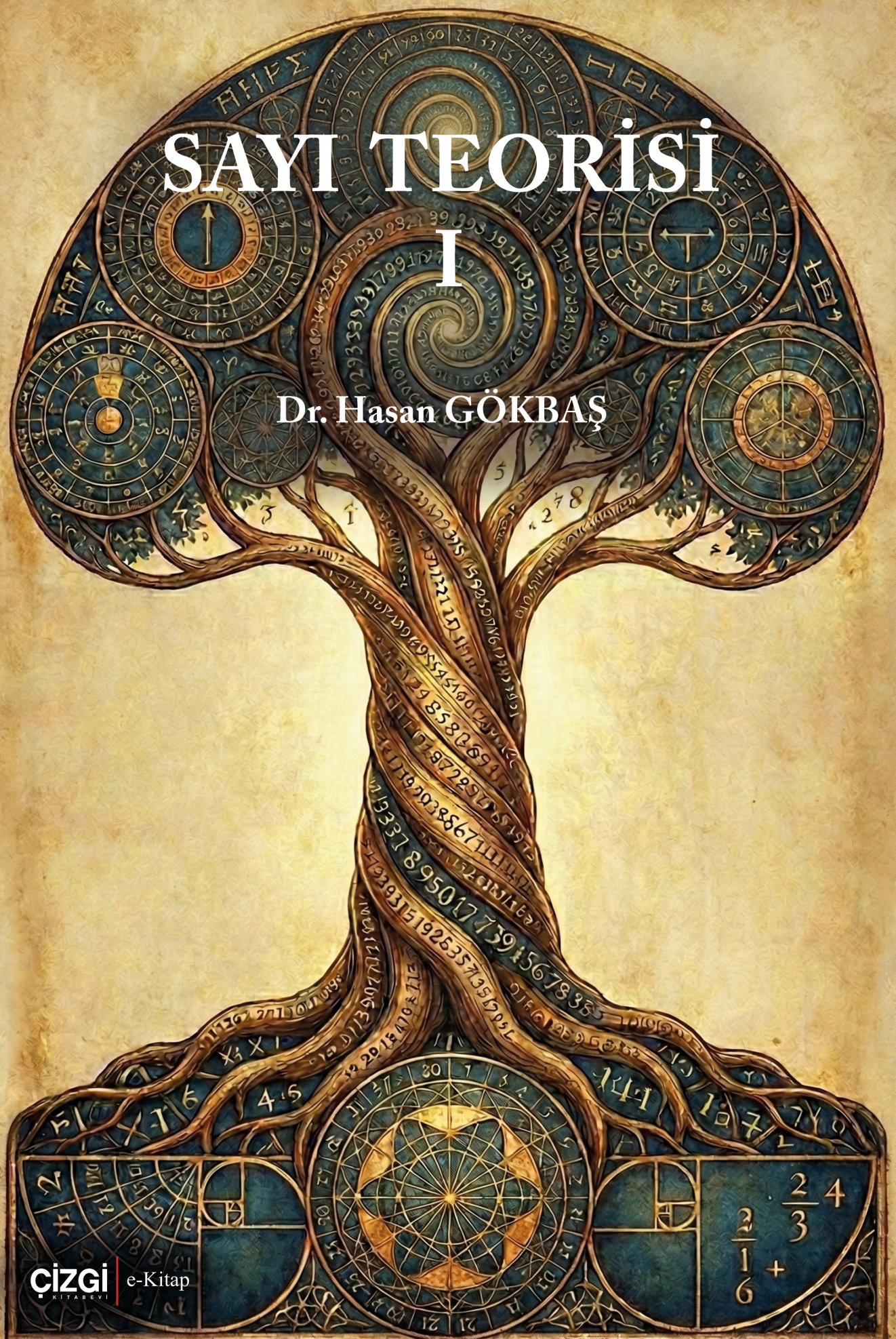
SAYI TEORİSİ
I

Dr. Hasan GÖKBAŞ



ÇİZGİ KİTABEVİ | e-Kitap

Çizgi Kitabevi Yayınları (e-kitap)

Şubat 2026

ISBN: 978-625-396-783-3
Yayıncı Sertifika No: 52493

KÜTÜPHANE BİLGİ KARTI
- Cataloging in Publication Data (CIP) -
GÖKBAŞ, Hasan
orcid: 0000-0002-3323-8205
SAYI TEORİSİ
1

Editör
Dr. Harun ÇİÇEK
orcid: 0000-0003-3018-3015

Baskıya Hazırlık: Çizgi Kitabevi Yayınları
Tel: 0332 353 62 65- 66

ÇİZGİ KİTABEVİ

Sahibiata Mah.
M. Muzaffer Cad. No:41/1
Meram/**Konya**
(0332) 353 62 65

Konevi Mah.
Larende Cad. No:20/A
Meram/**Konya**
(0332) 353 62 66

Siyavuşpaşa Mah.
Gül Sk. No:15 B
Bahçelievler/**İstanbul**
(0212) 514 82 93

www.cizgikitabevi.com
/ cizgikitabevi

İÇİNDEKİLER

ÖNSÖZ

Sayı teorisi, matematiğin en eski, en derin ve belki de en büyülü dallarından biridir. İnsanlık, binlerce yıldır sayıların sırlarını çözmeye çalışmaktadır: bir sayı neden asaldır, neden bölünmez, neden tam kare değildir, iki asalın toplamı neden her zaman çift sayı verir, sonsuz tane asal gerçekten var mıdır, yoksa bir yerde bitecek midir?

Bu soruların bazıları Pisagor'dan beri, cevaplandırılmayı beklemektedir. Ama ilginç olan şudur: bu sorulara verilen her yanıt, insanlığın teknolojiye, güvenliğe, iletişime ve hatta sanata bakışını derinden değiştirmiştir. Bugün milyarlarca insanın her gün farkında olmadan kullandığı internet bankacılığı, mesajlaşma uygulamaları, blockchain, dijital imzalar gibi hayatımızın vazgeçilmezleri arasında yer alan uygulamaların hepsinin temelinde sayı teorisinin sessiz ama güçlü sonuçları bulunmaktadır.

Elinizdeki bu kitap, sayı teorisine giriş niteliğinde yazılmış iki ciltlik bir çalışmanın ilk parçasıdır. Amacım, konuyu olabildiğince yalın, mantıksal sırayla ve mümkün olduğunca çok örnekle anlatmaktır. Üniversite düzeyinde ilk sayı teorisi dersini alan bir öğrencinin rahatlıkla takip edebileceği, lise son sınıf veya üniversite hazırlık öğrencilerinden meraklı ortaöğretim öğrencilerine kadar geniş bir kitlenin faydalanabileceği bir dil hedefim olmuştur.

Kitapta klasik konulara (bölünebilme, asal sayılar, kongrüanslar, Diophantine denklemler, aritmetiğin temel teoremi, vs.) yer verirken, aynı zamanda öğrencinin sıkça sorduğu "Peki bu nerede kullanılır?", "Bunun ispatı gerçekten gerekli mi?", "Daha kısa-daha zarif bir yol yok mu?" gibi sorulara da elimden geldiğince yanıt vermeye çalıştım.

Birinci cilt, sayı teorisinin temel yapı taşlarını (iyi sıralama, indüksiyon, bölünebilme kuralları, Euclid algoritması, asallık, temel aritmetik teoremi, basit kongrüanslar) olabildiğince sağlam bir şekilde

yerleştirmeyi amaçlıyor. İkinci ciltte ise daha ileri konulara (kuadratik karşılıklılık, ilkel kökler, Euler'in ϕ fonksiyonu, analitik sayı teorisine giriş, aritmetik fonksiyonlar, bazı açık problemler) geçmeyi planlıyorum.

Bu yolculukta yanımda olduğunuz için teşekkür ederim. Umarım sayfaları çevirirken zaman zaman "Aa, demek böyleymiş!" dediğiniz, zaman zaman da kalemi kâğıdı alıp kendi küçük keşiflerinizi yaptığınız anlar yaşarsınız.

Bitlis

Şubat 2026

Hasan Gökbaş

1. BÖLÜM

BAŞLANGIÇ

Sayı teorisi, matematiğin en önemli alanlarındandır. Antik çağlardan beri, insan uygarlığı üzerinde önemli bir etkisi olagelmiştir. Günümüze kadar birçok kişi, sayılar teorisinin çeşitli yönlerine katkılarda bulunmuştur. Sayı teorisi, Pisagor (MÖ 569-500), Öklid (MÖ 350), Eratosthenes (MÖ 276-196), Nicomachus (MS 60-120), Diophantus (MS 200–284), Harizmi (MS 780-850), Pisano (MS 1170-1250), Leibniz (MS 1646-1716), Gauss (MS 1777-1855) ve Euler (MS 1707-1783) gibi bilim insanlarının katkılarıyla yoluna devam etmiştir. Pisagor teoremiyle, matematikçileri kare sayılar ve kare sayılar toplamını incelemeye yönlendirmiştir. Öklid, asal sayılara dikkat çekmeye çalışmış, iki doğal sayının en büyük ortak bölenini veren algoritmasıyla doğal sayıların asal çarpanlarına ayrılmasında rol oynamıştır. Eratosthenes, asal sayıların seçilmesini, asal sayıların bir sınırının olmadığını göstermiştir. Nicomachus, asal, mükemmel sayılar gibi sayıların mistik özellikleri olabileceğini düşünmüş; sayıların küp toplamıyla üçgensel sayılar arasında ilişki olabileceğine dair çalışmalarda bulunmuştur. Diophantus, çözümü ve içeriğindeki tüm değişkenlerinin tam sayı olacağı denklem çalışmaları sunmuştur. Sayılamayacak kadar çok matematikçi sayılamayacak kadar çok çalışmalarda bulunarak sayı teorisine katkılar sunmuştur.

Sayı teorisi 1, 2, 3, … doğal sayılarıyla başladı. Toplama işlemi doğal sayılarda geçerlilik gösterirken, çıkarma işlemi doğal sayılarda her zaman geçerli olmamıştır. Buna neden elinde 3 adet nesne olan birinden 4 adet nesne alınamayacağıdır. Doğal sayılarda her zaman geçerli olmayan çıkarma işleminden dolayı -1, -2, -3, … gibi negatif doğal sayılara ihtiyaç duyulmuştur. Babil ve Maya uygarlıklarında ortaya çıktığına inanılan 0 kavramı, Hint uygarlığının aktif kullanımıyla Arap uygarlığı tarafından bir sayı olarak kabul görmüştür. Bu üç sayı topluluğu bir araya getirilerek tam sayılar olarak bilinecek yeni bir sayı topluluğu oluşturulmuştur. Toplama, çıkarma ve çarpma işlemi yeni sayı topluluğunda geçerli olurken bölme işlemi her zaman geçerlilik göstermemiştir. Sayı teorisi çalışmaları bölme işleminin de her zaman geçerli olacağı, rasyonel sayılar olarak isimlendirilecek yeni sayı topluluğuyla, sayılar

yolculuğuna devam etmiştir. Karşılaşılan sorunlara çözüm bulunarak günümüze kadar devam eden sayı teorisi çalışmaları yeni sayı topluluklarıyla yoluna devam etmektedir.

Matematiğin temelini teşkil eden sayılar matematiğin; soyut cebir, sayılar teorisi, soyut mantık, kompleks analiz gibi pek çok alanında büyük bir öneme sahiptir. 0, 1, 2, 3, … sayılarına doğal sayılar kümesi denir. Doğal sayılar ingilizce doğal anlamına gelen "natural" kelimesinden dolayı $\mathbb{N}$ sembolüyle gösterilir. …, -3, -2, -1, 0, 1, 2, 3, … sayılarına tam sayılar, 0, 1, 2, 3, … sayılarına negatif olmayan tam sayılar, 1, 2, 3, … sayılarına pozitif tam sayılar, 0, -1, -2, -3, … sayılarına pozitif olmayan tam sayılar, -1, -2, -3, … sayılarına negatif tam sayılar denir. Tam sayılar almanca sayılar anlamına gelen "zahlen" kelimesinden dolayı $\mathbb{Z}$ sembolüyle gösterilir. Yine, almanca bölüm anlamına gelen "quotient" kelimesinden dolayı, rasyonel sayılar $\mathbb{Q}$ sembolüyle gösterilir.

Tam sayılar kümesi aksiyomlarla kurulabilir, tam sayıların aritmetiği açıklanan aksiyomlarla yapılabilir. Pozitif tam sayıların kümesini karakterize eden aksiyomlar İtalyan matematikçi Giuseppe PEANO tarafından verilmiştir. Peano aksiyomları olarak da bilinen tam sayıların aşağıdaki özellikleri vardır:

i. 1 sembolüyle gösterilen bir pozitif tam sayı vardır.
ii. Her pozitif -n- tam sayısının -n'- şeklinde ardışığı denen bir tek pozitif tam sayısı vardır.
iii. Ardışığı 1 tam sayısı olan hiçbir pozitif tam sayı yoktur.
iv. Eğer $n' = m'$ olacak şekilde n ve m tam sayıları varsa $n = m$ olmalıdır.
v. Pozitif tam sayıların herhangi bir kümesi 1 sayısını ve bu kümeye ait herhangi bir sayının ardışığını ihtiva ediyorsa bu küme bütün pozitif tam sayıları ihtiva eder.

İyi Sıralama Prensibi

Tanım: Pozitif tam sayılardan oluşan, boş olmayan her kümenin bir en küçük elemanı vardır. Bu özelliğe iyi sıralama prensibi denir. $\mathbb{Z}^+ = \{1, 2, 3, 4, \dots\}$ kümesinin boş olmayan her A alt kümesinin bir en küçük elemanı vardır.

$1 \in A$ olursa ispat tamamdır. $1 \notin A$ olduğunu farz edelim. A kümesindeki $a > b$ şartını sağlayan b sayılarının kümesi B olsun. Bu durumda,

$B = \{b: b < a,\ a \in A\}$ olur. $1 \in B$ olduğu aşikardır. B kümesinin tanımından $b < a$ olduğundan $b + 1 \leq a$ olmalıdır. $(b + 1) \in B$ ise B kümesi bütün pozitif tam sayıları kapsamaktadır. Bu durum $A = \emptyset$ olduğu sonucu verecektir. Hâlbuki A kümesi boş kümeden farklı alınmıştı. Dolayısıyla $b + 1 \leq a$ şartını sağlayan $(b + 1)$ sayısı A kümesinin bir en küçük elemanı olacaktır.

Matematik İndüksiyon Prensibi

Tanım: A kümesi pozitif tam sayıların herhangi bir kümesi olsun. Eğer,

i. $1 \in A$,
ii. $n \in A$ olduğunda,
iii. $(n + 1) \in A$ oluyorsa A kümesi bütün pozitif tam sayıları kapsar.

Bu ifadeye matematik indüksiyon prensibi veya tümevarım prensibi denir. Tümevarım yöntemi; olmayana ergi, aksine örnek verme, çelişki metodu gibi matematikte önemli yeri olan bir ispat metodudur.

Örnek: $3 + 11 + 19 + 27 + \cdots + (8n - 5) = n(4n - 1)$ eşitliğinin her pozitif tam sayı için doğru olduğunu gösterelim.

Çözüm: Yukarıda verilen eşitliği sağlayan pozitif tam sayılar kümesine A ismini verelim.

i. $n = 1 \in \mathbb{Z}^+$ için $3 = 1 \cdot (4 \cdot 1 - 1) = 3$ eşitliği doğru çıkmaktadır.
ii. $n = k$ için $k \in \mathbb{Z}^+$ olduğunu kabul edelim.
iii. $n = (k + 1)$ için $(k + 1) \in \mathbb{Z}^+$ olduğunu göstermeliyiz.

$3 + 11 + 19 + 27 + \cdots + (8k - 5) = k(4k - 1)$ olduğunu biliyoruz.

$3 + 11 + 19 + 27 + \cdots + (8n - 5) + (8k + 3) = (k + 1)(4k + 1)$ eşitliğinin doğru olduğunu göstermeliyiz.

$3 + 11 + 19 + 27 + \cdots + (8k - 5) = k(4k - 1)$ eşitliğini yukarıdaki eşitliğin sol kısmında yerine yazalım:

$k(4k - 1) + (8k + 3) = (k + 1)(4k + 3)$ eşitliğini düzenleyelim:

$4k^2 + 7k + 3 = 4k^2 + 7k + 3$ eşitliği elde edilir.

$n = (k+1)$ için $(k+1) \in \mathbb{Z}^+$ olduğu görülür. Tümevarım yöntemiyle örnekte verilen eşitliğin, her pozitif tam sayı tarafından gerçeklendiği görülecektir.

Soru: $2^0 + 2^1 + 2^2 + 2^3 + \cdots + 2^{n-1} = 2^n - 1$ eşitliğinin her doğal sayı için geçerli olacağını gösteriniz.

Not: (İkinci Tümevarım Metodu) Her $n \geq a$ tam sayısı için bir P(n) önermesi verilmiş olsun.

i. $P(a)$ doğrudur,
ii. $m > 0$ bir tam sayı olmak üzere $a \leq k < m$ şartını sağlayan her k tam sayısı için $P(k)$ önermesinin doğru kabul edilmesi halinde,
iii. $P(m)$ önermesi doğrudur,

şartları sağlanıyorsa bu takdirde her $n \geq a$ tam sayısı için $P(n)$ önermesi doğrudur.

Örnek: $(n+1)! > 2^n$ eşitsizliğinin $n \geq 2$ her pozitif tam sayı için doğru olduğunu gösterelim.

Çözüm: Yukarıda verilen eşitliği sağlayan pozitif tam sayılar kümesine B ismini verelim.

i. $n = 2 \in \mathbb{Z}^+$ için $3! = 6 > 2^2 = 4$ eşitsizliği doğru çıkmaktadır.
ii. $n = k$ için $k \in \mathbb{Z}^+$ olduğunu kabul edelim.
iii. $n = (k+1)$ için $(k+1) \in \mathbb{Z}^+$ olduğunu göstermeliyiz.

$(k+1)! > 2^k$ olduğunu biliyoruz.

$(k+2)! > 2^{k+1}$ eşitsizliğinin doğru olduğunu göstermeliyiz.

$(k+2)! = (k+2)(k+1)! > 2 \cdot 2^k = 2^{k+1}$ eşitsizliği $(k+2) > 2$ eşitsizliği yardımıyla elde edilir.

$n = (k+1)$ için $(k+1) \in \mathbb{Z}^+$ olduğu görülür. Tümevarım yöntemiyle örnekte verilen eşitsizliğin, $n \geq 2$ her pozitif tam sayı tarafından gerçeklendiği görülecektir.

Soru: $\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{n\cdot(n+1)}=\frac{n}{n+1}$ eşitliğinin her pozitif tam sayı için doğru olduğunu gösteriniz.

Soru: Bernoulli Eşitsizliği olarak da bilinen, $(1+a)^n \geq 1+na$ eşitsizliğini $(1+a)>0$ olmak üzere her pozitif tam sayının gerçeklediğini gösteriniz.

Soru: $1^3+2^3+3^3+\cdots+n^3=\left(\frac{n(n+1)}{2}\right)^2$ eşitliğinin her pozitif tam sayı için doğru olduğunu gösteriniz.

Güvercin Deliği İlkesi

Tanım: $n>k$ olmak üzere k tane kutuya n tane nesne yerleştirilecekse, iki veya daha fazla nesneyi içeren en az bir kutu olmalıdır.

k adet kutunun hiçbirinin birden fazla nesnesi olmadığını kabul edelim. Bu durumda, toplam nesne sayısı k tane olacaktır. $n>k$ varsayımımızla çelişecektir. Dolayısıyla, n tane nesne k tane kutuya yerleştirilecekse, bir kutu birden fazla nesne içermek zorundadır.

Örnek: 731 kişinin olduğu bir grupta, en az 3 kişinin doğum günlerinin aynı olacağını gösterelim.

Çözüm: Bir yılda doğum günleri sayısının 365 olmasından dolayı en az 3 kişinin doğum günü, aynı günde olacaktır.

Soru: 7 beyaz, 5 mavi top içerisinden, çekilen topun kesinlikle mavi olması için en az kaç top çekileceğini bulunuz.

Tam sayıların şu özellikleri mevcuttur:

i. $a,b \in \mathbb{Z}$ için $a+b\in\mathbb{Z}$ ve $a\cdot b\in\mathbb{Z}$ (Kapalılık Özelliği),

ii. $a,b \in \mathbb{Z}$ için $a+b=b+a$ ve $a\cdot b=b\cdot a$ (Değişme Özelliği),

iii. $a,b,c \in \mathbb{Z}$ için $a+(b+c)=(a+b)+c$ ve $a\cdot(b\cdot c)=(a\cdot b)\cdot c$ (Birleşme Özelliği),

iv. $a,b,c \in \mathbb{Z}$ için $a\cdot(b+c)=a\cdot b+a\cdot c$ ve $(b+c)\cdot a=b\cdot a+c\cdot a$ (Dağılma Özelliği),

v. $a,b,c \in \mathbb{Z}$ için $a+c=b+c$ ise $a=b$ ya da

$a\cdot c=b\cdot c$ ise $a=b$ $c\neq 0$ (Kısaltma Özelliği),

vi. $a, b \in \mathbb{Z}$ için ya $a = b$ ya $a > b$ ya da $a < b$ (Üç Hal Kuralı),

vii. $a, b, c \in \mathbb{Z}$ için $a < b$ ve $b < c$ ise $a < c$ (Geçişme Özelliği),

viii. $a, b, c \in \mathbb{Z}$ için $a < b$ ise $a + c < b + c$ ya da $a \cdot c < b \cdot c, c > 0$ ya da $a \cdot c > b \cdot c, c < 0$ (Genişletme Özelliği),

ix. $|a| = \begin{cases} a, & a > 0 \\ 0, & a = 0 \\ -a, & a < 0 \end{cases}$ (Mutlak Değer Özelliği).

Teorem: k herhangi tam kare olmayan bir tam sayı olmak üzere, $r^2 = k$ eşitliğini sağlayan hiçbir rasyonel sayı yoktur.

İspat: $r^2 = k$ eşitliğini sağlayan, $(a, b) = 1$ olmak üzere, $r = \frac{a}{b}$ rasyonel sayısının olduğunu kabul edelim. $a^2 = k \cdot b^2$ eşitliği elde edilir. k pozitif tam sayısına karşılık $l^2 < k < (l+1)^2$ şeklinde olacak bir pozitif l tam sayısı vardır.

$$b^2 l^2 < a^2 < b^2 (l+1)^2$$

$$bl < a < b(l+1)$$

$$0 < a - bl < b.$$

Ayrıca, $(kb - al)^2 = k^2 b^2 - 2kbal + a^2 l^2 = ka^2 - 2kbal + (bl)^2 = k(a - bl)^2$ eşitliğinden $k = \frac{(kb-al)^2}{(a-bl)^2}$ elde edilir. $\frac{(kb-al)^2}{(a-bl)^2}$ ve $\frac{a}{b}$, k tam sayısının iki gösterimi olacaklardır. Buradan, $(a - bl) > b$ elde edilecektir. Elde edilen sonuç varsayımımızla çelişecektir. Dolayısıyla, k herhangi tam kare olmayan bir tam sayı olmak üzere, $r^2 = k$ eşitliğini sağlayan hiçbir rasyonel sayı yoktur.

Teorem: $r^2 = 2$ eşitliğini sağlayan hiçbir rasyonel sayı yoktur. Başka bir ifadeyle $\sqrt{2}$ irrasyonel bir sayıdır.

İspat: $r^2 = 2$ eşitliğini sağlayan en az bir rasyonel sayısının olduğunu kabul edelim. $r \in \mathbb{Q}$ olmasından dolayı $(a, b) = 1$ ve $b \neq 0$ olmak üzere, $r = \frac{a}{b}$ şeklinde yazılabilir. Eşitlik $\frac{a^2}{b^2} = 2$, $a^2 = 2b^2$ şekline dönüşür. Bu durum bize hem a^2 hem de a tam sayılarının çift sayı olacağı sonucuna götürür. $a = 2k$ olduğunu varsayarak eşitliği yeniden düzenleyelim. $4k^2 = 2b^2$ veya $2k^2 = b^2$ olur. Bu sonuçta bizi hem b^2 hem de b tam sayılarının çift sayı olacağı sonucuna götürür. $(a, b) \neq 1$ sonucu, başlangıçta ki varsayımımız $(a, b) = 1$ olmasıyla

çelişir. Dolayısıyla $r^2 = 2$ eşitliğini sağlayan hiçbir rasyonel sayı yoktur. Yani $\sqrt{2}$ irrasyonel bir sayıdır.

İrrasyonel sayı kavramı, Pisagor matematikçileri üyesi olan Hippasus (MÖ530-450)'la hayatımızda yer edinmiştir. Pisagor her ne kadar irrasyonel sayıların varlığını kabul etmemiş olsa da modern matematikçilerin kabulüyle irrasyonel sayılar günümüzde cebirsel ve transandantal olarak ikiye ayrılmıştır. Rasyonel ve İrrasyonel sayıların birleşimi olan Gerçek sayılar kümesi $\mathbb{R}$ sembolüyle gösterilir. Gerçek sayılar kavramı, gelişimine antik Yunan'da başlamıştır. Öklid, modern gerçek sayılar teorisine eşdeğer olan oranlar teorisini geliştirmiştir. 17. yüzyılda, John Napier ve Simon Stevin sonsuz ondalık genişleme kavramını tanıtmıştır. Cantor ve Dedekind, modern gerçek sayılar teorilerinin ortaya çıkmasına katkıda bulunmuşlardır.

Örnek: $\sqrt{2}$ irrasyonel sayısının yaklaşık değerini bulalım.

Çözüm: 2 sayısının karekökünü bölme benzeri bir algoritmayla yaklaşık olarak bulabiliriz.

1.adım: Verilen sayıyı sağdan sola doğru çift haneli olarak gruplara ayırırız.

2.adım: Ondalık olarak kaç basamak yaklaşık değer bulucaksak, verilen sayıyı, o ondalık basamak adeti kadar genişletiriz.

2 sayısını, üç ondalık basamağa kadar yaklaşık değerini bulmak için 2,0000 şeklinde yazarız.

2 sayısının karekökünü bulmak için 2 sayısından küçük, 2 sayısına yakın en büyük tam kare sayıyı buluruz,

$$1^2 = 1 \leq 2,$$

2 sayısından 1 sayısını çıkarırız: $2 - 1 = 1$,

Kalan olarak, ondalıklı kısmın ilk çiftini alarak 100 sayısını elde ederiz.

3.adım: Önceki adımda elde edilen tam kare sayının 2 katını alırız,

$$1 \cdot 2 = 2.$$

4.adım: Önceki adımda elde edilen sayının sağına bir rakam ekleyip, elde edilen yeni sayıyla o rakamla çarpımını bulunarak, iki önceki adımda elde edilen sayıya yakınlaşırız.

2 sayısının sağına 4 eklenerek 24 sayısını elde ederiz ve 24 sayısı 4 sayısıyla çarpılarak 96 sayısını elde ederiz. Bu sayı 100 sayısından çıkarılarak kalan 4 sayısını buluruz.

Tahminimiz 1,4 olur.

5.adım: Kalan olarak, ondalıklı kısmın ikinci çiftini alarak 400 sayısını elde ederiz.

Tahminimizden hareketle $14 \cdot 2 = 28$ sayısını buluruz ve bu sayının sağına bir rakam ekleyip elde edilen sayıyla o rakamı çarparak 400 sayısına yakınlaşırız. 281 sayısıyla 1 sayısı çarpılarak 281 sayısını elde ederiz. Bu sayı 400 sayısından çıkarılarak kalan 119 sayısını buluruz.

Tahminimiz 1,41 olur.

6.adım: Kalan olarak ondalıklı kısmın son çiftini indirerek 11.900 sayısını elde ederiz.

Tahminimizden hareketle $141 \cdot 2 = 282$ sayısını buluruz ve bu sayının sağına bir rakam ekleyip elde edilen sayıyla o rakamı çarparak 11.900 sayısına yaklaşırız. 2824 sayısıyla 4 sayısı çarpılarak 11.296 sayısını elde ederiz. Bu sayı 11.900 sayısından çıkarılarak kalan 604 sayısını buluruz.

Tahminimiz 1,414 olur.

2 sayısının karekökü yaklaşık olarak 1,414 olacaktır. Daha fazla hassasiyet için işlem devam ettirilebilir.

Soru: $\sqrt{2}$ irrasyonel sayısının yaklaşık değerini Newton-Raphson modeliyle bulunuz.

Binom Açılımı

Sayı Teorisi çalışmalarında sıklıkla kullanılabilecek sayma tekniklerinden biri de kombinasyon ismini verdiğimiz, aşağıdaki şekilde tanımlanacak olan yapıdır.

Tanım: $0 \leq r \leq n$ ve n ve r herhangi iki tam sayı olmak üzere,

$$\binom{n}{r} = \frac{n!}{r!\,(n-r)!}$$

şeklinde tanımlanan yapıya kombinasyon veya binom katsayıları denir.

Kombinasyon veya binom katsayıları, $n \geq 1$ olmak üzere, $(a+b)^n$ ifadesinden elde edilen bir özelliktir:

$(a+b)^0 = 1$

$(a+b)^1 = a+b$

$(a+b)^2 = a^2 + 2ab + b^2$

$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$

$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$ işlemi devam ettirilerek aşağıdaki genel yazıma ulaşılmaktadır:

$(a+b)^n =$

$$\binom{n}{0}a^n b^0 + \binom{n}{1}a^{n-1}b^1 + \cdots + \binom{n}{n-1}a^1 b^{n-1} + \binom{n}{n}a^0 b^n.$$

Bu açıklamadan yola çıkarak aşağıdaki tanım verilebilir.

Tanım: $0 \leq r \leq n$ ve n ve r herhangi iki tam sayı olmak üzere,

$$(a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^{n-r} b^r$$

şeklinde tanımlanan yapıya binom açılımı denir.

Örnek: $(x+y)^{10}$açılımında x^6y^4 teriminin katsayısını bulalım.

Çözüm: x^6y^4 teriminin kuvvetlerinden $r = 4$ olarak bulunur. $\binom{n}{r}a^n b^{n-r}$ ifadesinde, $n = 10$ ve $r = 4$ alındığında, $\binom{10}{4}a^6b^4 = \frac{10\cdot 9\cdot 8\cdot 7}{4\cdot 3\cdot 2\cdot 1}x^6y^4 = 210x^6y^4$ sonucu elde edilir. x^6y^4 teriminin katsayısının 210 olduğu görülür.

Örnek: $1^2 + 2^2 + 3^2 + \cdots + n^2$ değerini bulalım.

Çözüm: $(k+1)^3 - k^3 = 3k^2 + 3k + 1$ eşitliğini binom açılımından elde ederiz. Eşitliğin her iki tarafını, 1 sayısından $(n+1)$ sayısına kadar toplayalım.

$$2^3 - 1^3 = 3 \cdot 1^2 + 3 + 1$$

$$3^3 - 2^3 = 3 \cdot 2^2 + 6 + 1$$

$$4^3 - 3^3 = 3 \cdot 3^2 + 9 + 1$$

$$\vdots \quad = \quad \vdots$$

$$(n+1)^3 - n^3 = 3 \cdot n^2 + 3 \cdot n + 1$$

Eşitliğin her iki tarafı taraf tarafa toplanınca,

$$(n+1)^2 - 1 = 3 \cdot \sum_{k=1}^{n} k^2 + 3 \cdot \frac{n(n+1)}{2} + n \cdot 1$$

sonucuna ulaşırız. Eşitlik düzenlendiğinde,

$$(n+1)^2 - 1 - \frac{3n(n+1)}{2} - n = 3 \cdot \sum_{k=1}^{n} k^2,$$

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6},$$

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6},$$

değerini elde ederiz. Binom katsayılarının temsillerinden biri adını Pascal(MS 1623-1662)'dan alan Paskal üçgenidir.

$n = 0$						1						
$n = 1$					1		1					
$n = 2$				1		2		1				
$n = 3$			1		3		3		1			
$n = 4$		1		4		6		4		1		
$n = 5$	1		5		10		10		5		1	
$n = 6$	1		6		15		20		15		6	1
$\vdots$						$\vdots$						

Pascal üçgenindeki herhangi bitişik iki sayının toplamı, bu iki sayı arasında bir sonraki satırda yer alan sayıyı vermektedir. Örneğin; beşinci satırda yer alan 4 ve 6 bitişik sayılarının toplamı, bu iki sayı arasında bir sonraki satırda yer alacak 10 sayısını verir.

Binom katsayılarının bazı özellikleri şunlardır:

i. $\binom{n}{0} = \binom{n}{n} = 1$

ii. $\binom{n}{r} + \binom{n}{r-1} = \binom{n+1}{r}$

iii. $\binom{n}{k}\binom{k}{r} = \binom{n}{r}\binom{n-r}{k-r}$

iv. $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n$

v. $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^n \binom{n}{n} = 0$

vi. $0\binom{n}{0} + 1\binom{n}{1} + 2\binom{n}{2} - \cdots + n\binom{n}{n} = n2^{n-1}$

vii. $\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \binom{n}{6} + \cdots = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \binom{n}{7} + \cdots = 2^{n-1}$

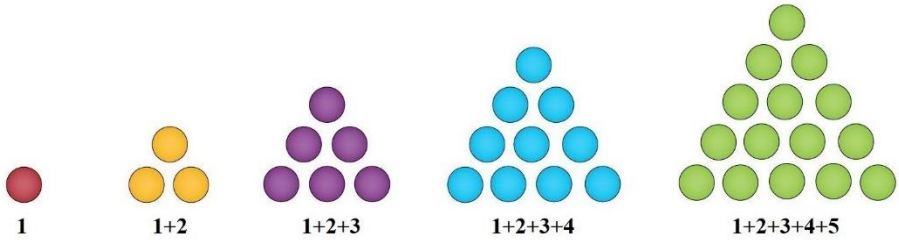
Örnek: $\binom{n}{0} + \binom{n+1}{1} + \binom{n+2}{2} = \binom{n+3}{2}$ eşitliğinin sağlandığını gösterelim.

Çözüm: $\binom{n}{0} = \frac{n!}{0!(n-0)!} = 1$, $\binom{n+1}{1} = \frac{(n+1)!}{1!(n+1-1)!} = (n+1)$, $\binom{n+2}{2} = \frac{(n+2)!}{2!(n+2-2)!} = \frac{(n^2+3n+2)}{2}$ ve $\binom{n+3}{2} = \frac{(n+3)!}{2!(n+3-2)!} = \frac{(n^2 5n+6)}{2}$ değerleri elde edilir.

$$1 + (n+1) + \frac{(n^2+3n+2)}{2} = \frac{2 + (2n+2) + (n^2+3n+2)}{2} = \frac{(n^2+5n+6)}{2}$$

işlem sonucundan eşitlik elde edilir.

Soru:



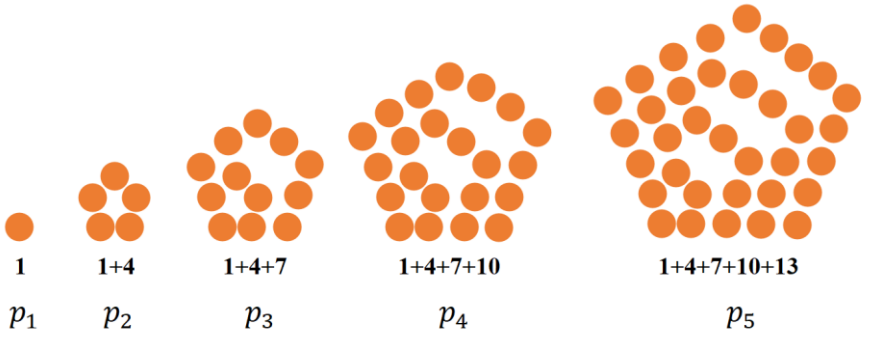
n. üçgensel sayı $t_n = \frac{n(n+1)}{2}$ şeklinde tanımlanmaktadır. $n \geq 1$ olmak üzere,

i) $t_n = \binom{n+1}{2}$,

ii) $t_1 + t_2 + t_3 + \cdots + t_n = \frac{n(n+1)(n+2)}{6}$, eşitliklerinin sağlandığını gösteriniz.

Soru: $\binom{2}{2} + \binom{3}{2} + \binom{4}{2} + \binom{5}{2} + \cdots + \binom{n}{2} = \binom{n+1}{3}$ eşitliğini $n \geq 2$ olmak üzere her tam sayı için geçerli olduğunu gösteriniz.

Soru:



n. beşgensel sayı $p_n = \frac{n(3n-1)}{2}$ şeklinde tanımlanmaktadır. $n \geq 1$ olmak üzere, $p_n = p_{n-1} + (3n-2)$ olduğunu gösteriniz.

Soru: $2^2 + 4^2 + 6^2 + \cdots (2n)^2 = \binom{n+2}{3}$ eşitliğinin sağlandığını gösteriniz.

UYGULAMALAR

1) $2m + 1 < 2^m$ eşitsizliğinin $m \geq 3$ her pozitif tam sayı için doğru olduğunu gösteriniz.
2) $2^n > n^2$ eşitsizliğinin $n \geq 5$ her pozitif tam sayı için doğru olduğunu gösteriniz.
3) $a \geq 1$ olmak üzere, $\frac{a(a^2+2)}{3}$ işlem sonucunun bir tam sayı olduğunu gösteriniz.
4) Ardışık herhangi üç tam sayıdan birinin 3 tam sayısıyla bölündüğünü gösteriniz(p bir tam sayı olmak üzere, herhangi bir tamsayının $3p$, $3p \mp 1$ formunda yazılabileceğini göz önüne alınız).
5) $k \geq r$, k ve r iki tam sayı olmak üzere $r|k!$ olduğunu gösteriniz.
6) $M = 1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + n \cdot n!$ sayısının [2, (n+1)] aralığındaki hiçbir tam sayıya bölünemediğini gösteriniz.
7) $4q + 1$ formundaki tam sayılar kümesinin çarpma işlemine göre kapalı olduğunu gösteriniz.
8) $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$ olduğunu gösteriniz.
9) 11 tam sayısıyla bölünebilme kuralını gösteriniz.
10) Bir tam sayının karesinin $3p$ ya da $3p + 1$ formunda yazılabileceğini gösteriniz.
11) $\binom{n}{0} + \binom{n+1}{1} + \binom{n+2}{2} + \cdots + \binom{n+k}{k} = \binom{n+k+1}{k}$ olduğunu gösteriniz.
12) $n \geq 1$ tek tam sayı ve $r = \frac{1}{2}(n-1)$ olmak üzere $\binom{n}{r} = \binom{n}{r+1}$ eşitliğinin geçerliliğini gösteriniz.
13) Catalan Eşitliği olarak tanımlanan, $n \geq 0$ her doğal sayısı için sağlanan $C_n = \frac{1}{n+1}\binom{2n}{n} = \frac{(2n)!}{n!(n+1)!}$ eşitliğini kullanarak, $C_n = \frac{2(2n-1)}{n+1} C_{n-1}$ eşitliğinin doğruluğunu gösteriniz.
14) $\frac{1}{2!} + \frac{2}{3!} + \frac{3}{4!} + \cdots + \frac{n-1}{n!}$ toplamının hiçbir zaman tam sayı olamayacağını gösteriniz.
15) $n \leq p \leq 2n$ olmak üzere p asal sayısının olduğunu gösteriniz (Bertrand's Postulate).
16) İki tek tam sayının kareleri farkının 8 sayısıyla bölünebildiğini gösteriniz.

17) $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + n \cdot (n+1) = \frac{n(n+1)(n+2)}{3}$ olduğunu gösteriniz.

18) $1^2 + 3^2 + 5^2 + \cdots + (2n-1)^2 = \binom{2n+1}{3}$ olduğunu gösteriniz.

19) $n^2 < n!$ Eşitsizliğinin $n \geq 4$ her pozitif tam sayı için gerçeklendiğini gösteriniz.

20) t_n, n. üçgensel sayı; p_n, n. beşgensel sayı ve $n \geq 1$ olmak üzere,

i) $p_n = t_{n-1} + n^2$,

ii) $p_n = 3t_{n-1} + n$,

iii) $p_n = 2t_{n-1} + t_n$, eşitliklerinin sağlandığını gösteriniz.

2. BÖLÜM

TAM SAYILARDA BÖLÜNEBİLME

Matematik evrenin doğal bir dilidir. Bir tür olarak varlığımızın en başından beri sayılar bizi derinden büyülemiştir. "Matematiğin Prensi" Carl Friedrich Gauss'a göre, sayı teorisi, gerçek sayılar kümesine ait sayılar arasında bir ilişki kuran, matematiğin en eski dallarından biri olmuştur. Sayı Teorisinin sadeliği, Gauss'un "Matematiğin Kraliçesi" olarak tanımladığı branşa katkıda bulunan matematikçileri büyülemiştir. Sayı Teorisi, günümüzde, teknoloji yazılım mühendisliğinin, özellikle güvenlik tabanlı yazılımın mutlak öncüsü sayılmaktadır. Sayı Teorisi, ünlü RSA (Rivest-Shamir-Adleman) algoritmasından blok zinciri dünyasına kadar sürükleyici bir hızlı evrim dönemi yaşayan kriptografinin kalbinde yer almıştır.

Tarihteki iki belirgin an, Sayı Teorisinin gelişiminde öne çıkmaktadır. İlk olarak, arkaik zamanlarda, Euclid kendi "en büyük ortak bölen" algoritmasını, geometrik gözlemler kullanarak kesirleri en basit biçimlerine sadeleştiren muhteşem bir adımlar dizisi ortaya koymuştur. Ardından, yaklaşık iki bin yıl sonra Gauss, Öklid'in Disquistiones Aritmeticae'deki kapsamlı kanıtlarıyla, çalışmalarını birleştirerek Öklid'in ilkelerini resmileştirmiştir.

Tanım: a, b tam sayılar olmak üzere $b = a \cdot k$ olacak şekilde bir k tam sayısı varsa a tam sayısı b tam sayısını böler denir. $a|b$ şeklinde gösterilir. $a \nmid b$ sembolü de a tam sayısının b tam sayısını bölmediğini gösterir. Tanımdan hareketle, a tam sayısı b tam sayısını bölerse a tam sayısı b tam sayısının bir bölenidir veya b tam sayısı a tam sayısının bir katıdır denir. Eğer $a|b$ ve $1 < a < b$ olursa a tam sayısına b tam sayısının bir öz böleni, 1 ve b sayılarına b tam sayısının trivial böleni denir.

Tam sayılarda bölünebilmenin aşağıdaki özellikleri vardır:

i. $a|a$ (Yansıma Özelliği),
ii. $a|b$ ve $b|a$ olduğunda $a = \mp b$ (Simetri Özelliği),
iii. $a|b$ ve $b|c$ olduğunda $a|c$ (Geçişme Özelliği),
iv. $a|b$ olduğunda $\forall c \in \mathbb{Z}$ için $a|b \cdot c$,
v. $m \neq 0$ ve $a|b$ olduğunda $m \cdot a|m \cdot b$ (Genişletme Özelliği),
vi. $\pm 1|a$,
vii. $\pm a|0$,
viii. $a|b, a > 0$ ve $b > 0$ olduğunda $b \geq a$,
ix. $a|b$ ve $a|c$ olduğunda $a|b \pm c$ (Toplama-Çıkarma Özelliği),
x. $a|b$ ve $c|d$ olduğunda $a \cdot c|b \cdot d$ (Çarpma Özelliği),
xi. $a|b$ ve $c|d$ olduğunda $\frac{a}{c}|\frac{b}{d}$ (Bölme Özelliği),
xii. $a|b$ ve $a \neq 0$ olduğunda $\frac{b}{a}|b$.

Teorem: (Kalanlı Bölme Teoremi) Herhangi $a > 0$ ve b tam sayıları için $b = aq + r$ ve $0 \leq r < a$ olacak şekilde bir tek q ve r tam sayı çifti vardır.

İspat: S, u pozitif veya negatif bir tam sayı olmak üzere $(b - u \cdot a)$ şeklindeki tam sayıların kümesini göstersin. $S = \{y: y = b - u \cdot a\}$ olur.

$u = \begin{cases} -1, & b \geq 0 \\ b, & b < 0 \end{cases}$ olacak şekilde seçilecek olursa $(b - u \cdot a)$ negatif olamayacaktır. S kümesinin elemanları da negatif olmayan elemanlardan oluşur. İyi sıralama prensibine göre S kümesinin bir en küçük elemanı vardır. r, bu en küçük eleman olsun. q tam sayısı da u tam sayısının buna karşılık değeri olsun. Buradan $r = b - q \cdot a \geq 0$ olur. Bu eşitlikten $r - a = b - q \cdot a - a = b - (1 + q)a < 0$ elde edilir. Bu eşitlik de $b = aq + r$ ve $0 \leq r < a$ olmasını gerektirir.

q ve r tam sayılarının tek olduğunu gösterelim. Bunun için aynı şartları sağlayan diğer bir q_1 ve r_1 tam sayı çiftinin varlığını kabul edelim. $r = r_1$ olduğunu göstermeliyiz.

q ve r çiftiyle beraber q_1 ve r_1 çifti için $b = aq + r$, $0 \leq r < a$ ve $b = aq_1 + r_1$, $0 \leq r_1 < a$ olur. Eğer $r \neq r_1$ ise $0 < r_1 - r < a$ olacak şekilde $r < r_1$ olduğunu varsayabiliriz. Bu durumda $r_1 - r = a(q - q_1)$ ve buradan $a|r_1 - r$ elde ederiz. Bu durum ancak $r_1 - r = 0$ olmasıyla mümkündür. Sonuçta $r_1 = r$ ve $q_1 = q$ olur.

Teoremde $a > 0$ olduğunu kabul etmiştik. Bu hipotez gerekli değildir. Teoremi; $a \neq 0$ olmak üzere a, b tam sayıları için $b = aq + r$ ve $0 \leq r < |a|$ olacak şekilde bir tek q ve r tam sayı çifti vardır, şeklinde ifade edebiliriz. b tam sayısının a tam sayısına bölünmesiyle, bir tek şekilde elde edilen q ve r tam sayılarına sırasıyla bölüm ve kalan denir.

Örnek: Herhangi bir tam sayının karesinin $k \in \mathbb{Z}$ olmak üzere, $5k$ veya $5k \mp 1$ formunda olduğunu gösterelim.

Çözüm: Herhangi bir tam sayı $p \in \mathbb{Z}$ olmak üzere $5p$, $5p \mp 1$ veya $5p \mp 2$ formunda yazılabileceğini kabul edelim. Bu sayıların karelerini alalım.

$(5p)^2 = 25p^2 = 5 \cdot 5p^2 = 5k$

$(5p \mp 1)^2 = 25p^2 \mp 10p + 1 = 5 \cdot (5p^2 \mp 2p) + 1 = 5k + 1$

$(5p \mp 2)^2 = 25p^2 \mp 20p + 4 = 5 \cdot (5p^2 \mp 4p + 1) - 1 = 5k - 1$

Bir tam kare sayının $k \in \mathbb{Z}$ olmak üzere, $5k$ veya $5k \mp 1$ formunda olduğu görülür.

Soru: Herhangi bir tam sayının küpünün $p \in \mathbb{Z}$ olmak üzere, $9p$, $9p + 1$, $9p + 8$ veya $9p$, $9p \mp 1$ formunda olduğunu gösteriniz.

Soru: 3 tam sayısıyla bölünebilme kuralını gösteriniz.

Soru: b tam sayı olmak üzere, $(a^3 - a)$ sayısının 3 tam sayısıyla bölünebildiğini gösteriniz.

Soru: $(a + b)$ değeri 4 tam sayısıyla bölünebilirse, $(a - 3b)$ değerinin de 4 tam sayısıyla bölünebileceğini gösteriniz.

En Büyük Ortak Bölen

İkisi aynı anda birden sıfır olmayan b ve c tam sayılarının ortak bölenleri kümesi her zaman 1 ve (-1) tam sayılarını içeren sonlu bir tam sayılar kümesidir. Sıfırdan farklı herhangi bir tam sayının yalnızca sonlu sayıda bölenleri olduğundan $b = c = 0$ durumu dışında sonlu sayıda ortak bölenleri vardır. b ve c tam sayılarından en az biri sıfır değilse bu tam sayıların ortak bölenleri mevcuttur.

Tanım: $a|b$ ve $a|c$ şartlarını sağlayan a tam sayısına b ve c tam sayılarının bir ortak böleni denir.

b ve c tam sayılarının a gibi ortak bölenlerinin en büyük olanına "en büyük ortak bölen" denir. $(b, c) = a$ veya $EBOB(b, c) = a$ şeklinde gösterilir.

Örnek: 12 ve 18 tam sayılarının ortak bölenlerini bulalım ve bu ortak bölen sayıların en büyüğünü belirleyelim.

Çözüm: 12 tam sayısının bölenlerinin kümesi:

$B_{12} = \{\mp 1, \mp 2, \mp 3, \mp 4, \mp 6, \mp 12\}$

18 tam sayısının bölenlerinin kümesi:

$B_{18} = \{\mp 1, \mp 2, \mp 3, \mp 6, \mp 9, \mp 18\}$ şeklinde olacaktır.

12 ve 18 tam sayılarının ortak bölenlerinin kümesi:

$B_{12} \cap B_{18} = \{\mp 1, \mp 2, \mp 3, \mp 6\}$ şeklinde olur ve bu kümenin en büyük elemanı 6 tam sayısı olacaktır. Dolayısıyla. $(12,18) = 6$ veya $EBOB(12,18) = 6$ şeklinde gösterilecektir.

Euclid Algoritması

İki tam sayının en büyük ortak böleni, iki tam sayının pozitif bölenlerinin listelenmesi ve ortak bölenlerinin belirlenmesinin ardından en büyük ortak bölenin seçilmesiyle bulunabilmektedir. Bu durum büyük sayılar için sorun oluşturmaktadır. Bölüm algoritmasının tekrar tekrar uygulanmasını içeren daha verimli bir yapı, Euclid tarafından verilmiştir. Bu yöntemin Euclid'den önce de kullanıldığına dair tarihsel kanıtlar olsa da bugün bu sistem Euclid Algoritması olarak anılmaktadır.

Teorem: a ve b tam sayıları $a > b$ olmak üzere,

$a = bq_1 + r_1, \qquad 0 < r_1 < |b|$

$b = r_1q_2 + r_2, \qquad 0 < r_2 < r_1$

$r_1 = r_2q_3 + r_3, \qquad 0 < r_3 < r_2$

$\vdots = \qquad \vdots \qquad\qquad \vdots$

$r_{j-2} = r_{j-1}q_j + r_j, \qquad 0 < r_j < r_{j-1}$

$r_{j-1} = r_jq_{j+1} + 0.$

a ve b tam sayılarının en büyük ortak böleni yukarıdaki bölme algoritmasında sıfırdan farklı son kalandır. $(a, b) = ma + nb$ ifadesini gerçekleyen m ve n tam sayıları yukarıdaki denklemlerden $r_{j-1}, r_{j-2}, \cdots, r_2, r_1$ tam sayıları yok edilerek bulunur.

İspat: a ve b tam sayılarından biri yani $b = 0$ ise a ve b tam sayılarının ortak bölenler kümesi a tam sayısının bölenler kümesiyle aynı olacaktır. $a = b$ olduğunda a ve b tam sayı çiftinin ortak bölenler kümesi a tam sayısının bölenler kümesiyle aynı olacaktır. Şimdi a ve b tam sayılarına bölme algoritması uygulayabiliriz.

$a = bq_1 + r_1,\ 0 < r_1 < |b|$. Burada a ve b tam sayı çiftlerinin bölenler kümesi (b, r_1) sayı çiftinin bölenler kümesiyle aynıdır. $r_1 = 0$

ise a ve b tam sayı çiftinin ortak bölenleri $(b, 0)$ sayı çiftinin ortak bölenleridir. Eğer $r_1 > 0$ ise a ve b tam sayı ortak bölenlerini bulma (b, r_1) sayı çiftinin ortak bölenlerini bulma işlemine indirgenmiş olacaktır. Burada $|b| < |a|$, $r_1 < |b|$ olduğundan (b, r_1) sayı çiftine bölme algoritması uygulanabilir. $b = r_1 q_2 + r_2,\ 0 \leq r_2 < r_1$ olacaktır. Aynı düşünceyle (a, b) sayı çiftinin ortak bölenler kümesinin (r_1, r_2) sayı çiftinin ortak bölenler kümesiyle aynı olduğu görülecektir. $r_2 = 0$ ise a ve b tam sayı çiftinin ortak bölenleri $(r_1, 0)$ sayı çiftinin ortak bölenleridir. Eğer $r_2 > 0$ ise a ve b tam sayı ortak bölenlerini bulma (r_1, r_2) sayı çiftinin ortak bölenlerini bulma işlemine indirgenmiş olacaktır. Bu işleme art arda devam edildiğinde ya bir yerde bitecektir ya da devam edip gidecektir. İkinci durum hiçbir zaman mümkün olmayacaktır. Çünkü bu durum pozitif tam sayıların $b > r_1 > r_2 > \cdots > r_j > \cdots$ azalan dizisi sonsuz olamaz ve iyi sıralama prensibi gereği bir en küçük elemanı vardır ifadesiyle çelişecektir. Sonuçta $r_{j+1} = 0$ olacak şekilde bir j olacaktır. Bu durumda sıfırdan farklı r_j değeri için $r_j | r_{j-1}$ olmalıdır. Sondan bir önceki denklemlerden $r_j | b$ ve $r_j | a$ elde edilir. Şimdi d_1, a ve b tam sayılarının herhangi bir böleni olmak üzere ilk denklemden $d_1 | r_1$, ikinci denklemden $d_1 | r_2$ ve sondan bir önceki denklemden $d_1 | r_j$ olacaktır. Bu durum da bizi $r_j = (a, b)$ sonucuna götürecektir.

$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{j-1}, r_j) = (r_j, 0) = r_j$ elde edilir.

Örnek: 12378 ve 3054 sayılarının en büyük ortak bölenini Euclid algoritması uygulayarak bulalım.

Çözüm:

$12378 = 4 \cdot 3054 + 162$

$3054 = 18 \cdot 162 + 138$

$162 = 1 \cdot 138 + 24$

$138 = 5 \cdot 24 + 18$

$24 = 1 \cdot 18 + \mathbf{6}$

$18 = 3 \cdot 6 + 0$

Bu eşitliklerde yer alan sıfır sayısından farklı, en büyük pozitif kalan tam sayının: 6 sayısının; 12378 ve 3054 tam sayı çiftinin en büyük ortak böleni olduğunu gösterir.

Yukarıdaki eşitlikleri sondan başlayarak, art arda uygulayarak kalanları ortadan kaldırdığımızda:

$6 = 24 - 18$

$= 24 - (138 - 5 \cdot 24)$

$= 6 \cdot 24 - 138$

$= 6 \cdot (162 - 138) - 138$

$= 6 \cdot 162 - 7 \cdot 138$

$= 6 \cdot 162 - 7 \cdot (3054 - 18 \cdot 162)$

$= 132 \cdot 162 - 7 \cdot 3054$

$= 132 \cdot (12378 - 4 \cdot 3054) - 7 \cdot 3054$

$= 12378 \cdot 132 + 3054 \cdot (-535)$ eşitliğini elde ederiz.

$6 = 12378x + 3054y$ olacak şekilde x ve y değerlerinin varlığı görülebilir. 132 ve (-535) değerleri eşitliği gerçekleyen tek değerler olmayacaklardır. Eşitliğin her iki tarafına da $3054 \cdot 12378$ değerini eklediğimizde,

$6 = 12378 \cdot (132 + 3054) + 3054 \cdot (-535 - 12378)$

$= 12378 \cdot 3186 + 3054 \cdot (-12913)$ şeklinde başka bir çözümünü daha bulmak mümkün olacaktır.

$12378 = 4 \cdot 3054 + 162$

$3054 = 19 \cdot 162 - 24$

$162 = 7 \cdot 24 - 6$

$24 = (-4) \cdot (-6) + 0$ eşitlik serisi de en büyük ortak bölenin negatifini üretmeye uygundur.

Tanım: a ve b tam sayılarının en büyük ortak böleni d olmak üzere,

i. $d|a$ ve $d|b$,
ii. Eğer $e|a$ ve $e|b$ ise $d \geq e$ durumları geçerlidir.

Not: Hepsi birden sıfır olmayan $b_1, b_2, \dots, b_n$ tam sayılarının en büyük ortak böleni $(b_1, b_2, \dots, b_n) = d$ şeklinde gösterilir.

Soru: 10, 15 ve 25 tam sayılarının en büyük ortak bölenini bulunuz.

Tanım: İkisi aynı anda sıfır olmayan a ve b tam sayılarının en büyük ortak böleni 1 ise a ve b tam sayılarına aralarında asal sayılar denir. Başka bir ifadeyle $(a, b) = 1$ olan sayılara aralarında asal sayılar denir.

Teorem: b ve c tam sayılarının en büyük ortak böleni d ise $d = (b, c) = bm + cn$ olacak şekilde m ve n tam sayıları vardır.

İspat: m ve n tamsayılar olmak üzere $bm + cn$ şeklindeki lineer bileşimlerin kümesi D olsun. D kümesi bütün tam sayıları kapsadığı unutulmamalıdır. m ve n tam sayılarını $bm + cn$ en küçük pozitif tam sayı olacak şekilde D kümesinden seçelim. $bm + cn = k$ olarak belirleyelim. $k|b$ ve $k|c$ olduğunu göstermeliyiz.

$k \nmid b$ olduğunu kabul edelim. Bölme algoritmasına göre $b = qk + r$ ve $0 \leq r < k$ olacak şekilde q ve r tam sayı çifti olacaktır. Bu eşitlikten, $r = b - kq = b - (bm + cn) = b(1 - qm) + c(-qn)$ elde edilir ki bu $r \in D$ olmasını gerektirecektir. Bu sonuç k tam sayısının D kümesinin

en küçük elemanı olduğu kabulüyle çelişmektedir. Bu durumda $k|b$ olmalıdır. Benzer şekilde $k|c$ olacağı da gösterilir.

d, b ve c tam sayılarının en büyük ortak böleni olduğundan $b = dB$ ve $c = dC$ $(B, C \in Z)$ yazılabilir.

$k = bm + cn = dBm + dCn = d(Bm + Cn)$ elde edilir.

Buradan $d|k$ sonucu elde edilir. Bu sonuçtan $d \leq k$ sonucuna ulaşılır. Halbuki d en büyük ortak bölen olduğundan $d < k$ olamaz. Bu durumda $d = k = bm + cn$ olmalıdır. Bu da istenilendir.

$d|b$, $d|c$ ve $x, y \in \mathbb{Z}$ olmak üzere $d|bx + cy$ ifadesi "Lineerlik Özelliği" olarak isimlendirilir.

Teorem: a ve b tam sayıları ikisi aynı anda sıfır olmayan tam sayılar olmak üzere, a ve b tam sayılarının aralarında asal olması, $1 = am + bn$ olacak şekilde m ve n tam sayılarının olmasını gerektirmektedir.

İspat: a ve b tam sayıları aralarında asal sayılarsa $(a, b) = 1$ olur. Bir önceki teoremimizden $1 = am + bn$ olacak şekilde m ve n tam sayılarının olacağını ifade edebiliriz. Bu eşitliğin bazı m ve n değerleri için doğru ve $(a, b) = e$ olduğunu kabul edelim. $e|a$ ve $e|b$ ifadelerinden $e|(am + bn)$ veya $e|1$ elde edilir ki bu da $e = 1$ olacağını gösterir. Bu sonuçtan da istenilene ulaşılır.

Örnek: $(a, b) = 1$, $a|c$ ve $b|c$ ise $ab|c$ olacağını gösterelim.

Çözüm: $a|c$ ve $b|c$ olduğundan $c = ar = bs$ ve $(a, b) = 1$ olduğunda lineerlik özelliğinden $1 = ax + by$ değerlerini elde ederiz.

$c = 1 \cdot c = c(ax + by) = acx + bcy$

$c = a(bs)x + b(ar)y = ab(sx + ry)$

$c = ab \cdot t$

elde edilir. Son eşitlikten $ab|c$ olacağı görülecektir.

Euclid Lemması

Tanım: a ve b tam sayıları ikisi aynı anda sıfır olmayan tam sayılar olmak üzere, $(a,b)=1$ ve $a|bc$ ise $a|c$ olur.

$(a,b)=1$ ve lineerlik özelliğinden $1=am+bn$ yazılabilir. Eşitliğin her iki tarafı c tam sayısıyla çarpılırsa $c=cam+cbn$ elde edilir. $a|bc$ ve $a|am$ ise $a|c$ elde edilir.

Teorem: a ve b tam sayıları arasında bölme algoritması $a=qb+r$ uygulanırsa $(a,b)=(b,r)$ eşitliği vardır.

İspat: $(a,b)=d$ ve $(b,r)=e$ olsun. $d|a$, $d|b$ ve $d|(a-qb)$ özelliğinden $d|r$ elde edilir. Bu da bize $d|e$ sonucunu verir. Benzer şekilde $e|b$, $e|r$ ve $e|(bq+r)$ özelliğinden $e|a$ elde edilir. Bu da bize $e|d$ sonucunu verir. Böylece $d=e$ elde edilir.

Örnek: 10672 ve 4147 tam sayılarının en büyük ortak bölenini bulalım.

Çözüm:

$10672 = 4147 \cdot 2 + 2378$

$4147 = 2378 \cdot 1 + 1769$

$2378 = 1769 \cdot 1 + 609$

$1769 = 609 \cdot 2 + 551$

$609 = 551 \cdot 1 + 58$

$551 = 58 \cdot 9 + 29$

$58 = 29 \cdot 2 + 0$

$(10672,\ 4147)=(4147,\ 2378)=(2378,\ 1769)=(1769,\ 609)=(609,\ 551)=(551,58)=(58,29)=29$ en büyük ortak bölen olacaktır.

Örnek: $29 = 10672x + 4147y$ şeklinde ifade edelim.

Çözüm:

$29 = 551 - 58 \cdot 9$

$29 = 551 - 9 \cdot (609 - 551 \cdot 1) = 10 \cdot 551 - 9 \cdot 609$

$29 = 10 \cdot (1769 - 609 \cdot 2) - 9 \cdot 609 = 10 \cdot 1769 - 29 \cdot 609$

$29 = 10 \cdot 1769 - 29 \cdot (2378 - 1769) = 39 \cdot 1769 - 29 \cdot 2378$

$29 = 39 \cdot (4147 - 2378) - 29 \cdot 2378 = 39 \cdot 4147 - 68 \cdot 2378$

$29 = 39 \cdot 4147 - 68 \cdot (10672 - 2 \cdot 4147) = (-68) \cdot 10672 + 175 \cdot 4147$

$29 = 10672 \cdot (-68) + 4147 \cdot (175)$

İşlem sonuçlarından $x = -68$ ve $y = 175$ olur.

Teorem: a, b ve $k > 0$ tam sayılar olmak üzere, $(ka, kb) = k(a, b)$ olur.

İspat: a ve b tam sayılar, $a > b$ olmak üzere, Euclid algoritması eşitliklerinin her iki tarafı $k > 0$ tam sayısıyla çarpılırsa

$ak = bkq_1 + kr_1, \qquad 0 < kr_1 < k|b|$

$bk = r_1kq_2 + kr_2, \qquad 0 < kr_2 < kr_1$

$r_1k = r_2kq_3 + kr_3, \qquad 0 < kr_3 < kr_2$

$\vdots = \qquad \vdots \qquad\qquad \vdots$

$r_{j-2}k = r_{j-1}kq_j + kr_j, \qquad 0 < kr_j < kr_{j-1}$

$r_{j-1}k = r_jkq_{j+1} + 0.$

ka ve kb tam sayılarına Euclid algoritması uygulandığında en büyük ortak böleni kr_j olacaktır. $(ka, kb) = kr_j = k(a, b)$ olacağı görülecektir.

Sonuç: $k < 0$ olması durumunda $-k = |k| > 0$ olacağı aşikardır. $(ka, kb) = (-ka, -kb) = (|k|a, |k|b) = |k|(a, b)$ olur.

Sonuç: Aşağıdaki durumların geçerliliğini ispat edelim.

1) $m \in \mathbb{Z}$ olmak üzere $(ma, mb) = |m|(a, b)$ olur.
2) $(a, b) = d$ olmak üzere $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ olur.
3) $(a, b) = (a + cb, b)$
4) $(a, b) = 1$ ise $(b - a, b) = 1$ elde edilir.
5) $(a, b) = 1$ ve $(a, c) = 1$ ise $(a, bc) = 1$ elde edilir.
6) $(a, b) = 1$ ve $c|(a + b)$ ise $(a, c) = (b, c) = 1$ elde edilir.
7) $(a, b) = 1$, $d|ac$ ve $d|bc$ ise $d|c$ olur.
8) $(a, b) = 1$ ise $(ac, b) = (c, b)$ olur.

İspat:

1) $(a, b) = d$ ve $e = (ma, mb)$ olsun. $e = |m|d$ olduğunu göstermeliyiz. $d = ap + bq$ yazılabilir. Eşitliği m sayısıyla genişletelim. $md = map + mbq$ olur. Bu eşitlikten md hem ma hem de mb değerlerini böleceğinden $md|e$ elde edilir. Ayrıca, $e|ma$ ve $e|mb$ olduğundan $e|md$ sonucuna ulaşılır. Buradan $|e| = |md|$ veya $e = |m|d$ elde edilir.

2) $e = \left(\frac{a}{d}, \frac{b}{d}\right) = 1$ olacak şekilde pozitif bir tam sayının olduğunu kabul edelim. Kabulümüzden $e|\frac{a}{d}$ ve $e|\frac{b}{d}$ yazılabilir. Buradan $(k_1, k_2) = 1$ olmak üzere $\frac{a}{d} = ek_1$ ve $\frac{b}{d} = ek_2$ eşitlikleri elde edilir. $a = dek_1$ ve $b = dek_2$ eşitliklerine ulaşılır. $e = 1$ ve $(k_1, k_2) = 1$ varsayımlarımızdan $e = \left(\frac{a}{d}, \frac{b}{d}\right) = 1$ elde edilir.

3) $(a, b) = d$ ve $(a + cb, b) = e$ olsun. $d|a$, $d|b$ ve lineerlik özelliğinden $d|a + bc$ olacaktır. Bu durumda $d|e$ elde edilir. $e|b$ ve $e|a + bc$ durumundan $e|a + bc - bc$ yazılabilir. Bu durumda da $e|d$ elde edilir. $d|e$ ve $e|d$ durumlarından $d = e$ sonucuna ulaşılır. $(a, b) = (a + cb, b)$ elde edilir.

4) a ve b pozitif tam sayılarının her ortak böleni d tam sayısıysa $(b-a)$ ve a sayılarının veya $(a-b)$ ve b sayılarının da her ortak böleni d tam sayısı olacaktır. Bu yüzden $(a,b)=1$ ise $(b-a,b)=1$ elde edilir.

5) $(a,b)=1$ ve $(a,c)=1$ ise lineerlik özelliğinden $1=am+bn=ap+cq$ olacak şekilde en az birer tane m,n,p ve q tam sayıları mevcuttur.

$1\cdot 1=(am+bn)(ap+cq)$

$1=a(amn+bnp+amp)+bcnp)$

$1=ak_1+bck_2$

işlemleri sonucunda $(a,bc)=1$ elde edilir.

6) $(a,b)=1$ ve lineerlik özelliğinden $1=am+bn$ yazılabilir. $c|(a+b)$ ise en az bir tane p tam sayısı için $cp=a+b$ oluşturulabilir. Bu eşitlikten $cp-b=a$ değeri kullanılarak,

$1=(cp-b)m+bn$

$1=cpm-bm+bn$

$1=cpm+b(n-m)=ck_1+bk_2$

$(c,b)=1$ elde edilir. Benzer yöntemle $(c,a)=1$ eşitliği de bulunur.

7) $(a,b)=1$ ve lineerlik özelliğinden $1=am+bn$ yazılabilir. Eşitliğin her iki tarafı c tam sayısıyla çarpılırsa $c=cam+cbn$ elde edilir. $d|ac$ ve $d|bc$ ise $d|c$ elde edilir.

8) $(c,b)=d$ olmak üzere $d|ab$ ve ayrıca $k|ac$ ve $k|b$ olması durumunda $k|d$ olduğunu göstermeliyiz. $d|c$ olduğundan $c=dn$ olacaktır, bu durumda $dna=ca$ olacağından $d|ca$ elde edilecektir. Lineer olma özelliğinden $d=au+cv$ yazılabilir. $k|ac$ ve $k|b$ kabulümüzden $kr=ac$ ve $kn=b$ olacaktır. $d=cu+knv$ elde edilir. $(a,b)=1$ eşitliğinden $1=ap+bq$ ve $c=cap+cbq$ yazılabilir.

$d=(acp+bqc)x+kny$

$d=axpc+bqcx+kny$

$d = krpx + knqcx + kny$

$d = k(rpx + nqcx + ny)$

$d|k$ elde edilir ki bu da istenendir.

Soru: $(a, b) = 1$ ve $c|a$ olduğunda $(b, c) = 1$ olacağını gösteriniz.

Örnek: $a|bc$ olduğunda $a|(a, b)(a, c)$ olacağını gösterelim.

Çözüm: $(a, b) = d$ ve $(a, c) = e$ olsun. $d = am + bn$ ve ve $e = ap + bq$ eşitliklerini yazabiliriz.

$d \cdot e = (am + bn)(ap + cq)$

$= a^2mp + acmp + banp + bcnq$

$= a(amp + cmp + bnp) + (bc)nq$

$a|bc$ eşitliği göz önüne alınarak $a|de$ elde edilir. Bu durum da bize $a|(a, b)(a, c)$ olacağını gösterir.

Soru: $(a, b) = 1$ olduğunda $(2a + b, a - 2b) = 1$ veya $(2a + b, a - 2b) = 3$ olacağını gösteriniz.

Soru: a ve b ikisi de sıfırdan farklı tam sayı olmak üzere, $(a, b) = (-a, b) = (a, -b) = (-a, -b)$ olduğunu gösteriniz.

Teorem: $b_1, b_2, b_3, \dots, b_r$ sıfırdan farklı tam sayılar olmak üzere, $(b_1, b_2, b_3, \dots, b_r) = ((b_1, b_2, b_3, \dots b_{r-1}), b_r)$ olur.

İspat: $(b_1, b_2, b_3, \dots, b_r) = d$ ve $((b_1, b_2, b_3, \dots b_{r-1}), b_r) = e$ olsun. (i=1, 2, 3, … , r) olmak üzere $d|b_i$ olduğundan, (i=1, 2, 3, … , r-1) olmak üzere $d|b_i$ olacağı açıktır. Bu durumda d|e elde edilir. Benzer şekilde e|d olduğu da gösterilir. Sonuçta d=e olacaktır.

Tam Sayılarda Modül

Tanım: Herhangi bir kümenin iki elemanının toplamı ve farkı yine o kümenin elemanı oluyorsa bu yapıya modül denir. $m, n \in S$ durumunda $(m \mp n) \in S$ olma durumu modül kavramıyla ifade

edilmektedir. Bütün sayı kümelerinin modülü bulunmaktadır. Tam sayıların modülü üzerinden işlemler gerçekleştirilecektir. $S = \{s = ax + by : a, b \in S; x, y \in \mathbb{Z}\}$ kümesi bir modül olarak ifade edilecektir.

Teorem: Sıfır modülü hariç S kümesinin elemanları bir pozitif tam sayının katlarını oluşturur.

İspat: S kümesinin en küçük pozitif tam sayısının d olduğunu kabul edelim. d tam sayısının bütün katları; $2d = d + d$, $3d = 2d + d$, ... S kümesine aittir. S kümesinin elemanlarının yalnızca bu sayılardan oluştuğunu göstermeliyiz. $n \in S$; $k, c \in \mathbb{Z}$ olmak üzere, $n = dk + c$, $0 \leq c < d$ yazılabilir. $d \in S$ olduğundan $dk \in S$ olacaktır. $n \in S$ olduğundan $(n - dk) \in S$ olacaktır. $c \in S$ olacaktır, $c < d$ ve d elemanı S kümesinin en küçük pozitif elemanı olduğundan $c = 0$ olmak zorundadır. Bu durumda istenilen gerçekleşecektir.

Teorem: $S = \{s = ax + by : a, b \in S; x, y \in \mathbb{Z}\}$ modülü $d = (a, b)$ sayısının bütün tam katlarının da bir kümesidir.

İspat: Önceki teoremden S kümesi pozitif k tam sayılarının tam katlarının bir kümesidir. Dolayısıyla k bu kümenin bütün elemanlarını böler, $k|a$ ve $k|b$ olacaktır. Bu durumda $k \leq d$ olacaktır. Bütün x ve y tam sayıları için $d|ax + by$ olur. d, S kümesinin bütün elemanlarını böler ve $d|k$ olacaktır. Bu durumda $d \leq k$ olacaktır. Buradan $d = k$ olduğu görülür.

Teorem: $ax + by = n$ denkleminin x ve y tam sayılarına göre çözülebilir olması için gerek ve yeter şart $d = (a, b)|n$ olmasıdır.
İspat: $d|a$ ve $d|b$ olması durumundan $d|ax + by$ ifadesinden $d|n$ olacaktır. $d|n$ olduğunda $d|ax + by$ olup, $d|ax$ ve $d|by$ olacaktır. Buradan da x ve y çözülebilirdir sonuca ulaşılacaktır.

En Küçük Ortak Kat

Sıfırdan farklı b ve c tam sayılarının ortak katlarının kümesi her zaman kendilerini de içeren sonsuz bir tam sayılar kümesidir. Sıfırdan farklı herhangi bir tam sayının sonsuz sayıda katları olacağından, b ve c sayılarının sonsuz sayıda ortak katları vardır.

Tanım: $a|m$ ve $b|m$ şartlarını sağlayan m tam sayısına a ve b tam sayılarının bir ortak katı denir. a ve b tam sayılarının m gibi ortak katlarının en küçük olanına "en küçük ortak kat" denir. $[a,b]=m$ veya $EKOK(a,b)=m$ şeklinde gösterilir.

Tanım: a ve b tam sayılarının en küçük ortak katı m olmak üzere,

i. $a|b$ ve $b|m$,
ii. Eğer $a|c$ ve $b|c$ ise $c \geq m$ durumları geçerlidir.

Örnek: 12 ve 18 tam sayılarının ortak katlarını bulalım ve bu ortak kat sayıların en küçüğünü belirleyelim.

Çözüm: 12 tam sayısının katlarının kümesi:

$K_{12}=\{12,24,36,48,60,72,84,96,108,120,\dots\}$

18 tam sayısının katlarının kümesi:

$K_{18}=\{18,36,54,72,90,108,126,144,162,180,\dots\}$

şeklinde olacaktır. 12 ve 18 tam sayılarının ortak katlarının kümesi: $K_{12}\cap K_{18}=\{36,72,108,\dots\}$ şeklinde olur ve bu kümenin en küçük elemanı 36 tam sayısı olacaktır. Dolayısıyla $[12,18]=36$ veya $EKOK(12,18)=36$ şeklinde gösterilecektir.

Not: Sıfırdan farklı $b_1,b_2,\dots,b_n$ tam sayılarının en küçük ortak katı $[b_1,b_2,\dots,b_n]=m$ şeklinde gösterilir.

Soru: 10, 15 ve 25 tam sayılarının en küçük ortak katını bulunuz.

Teorem: $[a,b]=m$ olması için gerek ve yeter şart $m>0$, $a|m$, $b|m$ ve a ile b tam sayılarının her n ortak katı için $m|n$ olmasıdır.

İspat: $[a,b]=m$ ve n, a ile b tam sayılarının herhangi bir ortak katı olsun. Bu durumda $m\leq n$ olacaktır. $m=n$ olursa $m|n$ olacaktır. Eğer $m<n$ olursa bölme algoritmasından $n=mq+r$, $0\leq r<m$ olacak şekilde q ve r tam sayıları vardır. Bu durumda $r=n-qm$ olur ve bölünebilmenin lineerlik özelliğinden r, a ve b tam sayılarının bir ortak katıdır. $r\neq 0$ durumu m tam sayısının tanımıyla çelişir. m tam sayısı en küçük ortak kat olduğundan $r=0$ olmalıdır ki $m|n$ sonucu elde edilir. $m>0$, $a|m$, $b|m$ ve a ile b tam sayılarının her n ortak katı için $m|n$ olsun. Bölünebilme özelliğinden $m\leq|n|$ olur ki m tam sayısı ortak katların en küçüğüdür.

Teorem: a ve b pozitif tam sayı olmak üzere $[a,b]=\frac{a\cdot b}{(a,b)}$ eşitliği sağlanır.

İspat: $p=\frac{a\cdot b}{(a,b)}$ tam sayısını inceleyelim. $(a,b)|b$ olduğundan p, a tam sayısının bir tam katı olacaktır. p, aynı düşünceyle b tam sayısının da bir tam katı olacaktır. Bu durumda p, a ve b tam sayılarının bir ortak katıdır. $q=[a,b]$ olmak üzere $\frac{q}{p}=\frac{q(a,b)}{a\cdot b}$ sayısını ele alalım. $(a,b)=ax+by$ lineerlik özelliğinden yazılabilir. Yukarıdaki eşitlikte bu ifadeyi yerine yazarsak $\frac{q}{p}=\frac{q(ax+by)}{a\cdot b}=\frac{qx}{b}+\frac{qy}{a}$ olacaktır. $\frac{q}{a}$ ve $\frac{q}{b}$ birer tam sayıdır. p, q tam sayısını böler ve p, a ve b tam sayılarının en küçük ortak katı olur. $\frac{1}{p}=\frac{ax+by}{a\cdot b}$ ifadesinden $p=\frac{a\cdot b}{(a,b)}$ elde edilir.

Teorem: $b_1, b_2, b_3, \dots, b_r$ sıfırdan farklı tam sayılar olmak üzere, $[b_1, b_2, b_3, \dots, b_r]=\left[[b_1, b_2, b_3, \dots b_{r-1}], b_r\right]$ olur.

İspat: $[b_1, b_2, b_3, \dots, b_r]=d$ ve $\left[[b_1, b_2, b_3, \dots b_{r-1}], b_r\right]=e$ olsun. $i=(1,2,3,\dots,r)$ olmak üzere $b_i|d$ olduğundan, $i=(1,2,3,\dots,r-1)$

olmak üzere $b_i|d$ olacağı açıktır. Bu durumda $d|e$ elde edilir. Benzer şekilde $e|d$ olduğu da gösterilir. Sonuçta $d = e$ olacaktır.

Soru: $(a, b) = [a, b]$ olması için gerek ve yeter şartın $(a, b) = 1$ olması gerektiğini gösteriniz.

Sonuç: Aşağıdaki durumların geçerliliğini ispat edelim.

1) a ve b sıfırdan farklı tam sayılar olmak üzere $(a, b) = [a, b]$ olması için gerek ve yeter şart $a = \mp b$ olmasıdır.
2) $k > 0$ olmak üzere $[ka, ka] = k[a, b]$ olur.
3) p, a ve b tam sayılarının ortak bir çarpanıysa $[a, b]|p$ olur.

İspat:

1) $(a, b) = [a, b] = d$ olsun. En büyük ortak bölen ve en küçük ortak kat özelliğinden $d = a \cdot b$ yazılabilir. $d|a$ olduğundan en az bir x tam sayısı için $d \cdot x = a$ elde edilebilir. $d^2 = dxb$ sonucu elde edilir. Bu eşitlik düzenlendiğinde $d = bx$ elde edilir, bu da bizi $b|d$ sonucuna götürür. Ayrıca $d|b$ olduğundan $d = \mp b$ sonucuna ulaşılır. Benzer şekilde $d = \mp a$ sonucuna da ulaşılır. Böylece $a = \mp b$ elde edilir. Yeter şart olarak $d = \mp a$ olsun. Bu durum bizi $a|b$ ve $b|a$ durumuna götürür. Böylece $(a, b) = [a, b]$ olacağı görülür.
2) $(ka, kb)[ka, kb] = k^2ab$ eşitliği en büyük ortak bölen ve en küçük ortak kat özelliğinden yazılabilir.

$k(a, b)[ka, kb] = k^2ab$

$(a, b)[ka, kb] = kab$

$(a, b)[ka, kb] = k(a, b)[a, b]$

$[ka, kb] = k[a, b]$ elde edilir.

3) $[a, b] = m$ olsun. Bölme algoritmasına göre $n = mq + r, 0 \leq r < m$ yazılabilir. Eğer $r = 0$ olursa $m|n$ olacaktır. Eğer $0 < r < m$ olursa $r = n - mq$ elde edilir. m ve n tam sayıları a ve b tam sayılarının çarpımı olduğundan $r = ax - ayq = a(x - yq)$ ve $r =$

$bu - bvq = b(u - vq)$ yazılabilir. Bu durum bize r tam sayısının a ve b tam sayılarının çarpımı olduğunu gösterir. Bu sonuç $[a, b] = m$ olmasıyla çelişir. $r < m$ olması mümkün değildir. Bu durum iddiamızı kanıtlamaktadır.

Soru: Sıfırdan farklı a ve b tam sayıları için aşağıdaki durumların sırasıyla gerçeklendiğini gösteriniz.

1. $(a, b) = |a|$,
2. $a|b$,
3. $[a, b] = |b|$.

Lineer Diophantine Eşitlikleri

Adını antik yunan matematikçilerinden Diophantus'dan (MS 214-298) alan, değişkenleri ve katsayıları tam sayılar olan denklemlerdir. a ve b ikisi de aynı anda sıfır olmayan tam sayılar, c, x ve y tam sayılar olmak üzere, $ax + by = c$ şeklindeki denklemlere Diophantine denklemleri denir.

Teorem: $ax + by = c$ Diophantine denkleminin çözümünün olması için gerek ve yeter şart $(a, b) = d$ olmak üzere $d|c$ olmasıdır. Ayrıca x_0 ve y_0 bu denklemin herhangi bir çözümü, $t \in \mathbb{Z}$ olmak üzere denklemin bütün çözümleri

$$x = x_0 + \left(\frac{b}{d}\right) t \text{ ve } y = y_0 + \left(\frac{a}{d}\right) t$$

şeklindedir.

İspat: Teoremin ikinci kısmı için x' ve y' verilen denklemin herhangi bir çözümü olsun. $ax_0 + by_0 = c = ax' + by'$ olsun. Bu eşitlikten $a(x' - x_0) = b(y_0 - y')$ elde edilir. $a = dr$ ve $b = ds$ eşitliğini sağlayan r ve s aralarında asal sayıları vardır. Önceki eşitlik yeniden düzenlendiğinde $r(x' - x_0) = s(y_0 - y')$ elde edilir. Bu durumda $r|s(y_0 - y')$ olur. (r, s)=1 olduğundan $r|(y_0 - y')$ olacaktır. Bu durumda bazı t gibi tam sayılar için $(y_0 - y') = rt$ eşitliğine

ulaşılır. Benzer şekilde $(x' - x_0) = st$ elde edilir. Elde edilen değerlerden

$$x' = x_0 + st = x_0 + \left(\frac{b}{d}\right) t \text{ ve } y' = y_0 - rt = y_0 - \left(\frac{a}{d}\right) t$$

sonuçlarına ulaşılır.

$$ax' + by' = a\left[x_0 + \left(\frac{b}{d}\right) t\right] + b\left[y_0 - \left(\frac{a}{d}\right) t\right]$$

$$= ax_0 + by_0 + \left[\left(\frac{ab}{d}\right) - \left(\frac{ab}{d}\right)\right] t$$

$$= c + 0 \cdot t$$

$$= c \text{ elde edilir.}$$

Örnek: $172x + 20y = 1000$ lineer Diophantine denkleminin çözüm kümesini bulalım.

Çözüm: Öklid algoritması uygulayarak 172 ve 20 sayılarının en büyük ortak bölenini bulalım.

$172 = 8 \cdot 20 + 12$

$20 = 1 \cdot 12 + 8$

$12 = 1 \cdot 8 + 4$

$8 = 2 \cdot 4 + 0$

$(172, 20) = 4$ olur. $4|1000$ olduğundan bu lineer Diophantine denkleminin çözümü vardır. Yukarıdaki eşitlikleri sondan başlayarak, art arda uygulayarak kalanları ortadan kaldırdığımızda,

$4 = 12 - 8$

$= 12 - (20 - 12)$

$= 2 \cdot 12 - 20$

$= 2 \cdot (172 - 8 \cdot 20) - 20$

$= 2 \cdot 172 + (-17) \cdot 20$

$4 \cdot 250 = 500 \cdot 172 + (-4250) \cdot 20$

$x_0 = 500$ ve $y_0 = (-4250)$ değerlerini elde ederiz. Diophantine denkleminin bütün çözümleri de t gibi tam sayılar için

$$x = 500 + \left(\frac{20}{4}\right) t = 500 + 5t$$

$$y = -4250 - \left(\frac{172}{4}\right) t = -4250 - 43t$$

şeklinde olacaktır.

Not: $(a, b) = 1$, x_0 ve y_0, $ax + by = c$ lineer Diophantine denkleminin özel çözümüyse bütün çözümler t gibi tam sayılar için

$$x = x_0 + bt \text{ ve } y = y_0 - at$$

şeklinde olacaktır.

Soru: $6x + 51y = 21$ lineer Diophantine denkleminin genel çözümünü bulunuz.

Soru: Bir kişi 51.000 lira tutarında eğitim çeki satın almak istemektedir. 2000 ve 5000 lira değerindeki çeklerin her birinden kaç tane satın alınması gerekmektedir.

UYGULAMALAR

1) $(a-1)$ sayısının (a^n-1) sayısının bir böleni olduğunu gösteriniz.
2) $c|e$ ve $d|e$ olmak üzere eğer $(c,d)=1$ ise $cd|e$ olduğunu gösteriniz.
3) a bir tam sayı olmak üzere, $a^{n+1}-(a-1)n-a$ sayısının $(a-1)^2$ sayısıyla bölünebildiğini gösteriniz.
4) $d|ac$ ve $d|bc$ ise $d|c$ olduğunu gösteriniz.
5) Herhangi tek tam sayının karesinin $8k+1$ formatında olduğunu gösteriniz.
6) a,b,c tam sayılar olmak üzere, $(a,bc)=1$ olması için gerek ve yeter şartın$(a,b)=(a,c)=1$ olması gerektiğini gösteriniz.
7) $a|(b+c)$ olması durumunda $a|b$ veya $a|c$ olup-olamayacağını gösteriniz.
8) Ardışık üç tam sayıdan birinin 3 sayısıyla bölünebildiğini gösteriniz.
9) $d|n$ olması durumunda $\left(2^d-1\right)|(2^n-1)$ olacağını gösteriniz.
10) a tek tam sayı olmak üzere, $24|a(a^2-1)$olacağını gösteriniz.
11) $(a,b)=1$ olması durumunda $(a+b,ab)=1$ olacağını gösteriniz.
12) a,b tam sayıları aralarında asal olmak üzere, $(a+b,a^2+b^2)=1$ veya $(a+b,a^2+b^2)=2$ olacağını gösteriniz.
13) $n\geq 1$, a,b pozitif tam sayı olmak üzere $a^n|b^n$ olursa $a|b$ olacağını gösteriniz.
14) a ve b pozitif tam sayı olmak üzere $(a,b)|[a,b]$ olduğunu gösteriniz.
15) $a|bc$ olması durumunda $a|(a,b)(a,c)$ olacağını gösteriniz.
16) $n\in\mathbb{N}$ olmak üzere $2n(2n+1)(2n+2)$ sayısını bölen en büyük doğal sayıyı bulunuz.
17) $21x-14y=49$ lineer Diophantine denklemini sağlayan bir değer bulunuz.

18) $a|b$ olması durumunda $(-a)|b$, $a|(-b)$ ve $(-a)|(-b)$ olacağını gösteriniz.

19) a ve b sıfırdan farklı tam sayılar olmak üzere,

   i. $(a,b) = [a,b]$ olması için gerek ve yeter şart $a = \pm b$ olmalıdır.

   ii. m, a ve b tam sayılarının bir ortak katıysa $[ka, kb]|m$.

20) Ardışık 4 tam sayının çarpımının 1 fazlasının bir tam kare sayıya eşit olacağını gösteriniz.

3. BÖLÜM

ASAL SAYILAR

Pozitif tam sayıların yukarı bölümlerde yer alan özelliklerine, birbiriyle çarpılarak veya birbirlerine bölünerek elde edilmesi özelliği de eklenebilir. 2 ve 3 sayılarının çarpımından 6, 1 ve 7 sayılarının çarpımından 7 sayısının elde edilebilirliği örnek verilebilir. 11 sayısının 1 ve 11 sayılarına, 10 sayısının 1, 2, 5 ve 10 sayılarına tam bölünebilirliği örnek verilebilir. Ayrıca 1 tam sayısından büyük a gibi tam sayıların ∓ 1 ve $\mp a$ tam sayılarına tam bölünebildiğini de yukarıdaki bilgilerimizden biliyoruz. Burada karşımıza, herhangi a gibi bir tam sayının ∓ 1 ve $\mp a$ tam sayı bölenlerinden başka tam sayı bölenlerinin olmadığı durumu ön plana çıkmaktadır.

Asal sayı, yalnızca 1 ve kendisi olmak üzere iki çarpana sahip olan bir tam sayıdır. Başka bir deyişle, bir asal sayı yalnızca 1 ve kendisi tarafından tam bölünebilir. Bilinen en büyük asal sayı $2^{136.279.841} - 1$ sayısıdır; bu sayı ondalık tabanda yazıldığında 41.024.320 basamağa sahiptir. Bu sayı, Great Internet Mersenne Prime Search (Büyük İnternet Mersenne Asal Sayı Araması) projesi kapsamında "Luke Duran"t tarafından keşfedilmiştir (31.12.2025). Öklid, en büyük asal sayının var olamayacağına dair bir ispat kaydetmiştir ve birçok matematikçi hala büyük asal sayılar aramaya devam etmektedir.

Bazı araştırmacılar, şifreli mesajları karıştırmak ve çözmek için asal sayıları kullanmıştır. Bu erken şifreleme biçimi, internet güvenliğinin yolunu açmış ve asal sayıları elektronik ticaretin kalbine yerleştirmiştir. Bu tür şifrelemenin güvenliği, iki büyük asal sayının çarpımı olan büyük bileşik sayıların çarpanlarına ayrılmasının zorluğuna dayanmaktadır.

Tanım: 1 sayısından büyük, 1 ve kendine tam bölünen pozitif tam sayılara asal sayı veya asal denir.

Tanım: 1 sayısından büyük, asal sayı olmayan tam sayılara da bileşik sayı denir.

2, 3, 5, 7, 11, 13, 17 ve 19 ilk sekiz asal sayıya, 4, 6, 8, 9, 10, 12, 14 ve 15 ilk sekiz bileşik sayıya örnektir.

Asal sayılar üzerine pek çok çalışmalar yapılmaktadır. Matematiğin iç dünyasının dışında diğer disiplinlerde de asal sayıları bulmak mümkündür. Güvenlik, biyoloji, zooloji, ekonomi gibi alanların asal sayıları kullandığı görülmektedir.

Teorem: p asal sayı ve $p|ab$ ise $p|a$ veya $p|b$ olur.

İspat: $p \nmid a$ olsun. p asal sayı olduğundan $(p, a) = 1$ olacaktır. Bu durumda $px + ay = 1$ yazılabilir. Eşitliğin her iki yanı b tam sayısıyla çarpıldığında $bpx + bay = b$ olacaktır. $p|bp$ ve $p|ab$ olduğundan $p|b$ elde edilecektir.

Teorem: p asal sayı ve $p|b_1 b_2 \dots b_n$ ise en az bir $i = (1, 2, 3, \dots, n)$ için $p|b_i$ olur.

İspat: $p|b_1 b_2 \dots b_n$ ise ya $p|b_1$ ya da $p|b_2 \dots b_n$ olacaktır. Benzer düşünceyle ya $p|b_2$ ya da $p|b_3 \dots b_n$ olacaktır. Bu düşünce sonlu adımda $p|b_1 b_2 \dots b_n$ ise en az bir $i = (1, 2, 3, \dots, n)$ için $p|b_i$ olura götürecektir.

Teorem: $p, p_1, p_2, \dots, p_n$ asal sayı ve $p|p_1 p_2 \dots p_n$ ise en az bir $i = (1, 2, 3, \dots, n)$ için $p = p_i$ olur.

İspat: $p|p_1 p_2 \dots p_n$ olursa bazı i değerleri için $p|p_i$ olacaktır. Her i değeri için p ve p_i asal sayı olduğundan ya $p = p_i$ ya da $p = 1$ olmalıdır. p asal sayı olduğundan $p = 1$ olamayacaktır.

Teorem: 1 sayısından büyük, herhangi pozitif bir tam sayı ya asal sayıdır ya da bileşik sayıdır.

İspat: Herhangi pozitif n tam sayısı asal sayıysa istenendir. Asal sayı değilse n tam sayısının 1 ile n arasında kalan bir böleni vardır. Bu bölen sayıların en küçüğü m ise m tam sayısı da asal sayıdır. Gerçekten m asal sayı olmasaydı en az bir l sayısı için $1 \leq l \leq m$, $l|m$ olacaktı. Buradan $l|m, m|n$ durumlarından $l|n$ olurdu ki bu da m tam sayısının tanımıyla çelişirdi. Bu durum bizi m tam sayısının asal sayı olma durumuna götürmektedir. O halde n ya asal sayıdır ya da n tam sayısından küçük p_1 asal sayısıyla bölünebilir. Bu durumda $n = p_1 n_1$, $1 < n_1 < n$ olacaktır. Burada n_1 asal sayıdır ki o zaman ispat bitecektir ya da n_1 sayısından küçük bir p_2 gibi bir asal sayıyla bölünecektir. Bu durumda $n = p_1 n_1 = p_1 p_2 n_2$, $1 < n_2 < n_1 < n$ olacaktır. Bu düşüncenin tekrar etmesiyle pozitif tam sayılardan oluşan $n, n_1, n_2, \dots, n_{k-1}, \dots$dizisine ulaşılacaktır. Bu dizi içinde iki durum düşünülebilir. İlk durumda uygun bir k değeri için $n_{k-1} = 1$ vardır. Bu durum bizi dizinin sonlu olmasına götürecektir. İkinci durumda k değeri ne olursa olsun $n_k > 1$ olur ki dizi sonsuzdur. Bu durum hiçbir zaman mümkün olamayacaktır. Dizinin oluşturuluş durumuna göre $n_k = p_{k+1} n_{k+1}$ olup $p_{k+1} > 1$ sayısından $n_k > n_{k+1}$ sayısı elde edilir. O halde, $n_1, n_2, \dots, n_{k-1}, \dots$ dizisi azalan bir dizidir. İyi sıralama prensibine göre n_m sayısı gibi bir en küçük elemana sahip olmalıdır. Bu nedenle dizi sonlu olamaz. Dizimiz sonlu olsaydı n_m sayısından sonra yukarıdaki uygulanan işlemle bir n_{m+1} sayısı elde edilirdi ki dizide n_m sayısından küçük bir pozitif tam sayı bulunmuş olurdu. Bu durumda n_m sayısının tanımına aykırı bir durum olurdu. $n > 1$ olmak üzere herhangi bir n tam sayısı, sonlu adımdan sonra $n_k = 1$ olacaktır. Yani

$n = p_1 n_1$

$n_1 = p_2 n_2$

$n_2 = p_3 n_3$

$\vdots \quad \vdots$

$n_{k-1} = p_k n_k$

$n_k = 1$, eşitliklerinden $n = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_k$ elde edilir. Burada p_i asal sayılarının birbirinden farklı olması gerekmez. Son haliyle $a_1, a_2, a_3, \ldots, a_k > 0$ ve $p_1 < p_2 < p_3 < \cdots < p_k$ olmak üzere $n = p_1^{a_1} p_2^{a_2} p_3^{a_3} \ldots p_k^{a_k}$ şeklinde yazılabilir ve n tam sayısının bu şekilde yazılmasına, n tam sayısının standart biçimi denir.

Teorem: $(a, b_i) = 1$ olduğunda $(a, b_1 b_2 \ldots b_n) = 1$ olur.

İspat: $(a, b_1 b_2 \ldots b_n) = d > 1$ olsun. Bu durumda öyle bir p asal sayısı için $p|d$ olacaktır. Diğer taraftan $d|a$, $d|b_1 b_2 \ldots b_n$ ve $p|d$ olduğundan $p|a$ ve $p|b_1 b_2 \ldots b_n$ olur. Bazı i değerleri için $p|b_i$ olacağı aşikardır. Sonuçta $p|a$ ve $p|d$ için $p|b_i$ elde edilir ki bu durum hipotezimizle çelişmektedir. $d = 1$ olmak zorundadır bu da istenilendir.

Teorem: $a|c, b|c$ ve $(a, b) = 1$ olduğunda $ab|c$ olur.

İspat: $a|c$ ve $b|c$ olmasından dolayı $c = ar = bs$ olacak şekilde r ve s tam sayıları vardır. $b|ar$ yazılabilir ama $(a, b) = 1$ olduğundan $b|r$ olacağı görülür. Bu durumda tekrar $r = bt$ olacak şekilde t tam sayısının varlığından bahsedilebilir. Son durumda $c = ar = abt$ sonucuna ulaşılır. Bu da bizi $ab|c$ sonucuna götürecektir.

Teorem: $m_1, m_2, \ldots, m_n$ ikişer ikişer aralarında asal sayı olmak üzere $i = (1, 2, 3, \ldots, n)$ için $m_i|a$ ise $m = m_1 m_2 \ldots m_n$ olduğunda $m|a$ olur.

İspat: İspatı indüksiyon yöntemiyle yapalım. $n = 1$ için $m_1|a$ ve $m = m_1$ olacağından $m|a$ olur. $n = k$ için ifadenin doğru olduğunu kabul edelim. Yani, $m = m_1 m_2 \ldots m_k$ olduğunda $m|a$ olacaktır. $n = k + 1$ için ifadenin doğruluğunu göstermeliyiz.

$(m_i, m_j) = 1$ olduğundan dolayı $m' = m_1 m_2 \ldots m_k$ olmak üzere $(m', m_{k+1}) = 1$ yazılabilir. Ayrıca $m'|a$ olacağı da unutulmamalıdır.

Üstelik $m_{k+1}|a$ olduğundan $m' \cdot m_{k+1}|a$ elde edilecektir. Bu durum bizi $n = k + 1$ için ifadenin $m|a$ olacağı sonucuna götürecektir ki bu da istenilendir.

Aritmetiğin Temel Teoremi

Asal sayılar başlığı altında gerçekleştirdiğimiz çalışmalar bizi sayılar konusunda ki gelişimimizin temel taşlarından birine götürmektedir. 1 sayısından büyük her tam sayı tek bir şekilde asal sayılara bölünebilmektedir.

Teorem: $n > 1$ tam sayısının standart yazım biçimi tektir. Çarpanlarının yerleri değişikliği dışında n tam sayısı asal sayıların çarpımı olarak tek türlü yazılabilmektedir.

İspat: p asal sayı olmak üzere $p|abc$ … 1 ise $p|a$ veya $p|b$ veya $p|c$ veya $\cdots$ $p|1$ olacaktır. Eğer $a, b, c, \ldots, 1$ sayıları 1 sayısı hariç asal sayıysa p sayısı bunlardan biri olmak zorundadır.

$n = p_1^{a_1} p_2^{a_2} p_3^{a_3} \ldots p_k^{a_k} = q_1^{b_1} q_2^{b_2} q_3^{b_3} \ldots q_j^{b_j}$ olduğunu varsayalım. Her i değeri için $p_i | q_1^{b_1} q_2^{b_2} q_3^{b_3} \ldots q_j^{b_j}$ olacağından her p sayısı bir q sayısı olacaktır. Benzer şekilde her q sayısı bir p sayısı olacaktır. Bu durumda $k = j$ olur. Ayrıca $p_1 < p_2 < p_3 < \cdots < p_k$ ve $q_1 < q_2 < \cdots < q_k$ küme elemanları artan sırada oluşturulduğunda her i değeri için $p_i = q_i$ olacaktır. Eşitliğimizin her iki tarafını $p_i^{b_i}$ sayısıyla bölelim. $a_i > b_i$ olması durumunda,

$p_1^{a_1} p_2^{a_2} p_3^{a_3} \ldots p_i^{a_i - b_i} \ldots p_k^{a_k} = p_1^{b_1} p_2^{b_2} p_3^{b_3} \ldots p_{i-1}^{b_{i-1}} p_{i+1}^{b_{i+1}} \ldots p_k^{b_k}$ elde edilir. Eşitliğin sol tarafı p_i sayısıyla bölünmesine rağmen sağ tarafı bölünmemiştir. Benzer şekilde $a_i < b_i$ olması durumunda da bu tür bir çelişkiye varılacaktır. Bu durumda $a_i = b_i$ elde edilir ki bu da ispat için istenendir.

Örnek: $p \neq 5$ tek asal sayı olmak üzere $p^2 - 1$ veya $p^2 + 1$ sayılarının 10 sayısıyla tam bölünebildiğini bulalım.

Çözüm: 5 asal sayısının dışındaki tek asal sayıları $10q+1$, $10q+3$, $10q+7$ ve $10q+9$ formları şeklinde yazmak mümkündür. Formlardan,

$p^2=(10q+1)^2=100q^2+20q+1$ ise $(p^2-1)=10(10q^2+2q)$ ve $10|(p^2-1)$

$p^2=(10q+3)^2=100q^2+60q+9$ ise $(p^2+1)=10(10q^2+6q+1)$ ve $10|(p^2+1)$

$p^2=(10q+7)^2=100q^2+140q+49$ ise $(p^2+1)=10(10q^2+14q+5)$ ve $10|(p^2+1)$

$p^2=(10q+9)^2=100q^2+180q+81$ise $(p^2-1)=10(10q^2+18q+8)$ ve $10|(p^2-1$, eşitlikleri elde edilir.

Örnek: $m>1$ tam sayısının kare sayısı olması için gerek ve yeter şartın m tam sayısının asal çarpanlarında ki tüm asal sayılarının üslerinin çift tam sayı olması gerektiğini gösterelim.

Çözüm: m tam sayısının tam kare sayı olduğunu kabul edelim. Bazı n gibi tam sayılar için $m=n^2$ yazılabilir. $n=p_1^{a_1}p_2^{a_2}p_3^{a_3}\dots p_i^{a_i}$ olduğunda $n^2=p_1^{2a_1}p_2^{2a_2}p_3^{a_3}\dots p_i^{2a_i}$ olacaktır ki m tam sayısının bütün asal çarpanları kuvvetinin iki olduğu görülür. m tam sayısının asal çarpanları kuvvetlerinin çift sayı olduğunu kabul edelim. $m=p_1^{a_1}p_2^{a_2}p_3^{a_3}\dots p_i^{a_i}$ tam kare bir sayı olduğundan $a_i=2b_i$ olmak üzere $m=p_1^{2b_1}p_2^{2b_2}p_3^{2b_3}\dots p_i^{2b_i}$ şeklinde yazılabilir. Bu durumda $m=\left(p_1^{b_1}p_2^{b_2}p_3^{b_3}\dots p_i^{b_i}\right)^2$ olacaktır.

Örnek: $n>2$ olmak üzere $n<p<n!$ eşitsizliğini sağlayan bir p asal sayısının varlığını gösterelim.

Çözüm: $n>2$ olmak üzere $n<n!-1<n!$ eşitsizliğini yazabiliriz. Eğer $(n!-1)$ asal sayıysa istenilendir. Eğer $(n!-1)$ asal sayı değilse $p<(n!-1)$ olacaktır. $p\leq n$ olduğunu farz edelim. Bu durumda p sayısı $1,2,3,\dots,n$ sayılarından biri olacaktır. Dolayısıyla $p|n!$ ve

$p|(n!-1)$ olacaktır. $(n!, n!-1) = 1$ olduğu da göz önüne alınırsa $p > n$ sonucuna ulaşılacaktır.

Soru: $p = 3n + 1$ şeklinde olan asal sayıların $6m + 1$ formatında da olacağını gösteriniz.

Örnek: Herhangi tek asal sayının $4k + 1$ veya $4k + 3$ formatında olacağını gösterelim.

Çözüm: Herhangi bir pozitif tam sayı, bölme algoritmasına göre, $r = 0, 1, 2, 3$ olmak üzere $p = 4q + r$ şeklinde yazılabilir.

$r = 0$ için $p = 4q = 2(2q)$ bir çift tam sayı belirtir,

$r = 1$ için $p = 4q + 1 = 2(2q) + 1$ bir tek tam sayı belirtir,

$r = 2$ için $p = 4q + 2 = 2(2q + 1)$ bir çift tam sayı belirtir,

$r = 3$ için $p = 4q + 3 = 2(2q) + 3$ bir tek tam sayı belirtir. Bu durumda herhangi bir tek asal sayının $4k + 1$ veya $4k + 3$ formatında olacağı görülür.

Eratosthenes Kalburu

Bir tam sayının asal/bileşik sayı olup olmadığının belirlenmesi, genel bir çözümünün bulunup bulunmadığını kolaylıkla söylemek mümkün görünmemektedir. Bir sayının asal sayılığı, Aritmetiğin Temel Teoremi yardımıyla bu sayının, en küçük asal sayıdan başlayarak bilinen asal sayılara art arda bölünmesiyle anlaşılabilmektedir. Ancak bu metot daha büyük asal sayıların varlığı nedeniyle çok büyük sayılar için uygulanması imkânsız hale gelmiştir.

Teorem: $n > 1$ bileşik tam sayısının $\sqrt{n}$ sayısından büyük olmayan bir asal çarpanı vardır.

İspat: n bileşik sayısını $1 < a \leq b < n$ olmak üzere $n = a \cdot b$ şeklinde yazalım. $a \leq \sqrt{n}$ olmalıdır. Bu durum söz konusu değilse $b \geq a > \sqrt{n}$ olmasını gerektirir ki bu sefer de $a \cdot b > n$ olması imkânsızdır. a tam

sayısını bölen, $p \leq a \leq \sqrt{n}$ olacak şekilde bir p asal sayısı olmalıdır. Ayrıca $p|a$ ve $a|n$ ise $p|n$ olur. Sonuç olarak p asal sayısı, $\sqrt{n}$ sayısından büyük olmayan, n bileşik sayısının bir çarpanı olacaktır.

Örnek: 509 sayısının asal olup olmadığını bulalım.

Çözüm: 509 sayısının karekök değerinin $22 < \sqrt{509} < 23$ aralığında bir değere karşılık geleceği görülebilir. 509 sayısının, 22 sayısından büyük olmayan asal sayılara bölünüp bölünmediğini kontrol etmeliyiz. Bahsi geçen asal sayılar: 2, 3, 5, 7, 11, 13, 17 ve 19 asal sayıları olacaktır. 509 sayısının bu asal sayılara bölünüp bölünmediğini kontrol ettiğimizde, bu asal sayılardan hiçbirine bölünmediği görülecektir. Sonuç olarak 509 sayısı asal sayı olacaktır.

$a > 1$ tam sayısından büyük herhangi bir tamsayının, kendisinden küçük herhangi bir asal sayıya bölünememesi durumunda a tam sayının asal sayı olduğu bilgisini önceki çalışmalarımızdan biliyoruz. Çalışmaları, Sayı Teorisinde önemli olmaya devam eden bir başka Yunan matematikçi Eratosthenestir. Eratosthenes, belirli bir n tam sayısının altındaki tüm asal sayıları bulmak için "Eratosthenes Kalburu" adı verilen bir teknik kullanmıştır. Bu metot, 2 tam sayısından itibaren verilen n tam sayısına kadar bütün tam sayıların bir liste şeklinde yazılmasına ve sonra bu listeden bileşik sayıların atılmasına dayanmaktadır. İlk olarak en küçük asal sayı olan 2 sayısından başlanır ve 2 sayısının, n tam sayısını geçmeyen bütün katları: 4, 6, 8, 10, … bu listeden çıkarılır. Sonra 3, daha sonra 5 ve diğer bütün asal sayılar için bu teknik sürdürülür. Her bileşik sayının kendisinin karekökünü geçmeyen bir asal sayı böleni olduğundan, listedeki her bileşik sayının $\sqrt{n}$ sayısını geçmeyen bir asal sayı böleni bulunacaktır. Böylece $\sqrt{n}$ sayısını geçmeyen her asalın bütün katları çıkarılarak, tüm bileşik sayılar

listeden çıkarılmış olacak ve geriye yalnızca n tam sayısını geçmeyen asal sayılar kalmış olacaktır.

Aşağıdaki tablo $n = 200$ sayısı için Eratosthenes Kalburunun nasıl uygulandığını göstermektedir.

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

151	152	153	154	155	156	**157**	158	159	160
161	162	**163**	164	165	166	**167**	168	169	170
171	172	**173**	174	175	176	177	178	**179**	180
181	182	183	184	185	186	187	188	189	190
191	192	**193**	194	195	196	**197**	198	**199**	200

Bu tablo incelendiğinde,

i. $14 < \sqrt{200} < 15$ olduğundan, listeden en son 13 asal sayının katları çıkarılarak 200 sayısına kadar asal sayıların elde edildiği görülecektir.

ii. 2 ve 5 sayılarının dışındaki bütün asal sayıların tablonun 1., 3. 7. ve 9. sütunlarında bulunduğu ve bu sütunlardaki asal sayıların değerinin birbirlerine yakın oldukları görülecektir.

iii. $10k + 1, 10k + 3, 10k + 7$ ve $10k + 9$ biçiminde sonsuz çoklukta asal sayının varlığından bahsedilebilecektir.

iv. Benzer şekilde $4k + 1$ ve $4k + 3$ şeklinde sonsuz çoklukta asal sayının olacağı görülecektir.

Teorem: (Euclid Teoremi) Sonsuz çoklukta asal sayı vardır.

İspat: $P = \{2, 3, 5, 7, \dots, p\}$ asal sayılar kümesi ve p sayısı da en büyük asal sayı olsun. Bu kümenin elemanları kullanılarak oluşturulan $q = 2 \cdot 3 \cdot 5 \cdot 7 \cdot \dots \cdot p + 1$ sayısını ele alalım. q sayısı $2, 3, 5, 7, \dots, p$ sayılarından biriyle bölünemez. Böylece q ya asal sayıdır ya da p ve q sayıları arasındaki bir asal sayıyla bölünür. Her iki durumda da p asal sayısından büyük bir asal sayı bulunabilecektir. Sonuç olarak asal sayılar sonsuz çoklukta olacaktır.

Teorem: (Dirichlet Teoremi) a ve b iki pozitif tam sayı ve $(a,b)=1$ olmak üzere $an+b$ şeklinde sonsuz çoklukta asal sayı vardır.

İspat: $(a,b)=d>1$ olduğunda her $n\geq 1$ sayısı için $d|an+b$ olacağından, $an+b$ sayısı hiçbir zaman asal olamayacaktır.

Teorem: a ve b iki pozitif tam sayı ve $(a,b)=1$ olmak üzere $an+b$ şeklinde sonsuz çokluktaki sayılar sadece asal sayılardan oluşmazlar.

İspat: $an+b=p$, şeklinde asal sayılardan oluştuğunu varsayalım. $n_k=n+kp, k\in\mathbb{N}^+$ olmak üzere,

$$a+n_kb=a+(n+kp)b=(a+nb)+kpb=p+kbp=p(1+kp)$$

şeklinde yazılabilir. $p|p(1+kp)$ olacağından $p|a+n_kb$ olacaktır. Bu durum varsayımımızla çelişmektedir. Sonuçta $an+b$ şeklinde sonsuz çokluktaki sayılar sadece asal sayılardan oluşmayacaklardır.

Teorem: p, bütün asal sayılar üzerinde değerler alabilen bir sayı olmak üzere $\sum_{i=1}^{\infty}\frac{1}{p}$ serisi ıraksaktır.

İspat: $2,3,5,7,\dots,p_j$ kümesini asalların ilk j tanesi olduklarını varsayalım. x sayısını geçmeyen ve p_j sayısından büyük olan herhangi bir p asalıyla bölünemeyen n doğal sayılarının kümesi de $N(x,j)$ olsun. Eğer böyle bir n sayısını, herhangi bir m asal sayısının karesiyle bölünemeyen bir sayı olmak üzere $n=n_1^2m$ biçiminde ifade ederek m sayısını $m=2^{\alpha_1}3^{\alpha_2}5^{\alpha_3}\dots p_j^{\alpha_j}$ şeklinde yazabiliriz. α değerleri 0 veya 1 olmak zorundadır. α üsleri için tam olarak 2^j seçim söz konusu olup, m için 2^j değerinden fazla farklı değer bulunamaz. Ayrıca $n_1\leq\sqrt{n}\leq\sqrt{x}$ olduğundan n_1 değerinin birbirinden farklı $\sqrt{x}$ değerinden fazla değeri bulunamaz. O halde istenilen biçimde n sayılarını en fazla $2^j\sqrt{x}$ sayıda oluşturabiliriz. $N(x,j)\leq 2^j\sqrt{x}$ olacaktır.

$\sum_{i=1}^{\infty}\frac{1}{p}$ serisinin yakınsak olduğunu varsayalım. $\sum_{i=1}^{\infty}\frac{1}{p}<\frac{1}{2}$ olacak biçimde, j. terimden sonraki kalan $\frac{1}{2}$ sayısından küçük olacak şekilde bir j indisi olacaktır. j bu özel değeri için $i>j$ olan bir takım p_i asallarıyla bölünebilen ve böylece $N(x,j)$ de sayılamayan $n\leq x$ olan tam sayılarının sayısını göz önüne alarak $N(x,j)$ değerini yeniden belirleyelim. Böyle bir i için k, $kp_i\leq x$ olacak şekilde en büyük tam sayı olmak üzere $p_i, 2p_i, \dots, kp_i$ tam sayıları $n\leq x$ olan n sayısının değerleridir. Bu halde, her $i>j$ için, n sayısının böyle en fazla $\frac{x}{p_i}$ değeri vardır. Buradan $N(x,j)$ değerinde sayılamayan $n\leq x$ eşitsizliğini gerçekleyen n sayısının değerlerinin sayısının en fazla $\sum_{i=j+1}^{\infty}\frac{x}{p_i}$ olduğu sonucuna varılacaktır. O halde $x-N(x,j)$; $p_{j+1}, p_{j+2}, \dots$ değerlerinden biri veya daha fazlasıyla bölünebilen ve $n\leq x$ olan n değerlerinin sayısıdır. $\sum_{i=1}^{\infty}\frac{1}{p}<\frac{1}{2}$ ifadesinden $x-N(x,j)\leq\sum_{i=j+1}^{\infty}\frac{x}{p_i}<\frac{x}{2}$ veya $\frac{x}{2}<N(x,j)$ bulunur. $N(x,j)\leq 2^j\sqrt{x}$ ifadesi yardımıyla her pozitif x tam sayısı için $\frac{x}{2}<2^j\sqrt{x}$ veya $x<2^{2j+2}$ elde edilir. Fakat pozitif tam sayılar kümesi sınırsız olduğundan bu sonuç açık olarak yanlış olacaktır. Bu durumda $\sum_{i=1}^{\infty}\frac{1}{p}$ serisi yakınsak olamayacaktır.

Teorem: $n>2$ ve p asal sayı olmak üzere,

$$p, p+d, p+2d, p+3d, \dots, p+(n-1)d$$

sayılarının hepsi asal sayıysa n doğal sayısından küçük her asal sayı d sayısını bölebilir.

İspat: n doğal sayısından küçük q asal sayısının d sayısını bölmediğini kabul edelim. $p, p+d, p+2d, p+3d, \dots, p+(q-1)d$ sayılarının q sayısıyla bölündüğünde farklı kalanları verdiğini varsayalım. j ve k tam sayıları $0\leq j<k\leq q-1$ olmak üzere $p+jd$ ve $p+kd$ sayıları q sayısıyla bölümünden aynı kalanı verecektir. Bu durumda $q|(k-$

$j)d$ olacaktır. $(q,d)=1$ eşitliği, $q|k-j$ olmasını gerektirecektir ki bu durum $k-j\leq q-1$ eşitsizliği için saçma olacaktır. Sonuçta bu kalanlardan biri sıfır olmalıdır. Bu da $0\leq t\leq q-1$ olacak şekilde bazı t değerleri için $q|p+td$ olması anlamına gelecektir. $p+td$ sayısının bileşik sayı olduğu görülecektir. $p<n$ olsaydı dizinin terimlerinden biri $p+pd=p(1+d)$ olurdu. Elde edilen çelişkiyle $q|p$ olduğu ispatlanmış olur.

Teorem: $4k+3$ biçiminde sonsuz çoklukta asal sayı vardır.

İspat: Bu biçimde $p_1, p_2, \dots, p_r$ gibi r tane sonlu sayıda asal sayı bulunduğunu varsayalım.

$$m=4\cdot p_1\cdot\ p_2\cdot\ \dots\cdot p_r-1=4(p_1\cdot\ p_2\cdot\ \dots\cdot p_r-1)+3$$

sayısını göz önüne alalım. m sayısı $4k+3$ biçiminde ve her i değeri için $m>p_i$olduğundan m sayısının bileşik sayı olacağı açıktır. $4k+1$ veya $4k+3$ biçiminde asal çarpanlarının bulunması gerektiği sonucuna varılır. $4k+1$ biçimindeki sayıların çarpımı yine bu biçimde olacağından m sayısının en az bir tane $4k+3$ biçiminde asal böleninin olacağı söylenebilir. Bu durumda bazı i değerleri için $p_i|m$ olacaktır. Fakat bu durumda da $p_i|1$ elde edilir ki bu durum varsayımımızla çelişir. Son durumda bu çelişki bizi $4k+3$ biçiminde sonsuz çoklukta asal sayı olduğunu gösterir.

Örnek: $p, q,$ 5 doğal sayısından büyük veya eşit asal sayılar olmak üzere, $24|p^2-q^2$ olacağını gösterelim.

Çözüm: 5 doğal sayısından büyük veya eşit olan asal sayılar tek sayı olmalıdır. Bu tür tek sayılar $4k\mp 1$ şeklinde düşünülebilir.

1.adım: Eğer iki asal sayı aynı kalanlıysa,

$$(p-q)(p+q)=4m(4n+2)=8t$$

2.adım: Eğer iki asal sayı farklı kalanlıysa,

$$(p-q)(p+q)=(4m+2)4n=8t$$

Bu tür tek sayılar $3k \mp 1$ şeklinde düşünülebilir

3.adım: Eğer iki asal sayı aynı kalanlıysa,

$$(p-q)(p+q) = 3m(3n \pm 1) = 3s$$

Eğer iki asal sayı farklı kalanlıysa,

$$(p-q)(p+q) = (3m \pm 1)3n = 3s$$

1. ve 2. adımda $8|(p-q)(p+q)$, 3. ve 4. adımda $3|(p-q)(p+q)$ olmaktadır. 3 ve 8 sayıları aralarında asal olduklarından dolayı, $24|(p-q)(p+q)$ olacaktır.

Euclid Sayıları

Bir asal sayıdan küçük veya eşit bütün asal sayıların çarpımıyla elde edilen sayılar, asal sayıların sonsuz çoklukta olduğunu göstermede kullanılmıştır. Bu çarpım $p^{\#}$ şeklide gösterilmek üzere; $p^{\#} + 1$ sayıları, Öklid Sayıları olarak isimlendirilir.

$2^{\#} + 1 = 2 + 1 = 3$

$3^{\#} + 1 = 2 \cdot 3 + 1 = 7$

$5^{\#} + 1 = 2 \cdot 3 \cdot 5 + 1 = 31$

$7^{\#} + 1 = 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$

$11^{\#} + 1 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$

sayılarının hepsi asal sayıdır. Ancak,

$13^{\#} + 1 = 59 \cdot 509$

$17^{\#} + 1 = 19 \cdot 97 \cdot 277$

$19^{\#} + 1 = 347 \cdot 27953$

sayıları asal sayı değildir. Öklid sayılarından hareketle aşağıdaki gibi sonsuz çoklukta elemanı olan sayı dizisini oluşturalım.

$n_1 = 2$

$n_2 = n_1 + 1$

$n_3 = n_2 \cdot n_1 + 1$

$n_4 = n_3 \cdot n_2 \cdot n_1 + 1$

$\vdots$

$n_k = n_{k-1} \cdot \ldots \cdot n_3 \cdot n_2 \cdot n_1 + 1$

$\vdots$

Bu sayı dizisinin her elemanı bir asal sayı tarafından bölünecektir. Ama bu sayılardan aynı asala bölünen iki sayı olmayacaktır. $i < k$ olmak üzere, $(n_i, n_k) = 1$ olacaktır. Bu durumda, p_n asal sayıların doğal sıralanışını göstermek üzere, $p_n \cdot \ldots \cdot p_3 \cdot p_2 \cdot p_1 + 1$ sayısı en az bir asal sayıya bölünebilecektir. p_{n+1} asal sayısı, $p_n \cdot \ldots \cdot p_3 \cdot p_2 \cdot p_1 + 1$ sayısından büyük olamayacaktır. Sonuç olarak,

$$p_n \leq p_{n-1} \cdot \ldots \cdot p_3 \cdot p_2 \cdot p_1 + 1, n \geq 2$$

elde edilebilir. Bu eşitsizliğin oldukça büyük bir değer aralığında olduğu görülebilir. Çalışmanın devamında Bonse,

$$p_n^2 \leq p_{n-1} \cdot \ldots \cdot p_3 \cdot p_2 \cdot p_1, n \geq 5$$

eşitsizliğini vermiştir. $n = 5$ için $p_5^2 < 210$ veya $p_5 \leq 14$ olduğu görülür. Daha iyi bir değer aralığıyla,

$$p_{2n} \leq p_n \cdot \ldots \cdot p_3 \cdot p_2 - 2, n \geq 3$$

eşitsizliği elde edilebilir. Bu eşitsizliklerden sonra aşağıdaki teorem verilebilir.

Teorem: p_n, n. asal sayı olmak üzere, $p_n \leq 2^{2^{n-1}}$ eşitsizliği geçerlidir.

İspat: İndüksiyon metoduyla ispatımızı yapalım. $n = 1$ için $2 \leq 2$ doğru olduğu görülür. $n > 1$ değeri için eşitsizliğimizin geçerli olduğunu göstermeliyiz.

Bu biçimde $p_1, p_2, \dots, p_r$ gibi r tane sonlu sayıda asal sayı bulunduğunu varsayalım.

$$p_{n+1} \leq p_n \cdot \dots \cdot p_3 \cdot p_2 \cdot p_1 + 1$$

$$p_{n+1} \leq 2^1 \cdot 2^2 \cdot \dots \cdot 2^{2^{n-1}} + 1 = 2^{1+2+2^2+\dots+2^{n-1}}$$

$1 + 2 + 2^2 + \dots + 2^{n-1} = 2^n - 1$ eşitliğinden faydalanılarak,

$$p_{n+1} \leq 2^{2^n-1} + 1$$

elde edilir. Ayrıca, $1 \leq 2^{2^n-1}$ olacağından,

$$p_{n+1} \leq 2^{2^n-1} + 2^{2^n-1} = 2 \cdot 2^{2^n-1} = 2^{2^n}$$

sonucuna ulaşılır ki bu durum da istenilendir.

Sonuç: $n \geq 1$ olması durumunda 2^{2^n} sayısından küçük, en az $n + 1$ tane asal sayı vardır.

Mersenne ve Fermat Sayıları

Bazı özel biçimdeki sayıların asal olup-olmadığını belirlemek için farklı metotlar ortaya atılmıştır. Bunlardan en çok tanınanı Mersenne ve Fermat Sayıları olmuştur. 2 sayısının pozitif bütün kuvvetlerinin çift sayı olduğu, $(2^n - 1)$ biçimindeki bütün sayıların da tek sayı olacağı bilinmektedir. 2 sayısının dışındaki bütün asal sayıların tek sayı olduğu ancak her tek sayının asal sayı olamayacağı da bir gerçektir. Asal sayıların genel teriminin ortaya konması adına pek çok çalışmalarda bulunulmuştur. Mersenne (MS 1588-1648) bilinen asallardan hareketle, p asal sayı olmak üzere, $(2^p - 1)$ biçimindeki sayıların da asal sayı olacağını ileri sürmüştür. Benzer şekilde, Fermat (MS 1607-1665) negatif olmayan her n tam sayısı için $\left(2^{2^n} + 1\right)$ biçimindeki sayıların da asal sayı olacağını ileri sürmüştür. Günümüz çalışmalarında her iki bilim insanının çalışmalarında hatalar olduğu ortaya konmuştur.

Mersenne, p asal sayı olmak üzere $(2^p - 1)$ sayısının bazı değerleri için asal sayılar bulmuştur. Bilinen en büyük Mersenne asalı $(2^{82589933} - 1)$ sayısıdır. Fermat, negatif olmayan her n tam sayısı için $\left(2^{2^n} + 1\right)$ biçimindeki sayıların asal olacağını ileri sürmüştür. Fermat sayısı p gibi bir asal sayıya eşit olduğunda, p kenarlı düzgün bir çokgenin pergelle ve cetvelle çizilebileceğinin Gauss tarafından ispat edilmesiyle Fermat sayılarının düzlem geometrisinde ki önemi de artmıştır. Bugün için $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257$ ve $F_4 = 65.537$ olmak üzere beş tane Fermat asalı bilinmektedir.

Matematik meraklısı her insanın, bitmek bilmeyen heyecanıyla, asal sayılarla ilgili çalışmalar hız kesmeden yoluna devam edecektir.

Teorem: Herhangi iki Fermat sayısı aralarında asaldır.

İspat: $k > 0$ olmak üzere herhangi iki F_n ve F_{n+k} Fermat sayılarını göz önüne alalım ve $m|F_n$, $m|F_{n+k}$ olduğunu kabul edelim. $F_{n+k} = 2^{2^{n+k}} + 1$ ise $F_{n+k} - 2 = 2^{2^{n+k}} - 1 = \left(2^{2^n}\right)^{2^k} - 1$ sayısında $x = 2^{2^n}$ yazılacak olursa $f(x) = x^{2^k} - 1$ şeklinde bir fonksiyon elde edilir. $f(-1) = 0$ olduğundan $f(x)$ fonksiyonunun $(x + 1)$ gibi bir çarpanının olduğu söylenebilecektir. $x + 1 = 2^{2^n} + 1 = F_n$ sayısı $f(x)$ fonksiyonunun bir çarpanı olacaktır. Bu durumda $F_n|F_{n+k}$ olup $m|F_n$, $m|(F_{n+k} - 2)$ ve $m|2$ elde edilir. F_n tek sayı olduğundan $m = 2$ olamayacaktır. Sonuçta $m = 1$ olur ve $(F_n, F_{n+k}) = 1$ elde edilir.

Örnek: $p_4 = 7$ olmak üzere $M_p = (2^p - 1)$ Mersenne sayısının asal sayı olup-olmadığını Lucas-Lehmer testini uygulayarak bulalım.

Çözüm: $p = 7$ iken $M_7 = (2^7 - 1) = 127$ sayısının asallık durumu için aşağıdaki algoritmayı oluşturalım.

$s_0 = 4$ olmak üzere,

$s_1 = s_0^2 - 2 = 4^2 - 2 = 14$ ve $s_1 = 14 \equiv 14\ (Mod 127)$,

$s_2 = s_1^2 - 2 = 14^2 - 2 = 194$ ve $s_2 = 194 \equiv 67\ (Mod 127)$,

$s_3 = s_2^2 - 2 = 67^2 - 2 = 4487$ ve $s_3 = 4487 \equiv 42\ (Mod 127)$,

$s_4 = s_3^2 - 2 = 42^2 - 2 = 1762$ ve $s_4 = 1762 \equiv 111\ (Mod 127)$,

$s_5 = s_4^2 - 2 = 111^2 - 2 = 12319$ ve $s_5 = 12319 \equiv 0\ (Mod 127)$,

$p - 2 = 7 - 2 = 5$ ve $s_5 \equiv 0\ (Mod\ 2^p - 1 = 127)$ olduğu için 127 sayısı asal sayıdır.

Not: $p > 2$ asal sayı olmak üzere, $M_p = (2^p - 1)$ Mersenne sayısının asallığı,

1. $s_0 = 4$,
2. $s_{(k+1)} = s_k^2 - 2 \equiv l\ (Mod\ 2^p - 1)$,

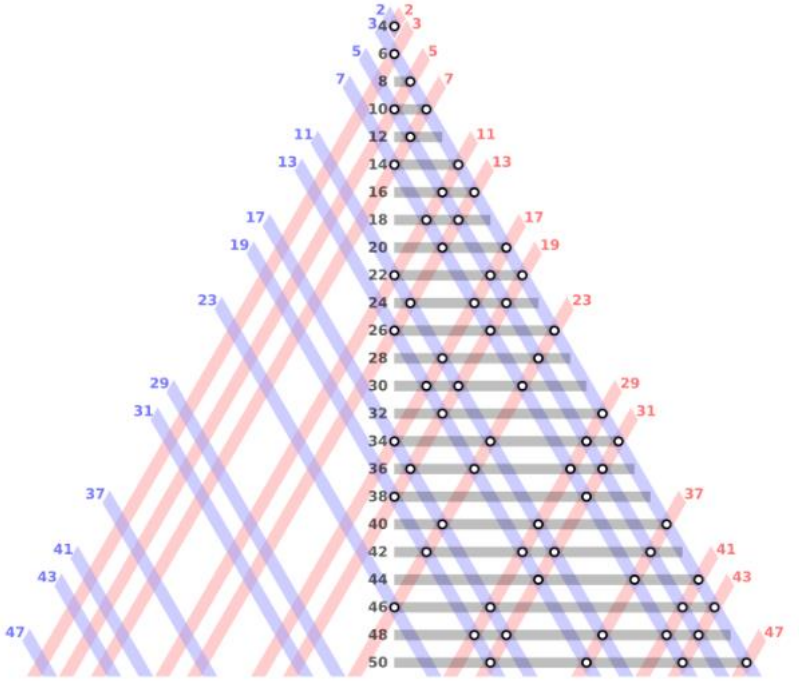
$s_{p-2} \equiv 0\ (Mod\ 2^p - 1)$ olduğunda M_p sayısı asal sayıdır.

Soru: $p = 11$ olduğunda $M_{11} = (2^{11} - 1) = 2047$ Mersenne sayısının asal sayı olup-olmadığını Lucas-Lehmer testi uygulayarak belirleyiniz.

Goldbach Sanısı

Bir dizinin genel teriminin verilmesi durumunda dizinin diğer terimlerinin bulunacağı ya da geometrik veya aritmetik bir dizinin elemanları arasındaki ilişkiyle ilgili bilgiler verildiğinde genel teriminin bulunacağı bilinmektedir. Asal sayılar dizisi için de böyle formüllerin var olup-olmadığı düşünülebilir. Asal sayıların dağılımında görülen büyük düzensizlik nedeniyle, n. asal sayıyı veren bir formül, bir asaldan sonra gelen bir diğer asalı veren bir rekürans denklem, verilen bir asaldan büyük bir asal sayıyı veren bir kural, herhangi bir tam sayıdan küçük olan asal sayıların sayısını veren bir bağıntı var mıdır? Soruları hep olumsuz kalmıştır, bugüne kadar.

11-13, 17-19 ve 100 000 000 061-100 000 000 063 gibi ikiz asal sayıları arasındaki farkın küçük olduğu gibi uzun aralıklar da olabilir. İkiz asal sayıların varlığıyla ilgili olarak birçok ölçüt olmasına rağmen, sayılarının sonlu veya sonsuz olduğuna dair bir kanıt sunulamamıştır. Bugüne kadar bilinen en büyük ikiz asallar $2996863034895 \cdot 2^{1290000} \pm 1$ sayılarıdır. Ardışık asal sayılar arasında etkili bir şekilde hesaplanan en büyük boşluk, asal sayıdan sonra 1676 rakamdan oluşan boşluğa denk gelmektedir.



Çözülmemiş başka bir asal sayı problemini, Goldbach (MS 1690-1764) Euler'e yazdığı bir mektupta ortaya atmıştır. Goldbach, iki sayısından büyük her çift doğal sayının iki tek asal sayının toplamı şeklinde yazılabileceğini ileri sürmüştür. Bu durumu ilk birkaç sayı için gerçekleştirmek kolaydır:

$4 = 2 + 2$ $14 = 7 + 7 = 3 + 11$

$6 = 3 + 3$ $16 = 3 + 13 = 5 + 11$

$8 = 3 + 5$ $18 = 5 + 13 = 7 + 11$

$10 = 5 + 5$ $20 = 3 + 17 = 7 + 13$

$12 = 5 + 7$ $22 = 3 + 19 = 5 + 17 = 11 + 11$

Goldbach hipotezinin, bilgisayarlar yardımıyla çok büyük sayılara kadar doğrulandığı gösterilmiş olsa da, henüz genel kabul görmüş bir ispatı yoktur. Çözülememiş en eski matematik problemleri arasındaki yerini korumaya devam etmektedir.

Örnek: $n^3 + 1$ formunda yazılabilecek tek asal sayının 2 olduğunu gösterelim.

Çözüm: n tam sayısının negatif olması durumunda $n^3 + 1$ sayısının pozitif ve asal sayı olamayacağı açıktır. $n^3 + 1 = (n + 1)(n^2 - n + 1)$ şeklinde çarpanlarına ayrılabilir. n doğal sayısının 1 sayısından büyük olması durumunda $n^3 + 1$ sayısı iki sayının çarpımı şeklinde yazılabilir duruma geleceğinden dolayı $n \geq 1$ durumlarının hiç birinde $n^3 + 1$ sayısı asal olamayacaktır. $n^3 + 1 = n + 1$ durumu kalıyor ki bu durumda $n = 1$ olacaktır. $n^3 + 1$ sayısı, 2 olacaktır.

Soru: $p > 3$ her ikiz asal sayının toplamının 12 sayısıyla tam bölünebildiğini gösteriniz.

UYGULAMALAR

1) p ve p^2+8 asal sayıları için p^3+4 sayısının asal sayı olduğunu gösteriniz.
2) $n \geq 2$ olmak üzere $\sqrt[n]{n}$ sayısının irrasyonel sayı olduğunu gösteriniz.
3) $n > 1$ olmak üzere $n!+1$ sayısını, n doğal sayısından büyük ve tek olan her p asal sayısının böldüğünü gösteriniz.
4) 2 doğal sayısından büyük her doğal sayı için $n < p < n!$ eşitsizliğini sağlayan bir asal sayının varlığını gösteriniz.
5) $n > 3$ olmak üzere n, $n+2$ ve $n+4$ sayılarının hepsinin birden asal olamayacağını gösteriniz.
6) p asal sayı olmak üzere p, $p+2$ ve $p+6$ sayılarının hepsinin birden asal sayı olması durumu üçlü-asallar olarak isimlendirilir. İlk üçlü-asal sayı grubunu bulunuz.
7) p asal sayı olmak üzere $p \cdot (p+2) - 2$ sonucunun da bir asal sayı olduğunu bulunuz.
8) p_n, nth asal sayı ve $n > 3$ olmak üzere, $p_n < p_1 + p_2 + \cdots + p_{n-1}$ olduğunu gösteriniz.
9) p asal sayı ve $1 \leq k \leq p-1$ olmak üzere $\binom{p}{k}$ sayısının p sayısıyla bölünebileceğini gösteriniz.
10) a pozitif tam sayı ve p asal sayı olmak üzere $(a, p^2) = p$ olduğunda $(a^2, p^2) = p^2$ olacağını gösteriniz.
11) n pozitif tam sayı ve p asal sayı olmak üzere $p|(n^p - n)$ olacağını gösteriniz.
12) $p \neq 2$ asal sayı olmak üzere $1+2+3+\cdots+p$ değerinin p asal sayısıyla bölünebilmesi için gerekli durumları belirleyiniz.
13) p ve $2^p - 1$ sayıları asal sayı olduğunda $2^{p-1}(2^p-1)$ sayısının mükemmel bir sayı olacağını gösteriniz.
14) p asal sayı ve $p|a^k$ olmak üzere $p|a$ olacağını gösteriniz.
15) p sayısı, n bileşik sayısını bölen bir asal sayı olsun. $p > \sqrt{n}$ olması durumunda, n bileşik sayısını bölen $q < \sqrt{n}$ olacak şekilde bir q asal sayısının olduğunu bulunuz.
16) $n > 1$ sayısından büyük ve $6k+3$ formunda olmayan bir tam sayıysa $n^2 + 2^n$ sayısının bileşik sayı olacağını gösteriniz.
17) $n \geq 2$ doğal sayı olmak üzere, $\sqrt[n]{n}$ sayısının irrasyonel sayı olacağını gösteriniz.
18) p_n, n. asal sayı olmak üzere, $n \geq 3$ doğal sayıları için $p_{n+3}^2 < p_n p_{n+1} p_{n+2}$ eşitsizliğinin gerçekleneceğini gösteriniz.
19) $6n+5$ formunda sonsuz sayıda asal sayının olduğunu gösteriniz.

20) p ve q ikiz asal olmak üzere, $pq - 2$ değerinin asal sayı olduğunu gösteriniz.

4. BÖLÜM

KONGRÜANSLAR

Bazı olaylar veya durumlar belirli aralıklarla tekrar eder. Bu şekilde tekrar eden, devreden olaylara veya durumlara periyodik olaylar denmektedir. Hayatımızda bu şekilde gerçekleşen durumları bolca görmek mümkündür. Yılın aylarının 12 ayda, haftanın günlerinin 7 günde, günün saatlerinin 24 saatte bir tekrar etmesi karşılaştığımız rutinlerimizdendir. Saat 17.00 olduğuna göre 62 saat sonra saatin kaç olacağı, gün perşembeyse 97 gün sonrasının hangi gün olacağı, dört günde bir gün nöbet tutan doktorun bir yılda kaç nöbet tutacağı gibi durumlar bu tür olaylara örnek gösterilebilir. Kongrüans aritmetiği saat aritmetiği olarak da bilinmektedir. Kongrüans teorisinin, sayılar teorisinde yaygın kullanımı bulunmaktadır. Bölünebilme bu alanlardan sadece bir tanesidir.

"**Tanım:** Sabit ve sıfırdan farklı bir m tam sayısı a ve b gibi herhangi iki tam sayının farkını bölüyorsa a tam sayısı b tam sayısına m modülüne göre kongrüenttir denir, $a \equiv b \ (mod\ m)$ biçiminde gösterilir. Eğer $m \nmid a - b$ olması durumunda a tam sayısının b tam sayısına kongrüent olmadığı söylenir, $a \not\equiv b \ (mod\ m)$ biçiminde gösterilir.

$6|18$ ifadesi $6|(22 - 4)$ şeklinde yazılabilir. Bu ifadeyi $22 \equiv 4 \ (mod\ 6)$ yazımına dönüştürebiliriz. $18 = 13 - (-5) = 78 - 60$ gibi eşitlikleri de olacağından $13 \equiv (-5) \ (mod\ 6)$ veya $78 \equiv 60 \ (mod\ 6)$ denklikleri de yazılabilir.

Not: a ve b tam sayılar olmak üzere, $a \equiv b \ (mod\ m)$ olması için gerek ve yeter şart l tam sayısı için $a = b + l \cdot m$ olmasıdır.

Teorem: a, b, c, d ve $m > 0$ tam sayılar olmak üzere $a \equiv b \ (mod\ m)$ ve $c \equiv d \ (mod\ m)$ olduğunda aşağıdaki durumlar geçerlidir:

i. $a \mp c \equiv b \mp d \ (mod\ m)$,
ii. $a \cdot c \equiv b \cdot d \ (mod\ m)$,
iii. $a \mp c \equiv b \mp c \ (mod\ m)$,
iv. $a \cdot c \equiv b \cdot c \ (mod\ m)$.

İspat:

i. $a \equiv b\ (mod\ m)$ olması $m|a-b$ devamında $a-b=m\cdot l$ olmasını gerektirir. Benzer şekilde $c-d=m\cdot k$ olacaktır. Bu iki eşitlikten $(a \mp c)-(b \mp d)=m\cdot(k+l)$ eşitliği elde edilir. $m|(a+c)-(b+d)$ ve $m|(a-c)-(b-d)$ eşitliklerinden $a \mp c \equiv b \mp d\ (mod\ m)$ elde edilir.

ii. $a \equiv b\ (mod\ m)$ ve $c \equiv d\ (mod\ m)$ olduğundan $m|a-b$ ve $m|c-d$ elde edilecektir. $(a-b)\cdot c$ ve $(c-d)b$ iki eşitlik de m tam sayısı tarafından bölünür. $(a-b)c+(c-d)b=ac-bd$ eşitliği de m tam sayısı tarafından bölüneceğinden $a\cdot c \equiv b\cdot d\ (mod\ m)$ elde edilir.

iii. $a \equiv b\ (mod\ m)$ denkliğinden $m|a-b$ elde edilir. $(a \mp c)-(b \mp c)=a-b$ ifadesi de m tam sayısına bölünecektir. Bu eşitlikten $a \mp c \equiv b \mp c\ (mod\ m)$ elde edilecektir.

v. $a \equiv b\ (mod\ m)$ denkliğinden $m|a-b$ elde edilir. $(a-b)c=ac-bc$ ifadesi de m tam sayısına bölünecektir. Bu eşitlikten $a\cdot c \equiv b\cdot c\ (mod\ m)$ elde edilecektir.

Gerçel sayılarda $a \neq 0$ olduğunda $a\cdot x=a\cdot y$ ise $x=y$ olacağını bilmekteyiz. $20 \equiv 8\ (mod\ 6)$ dekliğinde $5\cdot 4 \equiv 2\cdot 4\ (mod\ 6)$ ise $5 \not\equiv 2\ (mod\ 6)$ denksizliği elde edileceği için bu özellik kongrüanslarda genel olarak geçerli değildir.

Teorem: a, b, c, d ve $m>0$ tam sayılar olmak üzere aşağıdaki durumlar geçerlidir:

i. $(c,m)=d$ olmak üzere $ac \equiv bc\ (mod\ m)$ olması için gerek ve yeter şart $a \equiv b\ \left(mod\ \frac{m}{d}\right)$ olmasıdır,

ii. $ac \equiv bc\ (mod\ m)$ ve $(c,m)=1$ olması durumunda $a \equiv b\ (mod\ m)$ olacaktır.

İspat:

i. $ac \equiv bc\ (mod\ m)$ olduğunda en az bir $t \in \mathbb{Z}$ için $c(a-b)=mt$ olacaktır. Eşitliğin her iki tarafı d sayısına bölündüğünde $\frac{c}{d}(a-b)=\frac{mt}{d}$ eşitliği elde edilecektir. $\left(\frac{c}{d},\frac{m}{d}\right)=1$ olması $\frac{m}{d}|(a-b)$ olmasını gerektirecektir. Bu durumda $a \equiv b\ \left(mod\ \frac{m}{d}\right)$ elde edilecektir.

ii. Yukarıdaki eşitlikte $(c,m)=d=1$ olması durumunda $\equiv b\left(mod\ \frac{m}{d}\right)$ ifadesinden $a\equiv b\ (mod\ m)$ elde edilir.

$15\equiv 5\ (mod\ 10)$ olduğunda $(5,10)=5$ eşitliğinden $\frac{15}{5}\equiv\frac{5}{5}\ (mod\ \frac{10}{5})$ veya $3\equiv 1\ (mod\ 2)$ elde edilir. Benzer şekilde $42\equiv 7\ (mod\ 5)$, $(7,5)=1$ ve $\frac{42}{7}\equiv\frac{7}{7}\ (mod\ 5)$ veya $6\equiv 1\ (mod\ 5)$ elde edilir.

Sonuç: $a,b,\ m>0$ tam sayılar ve $a\equiv b\ (mod\ m)$ olmak üzere herhangi $n>0$ tam sayısı için $a^n\equiv b^n\ (mod\ m)$ eşitliği geçerlidir.

Sonuç: a herhangi bir tam sayı, $n_1$ve n_2 iki pozitif tam sayı olmak üzere $n_1|a$ ve $n_2|a$ olması durumunda $(n_1,n_2)|a$ olacaktır.

Teorem: a,b ve $t_1,t_2,\dots,t_k>0$ tam sayılar olmak üzere $a\equiv b\ (mod\ t_1)$, $a\equiv b\ (mod\ t_2)$, $a\equiv b\ (mod\ t_3)$, … , $a\equiv b\ (mod\ t_k)$ olursa $a\equiv b\ (mod\ (t_1,t_2,\dots,t_k))$ olacaktır.

İspat: $t_1|(a-b)$, $t_2|(a-b)$, … ,$t_k|(a-b)$ yazılabilir. Bu durum $(t_1,t_2,\dots,t_k)|(a-b)$ olmasını gerektirecektir. Kongrüans tanımından $a\equiv b\ (mod\ (t_1,t_2,\dots,t_k))$ elde edilecektir.

Teorem: $m\neq 0$ tam sayı olmak üzere tam sayılar kümesi üzerinde tanımlanan $a\equiv b\ (mod\ m)$ kongrüans bağıntısı bir denklik bağıntısı oluşturur.

İspat:

Yansıma Özelliği: $m|0$ özelliği kullanılarak $m|a-a$ yazılabilir. Tanım gereği $a\equiv a\ (mod\ m)$ elde edilecektir.

Simetri Özelliği: Eğer $a\equiv b\ (mod\ m)$ ise tanım gereği $m|a-b,\ a-b=m\cdot t$ yazılabilir. Buradan $b-a=m\cdot(-t)$ ve $m|b-a$ sonucuna ulaşılır. Tanım gereği $b\equiv a\ (mod\ m)$ elde edilecektir.

Geçişme Özelliği: Eğer $a\equiv b\ (mod\ m)$ ve $b\equiv c\ (mod\ m)$ ise tanım gereği $m|a-b, a-b=m\cdot t$ ve $m|b-c, b-c=m\cdot l$ yazılabilir. $a-c=(a-b)+(b-c)=mt+ml=(t+l)m$ sonucuna ulaşılır. Tanım gereği $a\equiv c\ (mod\ m)$ elde edilecektir.

Örnek: $ca\equiv cb\ (mod\ n)$ ve $(c,n)=d$ olması durumunda $a\equiv b\ (mod\ \frac{n}{d})$ olacağını gösterelim.

Çözüm: Kongürent hipotezimize göre, bazı k gibi tam sayılar için $ca - cb = c(a-b) = kn$ yazabiliriz. $(c,n) = d$ olması durumunda r ve s gibi asal sayılar için $c = dr$ ve $n = ds$ olacaktır. Bu değerleri ilk eşitlikte yerine yazdığımızda $r(a-b) = ks$ eşitliğini elde ederiz. Bu durumda $s|r(a-b)$ ve $(r,s) = 1$ olacaktır. Sonuç olarak $s|a-b$ elde edilir. Kongürent hipotezinden $a \equiv b \ (mod\ s)$ yazılır. $a \equiv b \ (mod\ \frac{n}{d})$ denkliği elde edilir.

Sonuç: $ca \equiv cb \ (mod\ p)$, p asal sayı olmak üzere $p \nmid c$ olması durumunda $a \equiv b \ (mod\ p)$ olacaktır.

Teorem: $i = 1, 2, 3, \dots, n$ olmak üzere $a_i \equiv b_i \ (mod\ m)$ olduğunda aşağıdaki durumlar geçerlidir:

i. x_i tam sayı olmak üzere $\sum_{i=1}^{n} a_i x_i \equiv \sum_{i=1}^{n} b_i x_i \ \ (mod\ m)$,
ii. $\prod_{i=1}^{n} a_i \equiv \prod_{i=1}^{n} b_i \ \ (mod\ m)$.

İspat:

i. $a_i \equiv b_i \ (mod\ m)$ olduğunda kongrüent hipotezinden en az bir $q_i \in \mathbb{Z}$ için $a_i - b_i \equiv mq_i$ olacaktır. $a_i x_i - b_i x_i \equiv mq_i x_i$ eşitliğinden $\sum_{i=1}^{n} a_i x_i - \sum_{i=1}^{n} b_i x_i \equiv m \sum_{i=1}^{n} q_i x_i$ elde edilir. Bu durumdan $\sum_{i=1}^{n} a_i x_i \equiv \sum_{i=1}^{n} b_i x_i \ \ (mod\ m)$ elde edilir.
ii. İspatımız indüksiyon prensibiyle gerçekleştirelim. $n = 1$ için iddianın aşikar olduğu görülür. $n = k$ için doğru olduğunu kabul ederek $\prod_{i=1}^{k} a_i \equiv \prod_{i=1}^{k} b_i \ (mod\ m)$ olduğunu varsayalım. En az bir $q_i \in \mathbb{Z}$ için $\prod_{i=1}^{k} a_i - \prod_{i=1}^{k} b_i = mq$ olacaktır.

$$\begin{aligned}\prod_{i=1}^{k+1} a_i - \prod_{i=1}^{k+1} b_i &= \prod_{i=1}^{k+1} a_i - b_{k+1} \prod_{i=1}^{k} a_i \\ &\quad + b_{k+1} \prod_{i=1}^{k} a_i - \prod_{i=1}^{k+1} b_i \\ &= (a_{k+1} - b_{k+1}) \prod_{i=1}^{k} a_i \\ &\quad + b_{k+1}\left(\prod_{i=1}^{k} a_i - \prod_{i=1}^{k} b_i\right) \\ &= mq_{k+1} \prod_{i=1}^{k} a_i + b_{k+1} mq \\ &= m\left(q_{k+1} \prod_{i=1}^{k} a_i + b_{k+1} q\right)\end{aligned}$$

elde edilir. Bu durumdan $\prod_{i=1}^{k+1} a_i \equiv \prod_{i=1}^{k+1} b_i \ (mod\ m)$ elde edilir ki indüksiyon prensibi gereği ifadenin doğru olduğunu gösterir.

Örnek: $1! + 2! + 3! + \cdots + 100!$ değerinin 18 ile bölümünden kalanını bulalım.

Çözüm: $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 6! \equiv 0\ (mod\ 18)$ olması durumunda,

$(6 + n)! \equiv 0\ (mod\ 18)$ olacağı aşikardır.

$1! + 2! + 3! + 4! + 5! + \cdots + 100! \equiv (1! + 2! + 3! + 4! + 5!)(mod\ 18)$

$1! + 2! + 3! + 4! + 5! + \cdots + 100! \equiv 153\ (mod\ 18)$

$1! + 2! + 3! + 4! + 5! + \cdots + 100! \equiv 9\ (mod\ 18)$. Kalan 9 olacaktır.

Kongrüans bağıntısı yansıma, simetri ve geçişme özelliklerini sağladığı için bir denklik bağıntısı oluşturur. Ayrıca denklik bağıntısı, kongrüans bağıntısı olarak da isimlendirilebilir. Denklik bağıntısı, denklik sınıfları formunda olacağından bu durum denklik sınıfları olarak cebirde yer almaktadır. Örneğin, herhangi bir pozitif tam sayının 7 sayısıyla bölümünden kalanlar 0, 1, 2, 3, 4, 5 ve 6 sayıları olacaktır. Burada kalan sayı olarak 2 sayısı seçilirse 2, 9, 16, 23, 30, … sayılarının da 7 sayısıyla bölümünden kalanlar hep 2 sayısı olacaktır. 2, 9, 16, 23, 30, … sayılarından oluşan küme, 7 modülüne göre kalan sınıfları kümesi olarak isimlendirilir ve [2] şeklinde gösterilir.

Örnek: 10^{515} sayısının 7 ile bölümünden kalanını bulalım.

Çözüm:

$10 \equiv 3\ (mod\ 7)$,

$10^2 \equiv 2\ (mod\ 7)$,

$10^3 \equiv 6\ (mod\ 7)$,

$10^4 \equiv 4\ (mod\ 7)$,

$10^5 \equiv 5\ (mod\ 7)$,

$10^6 \equiv 1\ (mod\ 7)$,

$(10^6)^{85} \cdot 10^5 = 10^{515} \equiv 1^{85} \cdot 10^5\ (mod\ 7)$,

$10^{515} \equiv 5\ (mod\ 7)$ olarak bulunur. Kalan 5 olacaktır.

Kalan Sınıfları

7, 22, -12, 73, -66, 110, 41 tam sayılar kümesinden seçilen bu sayılar, 7 modülüne göre, $7 \equiv 0\ (mod\ 7)$, $22 \equiv 1\ (mod\ 7)$, $-12 \equiv 2\ (mod\ 7)$, $73 \equiv 3\ (mod\ 7)$,

$-66 \equiv 4\ (mod\ 7), 110 \equiv 5\ (mod\ 7)$ ve $41 \equiv 6\ (mod\ 7)$ olacaktır. Buradan yukarıdaki sayıların her birinin, tam olarak 7 modülüne göre 0, 1, 2, 3, 4, 5, ve 6 sayılarından birine kongrüent olacağı görülecektir. 7, 22, -12, 73, -66, 110, 41 tam sayılarından oluşan kümeye 7 modülüne göre kalan sınıflar kümesi denilecektir.

Tanım: a herhangi bir tam sayı ve $m > 0$ tam sayısı olmak üzere $A = \{b: b \equiv a\ (mod\ m)\}$ kümesi m modülüne göre kalan sınıfları kümesi olarak isimlendirilir ve $[a]$ şeklinde gösterilir.

Tanım: Tam sayılar kümesinin $R = \{r_1, r_2, r_3, \dots, r_m\}$ kümesini göz önüne alalım. $\forall\ y\ \in\ \mathbb{Z}$ için $y \equiv r_j\ (mod\ m)$ olacak şekilde bir tek $r_j \in \mathbb{R}$ varsa $\mathbb{R}$ kümesine m modülüne göre bir tam kalan sınıfları sistemi oluşturmaktadır denir. Tanımımıza göre tam sayılardan oluşan bir cümle aşağıdaki şartları gerçekliyorsa bir tam kalan sınıfları sistemi oluştur demekteyiz.

i. Bu kümenin tam olarak m sayıda elemanı bulunmalıdır.
ii. Bu kümedeki herhangi iki eleman m modülüne göre birbirlerine kongrüent olmamalıdır. Yani $i \neq j$ için $r_i \not\equiv r_j\ (mod\ m)$ olmalıdır.

Bu durumda m modülüne göre $\mathbb{Z}_m$ kalan sınıfları sistemini $\overline{a}$ şeklinde, $x \equiv a\ (mod\ m)$ değerini gerçekleyen x tam sayılarının bulunduğu kalan sınıfını belirtmek üzere $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{m-1}\}$ şeklinde göstereceğiz. Örneğin $m = 5$ için kalan sınıfları kümesi $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ şeklinde oluşacaktır.

Sonuç: $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{m-1}\}$ kalan sınıfları kümesini ve c herhangi bir sayı olmak üzere $\{\overline{0+c}, \overline{1+c}, \overline{2+c}, \dots, \overline{m-1+c}\}$ kümesi de m modülüne göre kalan sınıfları kümesi olur.

Sonuç: $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{m-1}\}$ kalan sınıfları kümesini ve c, m tam sayısıyla aralarında asal herhangi bir sayı olmak üzere $\{\overline{c \cdot 0}, \overline{c \cdot 1}, \overline{c \cdot 2}, \dots, \overline{c \cdot (m-1)}\}$ kümesi de m modülüne göre kalan sınıfları kümesi olur.

Yukarıda verilen iki sonucun birleşimi, $\mathbb{Z}_m = \{\overline{a_1}, \overline{a_2}, \overline{a_3}, \dots, \overline{a_m}\}$ kalan sınıfları kümesini ve c, m tam sayısıyla aralarında asal herhangi bir sayı olmak üzere $\overline{c \cdot a_1 + d}, \overline{c \cdot a_2 + d}, \overline{c \cdot a_3 + d}, \dots, \overline{c \cdot a_m + d}$ kümesi de d tam sayı olmak üzere, m modülüne göre kalan sınıfları kümesi olur, sonucuna ulaştırır.

Örnek: $a^2 \equiv b^2 \ (mod\ n)$ olmasının $a \equiv b \ (mod\ n)$ olmasını gerektirmediğini gösterelim.

Çözüm: Örneğimizin sağlanamayacağını aksine ispat metoduyla gösterelim. $5^2 \equiv 4^2 \ (mod\ 3)$ tanım gereği, $3|25 - 16 = 9$ olacaktır. Ama $5 \equiv 4 \ (mod\ 3)$ tanım gereği $3|5 - 4 = 1$ ve $3 \nmid 1$ olmasından dolayı $5 \not\equiv 4 \ (mod\ 3)$ olacaktır.

Örnek: 41 sayısının $2^{20} - 1$ sayısını böldüğünü gösterelim.

Çözüm:

$2^1 \equiv 2 \ (mod\ 41)$

$2^2 \equiv 4 \ (mod\ 41)$

$2^3 \equiv 8 \ (mod\ 41)$

$2^4 \equiv 16 \ (mod 41)$

$2^5 \equiv 32 \equiv -9 \ (mod\ 41)$

$(2^5)^4 \equiv (-9)^4 \ (mod\ 41)$

$2^{20} \equiv 81 \cdot 81 \ (mod\ 41)$

$81 \equiv -1 \ (mod 41)$

$2^{20} \equiv (-1) \cdot (-1) \equiv 1 \ (mod\ 41)$

$2^{20} - 1 \equiv 0 \ (mod\ 41)$

son ifadeden tanım gereği, $41|2^{20} - 1$ olacaktır.

Örnek: a bir tek tam sayı olmak üzere $a^2 \equiv 1 \ (mod\ 8)$ olacağını gösterelim.

Çözüm: $k \in \mathbb{Z}$ olmak üzere tek tam sayıların kümesini $a = 4k + 1$ veya $a = 4k + 3$ formatında gösterebiliriz.

$(4k + 1)^2 = 16k^2 + 8k + 1 = 8 \cdot (2k^2 + k) + 1 \equiv 1 \ (mod\ 8)$

$(4k + 3)^2 = 16k^2 + 24k + 9 = 8 \cdot (2k^2 + 3k + 1) + 1 \equiv 1 \ (mod\ 8)$

a bir tek tam sayı olmak üzere $a^2 \equiv 1 \ (mod\ 8)$ olacaktır.

Teorem: $(m', m'') = 1, r'$ değerinin m' modülüne, r'' değerinin m'' modülüne göre tam kalan sınıfları üzerinden bütün değerleri almak üzere, $r''m' + r'm''$ değeri $m'm''$ modülüne göre tam kalan sınıflarındaki bütün değerleri alır.

İspat: $r''m' + r'm''$ değerlerinin sayısının $m'm''$ kadar olduğu açıktır. Bu değerlerden herhangi ikisinin $m'm''$ modülüne göre kongrüent olamayacağını göstermeliyiz.

$r_1''m' + r_1'm'' \equiv r_2''m' + r_2'm'' \ (mod\ m'm'')$ olsaydı $m'(r_1'' - r_2'') + m''(r_1' - r_2') \equiv 0 \ (mod\ m'm'')$ olurdu. Halbuki $m'm''$ ifadesiyle bölünebilme m' ifadesiyle bölünebilmeyi gerektirdiğinden $m'(r_1'' - r_2'') + m''(r_1' - r_2') \equiv 0 \ (mod\ m'm'')$ ifadesi $m'(r_1'' - r_2'') + m''(r_1' - r_2') \equiv 0 \ (mod\ m')$ ve $m''(r_1' - r_2') \equiv 0 \ (mod\ m')$ olmasını gerektirir ki $(m', m'') = 1$ olduğundan $r_1' \equiv r_2' \ (mod\ m')$ ve $r_1'' \equiv r_2'' \ (mod\ m')$ olurdu. Bu durum tam kalan sınıfları tanıma göre mümkün değildir. Böylece $m'm''$ sayıdaki sayıların hepsi $m'm''$ modülüne göre bir tam kalan sınıfları sistemi oluştururlar.

Teorem: $P(x) = \sum_{k=0}^{m} c_k x^k$ kat sayıları tam sayı olan bir polinom olmak üzere, $a \equiv b \ (mod\ n)$ olduğunda $P(a) \equiv P(b) \ (mod\ n)$ eşitliği geçerlidir.

İspat: $a \equiv b \ (mod\ n)$ ifadesinden $a^k \equiv b^k \ (mod\ n)$ ifadesine ulaşılacaktır. Bu eşitlikten de $c_k a^k \equiv c_k b^k \ (mod\ n)$ ifadesine ulaşılacaktır. Denkliğin her iki tarafının toplamı alınırsa $\sum_{k=0}^{m} c_k a^k \equiv \sum_{k=0}^{m} c_k b^k \ (mod\ n)$ elde edilecektir. Sonuç olarak $P(a) \equiv P(b) \ (mod\ n)$ değeri elde edilir.

Sonuç: a sayısı $P(a) \equiv 0 \ (mod\ n)$ ifadesinin bir çözümüyse $P(a) \equiv P(b) \ (mod\ n)$ olduğunda b sayısı da bir çözüm olacaktır.

Örnek: $29 \cdot 93 + 17 \cdot 16^4$ sayısının 7 ile bölümünden kalanı bulalım.

Çözüm: $16 \equiv 2 \ (mod\ 7)$ olduğundan $16^4 \equiv 2^4 \equiv 2 \ (mod\ 7)$ ve $17 \equiv 3 \ (mod\ 7)$ olduğundan $17 \cdot 16^4 \equiv 3 \cdot 2 \equiv 6 \ (mod\ 7)$ olacağı görülecektir. Benzer şekilde $29 \equiv 1 \ (mod\ 7)$ ve $93 \equiv 2 \ (mod\ 7)$ olacağından $29 \cdot 93 \equiv 2 \cdot 1 \equiv 2 \ (mod\ 7)$ olacaktır.

$29 \cdot 93 + 17 \cdot 16^4 \equiv 2 + 6 \equiv 1 \ (mod\ 7)$ elde edilir ki kalan sayının 1 olduğu görülür.

Bir tam sayının başka bir tam sayıya bölünmesini sağlayan tanımı aşağıda vereceğiz. Sayı sistemimizin temel alındığı özel bir durumu kapsayan notasyonu aşağıda bulacaksınız.

Tanım: $b > 1$, N herhangi bir pozitif tam sayı ve a_k değerleri $0, 1, 2, \dots, (b-1)$ değerlerinden biri olmak üzere,

$$N = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_2 b^2 + a_1 b^1 + a_0 b^0$$

şeklinde ifade edilebilir. Yeniden düzenleme yapıldığında $N = (a_m a_{m-1} \dots a_2 a_1 a_0)_b$ şeklinde olacaktır. Örneğin,

$105 = 1 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$

$105 = (1101001)_2$ olmaktadır.

Asal Kalan Sınıfları

Kongürans teorisinde bir m modülüyle aralarında asal olan sayılar önemli bir yere sahiptir. Eğer $\{r_1, r_2, \dots, r_m\}$ kümesi $(mod\ m)$ değerine göre bir tam kalan sınıfları sistemi ve $(k, m) = 1$ oluyorsa $\{kr_1, kr_2, \dots, kr_m\}$ kümesi de $(mod\ m)$ değerine göre bir tam kalan sınıfları sistemi oluştur.

Teorem: $x \equiv y\ (mod\ m)$ ise $(x, m) = (y, m)$ eşitliği geçerlidir.

İspat: $(x, m) = d$ ve $(y, m) = e$ olduğunu kabul edelim. $x \equiv y\ (mod\ m)$ olduğu için en az bir $q \in \mathbb{Z}, x - y = mq$ eşitliğini gerçekleyecektir. $d|x$ ve $d|m$ olduğundan dolayı $d|y$ olacak ve $d|e$ sonucuna ulaşılacaktır. Benzer şekilde $e|d$ elde edilecek ve iki ifadeden $d = e$ sonucu elde edilecektir.

İki tam kalan sınıfları sisteminde m sayısıyla aralarında asal olan aynı sayıda tam sayı bulunduğu ve bu tam sayıların ikişer ikişer m modülüne göre birbirlerine göre kongürent olamayacağı açıktır. 6 modülüne göre $\{1,2,3,4,5,6\}$ ve $\{7,8,-3,-2,17,18\}$ tam kalan sınıflarında 1-5 ve 7-17 tam sayı çiftleri 6 sayısıyla aralarında asaldır. Ayrıca $1 \equiv 7\ (mod\ 6)$ ve $5 \equiv 17\ (mod\ 6)$ olduğuna da dikkat edilmelidir. m modülüyle aralarında asal kalan sınıfları sisteminin, m modülüne göre tam kalan sınıfları sisteminden m ile aralarında asal olmayan tam sayıların atılmasıyla elde edilebileceği açıktır.

Lineer Kongrüanslar

Cebirsel denklemlerin çözümüne benzer, bir kongrüansın çözüm problemini ele alabiliriz. Bu bölümde

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n x^0,$$

kat sayıları tam sayı olan bir polinom olmak üzere, kongrüans denklemlerinin tam sayı çözümlerini bulmaya çalışacağız. $u \in \mathbb{Z}$ için $f(u) \equiv 0\ (mod\ m)$ oluyorsa u tam sayısına $f(x) \equiv 0\ (mod\ m)$ kongrüansının bir çözümü denir.

Sayılar teorisi içerisinde lineer kongrüanslar önemli bir yer tutmaktadır. $ax \equiv b\ (mod\ n)$ biçimindeki bir denkleme lineer kongrüans denir. Bu şekilde bir denklemin çözümünden kastedilen $ax_0 \equiv b\ (mod\ n)$ olacak şekilde bir x_0 tam sayısının var olmasıdır. Kongrüans tanımı gereği $ax_0 \equiv b\ (mod\ n)$ olabilmesi için gerek ve yeter şart $n|ax_0 - b$ yazılabilmesidir. Başka bir ifadeyle, $ax_0 - b = ny_0$ olacak şekilde bazı y_0 tam sayılarının bulunacak olmasıdır. $ax_0 \equiv b\ (mod\ n)$ lineer bağıntısını sağlayacak tüm tam sayıları bulma problemi $ax - ny = b$ lineer Diophantine denkleminin tüm çözümlerini elde etme problemine dönüşecektir. $ax_0 \equiv b\ (mod\ n)$ bağıntısının n modülünde eş olan iki çözümünü, normal anlamda eşit olmasalar bile "eşit" olarak ele almak uygun olacaktır. Örneğin, $x = 3$ ve $x = -9$ değerlerinin her ikisi de $3x \equiv 9\ (mod\ 12)$ denkliğini sağlamaktadır. $3 \equiv -9\ (mod\ 12)$ olduğundan farklı çözümler olarak kabul görmezler.

Tanım: $a, b, m > 0$ ve x değişkeni tam sayı olmak üzere, $ax \equiv b\ (mod\ m)$ formundaki kongrüanslara, bir değişkenli lineer kongrüanslar denir.

Teorem: $a \neq 0, b \neq 0, c$ tam sayılar ve (x_0, y_0) ikilisi $ax + by = c$ lineer denkleminin bir çözümü olmak üzere, $m = |b|$ düşünüldüğünde x_0, $ax \equiv c\ (mod\ m)$ lineer kongrüans denkleminin bir çözümüdür.

İspat: (x_0, y_0) ikilisi $ax + by = c$ lineer denkleminin bir çözümü olsun. Bu durumda $b|ax_0 - c$ olacaktır. $m = |b|$ düşünüldüğünde, x_0 değeri $ax \equiv c\ (mod\ m)$ denkleminin bir çözümü olacaktır. Karşıt tersi olarak x_0 değeri $ax \equiv c\ (mod\ m)$ denkleminin bir çözümü olsun. $m = |b|$ değeri $ax_0 - c$ değerini bölecektir. Bu durumda, bazı y_0 değerleri için $ax_0 - c = by_0$ eşitliği sağlanacaktır. Sonuçta (x_0, y_0) ikilisi $ax + by = c$ lineer denkleminin bir çözümü olacaktır.

Örnek: $221x + 35y = 11$ Diophantine denklemini lineer kongrüans kullanarak çözümünü bulalım.

Çözüm: $221x + 35y = 11$ Diophantine denklemi kullanılarak $221x \equiv 11\ (mod\ 35)$ yazılabilir. Eşitlik düzenlendiğinde $x \equiv 1\ (mod\ 35)$ elde edilir. Kongrüans tanımından

bazı tam sayılar için $x = 35t + 1$ eşitliğine ulaşılacaktır. $x_0 = 1$, $y_0 = \frac{1}{35}(11 - 221 \cdot 1) = -6$ olacaktır. Böyleyece, $x = 35t + 1$ ve $y = -221t - 6$ genel çözüm olacaktır.

Örnek: $5x \equiv 2\ (mod\ 26)$ Diophantine denklemini lineer kongrüans kullanarak çözümünü bulalım.

Çözüm: $5x \equiv 2\ (mod\ 26)$ kongrüansı kullanılarak $5x + 26y = 2$ Diophantine denklemi yazılabilir. $(5,26) = 1$ ve lineerlik özelliğinden $1 = 5a + 26b$ eşitliği elde edilir. $a = (-5)$ seçilerek $x_0 = (-10)$ ve bazı tam sayılar için $x = -10 + 26t$ olacaktır. $x \equiv -10\ (mod\ 26)$ olarak çözüm elde edilecektir.

Yukarıda yer alan iki örnekten lineer kongrüanslar ve Diophantine eşitliklerinin birbiriyle ilişkili olduğunu söylemek mümkündür.

Teorem: $(m, a) = 1, ax \equiv b\ (mod\ m)$ lineer kongrüansının $x = x_0$ olan bir tek çözümü vardır. Bütün çözümler $t \in \mathbb{Z}$ olmak üzere $x = x_0 + tm$ şeklinde olacaktır.

İspat: x_0 herhangi bir çözüm, $ax - ax_0 \equiv b - b \equiv 0\ (mod\ m), a(x - x_0) \equiv 0\ (mod\ m)$ olur. $(m, a) = 1$ olduğundan $x - x_0 \equiv 0\ (mod\ m)$ elde edilir. Bu durumsa $t \in \mathbb{Z}$ olmak üzere, bütün çözümlerin $x = x_0 + tm$ şeklinde olacağını gösterecektir.

Teorem: $a \neq 0, b \neq 0, m > 0$ tam sayılar, $ax \equiv b\ (mod\ m)$ lineer kongrüans denkleminin bir çözümünün bulunması için gerek ve yeter şart $(m, a)|b$ olmalıdır.

İspat: $(m, a) = d$, $ax \equiv b\ (mod\ m)$ lineer kongrüansının x_0 gibi bir tek çözümünün olduğunu varsayalım. O zaman, $ax_0 \equiv b\ (mod\ m)$, $t \in \mathbb{Z}$ olmak üzere, $ax_0 = b + tm$ olacaktır. $d|a$ ve $d|m$ olduğundan $d|b$ elde edilir.

$(m, a) = d|b$ ise $b = db_1$ ve $\left(\frac{a}{d}, \frac{m}{d}\right) = 1$ olmalıdır. Bu durumda $a = da_1$ ve $m = dm_1$ ve $a_1 x \equiv b_1\ (mod\ m_1)$ olacaktır. $(a_1, m_1) = 1$ olduğundan $ax \equiv b\ (mod\ m)$ lineer kongrüans denkleminin bir çözümü vardır.

Sonuç: $(m, a) = d$ ve $d|b$ olduğunda $ax \equiv b\ (mod\ m)$ lineer kongrüans denkleminin $(m, a) = d$ tane çözümü vardır. Bu çözümler x_0, denklemin tek çözümüyse, bütün çözümler $x \equiv x_0 + \left(\frac{m}{d}\right) t\ (mod\ m)$ şeklinde olacaktır.

Örnek: $8x \equiv 16\ (mod\ 24)$ lineer kongrüans denkleminin çözümünü bulalım.

Çözüm: $(8, 24) = 8$ ve $8|16$ ifadelerinden $x_0 = 2$ çözümü elde edilir. Bütün çözümler $t \in \mathbb{Z}$ olmak üzere $x = x_0 + tm = 2 + \left(\frac{24}{8}\right)t = 2 + 3t$ şeklinde olacaktır. Çözümler $x \equiv 2,5,8,11,14,17,20,23\ (mod\ 24)$ şeklinde olacaktır. Eğer, lineer kongrüans denklemi $8x \equiv 16\ (mod\ 23)$ şeklinde olsaydı, $(8, 23) = 1$ olduğundan $x_0 = 2$ şeklinde tek çözümü olacaktı.

Kongrüans Sistemleri

Küçük sayılar için bir kongrüansın çözümü m modülüne göre bütün kalan sınıfları denenerek bulunabilir. Eğer sayılar büyükse bir lineer kongrüansın çözümlerinin bulunması oldukça zor olacaktır. $a, b, c \in \mathbb{Z}$ olmak üzere $ax + by = c$ denkleminin çözüm kümesini sağlayan (x, y) tam sayı çiftlerini bulma probleminin $ax \equiv c\ (mod\ b)$ veya $by \equiv c\ (mod\ a)$ kongrüansının çözüm kümesini bulmaya denk olduğu söylenebilir.

Teorem: $a, b \in \mathbb{Z}, m \neq 0 \in \mathbb{Z}, n \neq 0 \in \mathbb{Z}$ olmak üzere, $x \equiv a\ (mod\ m)$ ve $x \equiv b\ (mod\ n)$ lineer kongrüans sisteminin;

i. $a \equiv b\ (mod\ (m, n))$ olduğunda çözümü vardır,
ii. $x \equiv x_0\ (mod\ [m, n])$ olan bir tek ortak çözümü vardır.

İspat:

i. $x \equiv a\ (mod\ m)$ olduğunda, $t \in \mathbb{Z}$ olmak üzere $x = a + tm$ çözümleri vardır. $x \equiv b\ (mod\ n)$ ise $a + tm \equiv b\ (mod\ n)$ ve $mt \equiv b - a\ (mod\ n)$ elde edilir. Bu lineer kongrüansın bir çözümünün bulunması için $(m, n)|(b - a)$ yani $a \equiv b\ (mod\ (m, n))$ olmasını gerektirir ki bu da istenilendir.

ii. $(m, n) = d$ olmak üzere $a \equiv b\ (mod\ d)$ şartı altında $x \equiv a\ (mod\ m)$ ve $x \equiv b\ (mod\ n)$ lineer kongrüans sisteminin çözümünü bulmak istiyoruz. $x \equiv a\ (mod\ m)$ olduğunda, $t \in \mathbb{Z}$ olmak üzere $x = a + tm$ çözümleri vardır. $x \equiv b\ (mod\ n)$ ise $a + tm \equiv b\ (mod\ n)$ ve $mt \equiv b - a\ (mod\ n)$ elde edilir. Buradan $q \in \mathbb{Z}$ olmak üzere $mt = b - a + nq$ olacaktır. $\frac{m}{d}t = \frac{b-a}{d} + \frac{n}{d}q$ ifadesinden $\frac{m}{d}t \equiv \frac{b-a}{d}\ (mod\ \frac{n}{d})$ elde edilecektir. $\left(\frac{m}{d}, \frac{n}{d}\right) = 1$ olduğundan bu kongrüans sisteminin t_0 gibi tek çözümü vardır. Dolayısıyla $x = a + tm$ ifadesinden $x_0 = a + mt_0$ olacaktır. x_0 değerinin kongrüans sisteminin ortak çözümü olduğunu göstermeliyiz. t_0, çözümü için $t \equiv t_0 (mod\ \frac{n}{d})$ ve $q \in$

$\mathbb{Z}$ olmak üzere $t = t_0 + q\frac{n}{d}$ olacaktır. Elde edilen bu değeri $x = a + tm$ eşitliğinde yerine yazarsak $x = a + m\left(t_0 + q\frac{n}{d}\right) = a + mt_0 + q\frac{mn}{d}$ ve $x = x_0 + q\frac{mn}{d}$ ve $x \equiv x_0\ (mod\ \frac{mn}{d})$ olacaktır. $mn = (m,n)[m,n]$ eşitliğinden $x \equiv x_0\ (mod\ [m,n])$elde edilir.

Sonuç: Aşağıda verilen kongrüans sisteminin çözümünün olabilmesi için gerek ve yeter şart $i \neq j$olan her i değeri için $(m_i, m_j)|(a_i - a_j)$ olmasıdır.

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

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

$$x \equiv \quad \vdots \quad ,$$

$$x \equiv a_r\ (mod\ m_r).$$

Bir çözüm bulunduğunda bu çözüm $m = [m_1, m_2, \cdots m_r]$ modülüne göre bir tekdir.

Örnek: $x \equiv 5\ (mod\ 11)$ ve $x \equiv 3\ (mod\ 23)$ sisteminin ortak çözümünü bulalım.

Çözüm: Verilen kongrüans sisteminin, $(11,23)|5 - 3 = 2$ olduğundan çözümü vardır. Sistemin ilk denkleminden, $t \in \mathbb{Z}$ olmak üzere $x = 5 + 11t$ elde edilir. Bu eşitliği sistemin ikinci denkleminde yerine yazarsak

$$5 + 11t \equiv 3\ (mod\ 23),$$

$$11t \equiv 3 - 5\ (mod\ 23),$$

$$2 \cdot 11t \equiv 2 \cdot (-2)(mod\ 23),$$

$$22t \equiv -4\ (mod\ 23),$$

$$-t \equiv -4\ (mod\ 23),$$

$$t \equiv 4\ (mod\ 23),$$

$q \in \mathbb{Z}$ olmak üzere $t = 4 + 23q$ elde edilir. Bu değeri yerine yazdığımızda $x = 5 + 11t = 5 + 11(4 + 23q) = 49 + (11 \cdot 23)q$ sonucuna ulaşılır. Eşitlik düzenlendiğinde, $x \equiv 49\ (mod\ 11 \cdot 23)$ elde edilir. Bu sonuç sistemin ortak çözümüdür.

Teorem (Çin Kalan Teoremi): $m_1, m_2, \dots, m_r \in \mathbb{Z}^+$ ikişer ikişer aralarında asal ve $a_1, a_2, \dots, a_r \in \mathbb{Z}$ olsun. Bu durumda,

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

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

$$x \equiv \quad \vdots \quad ,$$

$$x \equiv a_r \ (mod\ m_r).$$

sisteminin ortak çözümleri vardır. Ayrıca, bu çözüm $m_1 \cdot m_2 \cdot \dots \cdot m_r$ modülüne göre bir tekdir.

İspat: $m = m_1 \cdot m_2 \cdot \dots \cdot m_r$, $M_j = m|m_j$ olmak üzere, $i \neq j$ için $m_i|M_j$ ve $(m_j, M_j) = 1$ olarak bulunur. Buna göre $M_j x_j \equiv 1 \ (mod\ m_j)$ olacak şekilde bir tek x_j sayısı vardır. Bu durumda $i \neq j$ olduğundan $M_j x_j \equiv 0 \ (mod\ m_i)$ olacaktır.

Şimdi $x_0 = \sum_{j=1}^{r} M_j\, x_j a_j$ sayısını göz önüne alalım. Kabulümüze göre her i değeri için $M_i x_i a_i \equiv a_i \ (mod\ m_i)$, $i \neq j$ ve $M_j \equiv 0 \ (mod\ m_i)$ olduğundan,

$x_0 = \sum_{j=1}^{r} \frac{m}{m_j} x_j a_j \equiv \frac{m}{m_i} x_i a_i \ (mod\ m_i)$ bulunacaktır. Bu durum x_0 değerinin i değerinci kongrüansı sağladığını dolayısıyla sistemin bir ortak çözümü olduğunu gösterir. Bu ortak çözümün m modülüne göre bir tek olduğunu göstermeliyiz. x_0 ve x_i sistemin herhangi iki çözümüyse her i değeri için $x_1 \equiv a_i \equiv x_0 \ (mod\ m_i),$, $i \neq j$ için $(m_i, m_j) = 1$ olduğundan $m|(x_1 - x_0)$ ve böylece $x_1 \equiv x_0 \ (mod\ m)$ elde edilir. Bu bir çözümün olması durumunda m modülüne göre bir tek olduğunu gösterir.

Örnek: $x \equiv 2 \ (mod\ 3)$, $x \equiv 4 \ (mod\ 5)$ ve $x \equiv 5 \ (mod\ 7)$ lineer kongrüans sisteminin çözüm kümesini bulalım.

Çözüm: $m = 3 \cdot 5 \cdot 7 = 105$, $M_1 = \frac{105}{3} = 35$, $M_2 = \frac{105}{5} = 21$ ve $M_3 = \frac{105}{7} = 15$ olacaktır. $M_r x_r \equiv 1 \ (mod\ m_r)$ durumları sonuçlandırılmalıdır.

$$35x_1 \equiv 1 \ (mod\ 3),$$

$$21x_2 \equiv 1 \ (mod\ 5),$$

$$15x_3 \equiv 1 \ (mod\ 7),$$

kongrüans sistem çözümleri bulunmalıdır. $x_1 = 2$, $x_2 = 1$ ve $x_3 = 1$ olarak bulunur. Kongrüans sisteminin bir çözümü $x_0 = a_1M_1x_1 + a_2M_2x_2 + a_3M_3x_3 = 2 \cdot 35 \cdot 2 + 4 \cdot 21 \cdot 1 + 5 \cdot 15 \cdot 1 = 140 + 84 + 75 = 299$ ve $x_0 = 299 \equiv 89\ (mod\ 105)$ olacaktır.

Teorem: $m = m_1 \cdot m_2 \cdot \cdots \cdot m_r$, $m_1, m_2, \cdots, m_r$ sayıları ikişer ikişer aralarında asal olsun. O zaman $f(x) \equiv 0\ (mod\ m)$ kongrüansının bir çözümü olması için gerek ve yeter şart $f(x) \equiv 0\ (mod\ m_i)$ kongrüanslarının bir çözümünün bulunmasıdır. $N(m)$ ve $N(m_i)$ değerleri sırasıyla $f(x) \equiv 0\ (mod\ m)$ ve $f(x) \equiv 0\ (mod\ m_i)$ çözümlerinin sayısını belirtmek üzere $N(m) = N(m_1)N(m_2) \dots N(m_r)$ eşitliği sağlanır.

İspat: $f(x_0) \equiv 0\ (mod\ m)$ ve $m_i | m$ olduğundan $f(x_0) \equiv 0\ (mod\ m_i)$ olacaktır. Buna göre $f(x) \equiv 0\ (mod\ m)$ ifadesinin her çözümü $f(x) \equiv 0\ (mod\ m_i)$ ifadesinin de bir çözümü olacaktır. Karşıt olarak x_i $f(x) \equiv 0\ (mod\ m_i)$ sisteminin bir çözümü olsun, Çin Kalan Teoremine göre $x_0 \equiv x_i\ (mod\ m_i)$ olacak şekilde bir x_0 tam sayısı vardır. x_0 değeri için $f(x_0) \equiv f(x_i) \equiv 0\ (mod\ m_i)$ olacaktır. Modüller ikişer ikişer aralarında asal oldukları için $f(x_0) \equiv 0\ (mod\ m)$ olacaktır. Ayrıca, $f(x) \equiv 0\ (mod\ m_i)$ kongrüansların her bir çözümü için $x_0 \equiv x_i\ (mod\ m_i)$ kongrüansını gerçekleyen bir tek x_0 tam sayısını verdiğini biliyoruz. Her bir x_i değerinin $N(m_i)$ tane çözümünü ortaya koyarken $x_0 \equiv x_i\ (mod\ m_i)$ ve $f(x) \equiv 0\ (mod\ m_i)$ kongrüanslarını sağlayan x_0 tam sayılarının sayısının $N(m_1)N(m_2) \dots N(m_r)$ olacağı sonucuna ulaşılacaktır.

Örnek: $2x \equiv 3\ (mod\ 5)$, $4x \equiv 2\ (mod\ 6)$ ve $3x \equiv 2\ (mod\ 7)$ lineer kongrüans sisteminin çözüm kümesini bulalım.

Çözüm:

1.adım:

$2x \equiv 3\ (mod\ 5)$, $6x \equiv 9\ (mod\ 5)$, $x \equiv 4\ (mod\ 5)$ olur.

$4x \equiv 2\ (mod\ 6)$, $2x \equiv 1\ (mod\ 3)$, $4x \equiv 2\ (mod\ 3)$, $x \equiv 2\ (mod\ 3)$, $x \equiv 2\ (mod\ 6)$ olur. Ayrıca $(4, 6) = 2$ olduğundan $x + \frac{6}{2} \equiv 2 + 3 \equiv 5\ (mod\ 6)$ diğer bir çözümü olacaktır.

$3x \equiv 2\ (mod\ 7)$, $15x \equiv 10\ (mod\ 7)$, $x \equiv 3\ (mod\ 7)$ olur.

2.adım:

$m = 5 \cdot 6 \cdot 7 = 210$, $M_1 = \frac{210}{5} = 42$, $M_2 = \frac{210}{6} = 35$ ve $M_3 = \frac{210}{7} = 30$ olacaktır. $M_r x_r \equiv 1 \ (mod\ m_r)$ durumları sonuçlandırılmalıdır.

$$42x_1 \equiv 1 \ (mod\ 5),$$

$$35x_2 \equiv 1 \ (mod\ 6),$$

$$30x_3 \equiv 1 \ (mod\ 7),$$

kongrüans sistem çözümleri bulunmalıdır. $x_1 = 3, x_2 = 5$ ve $x_3 = 4$ olarak bulunur.

3.adım:

Kongrüans sisteminin çözümleri $x_0 = a_1M_1x_1 + a_2M_2x_2 + a_3M_3x_3 = 4 \cdot 42 \cdot 3 + 2 \cdot 35 \cdot 5 + 3 \cdot 30 \cdot 4 = 504 + 350 + 360 = 1214$ ve $x_0 = 1214 \equiv 164 \ (mod\ 210)$ olacaktır. $x_1 = a_1M_1x_1 + a_2M_2x_2 + a_3M_3x_3 = 4 \cdot 42 \cdot 3 + 5 \cdot 35 \cdot 5 + 3 \cdot 30 \cdot 4 = 504 + 875 + 360 = 1739$ ve $x_1 = 1739 \equiv 59 \ (mod\ 210)$ olacaktır.

Kongrüans sisteminin çözümlerinin sayısı, $N(210) = N(5)N(6)N(7) = 1 \cdot 2 \cdot 1 = 2$ olur.

Örnek: $3x + 4y \equiv 5 \ (mod\ 8)$ lineer kongrüans sisteminin çözüm kümelerini bulalım.

Çözüm: $3x \equiv 5 - 4y \ (mod\ 8)$, $(3, 8) = 1$ ve $1|(5 - 4y)$ olduğundan dolayı sistemin bir tek çözümü vardır. 8 modülüne göre $y = 0, 1, 2, 3, 4, 5, 6, 7$ değerlerini alacaktır.

1.çözüm: $y = 0$ için $3x \equiv 5 \ (mod\ 8)$, $9x \equiv 15 \ (mod\ 8)$, $x \equiv 7 \ (mod\ 8)$ olacaktır.

2.çözüm: $y = 1$ için $3x \equiv 5 - 4 \ (mod\ 8)$, $9x \equiv 3 \ (mod\ 8)$, $x \equiv 3 \ (mod\ 8)$ olacaktır.

3.çözüm: $y = 2$ için $3x \equiv 5 - 8 \ (mod\ 8)$, $9x \equiv 15 \ (mod\ 8)$, $x \equiv 7 \ (mod\ 8)$ olacaktır.

4.çözüm: $y = 3$ için $3x \equiv 5 - 12 \ (mod\ 8)$, $9x \equiv 1 \ (mod\ 8)$, $x \equiv 3 \ (mod\ 8)$ olacaktır.

5.çözüm: $y = 4$ için $3x \equiv 5 - 16 \ (mod\ 8)$, $9x \equiv 15 \ (mod\ 8)$, $x \equiv 7 \ (mod\ 8)$ olacaktır.

6.çözüm: $y = 5$ için $3x \equiv 5 - 20 \ (mod\ 8)$, $9x \equiv 3 \ (mod\ 8)$, $x \equiv 3 \ (mod\ 8)$ olacaktır.

7.çözüm: $y = 6$ için $3x \equiv 5 - 24 \ (mod\ 8)$, $9x \equiv 15 \ (mod\ 8)$, $x \equiv 7 \ (mod\ 8)$ olacaktır.

8.çözüm: $y = 7$ için $3x \equiv 5 - 28 \ (mod\ 8)$, $9x \equiv 3 \ (mod\ 8)$, $x \equiv 3 \ (mod\ 8)$ olacaktır.

$3x + 4y \equiv 5 \ (mod\ 8)$ lineer kongrüans sistemi, y tam sayısının herhangi bir değerine karşılık $x \equiv 3 \ (mod\ 8)$ ya da $x \equiv 7 \ (mod\ 8)$ olacaktır.

Teorem: $ax + by \equiv r\ (mod\ n)$ ve $cx + dy \equiv s\ (mod\ n)$ lineer kongrüans sistemleri, $(ad - bc, n) = 1$ olduğunda modül n değerine göre bir çözüme sahiptir.

İspat: $ax + by \equiv r\ (mod\ n)$ kongrüansı d, $cx + dy \equiv s\ (mod\ n)$ kongrüansı b tam sayılarıyla çarpılıp, çıkarma işlemi yapıldığında $(ad - bc)x \equiv (dr - bs)\ (mod\ n)$ kongrüansı elde edilir. t sayısı, $(ad - bc)$ sayısının n modülüne göre tersi ve $(ad - bc, n) = 1$ olmak üzere, $x \equiv t(dr - bs)\ (mod\ n)$ kongrüansına ulaşılır. Benzer yöntemlerle $y \equiv t(as - cr)\ (mod\ n)$ kongrüansına ulaşılır.

Örnek: $7x + 3y \equiv 10\ (mod\ 16)$ ve $2x + 5y \equiv 9\ (mod\ 16)$ lineer kongrüans sisteminin çözüm kümesini bulalım.

Çözüm: $(7 \cdot 5 - 2 \cdot 3, 16) = (29, 16) = 1$ olduğundan kongrüans sisteminin bir çözümü vardır. İlk kongrüansı 5, ikinci konfrüansı 3 tam sayısıyla çarpıp, çıkarma işlemi yapıldığında,

$29x \equiv 5 \cdot 10 - 3 \cdot 9 \equiv 23\ (mod\ 16)$, $13x \equiv 7\ (mod\ 16)$, $65x \equiv 35\ (mod\ 16)$, $x \equiv 3\ (mod\ 16)$ elde edilir. İlk kongrüansı 2, ikinci konfrüansı 7 tam sayısıyla çarpıp, çıkarma işlemi yapıldığında,

$29y \equiv 7 \cdot 9 - 2 \cdot 10 \equiv 43\ (mod\ 16)$, $13y \equiv 11\ (mod\ 16)$, $65y \equiv 55\ (mod\ 16)$, $y \equiv 7\ (mod\ 16)$ elde edilir. Kongrüans sisteminin çözüm kümesi $x \equiv 3\ (mod\ 16)$ ve $y \equiv 7\ (mod\ 16)$ olur.

Öneri: $\mathcal{S}$, elemanları tam sayı olan bir kare matris ve $m \in \mathbb{Z}^+$ olsun. $(det\mathcal{S}, m) = 1$, $\check{\mathcal{S}}$ matrisi m modülüne göre $\mathcal{S}$ matrisinin tersi ve $\widetilde{det\mathcal{S}}$ değeri m modülüne göre $det\mathcal{S}$ değerinin tersi olmak üzere $\check{\mathcal{S}} = \widetilde{det\mathcal{S}} \cdot adj\mathcal{S}$ eşitliği geçerlidir.

Örnek: $x + 2y + 3z \equiv 1\ (mod\ 7)$, $x + 3y + 5z \equiv 1\ (mod\ 7)$ ve $x + 4y + 6z \equiv 1\ (mod\ 7)$ lineer kongrüans sisteminin çözüm kümesini bulalım.

Çözüm:

$$\mathcal{S} = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 5 \\ 1 & 4 & 6 \end{bmatrix}, \mathcal{X} = \begin{bmatrix} x \\ y \\ z \end{bmatrix}, \mathcal{T} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

olmak üzere $\mathcal{S}\mathcal{X} \equiv \mathcal{T}\ (mod\ 7)$ yazılabilir. $det\mathcal{S} = -1$ ve $\widetilde{det\mathcal{S}} = 6$ olur. Gerekli işlemler yapılarak,

$$adj\mathcal{S} = \begin{bmatrix} -2 & 0 & 1 \\ -1 & 3 & -2 \\ 1 & -2 & 1 \end{bmatrix}$$

bulunur.

$$\check{\mathcal{S}} = \widetilde{det\mathcal{S}} \cdot adj\mathcal{S} = 6\begin{bmatrix} -2 & 0 & 1 \\ -1 & 3 & -2 \\ 1 & -2 & 1 \end{bmatrix} = \begin{bmatrix} -12 & 0 & 6 \\ -6 & 18 & -12 \\ 6 & -12 & 6 \end{bmatrix}.$$

$\mathcal{S}\mathcal{X} \equiv \mathcal{T}\ (mod\ 7)$, $\mathcal{X} \equiv \check{\mathcal{S}}\mathcal{T}\ (mod\ 7)$ olacağından,

$$\mathcal{X} = \begin{bmatrix} -12 & 0 & 6 \\ -6 & 18 & -12 \\ 6 & -12 & 6 \end{bmatrix}\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} -6 \\ 0 \\ 0 \end{bmatrix} \equiv \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}\ (mod\ 7).$$

Lineer kongrüans sisteminin çözüm kümesi, $x \equiv 1\ (mod\ 7)$, $y \equiv 0\ (mod\ 7)$ ve $z \equiv 0\ (mod\ 7)$ olarak bulunur.

UYGULAMALAR

1) $1^5 + 2^5 + 3^5 + \cdots + 99^5 + 100^5$ değerinin 4 sayısıyla bölümünden kalanını bulunuz.
2) $n < p < 2n$ ve p asal sayı olmak üzere $\binom{2n}{n} \equiv 0 \ (mod\ p)$ olduğunu gösteriniz.
3) $a \equiv b \ (mod\ n_1)$, $a \equiv b \ (mod\ n_2)$ ve $[n_1, n_2] = n$ olduğunda $a \equiv b \ (mod\ n)$ olduğunu gösteriniz.
4) $a \equiv b \ (mod\ n)$, $b \equiv c \ (mod\ n)$ ise $a \equiv c \ (mod\ n)$ olduğunu gösteriniz.
5) $a \equiv b \ (mod\ n)$ olduğunda herhangi bir pozitif k tam sayısı için $a^k \equiv b^k \ (mod\ n)$ olacağını gösteriniz.
6) 2 veya 3 sayısıyla bölünemeyen herhangi bir a tam sayısı için $a^2 \equiv 1 \ (mod\ 24)$ olduğunu gösteriniz.
7) a tek tam sayı, $n \geq 1$ olmak üzere, $a^{2^n} \equiv 1 \ (mod\ 2^{n+2})$ olduğunu gösteriniz.
8) $53^{103} + 103^{53}$ sayısının 39 sayısıyla bölümünden kalanını bulunuz.
9) $a^k \equiv b^k \ (mod\ n)$ ve $k \equiv j \ (mod\ n)$ olması durumunda $a^j \equiv b^j \ (mod\ n)$ olamayacağını gösteriniz.
10) 9^{3014} sayısının 7 sayısına bölümünden kalanını bulunuz.
11) k pozitif bir tam sayı olmak üzere, $(4^k - 11^k)$ sayısının 5 ile bölündüğünü gösteriniz.
12) a herhangi bir tek tam sayı ve $n \geq 1$ olmak üzere $a^{2^n} \equiv 1 \ (mod\ 2^{n+2})$ olacağını gösteriniz.
13) $p > 3$ asal sayısı için $(10^{2p} - 10^p + 1)$ sayısının 13 ile bölünebildiğini gösteriniz.
14) $x \equiv 5 \ (mod\ 6)$, $x \equiv 4 \ (mod\ 11)$ ve $x \equiv 3 \ (mod\ 17)$ lineer kongrüans sisteminin çözüm kümesini bulunuz.
15) Bir sayının 2, 3, 4, 5, 6 ile bölümünden kalan 1, 7 ile bölümünden kalan 0'dır. Bu durumu sağlayan en küçük doğal sayıyı bulunuz.

16) $17x \equiv 9\ (mod\ 276)$ lineer kongrüans sisteminin çözüm kümesini Çin Kalan Teoreminden faydalanarak bulunuz.

17) $4x + 51y \equiv 9\ (mod\ 35)$ kongrüans sisteminin çözüm kümesini bulunuz.

18) $3x + 4y \equiv 5\ (mod\ 13)$, $2x + 5y \equiv 7\ (mod\ 13)$ kongrüans sisteminin çözüm kümesini bulunuz.

19) $\begin{pmatrix} 2 & -1 \\ 3 & 4 \end{pmatrix}$ matrisinin, 5 modülü kullanılarak, toplama ve çarpma işlemlerine göre terslerini bulunuz.

20) $x + y \equiv 1\ (mod\ 7)$, $x + z \equiv 1\ (mod\ 7)$ ve $y + z \equiv 1\ (mod\ 7)$, sisteminin çözüm kümesini matrisleri kullanarak bulunuz.

KAYNAKLAR

1) Arias, P. J. (2024). *Elementary Number Theory*, Toronto Academic Press, Canada.
2) Burton, D. (2010). *Elementary Number Theory*. McGraw Hill, New York.
3) Chahal, J. S. (2021). *Algebraic Number Theory: A Brief Introduction*. Chapman and Hall Book, CRC Press, Boca Rato.
4) Effinger, G., ve Mullen, G. L. (2021). *Elementary Number Theory*. A Chapman and Hall Book, CRC Press, Boca Rato.
5) Fine, B., Moldenhauer, A., Rosenberger, G., Schürenberg, A., ve Wienke, L. (2023). *Algebra and Number Theory: A Selection of Highlights*. Walter de Gruyter GmbH, Berlin/Boston.
6) Guardia, J., Minculete, N., Savin, D., Vela, M., ve Zekhnini, A. (Eds.). (2024). *New Frontiers in Number Theory and Applications*. Birkhäuser, Switzerland.
7) Hunacek, M. (2023). *Introduction to Number Theory*. Chapman and Hall Book, CRC Press, Boca Rato.
8) Kundu, S., ve Mazumder, S. (2022). *Number Theory and Its Applications*. Levant Books, CRC Press, India.
9) Manescu-Avram, C. (2024). *Selection Tests in Number Theory for Mathematical Olympiads*. Springer, Switzerland.
10) Pongsriiam, P. (2023). *Analytic Number Theory for Beginners*. American Mathematical Society, Rhode Island.