YILDIZ TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

Bernoulli Sayıları

Necmi Engin

Yuksek Lisans Tezi

YILDIZ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BERNOULLİ SAYILARI

YÜKSEK LİSANS TEZİ

ARŞ.GÖR. NECMİ ENGİN

İSTANBUL - 1990

YILDIZ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BERNOULLİ SAYILARI

YÜKSEK LİSANS TEZİ

ARŞ.GÖR. NECMİ ENGİN

İSTANBUL – 1990

TEŞEKKÜR

Çalışmalarımda hiçbir zaman yardımını esirgemeyen sayın hocam Prof. Dr. Erol BALKANAY' a teşekkür ederim. Tezimin hazırlanması aşamasında yardımlarını esirgemeyen Uzman Recep AKKAYA, Arş. Gör. M.E. ÖZKAN ve arkadaşım Gökhan SARIKADILAR' a teşekkür ederim.

ÖZET

Bu çalısmada, Jacob BERNOULLI (1654-1705) tarafından bulunan fakat tartışması onun ölümünden sonra da devam eden ve Bernoulli Sayıları denen sayılar incelenmiştir.

Üç bölümden meydana gelen çalışmanın ilk bölümünde konu ile ilgili temel tanımlar, teoremler ve bilgisayar programları verilmiştir. Daha sonra Bernoulli Sayıları ile ilgili rekürans bağıntıları incelenmiş ve bu rekürans bağıntılarından faydalanarak, Matematiğin farklı alanlarında kullanılan Bernoulli polinomları ile Riemann-Zeta fonksiyonları belli bir mertebeye kadar hesaplanmıştır.

İkinci bölümde Bernoulli Sayılarının aritmetik özellikleri incelenmiş ve Clauss-von Staudt teoremi verilmiştir. Ayrıca burada Bernoulli Sayılarının payı ve paydası hakkında bilgiler verilmiştir.

Son bölüm Kummer kongrüansları ve regüler asal sayıların incelenmesine ayrılmıştır. Ayrıca Riemann-Zeta fonksiyonu kullanılarak Kummer kongrüanslarının modern bir yorumu yapılmıştır.

Yapılan bilgisayar programlarıyla 1754 tane Bernoulli Sayısı hesaplanmıştır. Daha fazla sayıda Bernoulli Sayısının hesaplanmasına, kullandığımız makinanın bellek kapasitesi yeterli olmamıştır.

SUMMARY

In this study we will introduce an important sequence of rational numbers discovered by Jacob BERNOULLI (1654-1705). These numbers, now called Bernoulli numbers, appear in many different areas of Mathematics.

These thesis consist of three chapters. Chapter I contains an introduction to the basic definition and theorems about Bernoulli numbers, Bernoulli polinomals and Riemann-Zeta functions. In this chapter, it is also given computer programs to evaluate the Bernoulli numbers.

In the chapter II we study the aritmetical properties of Bernoulli numbers and Clauss-von Staudt theorem.

In the last chapter, Kummer Congruences and regular primes have been examined.

1.BERNOULLI SAYILARI

Önce ilk n tamsayının k. kuvvetlerinin toplamını bulma problemini ele alacağız. Örneğin ;

$$1 + 2 + 3 + \ldots + (n-1) = \frac{n.(n-1)}{2}$$

$$1^2 + 2^2 + 3^2 + \ldots + (n-1)^2 = \frac{n.(n-1).(2n-1)}{6}$$

$$1^3 + 2^3 + 3^3 + \ldots + (n-1)^3 = \frac{n^2.(n-1)^2}{4}$$

olduklarını biliyoruz. Jakob Bernoulli bu formülleri, ilk n tamsayının 1.,2.,3.,...,10. kuvvetleri için biliyordu.

$$1^k + 2^k + 3^k + \ldots + (n-1)^k$$

toplamının her k için (k+1). dereceden n' e bağlı bir polinom olduğu bellidir. Bernoulli çalışmalarında; genel bir k sayısı için polinomun katsayılarını hesaplamayı başarmış. Kendi adını taşıyan sayıları tanımlayan ilk kişi olmuştur. J.Bernoulli, 1 saat 45 dakikadan daha az bir zaman içerisinde ilk 1000 tamsayının 10. kuvvetlerini toplayabilmeyi mükemmel bir şekilde başarmıştır.

Bu kez amacımız;

$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ Riemann-Zeta fonksiyonu olmak üzere,

$$\zeta(s) = 1 + \frac{1}{4} + \frac{1}{9} + \ldots$$

toplamının değerini belirlemek ve m>0 şeklindeki bir tamsayı için $\zeta(2m)$' i genelleştirmektir. L.Euler 1734' de

$\zeta(2) = \frac{\pi^2}{6}$ olduğunu göstermişti. Daha sonra her m>0 tamsayısı için $\zeta(2m)$' i hesapladı.

TANIM 1.1.

Eğer p asal sayısı, $Q(\zeta_p)$'nin sınıf sayısına bölünmüyorsa, reguler asal sayı olarak adlandırılır.■

Ayrıca Kummer bölünebilme özelliği içeren $\frac{(p-3)}{2}$ tane Bernoulli sayısının regularitesi için güzel ve elemanter bir yöntem keşfetti.

Şimdi incelediğimiz problemlere dönelim:

$$S_m(n) = 1^m + 2^m + 3^m + \ldots + (n-1)^m$$

şeklinde tanımlayalım. Bu toplamın değerini hesaplamak için basit bir tümevarım metodu verelim. Binom teoremine göre $(k+1)^{m+1}$ ifadesinin açılımı;

$$(k+1)^{m+1} = 1 + \overset{1}{C}_{m+1}.k + \overset{2}{C}_{m+1}.k^2 + \ldots + \overset{m}{C}_{m+1}.k^m + \overset{m+1}{C}_{m+1}.k^{m+1}$$

şeklindedir.

$\overset{m+1}{C}_{m+1} = 1$ olduğundan dolayı

$$(k+1)^{m+1} = 1 + \overset{1}{C}_{m+1}.k + \overset{2}{C}_{m+1}.k^2 + \ldots + \overset{m}{C}_{m+1}.k^m + k^{m+1}$$

olarak yazabiliriz. Şu halde

$$(k+1)^{m+1} - k^{m+1} = 1 + \overset{1}{C}_{m+1}.k + \overset{2}{C}_{m+1}.k^2 + \ldots + \overset{m}{C}_{m+1}.k^m$$

şekline getirmiş oluruz.

$k=0,1,2,3,\ldots,(n-1)$ değerlerini yerine koyarsak;

$k=0$ ise $1^{m+1} = 1$

$$k=1 \text{ ise } 2^{m+1}-1^{m+1} = 1 + \overset{1}{C}_{m+1}.1 + \overset{2}{C}_{m+1}.1^2 + \ldots + \overset{m}{C}_{m+1}.1^m$$

$$k=2 \text{ ise } 3^{m+1}-2^{m+1} = 1 + \overset{1}{C}_{m+1}.2 + \overset{2}{C}_{m+1}.2^2 + \ldots + \overset{m}{C}_{m+1}.2^m$$

. . . . . .

. . . . . .

$$k=n-1 \text{ ise } n^{m+1}-(n-1)^{m+1} = 1 + \overset{1}{C}_{m+1}.(n-1) + \overset{2}{C}_{m+1}.(n-1)^2 + \ldots + \overset{m}{C}_{m+1}.(n-1)^m$$

eşitliklerini bulmuş oluruz. Bunlar taraf tarafa toplanırsa;

$$n^{m+1} = n + \binom{1}{m+1}.(1+2+\ldots+(n-1)) + \binom{2}{m+1}.(1^2+2^2+\ldots+(n-1)^2)+$$

$$\ldots+ \binom{m}{m+1}.(1^m+2^m+\ldots+(n-1)^m) \qquad [1]$$

sonucu çıkar. Daha önce

$$S_m(n) = 1^m + 2^m + 3^m +\ldots+ (n-1)^m$$

şeklinde tanımlanmıştı. O halde

$$S_1(n) = 1 + 2 + 3 +\ldots+ (n-1)$$

$$S_2(n) = 1^2 + 2^2 + 3^2 +\ldots+ (n-1)^2$$

.
.
.

eşitlikleri [1] denkleminde yerine yazılırsa;

$$n^{m+1} = n + \binom{1}{m+1}.S_1(n) + \binom{2}{m+1}.S_2(n) +\ldots+ \binom{m}{m+1}.S_m(n) \quad [2]$$

sonucuna varmış oluruz.

Eğer $S_1(n)$, $S_2(n)$, ... , $S_{m-1}(n)$ için bir formül varsa o zaman [2] den $S_m(n)$ için bir formül elde ederiz.

Bernoulli $S_m(n)$' nin en büyük dereceli terimi $\frac{n^{m+1}}{m+1}$

olan (n+1). dereceden bir polinom olduğunu gözlemlemişti. Bu [2] eşitliğinden tümevarım vasıtasıyla kolayca bulunur. Ayrıca sabit terimler sıfırdır.

m=0,1,...,10 için n' nin katsayılarının;

$$\frac{-1}{2}, \frac{1}{6}, 0, \frac{-1}{30}, 0, \frac{1}{42}, 0, \frac{-1}{30}, 0, \frac{5}{66}$$

olduğu aşağıdaki şekilde hesaplanabilir:

m=1 için;

$$n^2 = n + \overset{1}{C}_2 \cdot S_1(n)$$

$$n^2-n = \frac{2!}{1!1!}.S_1(n) \quad ===> \quad S_1(n) = \frac{n.(n-1)}{2}$$

Burada n'li terimin katsayısı $\frac{-1}{2}$ dir.

m=2 için;

$$n^3 = n + \overset{1}{C}_3 \cdot S_1(n) + \overset{2}{C}_3 \cdot S_2(n)$$

$$n^3-n = \frac{3!}{2!1!}.S_1(n) + \frac{3!}{1!2!}.S_2(n)$$

$$n^3-n = 3.\frac{1}{2}.n(n-1) + 3.S_2(n)$$

$$S_2(n) = \frac{2n.(n^2-1)-3n.(n-1)}{6}$$

$$S_2(n) = \frac{2n.(n-1).(n+1)-3n.(n-1)}{6}$$

$$S_2(n) = \frac{n.(n-1).(2n+2-3)}{6}$$

$$S_2(n) = \frac{n.(n-1).(2n-1)}{6}$$

Burada n'li terimin katsayısı $\frac{1}{6}$ dir.

m=3 için

$$n^4 = n + \overset{1}{C}_4 \cdot S_1(n) + \overset{2}{C}_4 \cdot S_2(n) + \overset{3}{C}_4 \cdot S_3(n)$$

$$n^4-n = \frac{4!}{3!1!}.S_1(n) + \frac{4!}{2!2!}.S_2(n) + \frac{4!}{1!3!}.S_3(n)$$

$$n^4-n=\frac{4!}{3!1!}.\left(\frac{1}{2}.n(n-1)\right)+ \frac{4!}{2!2!}.\left(\frac{1}{6}.n(n-1)(2n-1)\right)+ \frac{4!}{1!3!}.S_3(n)$$

$$4.S_3(n) = n^4-n-2n.(n-1)-n.(n-1).(2n-1)$$

$$4.S_3(n) = n.(n^3-1)-2n.(n-1)-n.(n-1).(2n-1)$$

$$4.S_3(n) = n.(n-1).(n^2+n+1)-2n.(n-1)-n.(n-1).(2n-1)$$

$$4.S_3(n) = n.(n-1).(n^2+n+1-2-2n+1)$$

$$4.S_3(n) = n.(n-1).(n^2-n)$$

$$4.S_3(n) = n^2.(n-1)^2$$

$$S_3(n) = \frac{1}{4}.n^2.(n-1)^2$$

Burada n'li terim olmadığından katsayısı 0 olarak alınır.
Bu şekilde devam edilirse;

m=4 için n' li terimin katsayısı $\frac{-1}{30}$

m=5 için n' li terimin katsayısı 0

m=6 için n' li terimin katsayısı $\frac{1}{42}$

m=7 için n' li terimin katsayısı 0

m=8 için n' li terimin katsayısı $\frac{-1}{30}$

m=9 için n' li terimin katsayısı 0

m=10 için n' li terimin katsayısı $\frac{5}{66}$

olarak bulunacaktır.

TANIM 1.2.

$B_0, B_1, B_2 \ldots$ Bernoulli sayıları dizisi,

$B_0 = 1$ ve $B_1, B_2, \ldots, B_{m-1}$ hesaplanmış olmak üzere B_m;

$$(m+1).B_m = -\sum_{k=0}^{m-1} C_{m+1}^{k} .B_k \qquad [3]$$

şeklinde tanımlanır. Bu ifadede m=1,2,3,... yazılırsa;

$$1 + 2B_1 = 0$$

$$1 + 3B_1 + 3B_2 = 0$$

$$1 + 4B_1 + 6B_2 + 4B_3 = 0$$

$$1 + 5B_1 + 10B_2 + 10B_3 + 5B_4 = 0$$

.....

.....

elde edilir. Buradan

$$B_1=\frac{1}{2},\ B_2=\frac{1}{6},\ B_3=0,\ B_4=\frac{-1}{30},\ B_5=0,\ B_6=\frac{1}{42},\ldots$$

olarak bulunur. Daha sonra sıfırdan farklı Bernoulli sayılarının işaretinin +,-,-,+,-,+,... şeklinde değiştiğini göstereceğiz. Ayrıca 1' den büyük tek indisli Bernoulli sayılarının sıfır olduğu görülecetir.

PROGRAM 1.1

```
    Program Bernoulli_Sayilari ;
        Uses Dos, Crt, Printer ;
        Var
          I, K, F, N, M : Integer ;
          Pay,
          Payda         : Extended ;
          Bernoulli     : Array[0..1000] Of Extended ;

          Function Fakt( Fak : LongInt ) : Extended ;
        Var
          Faktoriyel : Extended ;
       Begin
          Faktoriyel := 1 ;
          If Fak = 0 Then
        Begin
          Fakt := Faktoriyel ;
          Exit ;
       End ;
     For N := 1 To Fak Do
     Begin
         Faktoriyel := Faktoriyel * N ;
       End ;
     Fakt := Faktoriyel ;
  End ;

Procedure Hesap ;
  Begin
            Pay := Fakt( K + 1 ) ;
            Payda := Fakt( K + 1 - I ) ;
            Payda := Payda * Fakt( I ) ;
    Bernoulli[K] := Bernoulli[K]-(Pay/Payda)*Bernoulli[I] ;
  End ;

Procedure Bernoulli_Hesap ;
  Begin
    For I := 0 To K-1 Do
   Begin
     If I <= 2 Then Hesap ;
      If (I>2) And (I/2=Int(I/2)) Then Hesap ;
      End ;
    Bernoulli[K] := Bernoulli[K]/(K+1) ;
  End ;
Procedure Bernoulli_Yaz ;
       Begin
            WriteLn( '   ',I,'      ',Bernoulli[I] ) ;
        End ;
        Begin
          Bernoulli[0] := 1 ;
           Write( 'M Degerini Giriniz : ' ) ;
```

```
ReadLn( M ) ;
   For K := 1 To M Do
 Begin
   Bernoulli[K] := 0 ;
 End ;
For K := 1 To M Do
Begin
 If K <= 2 Then Bernoulli_Hesap ;
 If (K>2) And (K/2=Int(K/2)) Then Bernoulli_Hesap ;
End ;
 ClrScr ;
   WriteLn( '  M          Bernoulli(M)    ' ) ;
   WriteLn( '-----        ------------------') ;
 For I := 0 To M Do
Begin
 If I <= 2  Then Bernoulli_Yaz ;
 If (I>2) AND (Int(I/2)=I/2) Then Bernoulli_Yaz ;
End ;
 Readln ;
End .
```

M Degerini Giriniz : 6

M	Bernolli(M)
0	$B_0 = 1$
1	$B_1 = \frac{-1}{2} = -0.50000000...$
2	$B_2 = \frac{1}{6} = 0.166666666...$
4	$B_4 = \frac{-1}{30} = -0.03333333...$
6	$B_6 = \frac{1}{42} = 0.02389523895...$
8	$B_8 = \frac{-1}{30} = -0.03333333...$
10	$B_{10} = \frac{5}{66} = 0.0757575757...$

LEMMA 1.1.

$\frac{t}{e^t-1}$ ifadesi origin cıvarında

$$\frac{t}{e^t-1} = \sum_{m=0}^{\infty} b_m . \left(\frac{t^m}{m!} \right)$$

şeklinde bir kuvvet serisine açılırsa, her m için $b_m=B_m$ olur.

İSPAT.

$$\frac{t}{e^t-1} = \sum_{m=0}^{\infty} b_m . \left(\frac{t^m}{m!} \right)$$

ifadesinin her iki yanını e^t-1 ile çarpalım.

$$t = (e^t-1) . \sum_{m=0}^{\infty} b_m . \left(\frac{t^m}{m!} \right) \qquad [4]$$

$$e^t-1 = 1 + \frac{t^2}{2!} + \frac{t^3}{3!} + \ldots + \frac{t^n}{n!} - 1$$

$$e^t-1 = \sum_{n=1}^{\infty} \frac{t^n}{n!}$$

şeklindedir. Bu ifade [4] de yerine yazılırsa,

$$t = \sum_{n=1}^{\infty} \frac{t^n}{n!} . \sum_{m=0}^{\infty} b_m . \left(\frac{t^m}{m!} \right)$$

$$t = \sum_{m=0}^{\infty} b_m . \left(\frac{t^m}{m!} \right) . \left(t + \frac{t^2}{2!} + \frac{t^3}{3!} + \ldots + \frac{t^n}{n!} \right)$$

$$t = \sum_{m=0}^{\infty} b_m . \left(\frac{t^{m+1}}{m!1!} + \frac{t^{m+2}}{m!2!} + \ldots + \frac{t^{m+n}}{m!n!} + \ldots \right)$$

elde edilir. Burada m=0 için;

$$t = b_0.\left(t + \frac{t^2}{2!} + \frac{t^3}{3!} + \ldots + \frac{t^n}{n!} + \ldots \right)$$

bulunur. Burada iki taraf birbirine özdeşlenirse

$$t = b_0.t \quad ===> \quad b_0 = 1 \text{ elde edilir.}$$

m=1 için benzer yolla;

$$t = b_0.\left(t + \frac{t^2}{2!} + \frac{t^3}{3!} + \ldots + \frac{t^n}{n!} + \ldots \right) +$$

$$b_1.\left(\frac{t^2}{1!} + \frac{t^3}{1!2!} + \ldots + \frac{t^{n+1}}{1!n!} + \ldots \right)$$

$$t = t + \frac{t^2}{2!} + \frac{t^3}{3!} + \ldots + \frac{t^n}{n!} + \ldots + b_1.\left(\frac{t^2}{1!} + \frac{t^3}{1!2!} + \ldots + \frac{t^{n+1}}{1!n!} + \ldots \right)$$

$$b_1.t^2 = \frac{-t^2}{2} \quad ===> \quad b_1 = \frac{-1}{2} \text{ elde edilir.}$$

Bu işlemi

$$\sum_{k=0}^{m} C_{m+1}^{k} .b_k = 0$$

şeklinde genelleştirebiliriz. Bu ise Bernoulli sayılarını tanımlayan [3] denklem sistemi ile aynıdır.

$$b_0 = B_0 = 1 \quad \text{ve} \quad b_1 = B_1 = \frac{-1}{2}$$

olduklarından dolayı $b_m = B_m$ olur.■

Şimdi $S_m(n)$ toplamının değerinin bulunması problemine dönelim. J.Bernoulli' nin çözümünü gösterelim.

TEOREM 1.1.

$m \geq 1$ için $S_m(n)$ toplamı,

$$(m+1).S_m(n) = \sum_{k=0}^{m} C_{m+1}^{k} B_k . n^{m+1-k}$$

şeklindedir.

İSPAT.

$$e^{kt} = \sum_{m=0}^{\infty} k^m . \left(\frac{t^m}{m!} \right)$$

açılımında $k = 0,1,2,\ldots,(n-1)$ koyalım:

$k = 0$ için $\quad 1 = \sum_{m=0}^{\infty} 0^m . \left(\frac{t^m}{m!} \right)$

$k = 1$ için $\quad e^t = \sum_{m=0}^{\infty} 1^m . \left(\frac{t^m}{m!} \right)$

$k = 2$ için $\quad e^{2t} = \sum_{m=0}^{\infty} 2^m . \left(\frac{t^m}{m!} \right)$

. .

. .

. .

$k = n-1$ için $\quad e^{(n-1)t} = \sum_{m=0}^{\infty} (n-1)^m . \left(\frac{t^m}{m!} \right)$

taraf tarafa toplanırsa,

$$1+e^t+e^{2t}+\ldots+e^{(n-1)t} = \sum_{m=0}^{\infty} (0^m+1^m+2^m+\ldots+(n-1)^m) . \left(\frac{t^m}{m!} \right)$$

olur. Daha önce

$$S_m(n) = 1^m + 2^m + 3^m + \ldots + (n-1)^m$$

şeklinde tanımlanmıştı. O zaman buradan

$$1+e^{t}+e^{2t}+\ldots+e^{(n-1)t} = \sum_{m=0}^{\infty} S_m(n).\left(\frac{t^m}{m!}\right) \qquad [5]$$

sonucu çıkar. Sol taraftaki toplamı

$$1+e^{t}+e^{2t}+\ldots+e^{(n-1)t} = \frac{e^{nt}-1}{e^{t}-1} \qquad [6]$$

şeklinde alalım ve t ile bölelim. Yani

$$\frac{e^{nt}-1}{e^{t}-1} = \frac{e^{nt}-1}{t}.\frac{t}{e^{t}-1}$$

şeklinde gözönüne alalım.

$$e^{nt}-1 = 1 + n.t + n^2.\frac{t^2}{2!} + n^3.\frac{t^3}{3!} + \ldots + n^k.\frac{t^k}{k!} - 1$$

$$\frac{e^{nt}-1}{t} = \sum_{k=1}^{\infty} n^k.\frac{t^{k-1}}{k!}$$

şeklinde ifade edebiliriz. Ayrıca

$$\frac{t}{e^{t}-1} = \sum_{j=0}^{\infty} B_j.\frac{t^j}{j!}$$

olduğunu lemma 1.1.' de göstermiştik. Ozaman

$$\frac{e^{nt}-1}{t}.\frac{t}{e^{t}-1} = \sum_{k=1}^{\infty} n^k.\frac{t^{k-1}}{k!}.\sum_{j=0}^{\infty} B_j.\frac{t^j}{j!} \qquad [7]$$

sonucuna varmış oluruz.

[6] ve [7] denklemlerinin sağ taraflarındaki ifadelerin t^m. terimlerini eşitleyelim;

$$\sum_{m=0}^{\infty} S_m(n).\left(\frac{t^m}{m!}\right) = S_0(n)+S_1(n).t+S_2(n).\frac{t^2}{2!}+\ldots+S_m(n).\frac{t^m}{m!}$$

$$\sum_{k=1}^{\infty} n^k.\frac{t^{k-1}}{k!}\ .\sum_{m=0}^{\infty} B_m.\frac{t^m}{m!}=(n+n^2.\frac{t}{2!}+\ldots+n^k.\frac{t^{k-1}}{k!}+\ldots)$$

$$*(B_0+\ B_1.\frac{t}{2!}+\ldots+B_m.\frac{t^m}{m!}+\ldots)$$

$$=n.B_0+n.B_1.t+n.B_2.\frac{t^2}{2!}+\ldots+n.B_m.\frac{t^m}{m!}+\ldots$$

$$+n^2.\frac{t}{2!}.B_0+n^2.\frac{t^2}{2!1!}.B_1+\ldots+n^2.\frac{t^{m+1}}{2!m!}.B_m+\ldots$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$+n^k.\frac{t^{k-1}}{k!}.B_0+n^k.\frac{t^k}{k!1!}.B_1+\ldots+n^k.\frac{t^{k-1+m}}{k!m!}.B_m$$

===>

$$S_m.\frac{t^m}{m!}\ =\ t^m.(\ n.\frac{B_m}{m!}\ +\ n^2.\frac{B_{m-1}}{(m-1)!}\ +\ldots+n^k.\frac{B_{m-1+k}}{(m+1-k)!}\ )$$

her iki tarafı (m+1)! ile çarpalırsa;

$$S_m.\frac{(m+1)!}{m!}\ =\ (m+1)!.(n.\frac{B_m}{m!}\ +\ n^2.\frac{B_{m-1}}{(m-1)!}\ +\ldots+n^k.\frac{B_{m-1+k}}{(m+1-k)!})$$

$$(m+1).S_m(n)\ =\ \overset{0}{C}_{m+1}.n.B_m+\overset{1}{C}_{m+1}.n^2.B_{m-1}+\ldots+\overset{k}{C}_{m+1}.n^k.B_{m-k+1}$$

olur. Bu ifadeyi

$$(m+1).S_m(n)\ =\ \sum_{k=0}^{m}\ \overset{k}{C}_{m+1}.n^{m+1-k}.B_k$$

seklinde yazabiliriz. Buda bize teoremin ispatını verir.■

Teorem 1.1' in sonucunu yeniden düzenlediğimizde Bernoulli polinomları olarak bilinen çok önemli polinom tipi ile karşılaşırız. Bu polinomlar

$$B_m(x) = \sum_{k=0}^{m} C_m^k \, B_k . x^{m-k}$$

ile tanımlanırlar. Dolayısıyla

$$B_1(x) = x - \frac{1}{2}$$

$$B_2(x) = x^2 - x + \frac{1}{6}$$

.....

.....

şeklindedir. O zaman Teorem 1.1

$$S_m(n) = \frac{1}{m+1} . (B_{m+1}(n) - B_{m+1})$$

şeklinde yazılabilir. Bu ifade Lemma1.1' deki her k≥1 için ispatlanan $B_{2k+1}=0$ sonucunu verir.

$B_1 = \frac{-1}{2}$ olduğundan

$$\frac{t}{e^{t-1}} + \frac{t}{2} = 1 + \sum_{k=0}^{\infty} B_k . \frac{t^k}{k!}$$

şeklinde alınabilir. Sol tarafta t yerine -t konulduğunda değişmediğinden, bu ifade t' nin bir çift fonksiyonudur.

PROGRAM 1.2

```
Program Bernoulli_Polinomlari ;

 Uses Dos, Crt, Printer ;
 Var
   I, K, F, N, M : Integer ;
   Pay,
   Payda         : Extended ;
   Bernoulli     : Array[0..1000] Of Extended ;
```

```
    Function Fakt( Fak : LongInt ) : Extended ;
  Var
      Faktoriyel : Extended ;
  Begin
      Faktoriyel := 1 ;
  If Fak = 0 Then
     Begin
          Fakt := Faktoriyel ;
          Exit ;
        End ;
       For N := 1 To Fak Do
     Begin
          Faktoriyel := Faktoriyel * N ;
        End ;
       Fakt := Faktoriyel ;
    End ;

Procedure Hesap ;
        Begin
            Pay := Fakt( K + 1 ) ;
            Payda := Fakt( K + 1 - I ) ;
            Payda := Payda * Fakt( I ) ;
    Bernoulli[K] := Bernoulli[K]-(Pay/Payda)*Bernoulli[I] ;
  End ;

Procedure Bernoulli_Hesap ;
        Begin
            For I := 0 To K-1 Do
            Begin
             If I <= 2 Then Hesap ;
     If ( I > 2 ) And ( I / 2 = Int( I / 2 ) ) Then Hesap ;
    End ;
   Bernoulli[K] := Bernoulli[K]/(K+1) ;
  End ;
        Begin
           Bernoulli[0] := 1 ;
            Write( 'M Degerini Giriniz : ' ) ;
            ReadLn( M ) ;
            For K := 1 To M Do
             Begin
               Bernoulli[K] := 0 ;
            End ;
        For K := 1 To M Do
      Begin
           If K <= 2 Then Bernoulli_Hesap ;
         If (K>2) And (K/2=Int(K/2)) Then Bernoulli_Hesap ;
      End ;
    For I := 1 To M DO
    Begin
        Write( 'B',I,'(X)=' ) ;
        For K := 0 To I Do
```

```
      Begin
          Pay := Fakt( I ) ;
          Payda := Fakt( I-K ) ;
          Payda := Payda * Fakt( K ) ;
     If (Bernoulli[K]>0) And (K>1) Then Write ('+') ;
 If Bernoulli[K]<>0 Then Write(Bernoulli[K]*Pay/Payda) ;
   If (Bernoulli[K]<>0) And (I<>K) Then Write('X^',I-K) ;
        End ;
     WriteLn ;
   End ;
  Readln ;
End .
```

```
        M Degerini Giriniz : 6
```

$$B_0(x) = 1$$

$$B_1(x) = x - \frac{1}{2}$$

$$B_2(x) = x^2 - x + \frac{1}{6}$$

$$B_3(x) = x^3 - \frac{3}{2}.x^2 + \frac{1}{2}.x$$

$$B_4(x) = x^4 - 2.x^3 + x^2 - \frac{1}{30}$$

$$B_5(x) = x^5 - \frac{5}{2}.x^4 + \frac{5}{3}.x^3 - \frac{1}{6}.x$$

$$B_6(x) = x^6 - 3.x^5 + \frac{5}{2}.x^4 - \frac{1}{2}.x^2 + \frac{1}{42}$$

Şimdi $m=1,2,3,\ldots$ için $\tau(2m)$ sayıları ile Bernoulli sayıları arasındaki ilişkiye dönelim :

TEOREM 1.2.

Bir m pozitif tamsayısı için;

$$2\tau.(2m) = (-1)^m.\frac{(\pi)^{2m}}{(2m)!}.B_{2m}$$

şeklindedir.

İSPAT.

İspat için Cotx açılımının kısmi kesirlerine ihtiyacımız vardır.

$$Cotx = \frac{1}{x} - 2.\sum_{n=1}^{\infty} \frac{x}{\pi^2 n^2 - x^2} \qquad [8]$$

Bu açılımı elde etmek için birçok yol vardır. Bunlardan biri Cosαt' nin Fourier serisinde t yerine 1 koymakla bulunur. Diğer bir sonuç ise Sinx' in sonsuz çarpımı açılımı olan

$$Sinx = x.\prod_{n=1}^{\infty}\left(1 - \frac{x^2}{\pi^2 n^2}\right)$$

ifadesinin logaritmasını alıp; türev almakla elde edilir. [8] denkleminin sağ tarafı geometrik seri formülü yardımıyla 0 cıvarında seriye açılırsa;

$$x.Cotx = 1 - 2.\sum_{m=1}^{\infty} \tau(2m).\frac{x^{2m}}{\pi^{2m}} \qquad [9]$$

elde edilir. [8] denkleminin sol tarafını başka bir yolla bulalım:

$$Cosx = \frac{e^{ix}+e^{-ix}}{2} \quad ve \quad Sinx = \frac{e^{ix}-e^{-ix}}{2i}$$

olduklarını biliyoruz. Bunlar Cotx' de yerine yazılırsa;

$$Cotx = \frac{Cosx}{Sinx} = \frac{\frac{e^{ix}+e^{-ix}}{2}}{\frac{e^{ix}-e^{-ix}}{2i}} = i.\frac{e^{ix}+e^{-ix}}{e^{ix}-e^{-ix}}$$

$$Cotx = i.\frac{e^{-ix}.(e^{2ix}+1)}{e^{-ix}(e^{2ix}-1)} = i.\frac{e^{2ix}+1-2+2}{e^{2ix}-1}$$

$$Cotx = i.\frac{e^{2ix}-1}{e^{2ix}-1} + i.\frac{2}{e^{2ix}-1}$$

$$Cotx = i + \frac{2i}{e^{2ix}-1}$$

$$x.Cotx = ix + \frac{2ix}{e^{2ix}-1}$$

elde edilir. Ayrıca bu ifadenin

$$x.Cotx = ix + \frac{2ix}{e^{2ix}-1} = 1 + \sum_{n=2}^{\infty} \frac{(2ix)^n}{n!}.B_n \qquad [10]$$

şeklinde ifade edilebileceğini gösterelim:

$e^{2ix}-1$ ifadesini 0 cıvarında seriye açalım;

$$e^{2ix}-1 = 2ix + \frac{(2ix)^2}{2!} + \frac{(2ix)^4}{4!} + \ldots + \frac{(2ix)^n}{n!}$$

şeklindedir. Buradan;

$$\frac{2ix}{e^{2ix}-1} = 1-ix+ \frac{(2ix)^2}{2!}.\left(\frac{1}{6}\right)+ \frac{(2ix)^4}{4!}.\left(\frac{-1}{30}\right)+\ldots$$

olur. Ayrıca

$$B_2 = \frac{1}{6} \quad , \quad B_4 = -\frac{1}{30} \quad , \quad \ldots$$

olduklarından dolayı bu ifade;

$$\frac{2ix}{e^{2ix}-1} = 1 - ix + \frac{(2ix)^2}{2!}.B_2 + \frac{(2ix)^4}{4!}.B_4 + \ldots$$

$$ix - \frac{2ix}{e^{2ix}-1} = 1 + \frac{(2ix)^2}{2!}.B_2 + \frac{(2ix)^4}{4!}.B_4 + \ldots$$

$$ix - \frac{2ix}{e^{2ix}-1} = 1 + \sum_{n=2}^{\infty} \frac{(2ix)^n}{n!}.B_n$$

olur. [8],[9],[10] ifadelerinden

$$x.\cot x = 1 - 2.\sum_{m=1}^{\infty} \gamma(2m).\frac{x^{2m}}{\pi^{2m}} = 1 + \sum_{m=2}^{\infty} \frac{(2ix)^m}{m!}.B_m$$

$$1 - 2\gamma(2).\frac{x^2}{\pi^2} - 2\gamma(4).\frac{x^4}{\pi^4} - \ldots - 2\gamma(2m).\frac{x^{2m}}{\pi^{2m}} - \ldots =$$

$$1 + \frac{(2ix)^2}{2!}.B_2 + \frac{(2ix)^4}{4!}.B_4 + \ldots + \frac{(2ix)^{2m}}{2m!}.B_{2m} + \ldots$$

Burada x^{2m}. terimler karşılıklı özdeşlenirse;

$$-2.\gamma(2m).\frac{x^{2m}}{\pi^{2m}} = \frac{(2ix)^{2m}}{2m!}.B_{2m}$$

$$-2.\gamma(2m).\frac{x^{2m}}{\pi^{2m}} = \frac{(i^2)^m.x^{2m}}{2m!}.B_{2m}$$

$$\frac{-2}{\pi^{2m}}.\tau(2m) = (-1)^m.\frac{2^{2m}}{2m!}.B_{2m}$$

elde edilir, ispatlanması gerekende budur.■

Euler tarafından bulunmuş olan bu sonuç onun olağanüstü hesaplamalarından biri olarak bilinir.

ÖRNEK

$$\frac{-2}{\pi^{2m}}.\tau(2m) = (-1)^m.\frac{2^{2m}}{2m!}.B_{2m}$$

m=1 için $B_2 = \frac{1}{6}$ olduğundan

$$\frac{-2}{\pi^2}.\tau(2) = (-1).\frac{2^2}{2!}.B_2$$

$$\frac{-2}{\pi^2}.\tau(2) = (-1).\frac{1}{6}$$

$$\tau(2) = \frac{\pi^2}{6};$$

m=2 için $B_2 = \frac{-1}{30}$ olduğundan

$$\frac{-2}{\pi^4}.\tau(4) = (-1)^2.\frac{2^4}{4!}.B_4$$

$$\frac{-2}{\pi^4}.\tau(4) = \frac{16}{24}.(\frac{-1}{30})$$

$$\tau(4) = \frac{\pi^4}{90};$$

m=3 için $B_6 = \frac{1}{42}$ olduğundan

$$\frac{-2}{\pi^6}.\tau(6) = (-1)^3.\frac{2^6}{6!}.B_6$$

$$\frac{-2}{\pi^6}.\tau(6) = \frac{-64}{720}.\left(\frac{1}{42}\right)$$

$$\tau(6) = \frac{\pi^6}{945};$$

olarak bulunacaktır.

PROGRAM 1.3

```
Program Bernoulli_Sayilari ile τ(2m)' nin iliskisi ;

   Uses Dos, Crt, Printer ;

  Type
    Str1    = String ;

  Var
    Str2,
    Str3    : Str1 ;

  I, K, F,
  N, M, C   : Integer ;
  Pay,
  Payda     : Extended ;
  Bernoulli : Array[0..1000] Of Extended ;
  Ksi       : Array[0..1000] Of Extended ;

 Function Fakt( Fak : LongInt ) : Extended ;
 Var
   Faktoriyel : Extended ;
 Begin
    Faktoriyel := 1 ;
  If Fak = 0 Then
    Begin
     Fakt := Faktoriyel ;
     Exit ;
    End ;
   For N := 1 To Fak Do
    Begin
     Faktoriyel := Faktoriyel * N ;
```

```
     End ;
    Fakt := Faktoriyel ;
  End ;

Procedure Hesap ;
      Begin
          Pay := Fakt( K + 1 ) ;
          Payda := Fakt( K + 1 - I ) ;
          Payda := Payda * Fakt( I ) ;
    Bernoulli[K] := Bernoulli[K]-(Pay/Payda)*Bernoulli[I] ;
  End ;

Procedure Bernoulli_Hesap ;
      Begin
        For I := 0 To K-1 Do
         Begin
          If I <= 2 Then Hesap ;
          If (I>2) And (I/2=Int(I/2)) Then Hesap ;
         End ;
        Bernoulli[K] := Bernoulli[K]/(K+1) ;
   End ;

Procedure Bernoulli_Sayi ;
       Begin
           Bernoulli[0] := 1 ;
           For K := 1 To 2*M Do
         Begin
               Bernoulli[K] := 0 ;
         End ;
        For K := 1 To 2*M Do
       Begin
          If K <= 2 Then Bernoulli_Hesap ;
        If (K>2) And (K/2=Int(K/2)) Then Bernoulli_Hesap ;
       End ;
  End ;
       Begin
          ClrScr ;
          Write( 'M Degerini Giriniz : ' ) ;
          ReadLn( M ) ;
          For K := 0 To M Do
         Begin
          Ksi[K] := 0 ;
         End ;
       Bernoulli_Sayi ;
      ClrScr ;
       WriteLn( '  M  ','  ','          T(M)           ' ) ;
       WriteLn( '-----','  ','-------------------------') ;
    For K := 0 To M Do
    Begin
        Payda := Fakt( 2*K ) ;
        Payda := Payda * (-2) ;
```

```
    If K/2 = Trunc( K/2 ) Then C := 1 Else C:= -1 ;
     Ksi[K] := C*Exp(2*K*Ln(2))*Bernoulli[2*K]/Payda ;
     End ;
  For K := 0 To M Do
  Begin
      Payda := 1/Ksi[K] ;
      Str( 2*K,Str2 ) ;
      Payda := Round( Payda ) ;
      Str( Payda,Str3 ) ;
      I := Length( Str3 ) ;
      Str3 := Copy( Str3,2,I-1 ) ;
      Write( '   ',Str2,' ' ) ;
    If Payda<0 Then Write( '   -') Else Write( '    ' ) ;
      WriteLn( 'c^',Str2,'/',Str3 ) ;
      ReadLn ;
     End ;
  ReadLn ;
End.
```

```
          M Degerini giriniz : 6
```

M	$\tau(M)$
0	1
1	$\frac{\pi^2}{6}$
2	$\frac{\pi^4}{90}$
3	$\frac{\pi^6}{945}$
4	$\frac{\pi^8}{9450}$
5	$\frac{\pi^{10}}{93555}$
6	$\frac{\pi^{12}}{924042}$

Teorem 1.2' den $m \geq 1$ için $(-1)^{m+1}.B_{2m} > 0$ dır. Çünkü $\tau(2m)$, herhangi bir m için pozitif bir reel sayıdır. Böylece çift indisli Bernoulli sayıları sıfırdan farklı ve ardışık olarak işaret değiştirirler.

Ayrıca Teorem 1.2, B_{2m}' nin artımının tahminine imkan verir.

$$|B_{2m}| > \frac{2.(2m)!}{(2\pi)^{2m}} \qquad [11]$$

Burada $\tau(2m) > 1$ olarak alındığı kolayca gözlemlenebilir.

$e^n > \frac{n^n}{n!}$ eşitsizliğini kullanarak

$$|B_{2m}| > 2.\left(\frac{m}{\pi e}\right)^{2m} \qquad [12]$$

elde edilebileceğini gösterelim:

$e^n.n! > n^n$ ifadesinde $n=2m$ alınırsa;

$e^{2m}.(2m)! > (2m)^{2m}$

$2m! > \frac{(2m)^{2m}}{e^{2m}}$ elde edilir. Bu [11] denkleminde

yerine yazılılırsa

$$|B_{2m}| > \frac{2.\left(\frac{2m}{e}\right)^{2m}}{(2\pi)^{2m}}$$

$$|B_{2m}| > 2.\left(\frac{m}{\pi e}\right)^{2m}$$

elde edilir. Bu ise çift indisli Bernoulli sayılarının çok süratli mertebeden artığını gösterir.

$n \Longrightarrow \infty$ gittiğinde $|B_{2n}/2n| \Longrightarrow \infty$ olur.

Bernoulli sayıları için yukarıda elde edilenler aşağıdaki şekilde özetlenebilir.

Sonuç 1.1 $k>1$ ve tek ise $B_k=0$ dır.

Sonuç 1.2 $m=1,2,\ldots$ için $(-1)^{m+1}.B_{2m}>0$ dır.

Sonuç 1.3 $m \Longrightarrow \infty$ gittiğinde $|B_{2m}/2m| \Longrightarrow \infty$ olur.

TANIM 1.3

p bir asal sayı olsun. Eğer $\operatorname{ord}_p(r)\geq 0$ ise $r\in Q$ rasyonel sayısına p-tamsayı adı verilir.

Diğer bir deyişle $r = \frac{a}{b}$, $a,b\in Z$ ve $p \nmid b$ ise r bir p-tamsayıdır.■

p-tamsayı kümesinin bir halka oluşturduğu gözlemlenebilir. Bu halka Z_p ile gösterilsin. Eğer r ve s Z_p halkasının elemanları ayrıca $\operatorname{ord}_p(r-s)\geq n$ ise ozaman; $r\equiv s \pmod{p^n}$ geçişini yapabiliriz. Buda

$r-s = \frac{a}{b}$ $\Longrightarrow$ $a,b\in Z$ olduğundan $p \nmid b$ ve $p^n \mid a$ demektir.

TEOREM 1.3

p asalları $p-1 \mid 2m$ şeklinde asallar olmak üzere;

$m\geq 1$ için

$$B_{2m} = A_{2m} - \sum_{p-1 \mid 2m} \frac{1}{p} \quad \text{dir.}$$

Buradaki toplam $p-1 \mid 2m$ şeklindeki tüm asal sayılar üzerindedir.■

SONUÇ 1.4

$p-1 \nmid 2m$ ise ozaman B_{2m} bir p-tamsayıdır. Eğer $p-1 \mid 2m$ ise o zaman $p.B_{2m}+1$ bir p-tamsayıdır. Daha kesin ifadeyle eğer $p-1 \mid 2m$ şeklinde ise ozaman;

$$\operatorname{ord}_p(pB_{2m} + 1) = \operatorname{ord}_p(p.B_{2m} + \frac{1}{p})$$

$$= 1 + \operatorname{ord}_p(p.B_{2m} + \frac{1}{p}) \geq 1$$

şeklindedir. Ohalde $p.B_{2m} \equiv 1 \pmod{p}$ dir.■

Ayrıca 6 tamsayısı ($m \geq 1$ için) B_{2m} 'nin paydasını daima böler. Çünkü 2-1 ve 3-1 6'nın bölenleridir.

Aşağıdaki tanım Kummer'a aittir.

TANIM 1.4

p bir asal sayı ve $n \in Z$ olsun. O zaman n sıfırdan farklı ise a tamsayısı $p^a \mid n$ fakat $p^{a+1} \nmid n$ olacak şekilde negatif olmayan bir tamsayıdır. Bu şekilde tanımlanan a tamsayısına n nin p deki mertebesi denir ve $\operatorname{ord}_p n$ ile gösterilir.

Eğer n=0 ise $\operatorname{ord}_p 0 = \infty$ dir.

yalnız ve ancak $p \nmid n$ ise $\operatorname{ord}_p n = 0$ şeklindedir.

($\operatorname{ord}_p n = 0 \iff p \nmid n$ şeklindedir.)

TEOREM 1.4

p bir asal sayı ve $a,b \in Z$ olsun. O zaman

$$\operatorname{ord}_p a.b = \operatorname{ord}_p a + \operatorname{ord}_p b \text{ dir.}$$

İSPAT

$\alpha = \operatorname{ord}_p a$, $\beta = \operatorname{ord}_p b$ alalım.

Burada tanımdan dolayı $a=p^{\alpha}.c$, $b=p^{\beta}.d$ gibi $c,d \in Z$ elemanları vardır. O halde çarpımı oluşturursak;

$$a.b = p^{\alpha}.c.p^{\beta}.d$$

$$a.b = p^{\alpha+\beta}.c.d \quad \text{elde edebiliriz.}$$

Bu ise $p^{\alpha+\beta} \mid a.b$ demektir. Ayrıca

$$\left.\begin{array}{l} a = p^{\alpha}.c \quad \text{den} \quad p \nmid c \\ b = p^{\beta}.d \quad \text{den} \quad p \nmid d \end{array}\right] \text{ şeklindedir. Buradan}$$

$p \nmid c$ ve $p \nmid d$ den $p \nmid c.d$ bulunur.

$a.b = p^{\alpha+\beta}.c.d$ idi.

$p^{\alpha+\beta} \mid a.b$ ve $p \nmid c.d$ ===> $p^{\alpha+\beta+1} \nmid a.b$

$\alpha+\beta = \operatorname{ord}_p(ab)$ bulunur. ■

TANIM 1.5

$$n = P_1^{a_1} . P_2^{a_2} \dots P_m^{a_m}$$ olsun.

Burada P_i' ler asal sayılar ve a_i 'ler negatif olmayan tamsayılardır. Bu şekilde tanımlanan n tamsayısı için ;

$$n = (-1)^{\epsilon(n)} . \prod_p p^{a(p)}$$

notasyonunu kullanacağız. Burada $n \in Z$ için

$$\epsilon(n) = \begin{cases} 1 & \text{eğer } n \text{ negatif ise} \\ 0 & \text{eğer } n \text{ pozitif ise} \end{cases}$$

şeklindedir. Ayrıca çarpma işlemi pozitif tamsayılar üzerinde tanımlıdır. a(p) kuvvetleri negatif olmayan tamsayılar olduklarından dolayı sonlu bir asal sayı için a(p)=0 dir.

Örneğin n=180 olsun. n' in asal çarpanları $n=2^2.3^2.5$ şeklindedir. O halde burada $\epsilon(n)=0$, $a(2)=2$, $a(3)=3$, $a(5)=1$ ve diğer asal sayılar için $a(p)=0$ şeklindedir.

TEOREM 1.5

Sıfırdan farklı her n tamsayısı için n nin asal çarpanları

$$n=(-1)^{\epsilon(n)} . \prod_p p^{a(p)}$$

şeklindedir. Burada kuvvetler n vasıtasıyla tek bir şekilde hesaplanır. O halde $a(p)=\operatorname{ord}_p n$ dir.

İSPAT

$$n = (-1)^{\epsilon(n)} . \prod_p p^{a(p)}$$

eşitliğinin her iki yanına ord_q fonksiyonu uygulanırsa;

$$\operatorname{ord}_q n = \operatorname{ord}_q (-1)^{\epsilon(n)} \cdot \prod_p p^{a(p)}$$

olur. Teorem 1 ve ord_q ' nun özelliklerinden dolayı

$$\operatorname{ord}_q n = \epsilon(n).\operatorname{ord}_q (-1) + \sum_p p^{a(p)} \quad \text{olur.}$$

Şu halde ord_q ' nun tanımından $\operatorname{ord}_q (-1) = 0$ ve

$$p \neq q \Longrightarrow \operatorname{ord}_q (p)=0$$

$$p = q \Longrightarrow \operatorname{ord}_q (p)=1$$

olarak alabiliriz. Böylece sağ taraf a(q) terimine indirgenmiş olur. Bu ise teoremin verir.■

TANIM 1.6

$p \in Z$ tek asal sayısı eğer $B_2, B_4, \ldots, B_{p-3}$ sayılarının herhangi birinin payına bölünmüyorsa, regulerdir denir aksi halde irreguler denir.

Örneğin 3 asal sayısı reguler bir asaldır.

Teorem 1.3' ün sonucundan $B_2, B_4, \ldots, B_{p-3}$ Bernoulli sayılarının p-tamsayı olduğunu söyleyebiliriz. Bu yüzden p;

$$\operatorname{ord}_p B_{2i} = 0 \qquad i = 1,2,3,\ldots,\frac{(p-3)}{2}$$

şeklinde ise reguler bir asal sayıdır.■

Z_p' de $\operatorname{ord}_p x = 0$ şeklindeki elemanlar kesinlikle Z_p' de

birimin bölenleridir. Eğer $B_2, B_4, \ldots, B_{p-3}$ Bernoulli sayıları Z_p' de birim iseler p regulerdir. Buna denk olarak ;

$1 < i \leq \frac{p-3}{2}$ için herhangi bir B_{2i}, Z_p' de birimsel olmuyorsa, p irregulerdir. İlk regular asallar;

$$\text{ord}_{37}(B_{32}) = 1 \quad \text{ve} \quad \text{ord}_{59}(B_{44}) = 1$$

eşitliklerini sağlayan 37 ve 59 asal sayılarıdır. Diğer bazı irregular asallar 67,101,103,149 ve 157 dir. Jensen 1915 yılında 4n+3 şeklindeki irreguler asalların sonsuz olduğunu ispatlamıştı.

Bundan sonraki bölümde irregular asal sayılar kümesinin sonsuz bir küme olduğunu L.Carlitz' in 1953 yılında vermiş olduğu ispatına bağlı olarak göstereceğiz.

TANIM 1.7

p bir irregular asal sayı olsun. $\{B_2, B_4, \ldots, B_{p-3}\}$ kümesinde p tarafından bölünebilen sıfırdan farklı Bernoulli sayılarının sayısına p' nin irregulerlik indexi adı verilir. 157, 2 indexli ilk asal sayıdır.

2. BERNOULLİ SAYILARINI İÇEREN KONGRÜANSLAR

Bu bölümde Bernoulli sayılarının aritmetik özelliklerini inceleyeceğiz. Bir önceki bölümde ispatlanan Teorem 1.1 ile başlayalım.

$m \geq k$ olmak üzere

$$C^{k}_{m+1} = \frac{(m+1)!}{(m+1-k)!.k!} = \frac{(m+1).m!}{(m+1-k).(m-k)!.k!} = \frac{m+1}{(m+1-k)} C^{k}_{m} \qquad [13]$$

olur.

$$(m+1).S_m(n) = \sum_{k=0}^{m} C^{k}_{m+1} . B_k . n^{m-k+1}$$

olduğunu daha önce göstermiştik. Bu ifade de [13] eşitliğini kullanırsak

$$(m+1).S_m(n) = \sum_{k=0}^{m} \frac{(m+1)}{(m-k+1)} . C_{m+1}^{k} . B_k . n^{m-k+1}$$

$$S_m(n) = \sum_{k=0}^{m} . C_m^k . B_k . \frac{n^{m-k+1}}{(m-k+1)} \qquad [14]$$

sonucu çıkar. Ayrıca

$C_m^k = C_m^{m-k}$ eşitliği [14] denkleminde kullanılırsa

$$S_m(n) = \sum_{k=0}^{m} . C_m^{m-k} . B_{m-k} . \frac{n^{k+1}}{(k+1)}$$

$$S_m(n) = B_m.n + B_{m-1}.\frac{n^2}{2!} + \ldots + B_0.\frac{n^{m+1}}{(m+1)!} \qquad [15]$$

olur. Bu eşitliğin sol tarafını toplayabilmek için aşağıdaki lemma' ya ihtiyacımız vardır.

LEMMA 2.1

p bir asal sayı ve k≥1 olmak üzere;

(a) $\frac{p^k}{k+1}$ bir p-tamsayıdır.

(b) Eğer k≥2 ise $\frac{p^k}{k+1} \equiv 0 \pmod p$

(c) k≥3 ve k≥5 için $\frac{p^{k-2}}{k+1}$ bir p-tamsayıdır.

İSPAT

(a)

$k \geq 1$ için $k+1 \leq p^k$ olduğunu tümevarım vasıtasıyla gösterelim.

$k=1$ için $1+1 = 2 \leq p$ sonuç doğrudur.

$k=k$ için $k+1 \leq p^k$ doğru kabul edilsin.

$k=k+1$ için doğru olduğunu gösterelim:

$k+1 \leq p^k$ doğru kabul edilmişti.

$k+1+1 \leq p^k+1$

$k+2 \leq p^k+1 < 2p^k \leq p^{k+1}$

$k+2 \leq p^{k+1}$

olur. Bu hipotezin doğruluğunu gösterir.

Bukez $(q,p)=1$ olmak üzere

$k+1=p^a q$ olarak alalım. O zaman

$$\frac{p^k}{k+1} = \frac{p^k}{p^a q} = \frac{p^{k-a}}{q}$$

olur.

$\frac{p^k}{k+1} \geq 1$ olduğundan $k \geq a$ bulunur. Böylece (a) ispatlanmış olur. ■

(b)

Bu kısmın ispatında (a)' daki benzer düşünceleri kullanacağız.

$k=2$ için $2+1 = 3 < p$ sonuç doğrudur.

$k=k$ için $k+1 < p^k$ doğru kabul edilsin.

$k=k+1$ için doğru olduğunu gösterelim:

$k+1 < p^k$ doğru kabul edilmişti.

$k+1+1 < p^k+1$

$$k+2 < p^k + 1 < 2p^k < p^{k+1}$$
$$k+2 < p^{k+1}$$

olur. Benzer şekilde

$(q,p)=1$ olmak üzere $k+1=p^a q$ olarak alalım. O zaman

$$\frac{p^k}{k+1} = \frac{p^k}{p^a q} = \frac{p^{k-a}}{q}$$

olur.

$\frac{p^k}{k+1} > 1$ olduğundan $k>a$ bulunur.

Gerçekten $\frac{p^k}{k+1} \equiv 0 \pmod p$ olduğunu gösterelim:

$k+1 < p^k$ olduğunu göstermiştik.

$k+1=p^a q$ olarak alınırsa

$$p^a q < p^k$$

$$0 < p^k - p^a q$$

$$0 < p^a (p^{k-a} - q)$$

olur. Eşitsizliğin sağ tarafı p' nin kuvveti şeklinde yazıldığından dolayı p ile tam bölünür. Yani

$p \mid p^a(p^{k-a}-q)$ olur. Bu ise $p^a(p^{k-a}-q) \equiv 0 \pmod p$ demektir.

Şu halde

$\frac{p^k}{k+1} \equiv 0 \pmod p$ olur. Bu ise (b) nin ispatını verir.

(c)

$k \geq 3$ ve $k \geq 5$ için $k+1 < p^{k-2}$ olduğu (a) ve (b)' deki benzer düşünceler kullanılarak $k-2>a$ bulunur. Buradan

$\frac{p^{k-2}}{k+1} = \frac{p^{k-2-a}}{q}$ bir p-tamsayıdır. ■

ÖNERME 2.1

$m \geq 1$ bir tamsayı ve p bir asal sayı olsun. O zaman $p.B_m$ p-tamsayıdır. Eğer $m \geq 2$, çift sayı ise o zaman

$$p.B_m \equiv S_m(n) \pmod{p} \text{ dir.}$$

İSPAT

Öncelikle p, eğer B_{2m}' nin paydasını bölüyorsa o zaman p^2 B_{2m}' nin paydasını bölmez. Her p için,

$p.B_1 = \frac{-p}{2}$ ' nin bir p-tamsayı olduğu açıktır.

İşleme tümevarım ile devam edelim.

$m>1$ kabul edilsin, [15] denkleminde n=p konursa;

$$S_m(p) = \sum_{k=0}^{m} \binom{k}{m} .B_{m-k}.\frac{p^{k+1}}{(k+1)}$$

$$= \sum_{k=0}^{m} \binom{k}{m} .p.B_{m-k}.\frac{p^{k}}{(k+1)} \qquad [16]$$

elde edilir. k=1,2,3,...,m için bu p-tamsayı $S_m(p) \in Z$' nin elemanlarını gösterir.

$k \geq 1$ için $p.B_{m-k}$ tümevarım hipotezinden dolayı p-tamsayıdır. Ayrıca Lemma 1.1' in (a) kısmından dolayı

$\frac{p^k}{k+1}$ p-tamsayı idi. O halde $p.B_m$' de bir p-tamsayıdır.

İkinci olarak idaadaki kongrüansı kurmak için;
$k \geq 1$ olduğunda

$$\operatorname{ord}_p \binom{k}{m}.(p.B_{m-k}.\frac{p^k}{k+1}) \geq 1$$

olduğunu göstermemiz yeterlidir.
$k \geq 2$ için Lemma 1.1' in (b) kısmından dolayı doğrudur.
k=1 için m' nin çift olması halinde

$$\operatorname{ord}_p \left(\frac{m}{2}.(p.B_{m-1}).p\right) \geq 1$$

olduğu gösterilmelidir. Gerçekten $m \geq 4$ olacak şekildeki çift m' ler için $B_{m-1} \equiv 0 \pmod{p}$ dır. Sadece $m=2$ için doğruluğunu gösterelim:

$$\operatorname{ord}_p (p.B_1.p) \geq 1$$

$$\operatorname{ord}_p (p^2.B_1) \geq 1$$

$$\operatorname{ord}_p (p^2) + \operatorname{ord}_p (B_1) \geq 1$$

$$2.\operatorname{ord}_p (p) + \operatorname{ord}_p \left(\frac{-1}{2}\right) \geq 1$$

$p = q$ için $\operatorname{ord}_q (p) = 1$

$p \neq q$ için $\operatorname{ord}_q (p) = 0$ olduğundan dolayı

$\operatorname{ord}_p (p^2.B_1) \geq 1$ sonucu çıkar. O halde $m=2$ için

$$\operatorname{ord}_p \left(\frac{m}{2}.(p.B_{m-1}).p\right) \geq 1$$ olur. ■

LEMMA 2.2

p bir asal sayı olsun. O zaman

eğer $p-1 \nmid m$ ise $S_m(p) \equiv 0 \pmod{p}$ dir.

Eğer $p-1 \mid m$ ise $S_m(p) \equiv -1 \pmod{p}$ dir.

İSPAT

g, mod p' ye göre bir ilkel kök olsun. O zaman

$S_m(p) = 1^m+2^m+\ldots+(p-1)^m$ olmak üzere

$$S_m(p) = 1^m+2^m+\ldots+(p-1)^m$$
$$= 1^m+g^m+g^{2m}+\ldots+g^{(p-2)m}$$

olur. Dolayısıyla

$$(g^m-1).S_m(p) \equiv g^{(p-1)m} - 1 \equiv 0 \pmod p$$

yazabiliriz. Eğer $p-1 \nmid m$ ise o zaman;

$$g^m \not\equiv 1 \pmod p \text{ ve } S_m(p) \equiv 0 \pmod p$$

olur. Öte yandan $p-1 \mid m$ ise o zaman;

$$S_m(p) = 1+1+\ldots+1 \equiv p-1 \pmod p$$

$$S_m(p) \equiv -1 \pmod p \text{ olur.} \blacksquare$$

Şimdi Teorem 1.3' ü bu varsayımı kullanarak ispatlayalım. m çift kabul edilsin Önerme 2.1' den dolayı $p.B_m$ bir p-tamsayı ve $p.B_m \equiv S_m(p) \pmod p$ şeklindedir. Ayrıca

$$p-1 \nmid m \Longrightarrow B_m \text{' nin p-tamsayı}$$

$$p-1 \mid m \Longrightarrow p.B_m \equiv -1 \pmod p$$

olduklarını Lemma 1.2' de göstermiştik. O zaman

$$A_m = B_m + \sum_{p-1 \mid m} \frac{1}{p} \quad \text{bir p-tamsayıdır.}$$

Buradan $A_m \in Z$ sonucu çıkar. Böylece ispat tamamalanmış olur. Şimdi $(U_m, V_m) = 1$ olmak üzere m. Bernoulli sayısını

$B_m = \dfrac{U_m}{V_m}$ şeklinde alalım. Burada m' i çift sayı kabul ediyoruz.

ÖNERME 2.2

$m \geq 2$, çift sayı ise o zaman her $n \geq 1$ için

$$V_m.S_m(n) \equiv U_m.n \pmod{n^2} \quad \text{dir.}$$

İSPAT

$k \geq 1$ ve sabit bir n tamsayısı için [15] denkleminin terimlerini

$$\binom{m}{k} . \left(B_{m-k} . \frac{n^{k-1}}{k+1}\right).n^2 = A_k^m .n^2 \qquad [17]$$

şeklinde alalım.

$p \neq 2,3$ ve $p \mid n$ için $\operatorname{ord}_p(A_k^m) \geq 0$ olduğunu göstereceğiz.

Ayrıca

eğer $2 \mid n \Longrightarrow \operatorname{ord}_2(A_k^m) \geq -1$

eğer $3 \mid n \Longrightarrow \operatorname{ord}_3(A_k^m) \geq -1$

olduklarını görelim. Öncelikle $p=2$, $m=2$ ve $k=1$ olsun.

O zaman

$$\operatorname{ord}_2(A_1^2) \geq \operatorname{ord}_2\left(C_2^1 \cdot \left(B_1 \cdot \frac{n^\circ}{2}\right)\right)$$

$$= \operatorname{ord}_2\left(2 \cdot \frac{-1}{2} \cdot \frac{1}{2}\right)$$

$$= \operatorname{ord}_2(-1) - \operatorname{ord}_2(2)$$

$$\geq -1 \quad \text{olur.}$$

Bu kez $p=3$, $m=3$ ve $k=2$ olsun.

$$\operatorname{ord}_3(A_2^3) \geq \operatorname{ord}_3\left(C_3^2 \cdot \left(B_1 \cdot \frac{n}{2}\right)\right)$$

$$= \operatorname{ord}_3\left(3 \cdot \frac{-1}{2} \cdot \frac{n}{3}\right)$$

$$= \operatorname{ord}_3(-n \cdot 2^{-1})$$

$$= \operatorname{ord}_3(-2) - \operatorname{ord}_3(n)$$

$$\geq -1 \quad \text{olur.}$$

Buradan n ve A_k^m 'nin Ortak Bölenlerinin En Büyüğü 6' nın

bir böleni olacaktır.Dolayısıyla $(B,n)=1$ ve $6 \mid 1$ olmak üzere

$$S_m(n)=B_m.n + \frac{An^2}{1.B}$$

olur. Eşitliğin her iki yanını $V_m.B$ ile çarparsak;

$$V_m.B.S_m(n) = B_{m+1}.n.V_m + \frac{A.n^2}{1.B}.V_m.B$$

$$V_m.B.S_m(n) \equiv B_{m+1}.n.V_m \pmod{n^2}$$

$(B,n)=1$ olduğundan dolayı

$$V_m.S_m(n) \equiv B_m.n.V_m \pmod{n^2}$$

olur. $6 \mid V_m$ den ise

$$V_m.S_m(n) \equiv n.\frac{U_m}{V_m}.V_m \pmod{n^2}$$

$$V_m.S_m(n) \equiv n.U_m \pmod{n^2}$$ olur.

ord $(B_{m-k}) \geq -1$ (her $m-k\geq 0$ ve her p için) olduğunu göstermek için önce $p \neq 2,3$ ve $p \mid n$ kabul edelim. $k=1,2$ halleri için bunu göstermek basittir. Bu hal için $t>1$ ve

tek sayı için $B_t=0$ ve $B_1=\frac{-1}{2}$ olduğu kullanılarak, deneme

yoluyla $\underset{p}{\text{ord}}\ 3 = 0$ elde edilir. $\underset{p}{\text{ord}}\ 3 > -1$ oldu.

O zaman

$$\underset{p}{\text{ord}}\ (B_{m-k}.\frac{n^{k-1}}{k+1}) \geq -1 + (k-1).\underset{p}{\text{ord}}\ n - \underset{p}{\text{ord}}\ (k+1)$$

$$\geq (k-2) - \underset{p}{\text{ord}}\ (k+1) \geq 0$$

bulunur. (Lemma 1.1' in (c) kısmından)

Eğer $k=1$ ise o zaman $m>2$, çift m' ler için $B_{m-1} = 0$ olur.

$m=2$ için mertebesi (-1) olan $\overset{m}{A}_k$;

$$A_1^2 = C_2^1.(B_1.\frac{n^{1-1}}{1+1}) = \frac{-1}{2} \quad \text{olur.}$$

$k>1$ için k çift veya $k=m-1$ olmadıkça $B_{m-k}=0$ şeklindedir. Fakat k' nın çift olması, $k=m-1$ için $\text{ord}_2(k+1)=0$ olmasını gerektirir.

$$A_{m-1}^m = C_m^{m-1}.(B_{m-m+1}.\frac{n^{m-1-1}}{m-1+1}) = m.(B_1.\frac{n^{m-2}}{m}) = \frac{-1}{2}.n^{m-2}$$

dir. $p=3$, $3 \mid n$ kabul edilsin. O zaman

$$\text{ord}_3(A_2^m) \geq \text{ord}_3(B_{m-2}.\frac{n}{3})$$

$$= \text{ord}_3(B_{m-2}) - \text{ord}_3 3 + \text{ord}_3 n$$

$$= -1 - 1 + 1$$

$$\geq -1$$

$$\text{ord}_3(A_3^m) \geq \text{ord}_3(B_{m-3}.\frac{n^2}{4})$$

$$= \text{ord}_3(B_{m-3}) - \text{ord}_3 4 + 2.\text{ord}_3 n$$

$$= -1 - 0 + 2$$

$$\geq 1$$

olur. Fakat $k\geq 4$ olduğunda

$$\text{ord}_3(\frac{3^{k-2}}{k+1}) \geq \text{ord}_3(3^{k-2}) - \text{ord}_3(k+1)$$

$$= (k-2).\text{ord}_3 3 - \text{ord}_3(k+1) \qquad [18]$$

$$= k-2 - \text{ord}_3(k+1)$$

$$\geq 0$$

olur. Buda bize teoremin ispatını verir.■

ÖRNEK

$B_2 = \frac{1}{6}$, $U_2=1, V_2=6$ ve $n=6$ olsun. O zaman kogrüans

$$6.(1^2 + 2^2 + 3^2 + 4^2 + 5^2) \equiv 6 \pmod{36}$$

şeklinde olur. Bu genelleştirilirse;

$$6.(1^2 + 2^2 + 3^2 + \ldots + (n-1)^2) \equiv n \pmod{n^2}$$ olur.

SONUÇ 2.1

$p-1 \nmid m$ olacak şekilde m çift ve p bir asal sayı olsun. O zaman;

$$S_m(p) \equiv p.B_m \pmod{p^2}$$ dir.

İSPAT

Teorem 1.3' den dolayı $p \nmid V_m$ dir. Önerme 2.2 de $n=p$ alınırsa

$$V_m.S_m(p) \equiv p.U_m \pmod{p^2}$$ olur.

$p \nmid V_m$ olduğundan dolayı kongrüansın her iki yanı V_m ile bölünebilir. O zaman

$S_m(p) \equiv p.\frac{U_m}{V_m} \pmod{p^2}$ olur. Buradan $Bm = \frac{U_m}{V_m}$

olduğundan dolayı

$$S_m(p) \equiv p.B_m \pmod{p^2}$$ sonucu çıkar.■

ÖNERME 2.3

$m \geq 2$ çift ve U_m, V_m bir önceki önermedeki gibi tanımlansın. a ve n tamsayılarını $(a,n)=1$ şeklinde alalım. O zaman

$$(a^{m-1}).U_m \equiv m.a^{m-1}.V_m.\sum_{j=1}^{n-1} j^{m-1}.\left[\frac{ja}{n}\right] \pmod{n}$$ [19]

şeklindedir. Burada $[\alpha]$, $k \leq \alpha \leq k+1$ koşulunu sağlayan tamsayıdır.

İSPAT

$1 \le j \le n$ olmak üzere ja ve q_j tamsayılarına bölme algoritması uygulayalım. O zaman

$$j.a = q_j.n + r_j \qquad 0 \le r_j \le q_j$$

olur. Ayrıca

$$\left[\frac{ja}{n} \right] = q_j \text{ dir.}$$

$(a,n)=1$ olduğundan $\{1,2,3,\ldots,n-1\}$ ve $\{r_1,r_2,r_3,\ldots,r_{n-1}\}$ kümeleri özdeştir. Binom açılımından

$$(j.a)^m = (r_j + q_j.n)^m$$

$$j^m a^m = r_j^m + \binom{m}{1} .q_j.n.r_j^{m-1} + \binom{m}{2} .q_j^2.n^2.r_j^{m-2} + \ldots + \binom{m}{m} . q_j.n^m$$

şeklindedir. Ayrıca $\binom{m}{1} = m$ olduğundan dolayı bu ifade

$$j^m a^m = r_j^m + m.q_j.n.r_j^{m-1} \pmod{n^2} \qquad [20]$$

şeklinde yazılabilir. Ayrıca

$ja = q_j.n + r_j$ eşitliğinden $ja \equiv r_j \pmod{n}$ dir. Buradan

$n \mid r_j - ja \Longrightarrow r_j - ja = n.k$ şeklinde bir $k \in Z$ vardır.

Dolayısıyla $r_j = ja + n.k$ olur. Binom açılımına göre

$$(r_j)^{m-1} = (ja + n.k)^{m-1}$$

$$r_j^{m-1} = j^{m-1}.a^{m-1} + \binom{m-1}{1} .n.k.j^{m-2}.a^{m-2} + \ldots + \binom{m-1}{m-1} .n^{m-1}.k^{m-1}$$

şeklindedir. Bu eşitlik [20] denkleminde yazılırsa;

$$j^m a^m = r_j^m + m.q_j.n.j^{m-1}.a^{m-1} \pmod{n^2} \text{ olur. Ayrıca}$$

$\left[\frac{ja}{n}\right] = q_j$ idi. O halde

$$j^m.a^m = r_j^m + m.a^{m-1}.n.\left[\frac{ja}{n}\right].j^{m-1} \pmod{n^2} \text{ olur.}$$

Bu kongrüansta $j=1,2,\ldots n-1$ koyalım ve toplayalım:

$$j=1 \Rightarrow 1^m.a^m = r_1^m + m.a^{m-1}.n.\left[\frac{1a}{n}\right].1^{m-1} \pmod{n^2}$$

$$j=2 \Rightarrow 2^m.a^m = r_2^m + m.a^{m-1}.n.\left[\frac{2a}{n}\right].2^{m-1} \pmod{n^2}$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$j=n-1 \Rightarrow (n-1)^m.a^m = r_{n-1}^m + m.a^{m-1}.n\left[\frac{(n-1)a}{n}\right](n-1)^{m-1} \pmod{n^2}$$

$$1^m.a^m + 2^m.a^m + \ldots + (n-1)^m.a^m = r_1^m + r_2^m + \ldots + r_{n-1}^m + m.a^{n-1}.n.$$

$$\sum_{j=1}^{n-1} j^{m-1}.\left[\frac{ja}{n}\right] \pmod{n^2}$$

$$S_m(n).a^m \equiv S_m(n) + m.a^{m-1}.n.\sum_{j=1}^{n-1} j^{m-1}.\left[\frac{ja}{n}\right] \pmod{n^2}$$

$$(a^m-1).S_m(n) \equiv m.a^{m-1}.n.\sum_{j=1}^{n-1} j^{m-1}.\left[\frac{ja}{n}\right] \pmod{n^2}$$

olur. Bir önceki sonuçtan dolayı

$\frac{S_m(n)}{n} \equiv B_m \pmod{p}$ idi. O halde

$$(a^m-1).\frac{S_m(n)}{n} \equiv m.a^{m-1}.\sum_{j=1}^{n-1} j^{m-1}.\left[\frac{ja}{n}\right] \pmod{n^2}$$

$$(a^{m}-1).B_{m} \equiv m.a^{m-1}.\sum_{j=1}^{n-1} j^{m-1}.\left[\frac{ja}{n}\right] \quad (\mathrm{mod} n^{2})$$

olur. Burada bu ifade

$$(a^{m}-1).U_{m} \equiv m.a^{m-1}.V_{m}\sum_{j=1}^{n-1} j^{m-1}.\left[\frac{ja}{n}\right] \quad (\mathrm{mod} n^{2})$$

şeklinde yazılabilir. İspatlanması gerekende budur.■

SONUÇ 2.2

p asal sayısı $p \equiv 3 \pmod 4$ şeklinde olsun. $m = \frac{p+1}{2}$

alalım. O zaman eğer $p>3$ ise

$$2.(2 - (2/p)).B_{m} \equiv -\sum_{j=1}^{m-1} (j/p) \pmod p \quad \text{dir.}$$

(Burada (x/p) Legender sembolünü göstermektedir.)

İSPAT

$$m = \frac{p+1}{2} \quad ===> \quad m-1 = \frac{p-1}{2}$$

olur. O halde Euler kriterinden dolayı her a tamsayısıiçin;

$a^{m-1} \equiv (a/p) \pmod p$ olur.

Önerme 2.3' deki kongrüans gözönüne alınısın.

$$(a.a^{m-1}-1).U_{m} \equiv m.a^{m-1}.V_{m}.\sum_{j=1}^{n-1} j^{m-1}.\left[\frac{ja}{n}\right] \pmod n$$

Burada a=2 ve n=p alınırsa

$$(2.2^{m-1}-1).U_{m} \equiv m.2^{m-1}.V_{m}.\sum_{j=1}^{p-1} j^{m-1}.\left[\frac{2j}{p}\right] \pmod p$$

olur. Ayrıca Euler kriterinden dolayı bu ifade

$$(2.(2/p)-1).U_m \equiv m.2^{m-1}.V_m. \sum_{j=1}^{p-1} (j/p).\left[\frac{2j}{p}\right] \pmod p$$

$1 \leq j < m-1$ için $\left[\frac{2j}{p}\right] = 0$

$m \leq j < p$ için $\left[\frac{2j}{p}\right] = 1$

şeklindedir. Ayrıca Teorem 1.3' den dolayı

$2m \equiv 1 \pmod p$ ve $p \mid V_m$ şeklindedir. Şu halde

$$2.(2 - (2/p)).B_m \equiv \sum_{j=m}^{p-1} (j/p) \pmod p \qquad [21]$$

olur. Ayrıca

$$\sum_{j=1}^{p-1} (j/p) = 0 \quad \text{olduğundan}$$

$$\sum_{j=1}^{m-1} (j/p) + \sum_{j=1}^{p-1} (j/p) = 0$$

$$\sum_{j=1}^{m-1} (j/p) = - \sum_{j=1}^{p-1} (j/p)$$

olur. Bu ifade [21] de yerine yazılırsa

$$2(2 - (2/p)).B_m \equiv - \sum_{j=1}^{m-1} (j/p) \pmod p$$

sonucuna varılmış olur. İspatlanması gerekende budur. ■

Yukarıdaki sonuç sınıf sayılarının, Bernoulli sayıları ile ilişkilerinin bazı ilginç sonuçlarını göstermek için kullanılabilir:

p bir asal sayı olsun. $p \equiv 3 \pmod 4$ ve $Q(\sqrt{-p})$ imajiner quadritik sayı cismi gözönüne alınsın. h, $Q(\sqrt{-p})$' nin sınıf sayısını göstersin.

Eğer p>3 ise

$$(2 - (2/p)).h = \sum_{1 \le x \le p/2} (j/p) \qquad [22]$$

dir. Yukarıdaki sonuç ve [22] bağıntısı yardımıyla h için;

$$-2.(2 - (2/p)).B_{p+1/2} \equiv (2 - (2/p)).h \pmod p$$

$$-2.B_{p+1/2} \equiv h \pmod p$$

kongrüansı yazılabilir. Bu oldukça önemli bir kongrüanstır. Vornio kongrüansları, Bernoulli sayılarının bir çok özelliğini elde etmemize yardımcı olur. Aşağıdaki Önerme B_{2m}' nin paydası hakkında birçok bilgi verir.

ÖNERME 2.4

Eğer $p-1 \nmid m$ ise o zaman $\dfrac{B_m}{m}$ bir p- tamsayıdır.

İSPAT

Teorem 1.3' den dolayı B_m bir p-tamsayıdır. $p \nmid m_o$ olacak şekilde $m=p^t.m_o$ alalım. [19] kongrüansında $n=p^t$ koyalım. O zaman;

$$(a^{m-1}).U_m \equiv m.a^{m-1}.V_m.\sum_{j=1}^{p^t-1} j^{m-1}.\left[\frac{ja}{p^t}\right] \pmod{p^t}$$

olacağından

$$(a^{m-1}).U_m \equiv 0 \pmod{p^t} \text{ şeklindedir.}$$

a, mod p' ye göre bir ilkel kök seçilsin. Dolayısıyla

$$a^{p-1} \equiv 1 \pmod p$$

$$p \nmid a^{p-1}-1 \text{ olur.}$$

$p-1 \nmid m$ olduğundan $p-1 \nmid a^m-1$ alabiliriz. O halde

$U_m \equiv 0 \pmod p$ alabiliriz. Böylece

$$\frac{B_m}{m} = \frac{U_m}{m.V_m} \quad \text{bir p-tamsayıdır.}$$

ÖRNEK.

a) m=22, p=11 olsun.

$$B_{22} = \frac{11.131.593}{2.3.23}$$ olduğundan

$\frac{B_{22}}{22}$ (mod 11)' e göre bir p-tamsayıdır.

Sonuçta $\frac{B_{22}}{22}$ Z_{11}' de bir birimseldir.

b) m=50, p=5 olsun.

$$B_{22} = \frac{5.5.417202699.47464429777438199}{2.3.11}$$ olduğundan

$\frac{B_{50}}{50}$ (mod 5)' e göre bir p-tamsayıdır.

Sonuçta $\frac{B_{50}}{50}$ Z_5' de bir birimseldir.

3. KUMMER KONGRUANSLARI

Teorem 3.1

$m \geq 2$ ve çift, p bir asal sayı ve $p-1 \nmid m$ olduğunu kabul edelim.

$C_m=(1-p^{m-1}).\frac{B_m}{m}$ olarak tanımlansın. Eğer

$m' \equiv m \pmod{\phi(p^n)}$ ise,

$C_{m'} \equiv C_m \pmod{p^n}$ dir.

İSPAT

Her zamanki gibi $B_m = \frac{U_m}{V_m}$ olarak yazalım. $t = \text{ord}_p\, m$ olsun.

Önerme 2.4' den dolayı $p^t \mid U_m$ dir. [19] kongrüansında $n = p^{\alpha+t}$ konursa;

$$(a^{m-1}).U_m \equiv m.a^{m-1}.V_m.\sum_{j=1}^{p^{\alpha+t}-1} j^{m-1}.\left[\frac{ja}{p^{\alpha+t}}\right] \pmod{p^{\alpha+t}}$$

olur. p^t, m ile U_m' nin her ikisinide böldüğünden dolayı kongrüansın her iki yanı p^t ile bölünebilir.

p ile $\frac{m.V_m}{p^t}$ aralarında asal olduğundan

$$\frac{(a^{m-1})}{m}.B_m \equiv a^{m-1}.\sum_{j=1}^{p^{\alpha+t}-1} j^{m-1}.\left[\frac{ja}{p^{\alpha+t}}\right] \pmod{p^\alpha} \quad [23]$$

kongrüansını yazabiliriz. Bu kongruansın yardımıyla teoremi ispatlayabiliriz. Önce $e=1$ durumunu ispatlayalım. O zaman $p \mid j$ olan j' li terimleri atabiliriz. Eğer

$p \nmid j$ ise $j^{p-1} \equiv 1 \pmod p$ dir. Ayrıca

$p \nmid a$ ise $a^{p-1} \equiv 1 \pmod p$ dir.

Dolayısıyla $m' = m.(p-1)$ alınırsa, yukarıdaki [23] kongrüansında m yerine m' yazılırsa kongrüansın sağ tarafı değişmez. Bu nedenle

$$\frac{(a^{m'}-1)}{m'}.B_{m'} \equiv \frac{(a^m-1)}{m}.B_m \pmod p \text{ yazılabilir.}$$

$a \pmod p$' ye göre ilkel kök seçilsin. $p-1 \nmid m$ olduğundan

$a^{m'}-1 \equiv a^m-1 \equiv \pmod p$ olur. Sonuç olarak

$$\frac{B_{m'}}{m} \equiv \frac{B_m}{m} \pmod p \text{ olur.}$$

Bu kez $e>1$ durumunu inceleyelim:
Yukarıdaki gibi hareket edemeyiz, çünkü p ile bölünebilen j' li terimler kolaylikla yok edilemez. Bu nedenle

$$\sum_{j=1}^{p^{\alpha+t}-1} j^{m-1}.\left[\frac{ja}{p^{\alpha+t}}\right] = \sum_{j=1}^{p^{\alpha+t}-1} j^{m-1}.\left[\frac{ja}{p^{\alpha+t}}\right]$$

$$+p^{m-1}.\sum_{j=1}^{p^{\alpha+t}-1} j^{m-1}.\left[\frac{ja}{p^{\alpha+t}}\right] \qquad [24]$$

yazalım. [24]' te e yerine e-1 alıp m-1≥1 olduğu hatırlanırsa, o zaman

$$\frac{p^{m-1}.(a^{m-1})B_m}{m} \equiv p^{m-1}.a^{m-1}.\sum_{i=1}^{p^{\alpha+t-1}-1} i^{m-1}.\left[\frac{ia}{p^{\alpha+t-1}}\right] \pmod{p^{\alpha}}$$

olur. Bu [24] ifadesinde yerine konursa;

$$\frac{(a^{m-1})B_m}{m} \equiv a^{m-1}.\sum_{\substack{j=1\\(p,j)=1}}^{p^{\alpha+t}-1} j^{m-1}.\left[\frac{ja}{p^{\alpha+t}}\right] + \frac{p^{m-1}.(a^{m-1})B_m}{m} \pmod{p^{\alpha}}$$

ve

$$\frac{(1-p^{m-1}).(a^{m-1}).B_m}{m} \equiv a^{m-1}.\sum_{\substack{j=1\\(p,j)=1}}^{p^{\alpha+t}-1} j^{m-1}.\left[\frac{ja}{p^{\alpha+t}}\right] \pmod{p^{\alpha}} \qquad [25]$$

olur. Eğer $p \mid j$ ve $m' \equiv m \pmod{\Phi(p^{\alpha})}$ ise, o zaman

$$j^{m'-1} \equiv j^{m-1} \pmod{p^{\alpha}} \text{ dir.}$$

Dolayısıyla $m' \equiv m \pmod{\Phi(p^{\alpha})}$ olmak üzere m yerine m' alınırsa [25] ' in sağ tarafı (mod p^{α})' ye göre değişmez. O zaman ispat için e=1 halindeki gibi hareket edilebilir.■

Yukarıdaki teorem ile verilen kongrüanslar Kummer kongrüansları olarak bilinir. Bu kongrüansların modern bir yorumu aşağıdaki şekilde yapılabilir:

$\gamma(s) = \sum_{n=1}^{\infty} n^{-s}$ Riemann-Zeta fonksiyonu gözönüne alınsın.

$\gamma(s)$ fonksiyonu s=1 noktası hariç, tüm komplex düzlemde holomorfik bir fonksiyona genişletilebilir ki, s=1' de 1 rezüdülü basit bir kutup vardır. Ayrıca $\gamma(s)$ fonksiyonu

$$\zeta(1-s) = 2.(2\pi)^{-s}.\cos\left(\frac{\pi s}{2}\right).\Gamma(s).\zeta(s)$$

fonksiyonel denklemini sağlar. Riemann-Zeta fonksiyonunun en önemli özelliklerinden biride;

$s \longrightarrow \infty$ giderken $\zeta(s) \longrightarrow \infty$ gitmesidir.

$\zeta(1-s)$ gözönüne alınırsa, bu fonksiyonda

$s \longrightarrow \infty$ giderken $\zeta(s) \longrightarrow \infty$ gider.

Yukarıda sözü edilen

$$\zeta(1-s) = 2.(2\pi)^{-s}.\cos\left(\frac{\pi s}{2}\right).\Gamma(s).\zeta(s)$$

fonksiyonel denklemi gözönüne alınsın. Γ fonksiyonunda m pozitif tamsayısı için $\Gamma(m)=m!$ dir.

$m \geq 2$ ve çift kabul edilsin. Teorem 1.2' yi ve yukarıdaki fonksiyonel denklemi birlikte gözönüne alırsak,

$$\zeta(1-s) = \frac{-B_m}{m} \quad \text{olur.}$$

Ayrıca $\zeta^*(1-s) = (1-p^s).\zeta^*(s)$ olarak tanımlansın.

O zaman

$$\zeta^*(1-m) = -(1-p^{m-1}).\frac{B_m}{m} \quad \text{olur.}$$

Teorem 3.2'den dolayı

$m' \equiv m \pmod{\Phi(p^s)}$ ise; o zaman

$$\zeta^*(1-m') \equiv \zeta^*(1-m) \pmod{p^s} \qquad [26]$$

olur.

TANIM 3.1

Bir p sabit asal sayısı icin;

$$d(n,m) = p^{-ord_p(n-m)}$$

fonksiyonu Z' de bir metrik tanımlar. Buna p-adic Metrik adı verilir. Bu metrikte iki tamsayının farkları p' nin yüksek bir kuvvetiyle bölünüyorsa o zaman bu tamsayılara komşudurlar denir.

TEOREM 3.2

İrreguler asal sayılar kümesi sonsuz bir kümedir.

İSPAT

$\{P_1,P_2,\ldots,P_m\}$ irreguler asal sayılar kümesi olsun. Bu kümenin dışında başka bir irreguler asal sayısının bulunduğunu ispatlayacağız.

$k \geq 2$ ve $n = k.(p_1-1).(p_2-1)\ldots(p_m-1)$ olsun.

Eğer küme boş ise n=k alalım. Sonuç 1.3' den yaralanarak

k' yi; $k.|B_n/n| > 1$ olacak şekilde büyük seçelim.

$ord_p\left(\frac{B_n}{n}\right) > 0$ olacak şekilde bir p asal sayısı seçelim.

Claussen-von Staudt'tan dolayı $p-1 \nmid n$ şeklindedir. Dolayısıyla $i = 1,2,\ldots,s$ için $p \neq p_i$ olur. Ayrıca $p \neq 2$ dir. p' nin irreguler olduğunu göstereceğiz.

$n \equiv m \pmod{p-1}$ olsun. Burada $0 \leq m \leq p-1$ şeklindedir. O zaman $m \neq 0$ ve çifttir. Dolayısıyla $2 \leq m \leq p-3$ şeklindedir. Kummer kongüranslarından dolayı

$$\frac{B_n}{n} \equiv \frac{B_m}{m} \pmod{p} \text{ dir.}$$

$$ord_p\left(\frac{B_m}{m}\right) = ord_p B_m > 0$$

sonucu çıkar. Bu da p' nin irreguler olduğunu gösterir.

KAYNAKÇA

1- L.Carlitz. Aritmetic properties of generalized Bernoulli numbers. J.Riene und Angev. Math., 201-202 (1959),

2- L.Carlitz. A note on irreguler primes. Proc. Am. Math. Soc., 5. 329-331 (1954),

3- D.J.S. Robinson. A Course in the theory of Groups. Springer-Verlag, New York Heidelberg Berlin. (1982),

4- K.Ireland, M.Rosen. A Classical Introduction to Modern Number Theory. Springer-Verlag, New York Heidelberg Berlin. (1982),

5- W.Johnson. Irregular primes and cyclotomic inveriants. Math. Comp., 29 (1975),

6- N.Koblitz. p-adic Numbers, p-adic Analysis and Zeta Functions. New York. Springer-Werlag. (1977),

7- K.Ribbet. A modular construction of unramified p-extensions of $Q(\mu_p)$. Invent. Math., 34 (1977),

8- A.vander Poorten. A proof that Euler missed... Apery's proof of the irrationality of $\gamma(3)$; An informal report. The Mathematical intelligencer 1. no. 142 (1978),

9- S.Wagstaff. Iregular primes to 125.000. Math. Comp., 32. no. 142 (1978).

ÖZGEÇMİŞ

Doğum yer ve yılı = İstanbul - 1964

İlk öğrenim = Devrim İlk Okulu - 1975

Orta öğrenim = İstanbul Tuna Lisesi - 1981

Yüksek öğrenim = Yıldız Üniversitesi - 1988

Görevi = Araştırma Görevlisi

Medeni Hali = Bekar