrt[3]{x}}{\log x} + \frac{4.\sqrt[4]{x}}{\log x} ... < \frac{x}{\log x}$$

$$\pi(\sqrt{x}) + \pi(\sqrt[3]{x}) + \pi(\sqrt[4]{x}) ... < \pi(x)$$

Böylece ispat tamamlanır. Yani $\pi'(x) \sim \pi(x)$ olur. ■

Bu ispatla birlikte aslında göstermek istediğimiz şey asal sayılar ile onların üslerini

aynı kategoride değerlendirmemizin asal sayı teoremini bozmadığıdır.

Şimdiye kadar nokta üzerinde yer alan (yani 1), eksenler üzerinde yer alan (asal sayılar ve üsleri) tam sayıları inceledik. Şimdi ise düzlemde yer alan (bundan sonra iki boyutlu tam sayı olarak adlandıracağız) tam sayıları inceleyeceğiz.

İki boyutlu kompozit sayılar, iki farklı asal çarpana sahip olan sayılardır. Yani sembolik olarak gösterecek olursak $\omega(n) = 2$ eşitliğini sağlayan n tam sayılarıdır. Örneğin sıraya göre 2 boyutlu kompozit sayılar şöyledir: 6, 10, 12, 14, 15, 18, 20, 21 ...

Bu sayılardan bazılarının çarpanları 2 ve 3, bazılarının 2 ve 5 bazılarının 3 ve 7 olabilir ve bu şekilde sonsuz farklı kombinasyon vardır. Biz çarpanları sadece p_1 ve p_2 asal sayılarından oluşan n doğal sayısına kadar olan iki boyutlu kompozit sayıların fonksiyonunu $\pi_{p_1,p_2}(n)$ olarak gösterelim. Aşağıdaki teoremde, bu fonksiyonun analitik davranışı incelenmiştir.

Teorem 3.1. *Asal çarpanlarının kümesi $\{p_1, p_2\}$ olan n'den küçük tam sayıların adedi $\pi_{p_1,p_2}(n)$ olsun. O halde aşağıdaki asimptotik ifade geçerlidir.*

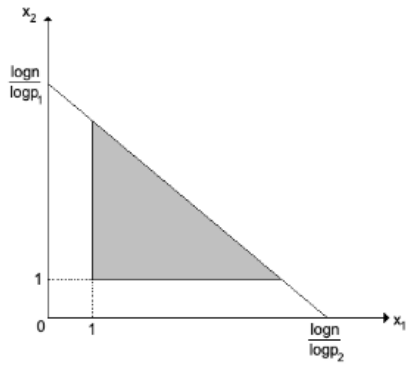
$$\pi_{p_1,p_2}(n) \sim \frac{\log^2 n - (\log n)(\log p_1 + \log p_2)}{2.\log p_1.\log p_2}. \tag{3.17}$$

İspat. İki boyutlu kompozit sayılar $p_1^{x_1}.p_2^{x_2}$ formundadır. $p_1^{x_1}.p_2^{x_2} < n$ olması istendiğine göre her iki tarafında logaritması alınırsa,

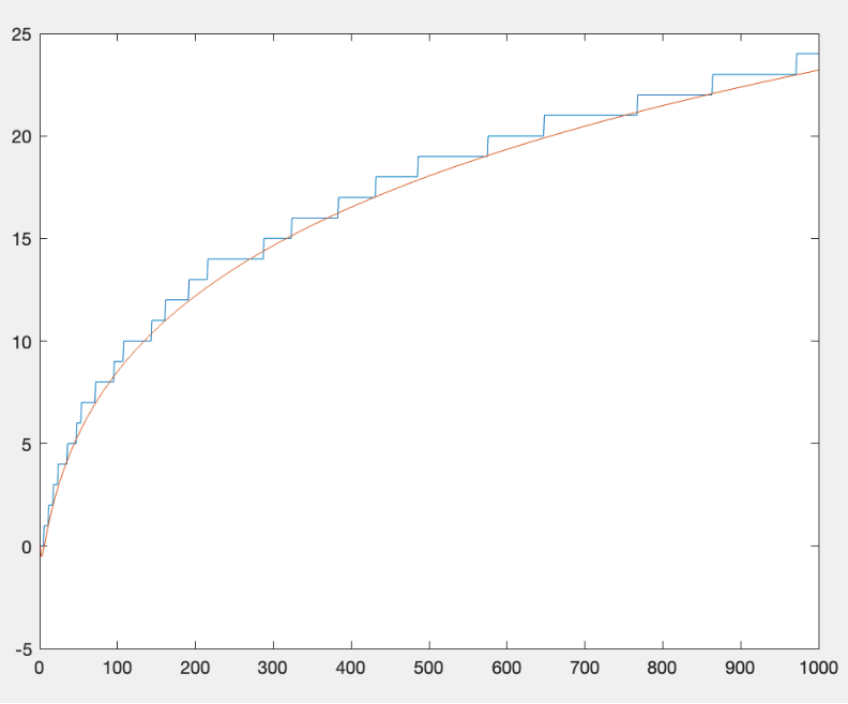
$$x_1.\log p_1 + x_2.\log p_2 < \log n.$$

Bu eşitsizliği sağlayan kaç farklı (x_1, x_2) tam sayı ikilisinin olacağı bize $\pi_{p_1,p_2}(n)$ değerini verecektir. Eksenleri x_1 ve x_2 olan koordinat düzleminde yukarıdaki eşitsizliği gösterirsek Şekil 3.5'i elde ederiz ve buradaki taralı alan da $\frac{\log^2 n-(\log n)(\log p_1+\log p_2)}{2.\log p_1.\log p_2}$ değerine sahiptir. x_1 ve x_2 değerlerinden biri 0 olduğu durumda iki boyutluluk bozulacağından alan hesabı $1 \leq x_1$ ve $1 \leq x_2$ değerleri için yapılmıştır. ■

Bu yaklaşıma göre $\pi_{2,3}(1000)$ için gerçek değer ve yaklaşık değer karşılaştırması Şekil 3.6 ile verilmiştir.



Şekil 3.5 n'den küçük 2 boyutlu asal kuvvletlerin bölgesi



Şekil 3.6 çarpanları 2 ve 3 olan 1000'den küçük sayılar ve yaklaşık değer karşılaştırması

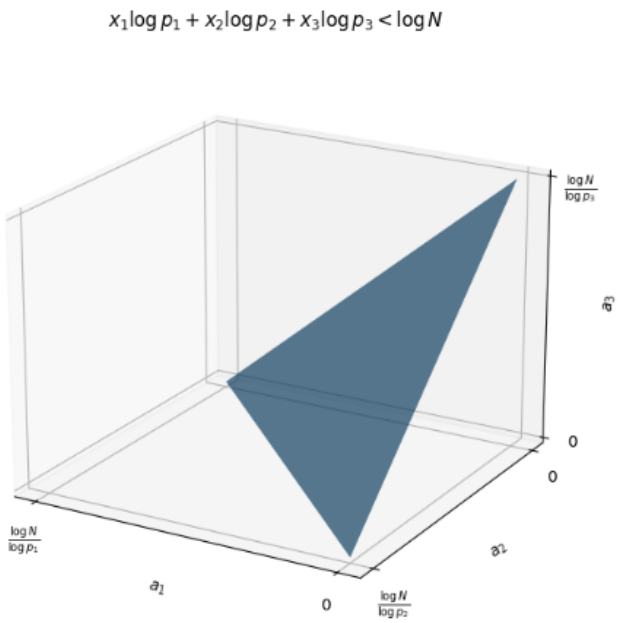
Bunu genelleştirecek olursak, $\pi_{p_i}(n)$, n'den küçük, asal çarpanları p_i'ler olan ($i = 1, 2, 3...k$) tam sayıların adedini veren fonksiyon olsun.

Sonuç 3.4.

$$\pi_{p_1,p_2,...p_k}(n) \sim \frac{1}{k!}\prod_{i=1}^{k}\left(\lfloor\frac{\log n}{\log p_i}\rfloor + 2\right).$$

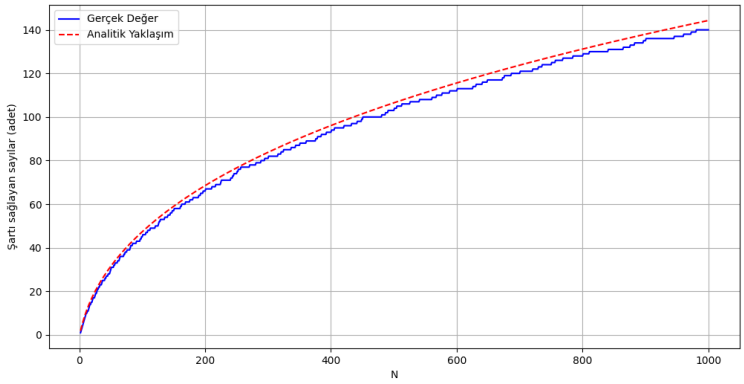
Şekil 3.5 düşünülürse, burada sadece boyut sayısı artacağından cismin eksenleri kestiği noktaların çarpımı cismin hacmini verir. Yani her bir eksende $\lfloor\frac{\log n}{\log p_i}\rfloor + 2$ tam sayı olduğundan, hacim hesabı gereği bunların çarpımının $k!$ değerine oranı

hata payları ile beraber yaklaşık olarak eşitsizliği sağlayan tam sayı değerlerini verecektir.



Şekil 3.7 $a_1 \log p_1 + a_2 \log p_2 + a_3 \log p_3 = \log N$ grafiği

Ancak daha iyi alt ve üst sınırlar belirlemek hata payını azaltır ve bu varsayımı güçlendirebilir. Bu tezde bunun teorik ispatı verilmedi fakat bilgisayar üzerinde hesaplanıp sonuçlar Şekil 3.7 ile verilerek bunun güçlü bir varsayım olduğunu gösterilmiştir.



Şekil 3.8 Asal çarpanları 2,3,5 veya 7 olan N'den küçük kompozit sayıların adedi ve analitik karşılaştırması

Bu yöntemin daha büyük boyutlar için analizini bu tezde çalışmadık. Bu yöntemin geliştirilmesinin önündeki engel, boyut arttıkça hata teriminin de üstel olarak büyümesidir. O yüzden bu çalışma geliştirilirken sınırlar olabildiğince

daratılmalıdır. Bu çalışmanın asıl hedefi, asal sayıları tek başına incelemek yerine, bütün pozitif tam sayıları olabildiğince kategorilere ayırıp asal sayma fonksiyonundaki hata paylarını azaltmaktır.

3.6 Asal Sayıların Sonsuzluğunun Bir İspatı

Asal sayıların sonsuzluğuna dair literatürde birçok ispat bulunmaktadır. Önceki bölümlerde Euclid'in ispatı verilmişti. Euler ise $\sum_p \frac{1}{p}$ serisinin ıraksaklığını göstererek farklı bir ispatta bulunmuştur [2]. Kummer'ın cebirsel ve Furstenberg'in topolojik ispatları da farklı çalışmalar olarak incelenmeye değerdir [70, 71].

Bizim ispatımız bir önceki bölümde paylaştığımız hipoteze dayalı olduğundan kesin bir ispat olarak kabul edilemez. Ancak hipotez ispatlanırsa veya yöntem hipotezden bağımsız olarak güncellenirse kesin ispat haline getirilebilir.

İspata geçersek, k adet asal sayımız olsaydı ve p_1, p_2 . . .p_k olsaydı, bunlarla yazılabilecek tam sayılar, a_i'ler doğal sayılar olmak üzere, $p_1^{a_1}$, $p_2^{a_2}$ . . . $p_k^{a_k}$ şeklide olurdu ve bunların tüm pozitif tam sayıları örtmesi beklenirdi. Bir N doğal sayısını üst sınır olarak kabul edersek;

$$p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \ldots \cdot p_k^{a_k} < N.$$

Bu sınırlı sayıdaki asalların N'den küçük tüm doğal sayıları örtmesi gerektiğinden, yukarıdaki eşitsizliği sağlayan $(a_1, a_2, \ldots, a_k)$ şeklinde N adet vektör olması gerekir. O halde her iki tarafın da doğal logaritması alınırsa,

$$a_1 \log(p_1) + a_2 \log(p_2) + a_k \log(p_k) < \log(N)$$

olur. Bu basit lineer eşitsizlikte $a_1, a_2, a_3, \ldots, a_k$ değerleri eşitsizliğin değişkenleri, $\log(p_1), \log(p_2), \ldots, \log(p_k)$ değerleri ise katsayılarıdır. Burada $\frac{\log(N)}{\log(p_i)}$ değerleri a_i'lerin alabileceği maksimum değerlerdir. Örneğin $a_1 = \frac{\log N}{\log p_1}$ ve $a_2, a_3, a_4 ... = 0$ seçildiğinde eşitsizlik sağlanmaz. Her bir değişkenin alabileceği maksimum tam sayı değerleri ise $\lfloor \frac{\log(N)}{\log(p_i)} \rfloor$ olur. Yani bir a_i değişkeni bu eşitsizliğin sağlanabilmesi için $0, 1, 2, 3, .. \lfloor \frac{\log(N)}{\log(p_i)} \rfloor$ olmak üzere $\lfloor \frac{\log(N)}{\log(p_i)} \rfloor + 1$ değer alabilir ki bu da $\lceil \frac{\log(N)}{\log(p_i)} \rceil$ anlamına gelir. Bunu $\frac{\log(N)}{\log(p_i)} + O(1)$ şeklinde ifade edebiliriz. Sonuç 3.4 ile verilen hipotezimizi kullanırsak,

$$\frac{1}{k!}\prod_{i=1}^{k}\left(\frac{\log N}{\log p_i}+O(1)\right)>N.$$

Eşitsizliğin sol tarafının en hızlı büyüyen terimi $\log^k N$'dir. Bu durumda sol taraf $O(\log^k N)$ şeklinde yazılabilir.

$$O(\log^k N)>N.$$

O notasyonu tanımı gereği bu eşitsizlik, pozitif bir reel sayı M ve reel bir n_0 alındığında, tüm $N>n_0$ değerleri için,

$$M\cdot\log^k N>N$$

olduğunu ifade eder. Eşitsizlikte yine her iki tarafın logaritması alınırsa,

$$\log M+k\cdot\log\log N>\log N$$

elde edilir. Elde edilen eşitsizlikte ifade düzenlenirse,

$$k>\frac{\log N-\log M}{\log\log N}.$$

Burada $N\to\infty$ için $\frac{\log N-\log M}{\log\log N}\to\infty$ olduğundan $k\to\infty$ olur ki bu da asal sayıların sınırlı sayıda olmadığını gösterir.

4
SONUÇLAR

Bu tez çalışması, sayılar teorisi alanındaki Türkçe kaynak eksikliğini göz önünde bulundurarak, bu alandaki önemli bir boşluğu doldurmayı amaçlamıştır. Çalışmada, sadece tek bir konuyu incelemekle sınırlı kalınmayıp, asal sayılarla ilgili daha kapsamlı konular üzerinde durularak geniş bir literatür taraması gerçekleştirilmiştir.

Asal sayıların modüler uzayda uniform dağılımı temel alınarak bir Pseudo Random Number Generator (PRNG) algoritması geliştirilmiş ve bu algoritma, NIST'in belirlediği standartlara uygun test araçlarından başarıyla geçmiştir. Algoritmanın kriptografik olarak güvenli olup olmadığı detaylandırılmadan tartışılmıştır. Öte yandan bilgisayar üzerinde yapılan denemelerde algoritmanın periyodunun bir kriptografik algoritma için yeterince uzun olduğu görülmüştür. Sıradaki asal sayıyı hesaplayacak analitik yaklaşımların olmaması, algoritmanın geri dönüştürülemez olmasını sağlamaktadır. Bu da algoritmanın kriptografik anlamada güvenilirliğini artıran hususlardan biri olarak görülebilir. Yine deterministik asallık testleri yerine olasılıksal testler kullanılması, algoritmanın geri dönüştürülemezliğini daha da artıracak ve onu daha güvenli hale getirecektir.

Asal sayma fonksiyonuna asimptotik bir analitik fonksiyon tanımlanmış ve Abel kısmi toplam formülü, belirli bir hipotez altında genişletilerek analitik sayı teorisi için değerli bir araç oluşturulmuştur. Bu araç daha sonra asal sayı teoreminin yeni bir ispatı olarak kullanılmıştır.

Asal indisli diziler üzerindeki toplama işlemi incelenmiş ve Riemann-Stieltjes integrasyonu ile Abel kısmi toplam formülü kullanılarak aynı sonuçlar elde edilerek bu iki yöntem arasındaki ilişki açıkça gösterilmiştir.

Birçok farklı ispatı bulunan asal sayıların sonsuzluğunun farklı bir ispatı daha sunulmuştur. Burada sınırlı sayıda asalların keyfi kuvvetlerinin belirli bir büyüklüğün altında kalan sayıları örtüp örtmediği araştırılmıştır.

KAYNAKÇA

[1] D. M. Burton, *The History of Mathematics: An Introduction*, 7th. McGraw-Hill, 2011, p. 514, isbn: 978-0-07-338315-6.

[2] L. Euler, "Variae observationes circa series infinitas," *Commentarii academiae scientiarum Petropolitanae*, vol. 9, pp. 160–188, 1737. [Online]. Available: https://scholarlycommons.pacific.edu/euler-works/72/.

[3] L. Euler, "Theoremata arithmetica nova methodo demonstrata," *Novi Commentarii academiae scientiarum Petropolitanae*, 1763.

[4] L. Euler, *Variae observationes circa series infinitas*, Euler Archive - All Works, Paper No. 72, 1744.

[5] C. F. Gauss, *Carl Friedrich Gauss Werke*. Göttingen; Leipzig: [Göttingen]; Leipzig, in Commission bei B. G. Teubner, 1863, vol. 1-6.

[6] P. G. L. Dirichlet, "Beweis des satzes, dass jede unbegrenzte arithmetische progression, deren erstes glied und differenz ganze zahlen ohne gemeinschaftlichen factor sind, unendlich viele primzahlen enthält," *Abhandlungen der Königlichen Preussischen Akademie der Wissenschaften*, 1837.

[7] P. Tchebychev, "Mémoire sur les nombres premiers," *Journal de mathématiques pures et appliquées*, 1st ser., pp. 366–390, 1852, Proof of the postulate: 371-382.

[8] F. Mertens, "Ein beitrag zur analytischen zahlentheorie," *Journal für die reine und angewandte Mathematik (Crelle's Journal)*, vol. 78, pp. 46–62, 1874.

[9] B. Riemann, "Über die anzahl der primzahlen unter einer gegebenen größe," *Monatsberichte der Berliner Akademie*, 1859, Reprinted in Gesammelte Mathematische Werke, Teubner, Leipzig, 1892, pp. 145–155.

[10] G. H. Hardy, J. E. Littlewood, "Some problems of 'partitio numerorum'; iii: On the expression of a number as a sum of primes," *Acta Mathematica*, vol. 44, no. 1, pp. 1–70, 1923.

[11] B. Green, T. Tao, "The primes contain arbitrarily long arithmetic progressions," *Annals of Mathematics*, vol. 167, no. 2, pp. 481–547, 2008. doi: 10.4007/annals.2008.167.481. arXiv: math.NT/0404188.

[12] D. A. Goldston, J. Pintz, C. Y. Yıldırım, "Primes in tuples i," *Annals of Mathematics*, vol. 170, no. 2, pp. 819–862, 2009. doi: 10.4007/annals.2009.170.819.

[13] Y. Zhang, "Bounded gaps between primes," *Annals of Mathematics*, vol. 179, no. 3, pp. 1121–1174, 2014.

[14] J. Maynard, "Small gaps between primes," *Annals of Mathematics*, vol. 181, no. 1, pp. 383–413, 2015. doi: 10.4007/annals.2015.181.1.7.

[15] D. H. J. Polymath, "Variants of the selberg sieve, and bounded intervals containing many primes," *Research in the Mathematical Sciences*, vol. 1, no. 12, 2014. doi: 10.1186/s40687-014-0012-7.

[16] A. Ivić, *The Riemann Zeta-Function: The Theory of the Riemann Zeta-Function with Applications*. Wiley-Interscience, 2003.

[17] J. B. Conrey, "The riemann hypothesis," *Notices of the AMS*, vol. 50, no. 3, pp. 341–353, 2003.

[18] J. Neukirch, *Algebraic Number Theory*. Springer-Verlag, 1999.

[19] E. Titchmarsh, D. Heath-Brown, *The Theory of the Riemann Zeta-function*. Oxford University Press, 1986.

[20] G. L. Miller, "Riemann's hypothesis and tests for primality," *Journal of Computer and System Sciences*, vol. 13, no. 3, pp. 300–317, 1976. doi: 10.1145/800116.803773.

[21] A. W. Dudek, "On the riemann hypothesis and the difference between primes," *International Journal of Number Theory*, vol. 11, no. 03, pp. 771–778, 2015. doi: 10.1142/S1793042115500426. [Online]. Available: https://doi.org/10.1142/S1793042115500426.

[22] M. Cully-Hugill, A. Dudek, "A conditional explicit result for the prime number theorem in short intervals," *Research in Number Theory*, vol. 8, no. 61, 2022. doi: 10.1007/s40993-022-00358-1.

[23] J. B. Conrey, "The riemann hypothesis," *Notices of the AMS*, vol. 50, no. 3, pp. 341–353, 2003. [Online]. Available: https://www.ams.org/notices/200303/fea-conrey-web.pdf.

[24] E. Bombieri, "The riemann hypothesis - official problem description," *Clay Mathematics Institute*, 2000. [Online]. Available: https://www.claymath.org/sites/default/files/official_problem_description.pdf.

[25] M. Watkins, "Prime numbers and the riemann hypothesis," *American Scientist*, vol. 92, no. 4, pp. 282–287, 2004. [Online]. Available: https://www.americanscientist.org/article/prime-numbers-and-the-riemann-hypothesis.

[26] S. Cook, "The complexity of theorem proving procedures," in *Proceedings of the Third Annual ACM Symposium on Theory of Computing*, ACM, 1971, pp. 151–158, isbn: 9781450374644. doi: 10.1145/800157.805047.

[27] L. A. Levin, "", vol. 9, no. 3, pp. 115–116, 1973, In Russian, English translation: Universal search problems, issn: 0555-2923.

[28] M. O. Rabin, "Probabilistic algorithm for testing primality," *Journal of Number Theory*, vol. 12, no. 1, pp. 128–138, 1980. doi: 10.1016/0022-314X(80)90084-0.

[29] R. Baillie, S. Wagstaff, "Lucas pseudoprimes," in *Mathematics of Computation*, vol. 35, 1980, pp. 1391–1417. doi: 10.1090/S0025-5718-1980-0583518-6.

[30] M. Agrawal, N. Kayal, N. Saxena, "PRIMES is in P," *Annals of Mathematics*, vol. 160, no. 2, pp. 781–793, 2004. doi: 10.4007/annals.2004.160.781.

[31] A. O. L. Atkin, F. Morain, "Elliptic curves and primality proving," *Mathematics of Computation*, vol. 61, no. 203, pp. 29–68, 1993. doi: 10.1090/S0025-5718-1993-1199989-X.

[32] A. R. Öztek, "Elliptic curve primality tests / eliptik eğri asallık testleri," English, Master's Thesis, Fatih University, Institute of Science, Istanbul, Turkey, 2006, p. 62.

[33] R. L. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978. doi: 10.1145/359340.359342.

[34] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987. doi: 10.2307/2007884. [Online]. Available: https://www.jstor.org/stable/2007884.

[35] V. Miller, "Use of elliptic curves in cryptography," in *Advances in Cryptology – CRYPTO '85 Proceedings*, ser. Lecture Notes in Computer Science, vol. 85, Springer, 1986, pp. 417–426. doi: 10.1007/3-540-39799-X_31.

[36] G. H. Hardy, E. M. Wright, *An Introduction to the Theory of Numbers*, 6th ed. Oxford University Press, 2008, isbn: 978-0199219865.

[37] K. H. Rosen, *Elementary Number Theory and its Applications*, 3rd ed. Addison-Wesley, 1993, isbn: 978-0-201-57889-8.

[38] É. Bézout, *Théorie générale des équations algébriques*. Paris, France: Ph.-D. Pierres, 1779.

[39] I. Niven, H. S. Zuckerman, H. L. Montgomery, *An Introduction to the Theory of Numbers*, 5th ed. John Wiley Sons, 1991, isbn: 978-0471625469.

[40] R. M. Solovay, V. Strassen, "A fast monte-carlo test for primality," *SIAM Journal on Computing*, vol. 6, no. 1, 1977. doi: 10.1137/0206006.

[41] C. K. Caldwell, A. Reddick, Y. Xiong, W. Keller, "The history of the primality of one: A selection of sources," *Journal of Integer Sequences*, vol. 15, 2012.

[42] C. F. Gauss, *Disquisitiones Arithmeticae*, Second, corrected edition, trans. by A. A. Clarke. New York: Springer, 1986.

[43] *Fundamental theorem of arithmetic - history*. [Online]. Available: https://en.wikipedia.org/wiki/Fundamental_theorem_of_arithmetic#History (visited on 12/29/2023).

[44] Y. Arslan, "Aritmetiğin temel teoremi ve tarihsel gelişimi," Yüksek Lisans Tezi, Master's Thesis, Yıldız Teknik Üniversitesi, Fen Bilimleri Enstitüsü, 2002.

[45] F. R. S. Horsley Rev. Samuel, " or, the sieve of eratosthenes. being an account of his method of finding all the prime numbers," *Philosophical Transactions (1683–1775)*, vol. 62, pp. 327–347, 1772.

[46] S. Datta, *Time complexity of sieve of eratosthenes algorithm*, https://www.baeldung.com/cs/sieve-of-eratosthenes, Son erişim: 13 Temmuz 2024, 2024.

[47] K. G. der Wissenschaften zu Göttingen, Ed., *Werke*. Leipzig: B. G. Teubner, 1917, vol. 10.1.

[48] A.-M. Legendre, *Essai sur la théorie des nombres*, 1st ed. Paris, 1798, Supplément à l'Essai sur la théorie des nombres.

[49] A.-M. Legendre, *Essai sur la théorie des nombres*, 2nd ed. Paris, 1808, Second supplément à l'Essai sur la théorie des nombres.

[50] D. Zagier, "The first 50 million prime numbers," *The Mathematical Intelligencer*, vol. 0, no. 1, pp. 7–19, 1977.

[51] A. F. Möbius, "Über eine besondere art von umkehrung der reihen," *Journal für die reine und angewandte Mathematik*, vol. 1831, no. 9, pp. 105–123, 1831.

[52] J. Hadamard, "Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques," *Bulletin de la Société Mathématique de France*, vol. 24, pp. 199–220, 1896.

[53] C.-J. d. l. Vallée-Poussin, "Recherches analytiques sur la théorie des nombres premiers," *Annales de la Société Scientifique de Bruxelles*, vol. 20, pp. 183–256, 1896.

[54] C. K. Caldwell, *2996863034895* $\times$ $2^{1290000}$ *- 1*, The Prime Pages, Available online: https://primes.utm.edu/primes/page.php?id=13000, Martin, TN, year of publication here.

[55] D. H. J. Polymath *et al.*, "Variants of the selberg sieve, and bounded intervals containing many primes," *Research in the Mathematical Sciences*, vol. 1, no. 12, 2014.

[56] A. Ingham, *The Distribution of Prime Numbers*. Cambridge University Press, 1932.

[57] P. Erdös, A. Selberg, "An elementary proof of the prime number theorem," *Annals of Mathematics*, vol. 50, no. 2, pp. 305–313, 1949.

[58] A. Selberg, "An elementary proof of the prime-number theorem," *Annals of Mathematics*, pp. 305–313, 1949.

[59] V. Bergelson, F. K. Richter, "Dynamical generalizations of the prime number theorem and disjointness of additive and multiplicative semigroup actions," *Duke Mathematical Journal*, vol. 171, no. 15, pp. 3133–3200, 2022.

[60] T.-J. Stieltjes, "Recherches sur les fractions continues," *Annales de la Faculté des sciences de Toulouse pour les sciences mathématiques et les sciences physiques*, 1st ser., vol. 8, no. 4, J1–J122, 1894. [Online]. Available: http://www.numdam.org/item/AFST_1894_1_8_4_J1_0/.

[61] F. Gerard, "Estimating prime power sums," 2022, Mentored by Lawrence Washington, University of Maryland.

[62] L. Blum, M. Blum, M. Shub, "Comparison of two pseudo-random number generators," in *Advances in Cryptology: Proceedings of CRYPTO '82*, Plenum, 1982, pp. 61–78.

[63] W. H. Payne, J. R. Rabung, T. P. Bogyo, “Coding the lehmer pseudo-random number generator,” *Commun. ACM*, vol. 12, no. 2, 1969.

[64] W. E. Thomson, “A Modified Congruence Method of Generating Pseudo-random Numbers,” *The Computer Journal*, vol. 1, no. 2, pp. 83–83, 1958.

[65] A. Rotenberg, “A new pseudo-random number generator,” *J. ACM*, pp. 75–77, 1960.

[66] E. A. E. Al., “A new method for hybrid pseudo random number generator,” *INFORMACIJE MIDEM-JOURNAL OF MICROELECTRONICS ELECTRONIC COMPONENTS AND MATERIALS*, pp. 303–311, 2014.

[67] W. H. Press, S. A. Teukolsky, W. T. Vetterling, B. P. Flannery, *Numerical Recipes 3rd Edition: The Art of Scientific Computing*. Cambridge University Press, 2007.

[68] E. Avaroglu, I. Koyuncu, A. B. Ozer, M. Turk, “Hybrid pseudo-random number generator for cryptographic systems,” *NONLINEAR DYNAMICS*, vol. 82, no. 1-2, pp. 239–248, Oct. 2015. doi: 10.1007/s11071-015-2152-8.

[69] G. Sarıkaya, “The evaluation and comparison of primality testing algorithms,” Master’s Thesis, İstanbul Teknik Üniversitesi, 2019.

[70] E. E. Kummer, “Über die ergänzungssätze zu den allgemeinen reciprocitätsgesetzen,” *Journal für die reine und angewandte Mathematik*, vol. 1851, pp. 203–220, 1851. [Online]. Available: https://eudml.org/doc/146765.

[71] H. Furstenberg, “On the infinitude of primes,” *American Mathematical Monthly*, vol. 62, no. 5, p. 353, 1955. [Online]. Available: https://www.jstor.org/stable/2307043.

TEZDEN ÜRETİLMİŞ YAYINLAR

Konferans Bildirisi

1. Turan, M., Onar, S. (2024, Mayıs). A new analytic framework for arithmetic integrals: Proving the prime number theorem. 7th International Hybrid Conference on Mathematical Advances and Applications, İstanbul, Türkiye.