Bernoulli Sayıları Üzerine

Ali Nesin / *anesin@bilgi.edu.tr*

exp x sayısını, MD-2007-IV, sayfa 28'de,

$$\exp x = \sum_{i=0}^{\infty} \frac{x^i}{i!}$$

olarak tanımlamıştık. Bu yazının amacı için, exp x'i yukardaki gibi bir seri olarak görmek yerine, bir "biçimsel kuvvet serisi", yani katsayıları bir zaman sonra 0 olmak zorunda olmayan bir tür "sonsuza kadar uzayıp giden polinom" olarak görebiliriz [MD-2004-II, sayfa 32-38]. Bu biçimsel kuvvet serisinin katsayıları $\mathbb{Q}$'dedir elbette. Yani eğer istersek,

$$\exp x \in \mathbb{Q}[[x]]$$

varsayımını yapabiliriz. Analizde biraz daha ileri seviyede olan okur, exp x'i bir fonksiyon olarak alıp yukardaki eşitliği exp x'in Taylor serisi olarak da görebilir. Dediğimiz gibi bu bakış açılarının hiçbiri bu yazı için farketmeyecek. Ama biz exp x'i daha çok bir kuvvet serisi olarak görme taraftarıyız.

Şimdi

$$\frac{x}{\exp x - 1} \tag{1}$$

ifadesine bakalım. Bu ifadeyi biraz açmamız gerekir, çünkü ne demek olduğu pek belli değil. Eğer bu ifadeyi bir fonksiyon olarak görmek istersek, $x = 0$ durumunda ne anlama geldiğini açıklamalıyız. Sürekliliği korumak amacıyla, $x = 0$ ise fonksiyonu 1 olarak tanımlayalım, çünkü

$$\lim_{x\to 0} \frac{x}{\exp x - 1} = 1$$

dir. (Neden?) Ama daha da doğrusu bu ifadeyi biçimsel bir Laurent serisi, yani biçimsel bir kuvvet serisi (yani x) bölü bir başka biçimsel kuvvet serisi (exp $x - 1$) olarak görmektir. Biraz hesap yaparsak paydayı ortadan kaldırıp bu ifadeyi bir Laurent serisi yerine biçimsel bir kuvvet serisi olarak yazabiliriz:

$$\frac{x}{\exp x - 1} = \frac{x}{\sum_{i=0}^{\infty} \frac{x^i}{i!} - 1} = \frac{x}{\sum_{i=1}^{\infty} \frac{x^i}{i!}}$$
$$= \frac{x}{x\sum_{i=1}^{\infty} \frac{x^{i-1}}{i!}} = \frac{1}{\sum_{i=1}^{\infty} \frac{x^{i-1}}{i!}}$$
$$= \frac{1}{1+\sum_{i=2}^{\infty} \frac{x^{i-1}}{i!}} = \frac{1}{1+\sum_{i=1}^{\infty} \frac{x^{i}}{(i+1)!}}.$$

En sondaki ifadenin paydasında bulunan kuvvet serisinin tersi vardır, çünkü sabit sayısı 1'dir ve sabit sayısı tersinir olan kuvvet serileri tersinirdir (yani çarpımsal tersleri de kuvvet serileridir, MD-2004-II, sayfa 34, Teorem 2). Nitekim,

$$\frac{1}{1+\sum_{i=1}^{\infty} \frac{x^{i}}{(i+1)!}}$$
$$= 1 - \left(\sum_{i=1}^{\infty} \frac{x^{i}}{(i+1)!}\right) + \left(\sum_{i=1}^{\infty} \frac{x^{i}}{(i+1)!}\right)^2$$
$$- \left(\sum_{i=1}^{\infty} \frac{x^{i}}{(i+1)!}\right)^3 + \left(\sum_{i=1}^{\infty} \frac{x^{i}}{(i+1)!}\right)^4 - \cdots$$

olur. Sağ taraftaki sonsuz toplam fazla korkutmasın (biraz korkutabilir ama!) çünkü bu toplam sonsuz bile olsa x'in her kuvvetinin katsayısı hesaplanabilir. Örneğin, x^3'e kadar olan katsayıları hesaplamak için "modülo x^4" çalışıp, yani $x^4 = 0$ eşitliğini varsayıp, sadece

$$1 - \left(\sum_{i=1}^{3} \frac{x^{i}}{(i+1)!}\right) + \left(\sum_{i=1}^{3} \frac{x^{i}}{(i+1)!}\right)^2 - \left(\sum_{i=1}^{3} \frac{x^{i}}{(i+1)!}\right)^3$$

polinom çarpımını hesaplamak yeterlidir. [Bkz. MD-2004-II, sayfa 35, Önsav 4.]

Demek istediğimiz şu ki,

$$\frac{x}{\exp x - 1}$$

ifadesi (kuvvet serisi olarak, ama fonksiyon olarak da)

$$1 - \left(\sum_{i=1}^{\infty} \frac{x^{i}}{(i+1)!}\right) + \left(\sum_{i=1}^{\infty} \frac{x^{i}}{(i+1)!}\right)^2 - \left(\sum_{i=1}^{\infty} \frac{x^{i}}{(i+1)!}\right)^3$$
$$+ \left(\sum_{i=1}^{\infty} \frac{x^{i}}{(i+1)!}\right)^4 - \left(\sum_{i=1}^{\infty} \frac{x^{i}}{(i+1)!}\right)^5 + \cdots$$

ifadesine eşittir. Biraz zahmetle de olsa bu ifadenin ilk birkaç terimini hesaplayabiliriz:

$$1 - \frac{x}{2} + \frac{x^2}{6\times 2!} - \frac{x^4}{30\times 4!} + \frac{x^6}{42\times 6!} - \frac{x^8}{30\times 8!} + \frac{5x^{10}}{66\times 10!} - \cdots$$

Okura bu terimlerin birkaçını elle hesaplamasını tavsiye ederiz. Her öğrenci bu tür hesapları hayatında birkaç kez yapmalıdır.

Sonuç olarak, (1) ifadesi aslında biçimsel bir kuvvet serisidir. Bu biçimsel kuvvet serisinin katsayılarını $B_k/n!$ olarak yazalım:

$$\frac{x}{\exp x - 1} = \sum_{j=0}^{\infty}\left(\sum_{i=1}^{\infty}\frac{x^i}{(i+1)!}\right)^j = \sum_{k=0}^{\infty} B_k \frac{x^k}{k!}.$$

B_k sayılarına, bu sayıları ilk bulan kişi olan Jacob Bernoulli'nin onuruna ***Bernoulli sayıları*** denir. İlk Bernoulli sayıları şöyledir:

$B_0 = 1$,
$B_1 = -1/2$,
$B_2 = 1/6$,
$B_4 = -1/30$,
$B_6 = 1/42$,
$B_8 = -1/30$,
$B_{10} = 5/66$,
$B_{12} = -691/2.730$,
$B_{14} = 7/6$,
$B_{16} = -3.617/510$,
$B_{18} = 43.867/798$,
$B_{20} = -174.611/330$.

Birazdan kanıtlayacağımız üzere, $n > 1$ bir tek sayıysa, $B_n = 0$'dır.

Sanıldığının tersine Bernoulli sayılarını hesaplamak için kapalı formüller vardır, ama bildiğim kadarıyla bu formüllerin hiçbiri basit değildir. Yani Bernoulli sayılarını hesaplamak kolay değildir.

Matematiğin hemen hemen her dalında karşılaşılır Bernoulli sayılarıyla: Sayılar kuramında (Riemann zeta fonksiyonunda ya da birazdan göreceğimiz üzere 1'den n'ye kadar olan doğal sayıların k'ıncı kuvvetlerinin toplamında), analizde (tanjant fonksiyonunun Taylor serisinde ya da Euler-MacLaurin formülünde), topolojide (Kervaire-Milnor formülünde) ve kombinatorikte.

Teorem 1. *Eğer $k > 1$ bir tek sayıysa, o zaman $B_k = 0$ olur.*

Kanıt: Basit bir hesap yapalım önce:

$$\frac{x}{\exp x - 1} + \frac{x}{2} = \frac{x}{2}\left(\frac{2}{\exp x - 1} + 1\right) = \frac{x}{2}\cdot\frac{\exp x + 1}{\exp x - 1}$$
$$= \frac{x}{2}\cdot\frac{\exp(-x/2)}{\exp(-x/2)}\cdot\frac{\exp x + 1}{\exp x - 1}$$
$$= \frac{x}{2}\cdot\frac{\exp(x/2) + \exp(-x/2)}{\exp(x/2) - \exp(-x/2)}.$$

Yukardaki ifadeleri ister fonksiyon olarak, ister biçimsel kuvvet serisi olarak görün, farketmez. En sağdaki ifadede x yerine $-x$ koyarsak, ifade değişmez. Demek ki soldaki ifade de bu değişimden etkilenmez. Ama $B_1 = -1/2$ olduğundan, soldaki ifade,

$$\sum_{k\neq 1} B_k \frac{x^k}{k!}$$

ifadesine eşittir. Bütün bunlardan,

$$\sum_{k\neq 1} B_k \frac{x^k}{k!} = \sum_{k\neq 1} B_k \frac{(-x)^k}{k!}$$

eşitliği çıkar. Ama iki biçimsel kuvvet serisi, ancak ve ancak aynı katsayılara sahipse eşittir. Demek ki, k tekse ve 1'den değişikse,

$$\frac{B_k}{k!} = \frac{-B_k}{k!},$$

yani $B_k = 0$ olur. □

Şimdi B_k'ları tümevarımla hesaplamaya yarayacak bir formül bulalım:

Teorem 2. *Her $n > 1$ için*

$$\sum_{k=0}^{n-1}\binom{n}{k}B_k = 0$$

olur.

Kanıt: Kolay bir hesap:

$$\frac{x}{\exp x - 1} = \sum_{k=0}^{\infty}\frac{B_k}{k!}x^k$$

eşitliğinden

$$x = \left(\sum_{k=0}^{\infty}\frac{B_k}{k!}x^k\right)\left(e^x - 1\right)$$

çıkar. Bunu açarsak,

$$x = \left(\sum_{k=0}^{\infty}\frac{B_k}{k!}x^k\right)\left(e^x - 1\right)$$
$$= \left(\sum_{k=0}^{\infty}\frac{B_k}{k!}x^k\right)\left(\sum_{\ell=1}^{\infty}\frac{x^\ell}{\ell!}\right)$$
$$= \sum_{n=1}^{\infty}\left(\sum_{k+\ell=n,\,\ell\geq 1}\frac{B_k}{k!\,\ell!}\right)x^n$$
$$= \sum_{n=1}^{\infty}\frac{1}{n!}\left(\sum_{k=0}^{n-1}\binom{n}{k}B_k\right)x^n$$

elde ederiz. İfadelere biçimsel kuvvet serisi muamelesi çekip her iki tarafın katsayılarını eşitlediğimizde $n \geq 2$ için,

$$\sum_{k=0}^{n-1}\binom{n}{k}B_k = 0$$

elde ederiz. □

Yukardaki teoremden tümevarımla,

$$n!B_{n-1} \in \mathbb{Z}$$

ilişkisi kolaylıkla elde edilir, yani B_n sayıları paydasında $(n + 1)!$ olan kesirli sayılardır. Ama birazdan bundan çok daha güçlü bir teorem kanıtlayacağız.

Bernoulli sayıları

$$S_k(n) = 1^k + 2^k + \cdots + (n-1)^k$$

toplamlarını bulmada çok işe yararlar:

Teorem 3. *Her* $k \geq 0$ ve $n > 1$ *için*

$$S_k(n) = \sum_{i=0}^{k} \binom{k}{i} \frac{B_i}{k+1-i} n^{k+1-i}$$

olur.

Daha açık biçimde yazacak olursak, teorem, $S_k(n)$ sayılarının

$$\binom{k}{0}\frac{B_0}{k+1}n^{k+1} + \binom{k}{1}\frac{B_1}{k}n^k + \binom{k}{2}\frac{B_2}{k-1}n^{k-1} + \cdots + \binom{k}{k}\frac{B_k}{1}n^1$$

biçiminde yazıldığını söylüyor.

Kuvvetlerin Toplamı

1'den n'ye kadar olan doğal sayıların k'ıncı kuvvetlerinin toplamı eski çağlardan beri matematikçileri meşgul etmiştir. Bu konuda çalışan öncü matematikçilerden bazıları: Pisagor (MÖ ~572-497), Arşimet (MÖ 287-212), Hintli Aryabhata (doğumu 476), İranlı Ebubekir el Karacı (doğumu 1019), Mısırlı Al Haytam (965-1039).

İngiliz matematikçi Thomas Hariot (1560-1621), dördüncü kuvvetlere kadar olan toplamları veren simgesel bir formül bulan ilk matematikçi olmuştur. 1631'de, Alman Johann Faulhaber (1580-1635) **Academia Algebra** adlı kitabında toplamları 17'nci kuvvete kadar hesaplamıştır. İsviçreli matematikçi Jacob Bernoulli (1654-1705), sabit bir $B_0, B_1, B_2, B_3, \ldots$ dizisi kullanarak kuvvetlerin toplamını tek elden veren bir formül bulan ilk matematikçi olmuştur. Formülü bulduğunda, bir mektubunda "Bu cetvel (yani B_k dizisi) sayesinde, 1000'e kadar olan sayıların onuncu kuvvetlerinin toplamının 91.409.924.241.424.243.424.241.924.242.500 olduğunu bulmak bir çeyrek saatin yarısından daha az zamanımı aldı," diye yazmıştır.

Teorem 3 Üzerine Notlar:

1) $S_k(n) = 1^k + 2^k + \cdots + (n-1)^k$ toplamında, yazmadığımız 0^k'yı da sayarsak tam n tane sayı var. Öte yandan, teoremdeki formülde toplanacak k tane terim var.

2) $S_k(n) = 1^k + 2^k + \cdots + (n-1)^k$ ifadesinin polinoma benzer bir yanı yok. Bu ifadede n yerine x koymak ancak bir çılgınlık belirtisi olarak görülebilir. Öte yandan, teoremdeki formülde n'yi bir değişken olarak alırsak, bu ifadenin bir polinom olduğunu görürüz.

$$S_k(x) = \sum_{i=0}^{k} \binom{k}{i} \frac{B_i}{k+1-i} x^{k+1-i} \in \mathbb{Q}[x].$$

Oldukça şaşırtıcı.

3) Teorem sayesinde, $(B_i)_i$ dizisini bilirsek $S_k(n)$ sayılarını bir çırpıda hesaplayabiliriz.

Teorem 3'ün Kanıtı: Her şey basit bir hesaptan çıkıyor aslında. Bir yandan

$$1 + e^x + e^{2x} + \cdots + e^{(n-1)x} = \frac{e^{nx}-1}{e^x-1} = \frac{e^{nx}-1}{x}\frac{x}{e^x-1}$$

$$= \frac{\sum_{i=0}^{\infty}\frac{(nx)^i}{i!} - 1}{x} \cdot \sum_{j=0}^{\infty} \frac{B_j}{j!}x^j$$

$$= \sum_{i=1}^{\infty} \frac{n^i}{i!}x^{i-1} \cdot \sum_{j=0}^{\infty}\frac{B_j}{j!}x^j$$

$$= \sum_{i=0}^{\infty} \frac{n^{i+1}}{(i+1)!}x^i \cdot \sum_{j=0}^{\infty}\frac{B_j}{j!}x^j$$

$$= \sum_{k=0}^{\infty}\left(\sum_{i+j=k}\frac{1}{(i+1)!j!}B_j n^{i+1}\right)x^k$$

$$= \sum_{k=0}^{\infty}\frac{1}{(k+1)!}\left(\sum_{i+j=k}\frac{(k+1)!}{(i+1)!j!}B_j n^{i+1}\right)x^k$$

$$= \sum_{k=0}^{\infty}\frac{1}{(k+1)!}\left(\sum_{i+j=k}\binom{k+1}{i}B_j n^{i+1}\right)x^k$$

$$= \sum_{k=0}^{\infty}\frac{1}{(k+1)!}\left(\sum_{i=0}^{k}\binom{k+1}{i}B_{k-i} n^{i+1}\right)x^k$$

eşitliği, öte yandan,

$$1 + e^x + e^{2x} + \cdots + e^{(n-1)x} = \sum_{i=0}^{n-1} e^{ix}$$

$$= \sum_{i=0}^{n-1}\sum_{k=0}^{\infty}\frac{(ix)^k}{k!} = \sum_{i=0}^{n-1}\sum_{k=0}^{\infty}\frac{i^k x^k}{k!}$$

$$= \sum_{k=0}^{\infty}\left(\sum_{i=0}^{n-1}\frac{i^k}{k!}\right)x^k$$

$$= \sum_{k=0}^{\infty}\frac{1}{k!}\left(\sum_{i=0}^{n-1} i^k\right)x^k$$

$$= \sum_{k=0}^{\infty}\frac{1}{k!}S_k(n)x^k$$

eşitliği geçerli. Katsayıları eşitleyerek,

$$\frac{1}{k!}S_k(n) = \frac{1}{(k+1)!}\sum_{i=0}^{k}\binom{k+1}{i}B_{k-i} n^{i+1}$$

yani

$$S_k(n) = \frac{1}{k+1}\sum_{i=0}^{k}\binom{k+1}{i}B_{k-i}\,n^{i+1}$$

elde ederiz. Bu formülde i yerine $k - i$ alırsak, kolaylıkla teoremdeki formülü buluruz. □

Teorem 2'den, $n!B_{n-1} \in \mathbb{Z}$ sonucunu elde etmiştik, yani B_n'yi paydasında $(n + 1)!$ olan bir sayı olarak yazabiliriz. Şimdi bundan daha güçlü bir sonuç elde edeceğiz: B_n, paydasında

$$\prod_{p \text{ asal ve } p-1,\ n\text{'yi böler}} p$$

olan bir kesirli sayıdır. Yazar, sonucun öneminden çok kanıtın güzelliğinden etkilendiğini itiraf eder!

Teorem 4 [von Staudt-Clausen 1840]. *Eğer k bir çift sayıysa, o zaman,*

$$B_k + \sum_{q \text{ asal ve } q-1|k} \frac{1}{q} \in \mathbb{Z}$$

olur.

Aşağıda, formülün doğruluğuna delil olarak birkaç örnek sunduk.

$$B_2 + \frac{1}{2} + \frac{1}{3} = 1,$$
$$B_4 + \frac{1}{2} + \frac{1}{3} + \frac{1}{5} = 1,$$
$$B_6 + \frac{1}{2} + \frac{1}{3} + \frac{1}{7} = 1,$$
$$B_8 + \frac{1}{2} + \frac{1}{3} + \frac{1}{5} = 1,$$
$$B_{10} + \frac{1}{2} + \frac{1}{3} + \frac{1}{11} = 1,$$
$$B_{12} + \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{13} = 1,$$
$$B_{14} + \frac{1}{2} + \frac{1}{3} = 2,$$
$$B_{16} + \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{17} = -6,$$
$$B_{18} + \frac{1}{2} + \frac{1}{3} + \frac{1}{7} + \frac{1}{19} = 56,$$
$$B_{20} + \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{11} = -528.$$

Teorem 4'ün kanıtı uzun sürecek. Önce bir tanım gerekiyor; ardından birkaç yardımcı sonuç kanıtlayacağız.

p bir asal sayı olsun. Eğer $q \neq 0$ bir kesirli sayıysa, p'ye bölünmeyen a ve b tamsayıları ve bir n tamsayısı için,

$$q = p^n \frac{a}{b}$$

olur. n tamsayısı q tarafından belirlenmiştir. Bu durumda,

$$\mathrm{val}_p(q) = n$$

yazalım. Ayrıca

$$\mathrm{val}_p(0) = \infty$$

tanımını yapalım. Böylece

$$\mathrm{val}_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$$

bir fonksiyon olur. Birkaç örnek verelim:

$$\mathrm{val}_p(1) = \mathrm{val}_p(1) = 0,$$
$$\mathrm{val}_3(9/7) = 2,$$
$$\mathrm{val}_7(9/7) = -1,$$
$$\mathrm{val}_2(9/7) = 0,$$
$$\mathrm{val}_5(250/7) = 3,$$
$$\mathrm{val}_p(p^n) = n.$$

Eğer her $x \in \mathbb{Z}$ ve her $n \in \mathbb{N} \setminus \{0\}$ için,

$$x + \infty = \infty + x = \infty,\ x < \infty,\ n\infty = \infty$$

varsayımlarını yaparsak, bu fonksiyonun şu özellikleri vardır:

val_p Fonksiyonunun Özellikleri: *Her a ve b kesirli sayısı, her $n > 0$ doğal sayısı ve her p asal sayısı için şu özellikler geçerlidir:*

i. $\mathrm{val}_p(a) = \infty \Leftrightarrow a = 0$,
ii. $a \in \mathbb{Z} \Leftrightarrow$ *Her p asal sayısı için* $\mathrm{val}_p(a) \geq 0$,
iii. $\mathrm{val}_p(1) = \mathrm{val}_p(-1) = 0$,
iv. $\mathrm{val}_p(a) = \mathrm{val}_p(-a)$,
v. $\mathrm{val}_p(ab) = \mathrm{val}_p(a) + \mathrm{val}_p(b)$,
vi. $\mathrm{val}_p(a^{-1}) = -\mathrm{val}_p(a)$,
vii. $\mathrm{val}_p(a^n) = n \cdot \mathrm{val}_p(a)$,
viii. $\mathrm{val}_p(a + b) \geq \min\{\mathrm{val}_p(a), \mathrm{val}_p(b)\}$,
ix. Eğer $\mathrm{val}_p(a) \neq \mathrm{val}_p(b)$ ise,
$\mathrm{val}_p(a + b) = \min\{\mathrm{val}_p(a), \mathrm{val}_p(b)\}$.

Kanıt: Bunların her birinin kanıtı kolaydır ve okura bırakılmıştır. □

v ve viii özellikleri iki sayıdan n sayıya genelleştirilebilir elbet.

Önemli bir olgu sıkıştıralım araya: (i, iii, vii) özellikleri sayesinde, eğer $\lambda \in (0, 1)$ ise

$$d(a, b) = \lambda^{\mathrm{val}_p(n)}$$

tanımı $\mathbb{Q}$ üzerine bir metrik verir; genellikle $\lambda = 1/p$ alınır. (Bkz. sayfa 35, Örnek 13.)

Teorem 4'ün kanıtında kullanacağımız bir sonucu kanıtlayalım şimdi.

Bundan böyle p bir asal ve $k > 0$ bir doğal sayıyı temsil edecek.

Önsav 5. $m > 0$ *bir doğal sayıysa*

$$S_k(p^{m+1}) \equiv pS_k(p^m) \bmod p^{m+1}$$

olur.

Kanıt: Eğer $k = 1$ ise sonuç kolay ve okura bırakılmıştır. Bundan böyle $k > 1$ olsun. Eğer k tek ise, sonuç Teorem 1'den çıkar. Bundan böyle k'nın çift olduğunu varsayalım. Eğer $0 \le i < p^{m+1}$ ise, i'yi p^m'ye bölerek, bir ve bir tek $0 \le u < p$ ve $0 \le v < p^m$ özelliklerini sağlayan (u, v) çifti için

$$i = up^m + v$$

elde ederiz. Bu olguyu kullanarak $S_k(p^{m+1})$ sayısını mod p^{m+1} hesaplayalım.

$$\begin{aligned}
S_k\left(p^{m+1}\right) &= \sum\nolimits_{0\le i<p^{m+1}} i^k \\
&= \sum\nolimits_{0\le u<p,\,0\le v<p^m} (up^m + v)^k \\
&\equiv \sum\nolimits_{0\le u<p,\,0\le v<p^m} (v^k + kv^{k-1}up^m) \\
&= \sum\nolimits_{0\le u<p,\,0\le v<p^m} v^k + kp^m \sum\nolimits_{0\le u<p,0\le v<p^m} v^{k-1}u \\
&= pS_k(p^m) + kp^m \sum\nolimits_{0\le u<p,0\le v<p^m} v^{k-1}u \\
&= pS_k(p^m) + kp^m \sum\nolimits_{0\le v<p^m} v^{k-1} \sum\nolimits_{0\le u<p} u \\
&= pS_k(p^m) + kp^m \frac{p(p-1)}{2} \sum\nolimits_{0\le v<p^m} v^{k-1}.
\end{aligned}$$

Eğer $p \ne 2$ ise sonuç hemen çıkar. Eğer $p = 2$ ise, sonuç k'nın çift olmasından çıkar. □

Sonuç 6. $n, m > 0$ *doğal sayı olsunlar. O zaman*

$$\frac{S_k\left(p^n\right)}{p^n} - \frac{S_k\left(p^m\right)}{p^m} \in \mathbb{Z}$$

olur.

Kanıt: Bir önceki önsava göre, her $m > 0$ için,

$$\frac{S_k\left(p^{m+1}\right)}{p^{m+1}} - \frac{S_k\left(p^m\right)}{p^m} \in \mathbb{Z}$$

olur. Sonuç (teleskopik toplamlar sayesinde), bundan hemen çıkar. □

Sonuç 7. $\mathrm{val}_p\left(B_k - \dfrac{S_k(p)}{p}\right) \ge 0.$

Kanıt: Teorem 3'e göre

$$S_k(n) = \sum\nolimits_{i=0}^{k} \binom{k}{i} \frac{B_i}{k+1-i} n^{k+1-i}.$$

Demek ki,

$$\frac{S_k(n)}{n} = \sum\nolimits_{i=0}^{k} \binom{k}{i} \frac{B_i}{k+1-i} n^{k-i}.$$

Şimdi burada n yerine p^n alalım:

$$\frac{S_k(p^n)}{p^n} = \sum\nolimits_{i=0}^{k} \binom{k}{i} \frac{B_i}{k+1-i} p^{n(k-i)}.$$

Dolayısıyla,

$$\frac{S_k(p^n)}{p^n} - B_k = \sum\nolimits_{i=0}^{k-1} \binom{k}{i} \frac{B_i}{k+1-i} p^{n(k-i)}.$$

olur. Şimdi iki tarafın da val_p'sini alacağız. Sağ taraftaki

$$\binom{k}{i} \frac{B_i}{k+1-i}$$

katsayılarının val_p'lerinin en küçüğüne v diyelim. O zaman, val_p'nin v ve viii özelliklerinden dolayı

$$\mathrm{val}_p\left(\frac{S_k(p^n)}{p^n} - B_k\right) \ge v + n$$

olur. Demek ki n'yi yeterince büyük seçerek,

$$\mathrm{val}_p\left(\frac{S_k(p^n)}{p^n} - B_k\right)$$

sayısını dilediğimiz kadar büyük, örneğin pozitif yapabiliriz. Böyle bir n seçelim. Ayrıca, Sonuç 6'ya göre,

$$\mathrm{val}_p\left(\frac{S_k(p)}{p} - \frac{S_k\left(p^n\right)}{p^n}\right) \ge 0$$

olur. Son iki sonucu bir araya getirerek ve viii özelliğini kullanarak istediğimiz sonucu elde ederiz. □

Önsav 8. $S_k(p) \equiv \begin{cases} -1\,(\mathrm{mod}\,p) & \textit{eğer } (p-1) \mid k \textit{ ise} \\ 0\,(\mathrm{mod}\,p) & \textit{aksi halde} \end{cases}$

Kanıt: p bir asal olduğundan, $\mathbb{Z}/p\mathbb{Z}$ sonlu (p elemanlı) bir cisimdir. Dolayısıyla

$$(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{Z}/p\mathbb{Z} \setminus \{0\},$$

kümesi, çarpma altında, $p - 1$ elemanlı döngüsel bir gruptur [MD-2004-I, sayfa 16, Sonuç 4]. Dolayısıyla eğer $p - 1$ sayısı k'yı bölmüyorsa, $(\mathbb{Z}/p\mathbb{Z})^*$ grubunun k'ıncı kuvveti 1 olmayan bir elemanı vardır. Bu elemanın $\mathbb{Z}$'deki bir temsilcisine a diyelim. O zaman,

$$\begin{aligned}
S_k(p) &= \sum\nolimits_{i=1}^{p-1} i^k \equiv \sum\nolimits_{i=1}^{p-1} (ai)^k = \sum\nolimits_{i=1}^{p-1} a^k i^k \\
&= a^k \sum\nolimits_{i=1}^{p-1} i^k = a^k S_k(p)
\end{aligned}$$

olur. Ama $a^k \not\equiv 0 \bmod p$. Dolayısıyla bu durumda $S_k(p) \equiv 0 \bmod p$ olur.

Şimdi $p - 1$'in k'yı böldüğünü varsayalım. O zaman her $i \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ için $i^k = 1$ olur. Dolayısıyla,

$$S_k(p) = \sum\nolimits_{i=1}^{p-1} i^k \equiv \sum\nolimits_{i=1}^{p-1} 1 = p - 1 \equiv -1$$

olur. □

Sonuç 9. *Eğer $p-1$, k'yı bölmüyorsa $S_k(p^n)/p^n \in \mathbb{Z}$. Aksi halde $S_k(p^n)/p^n + 1/p \in \mathbb{Z}$.*

Kanıt: Sonuç 6'nın $m = 1$'e uygulanmasından ve Önsav 8'den hemen çıkar.

Sonuç 10. *Eğer $p-1$, k'yı bölmüyorsa* $\mathrm{val}_p(B_k) \geq 0$. *Aksi halde* $\mathrm{val}_p(B_k + p^{-1}) \geq 0$.

Kanıt: Sonuç 7'ye göre

$$\mathrm{val}_p\left(B_k - \frac{S_k(p)}{p}\right) \geq 0.$$

Eğer $p-1$, k'yı bölmüyorsa, Sonuç 9'a göre,

$$S_k(p)/p \in \mathbb{Z},$$

yani

$$\mathrm{val}_p(S_k(p)/p) \geq 0.$$

Dolayısıyla,

$$\mathrm{val}_p(B_k) = \mathrm{val}_p\left(\left(B_k - \frac{S_k(p)}{p}\right) + \frac{S_k(p)}{p}\right)$$
$$\geq \min\left\{B_k - \frac{S_k(p)}{p}, \frac{S_k(p)}{p}\right\} \geq 0.$$

Eğer $p-1$, k'yı bölüyorsa, Sonuç 9'a göre,

$$S_k(p)/p + 1/p \in \mathbb{Z},$$

yani

$$\mathrm{val}_p(S_k(p)/p + 1/p) \geq 0.$$

Dolayısıyla,

$$\mathrm{val}_p\left(B_k + \frac{1}{p}\right) = \mathrm{val}_p\left(\left(B_k - \frac{S_k(p)}{p}\right) + \left(\frac{S_k(p)}{p} + \frac{1}{p}\right)\right)$$
$$\geq \min\left\{B_k - \frac{S_k(p)}{p}, \frac{S_k(p)}{p} + \frac{1}{p}\right\} \geq 0.$$

İstediğimizi kanıtladık. □

Teorem 4'ün Kanıtı [Witt]: W_k sayıları şöyle tanımlansın:

$$W_k = B_k + \sum_{q \text{ asal ve } q-1|k} \frac{1}{q}.$$

p herhangi bir asal olsun.

Eğer $p-1$ sayısı k'yı bölüyorsa, yani W_k'nın yukardaki tanımındaki toplamda yer alıyorsa, o zaman, Sonuç 10'a göre,

$$\mathrm{val}_p(W_k) = \mathrm{val}_p\left(B_k + \frac{1}{p} + \sum_{\substack{q \text{ asal ve } q-1|k \\ \text{ve } q \neq p}} \frac{1}{q}\right)$$
$$\geq \min\left\{\mathrm{val}_p\left(B_k + \frac{1}{p}\right), \mathrm{val}_p\left(\sum_{\substack{q \text{ asal ve } q-1|k \\ \text{ve } q \neq p}} \frac{1}{q}\right)\right\}$$
$$\geq 0$$

olur.

Eğer $p-1$ sayısı k'yı bölmüyorsa, yani W_k'nın yukardaki tanımındaki toplamda yer almıyorsa, o zaman, gene Sonuç 10'a göre,

$$\mathrm{val}_p(W_k) = \mathrm{val}_p\left(B_k + \sum_{q \text{ asal ve } q-1|k} \frac{1}{q}\right)$$
$$\geq \min\left\{\mathrm{val}_p(B_k), \mathrm{val}_p\left(\sum_{q \text{ asal ve } q-1|k} \frac{1}{q}\right)\right\}$$
$$\geq 0$$

olur.

Demek ki p hangi asal sayı olursa olsun,

$$\mathrm{val}_p(W_k) \geq 0.$$

Bu da aynen $W_k \in \mathbb{Z}$ demektir. Teorem 4'ün kanıtı bitmiştir. □

Kaynakça

J. W. S. Cassels, **Local Fields**, London Mathematical Society, Student Texts 3 (1986).