TÜMEVARIM: KLASİK

Hemen söyleyelim: Bu yazının temel konusu bir zamanlar birbirlerine denk olan ama günümüz matematiğinde birer teorem olmaya terfi eden,

- **İyi Sıralama İlkesi**
- **Matematiksel tümevarım**

kavramlarıdır. Aslında, burada geçen iyi sıralama ilkesi, matematiksel tümevarım (kısaca tümevarım) kavramının anlamak için bir araç olarak kullanılmakta. Tümevarım, bir yönüyle doğal sayılar kümesini tanımlayan ana maddelerden biri olmasının yanında, ve dolayısıyla, "ilk sonsuz küme" tümevarım olmadan tanımlanamaz. Ayrıca, sonsuz bir küme yoksa tümevarım da yoktur!

Bu yazıyı takip etmesi planlanan bir sonraki yazının konusu kalkülüsün birçok temel teoremini kanıtlayacak güçte olan tümevarımın bir genellemesi olacak. Bu ikinci yazıdan sonra mevcut yazının, en azından eğitsel olarak, anlamı daha iyi yorumlanabilecektir.

Bir kavramın ilki, daha geniş bir bakış açısıyla ilk izleri, anlaşılmaya çalışılmadan o kavramın anlaşılmasında her zaman bazı şeylerin eksik kalması doğaldır. Örneğin, yaklaşık bin yıl önce 1'den 10'a kadar olan sayıların toplamının karesinin o sayıların küplerinin toplamına eşit olduğunu gösteren al-Karaji'nin, bunu göstermekle derdinin ne olduğunu anlamadan, bu "doğru" olan ifadeyi, neden doğru olduğunu sorgulamadan alıp heybeye atmak kabul edilebilir mi? Bu tür sorulara sıkıştırılmış ve baskıcı yanıtlar aramamak da gerekir; insanın kendinin ne olduğunu anlamadan yaşamayı heybesine attığını unutmamak gerekir.

Otuz beş katlı bir binadan bırakılan bir taşın her zaman yere düşeceğinin fiziki gözlemlerle mümkün olmamasına karşın, (kim demiş mümkün değil, diye!) beş bin kez bırakılan taşın yere düştüğü gözlemlense bile bu gözlemden bırakılan beş bin birinci taşın düşeceği sonucu çıkmaz ama insanın "düşer" diyesi gelir. Bu yaklaşımla bir başkası taş yerine elma alarak bunu deneyecek olursa çarşı karışabilir ve bu durum yaygınlaşırsa da dünya bir akıl hastanesine dönüşebilir. İşte hem hatırı sayılır "düşer"i ziyan etmemek hem de kişilerin akıl sağlığını korumak için konuyu kavramlaştırmak gerekiyor. Bu kavramlaştırmaya (yanılmıyorsam) "eksik tümevarım" deniyor. Eksik giderilecek!

Anlamak, "Ceviz mi ceviz ağacından yoksa ceviz ağacı mı cevizden olur?" sorusunu sormadan olamayacağı gibi, anlamak "doğru"yu bulmak da değildir. Evet evet, haklısınız, anlamak yanlışı göstermek de değildir. Anlamayı anlamak ise bambaşka bir durumdur; bunun için gerekli şeylerden biri, "anlamak, yanlış bir eylem midir?" sorusuna yanıt vermeden muhattap olabilmektir.

Bu çerçevede, "tümevarım"ın geçmişi ve bugünü, detaylara girilmeden de olsa bulanık geçmişi, daha belirgin izleri ve güncel hali anlaşılamaya çalışılacak. Bu anlaşılmanın eksik olması, tümevarımın geleceğini anlayabilmek ve evrimleşebilmesinin yolunu açmak için bir kazanç olacaktır!

"Tümevarımın ne işe yaradığına ilişkin bir örnek verilebilir mi?" sorusuna verilecek yanıtlardan birinin, "herhangi bir doğal sayının bir ile toplamının birden büyük olduğunu göstermek" olabilir. Bir başka örnek istenirse de, "herhangi bir doğal sayının bir ile toplamının birden küçük olmadığını göstermek" olabilir. Bunun yanında,

$$1 + 1 < 1$$

olmadığını göstermede tümevarımın bir katkısının olmadığı söylenebilir. Daha felsefi bir yanıt ise sonsuzluk kavramı ne işe yararsa tümevarım da o dereceli işe yarar, biçiminde olabilir.

İlk olmadan "var olmak" olmaz! Çoğalmadan var olmak da çekilmezdir. Adem ve Havva ikilisinin üremeden var olmaları sıkıcı olmaz mıydı? Diğer taraftan çoğalmak, yani tüme varmak, meydan okumaktır ve tehlikelidir; tüme varma Tanrı'nın elindeki oyuncağı alma eylemidir. Sonuçta bakmışınız ki Tanrı'nın elinden almaya çalıştığınız oyuncak zaten ta başta sizin elindeymiş; süprizlere açık olmak da gerekir.

Tümevarım, en genel haliyle, ilki ve çoğalma modeli olan bir yapıdır. Daha kavramsal olarak, tümevarım, tanımsız iki şeyden değil, üç temel şeyden oluşan bir üçlüdür, sıralıdır da, bu sayı detaya bağlı olarak artırılabilir de. Bu üçlüyü oluşturan şeylerden biri, çoğalanların genel adıdır: doğal sayı! Doğal sayıların topluluğu ω ile gösterilir. Çoğalmadan var olan bir başka sayı daha vardır: Sıfır. Sıfır, 0 sembolü ile gösterilir. Sıfırdan başka bütün sayıları içeren ve başka hiç birşey içermeyen topluluk $\mathbb{N}$ ile gösterilecek. Çok standart olmasa da ω'ya **doğal sayılar kümesi** ve $\mathbb{N}$'ye **sayma sayılar kümesi** denir[1].

Asal sayıların sayısının "sonsuz" olduğunun kanıtı için Öklid'in Elemanları, Kitap IX'ın 20. Önerme'si olan "*Asal sayıların miktarı, seçilen her asal sayı topluluğunun*

[1]Kaynakların çoğunda $\mathbb{N}$'ye doğal sayılar kümesi ve ω'ya negatif olmayan tam sayılar kümesi de denir.

miktarından fazladır"ın kanıtı referans alınır [5]. Aslında bu ifadenin kendisi, günümüzde "Matematiksel Tümevarım" olarak bilinen kavramın ilkel bir uygulanmasıdır. Genel olarak tümevarım yönteminin esas bileşenlerinden biri, "verilen miktardan daha fazlası vardır"dır. Burada yer alan "verilen miktardan daha fazlası vardır" ifadesinde yer alan "verilen miktar" bir ilk varlığın kabulü ve "daha fazlası" bir anlamda durmadan yapılan bir çoğalmayı çağrıştırmaktadır. Bir varsa iki var, bir ve iki varsa üç vardır, ve böyle devam eder, nereye kadar, sonsuza kadar![2] Kimbilir, belki de tümevarımsal bakış açısı sonsuza kontrollü bir biçimde yaklaşma sanatıdır.

Sayma sayılarını iki evrede incelemek gerekir; 1889 öncesi ve sonrası. Peano, 1889 yılında yayınlanan *Arithmetices Principa Nova Methodo Expsita* adlı eserinde, "1"i bulunduğu toplulukta belirli özellikleri sağlayan bir simge olarak varsayıp, 2 sayısını, "=" ve "+" sembolleri çerçevesinde,

$$2 = 1 + 1$$

olarak tanımladı. Peano, hemen sonrası "3" sayısını

$$3 = 2 + 1$$

olarak tanımladı. Sonrasında "4" sayısını tanımlamış olsa da "8327" sayısını tanımlamadı![3] Sayma sayılar topluluğunun hangi tür topluluklara eşit oluduğunu belirleyen en temel aksiyomlardan biri, "tümevarım" aksiyomudur. Bu tanımlanmadan sonra tümevarım kendisine meşru bir alan açmıştır. Peano'nun bu eseri öncesi sayılar, "tanımlanmamış" olsalarda, onlar üzerinden elde edilen sonuçlar Peano'nun aksiyomatik yapısına elbette uyumlu olmuştur; yani çürüğe çıkan, ya da ölen yiten bir sayı yoktur[4]. Ancak, bu yapı, birçok açıdan yetersizdi; örneğin tam sayıları tanımlayabilmek için daha bir üst perdeden bakmak gerekiyordu, bu, Zermelo-Fraenkel küme sisteminde sağlanabilmiştir. Bu bakış açısı içerisinde, boşküme tanımsız bir obje olarak ele alınıp, 0 sayısı,

$$0 = \varnothing$$

olarak tanımlanmış ve "1" sayısı

$$1 = \{\varnothing\}$$

olarak tanımlanarak, tanımsız bir sembol olmaktan kurtulmuştur. Bunun yanında her n doğal sayısı için,

---

[2]Buna potansiyel sonsuz deniliyor!

[3]Peano, bu durumu, "... benzer biçimde tanımlanır" diye geçiştirdi.

[4]Bu sayılara **Peano doğal sayılar** denilecek olursa sıfır, bir Peano doğal sayı olmamasının ötesinde bu sistem içinde "sıfır" diye birşey yoktur!

$$n + 1 = n \cup \{n\}$$

olarak tanımlanmıştır[5]. Ayrıca, bu yapı içerisinde tümevarım da bir aksiyom olmaktan kutulup, bir sonuç mertebesine ulaşmıştır.

Her ne kadar yukarıdaki paragrafta doğal sayıların ilk olarak Peano tarafından tanımlandığı sonucu çıkartılacak olsa da bu, bazı anlamlarda eksik olacaktır. Richard Dedekind, 1888 yılında yayınlanan "Was sind und was sollen die Zahlen?" (Sayılar nedir ve nasıl olmalıdır?) adlı eserinde doğal sayıları Peano tanımına denk olacak biçimde tanımlamıştı. Bu konuya bu yazıda yer verilecektir.

Tümevarımla çok çok önemli teoremlerin kanıtlanabilmesine karşın çok temel teoremlerin bu yöntemle verilen kanıtları şimdilik yoktur. Örneğin, *reel sayıların kapalı ve sınırlı aralığında tanımlı reel değerli sürekli bir fonksiyonun görüntü kümesinin sınırlı* olduğunun tümevarımla verilmiş bir kanıtı, günümüzde yoktur. Verilebilir mi, ayrı bir soru. Buna karşın, bahsi edilen "temel teoremleri" kanıtlayacak bir biçimde tümevarım kavramı genellenebilir. Bu yazının bir sonrakinde bu tür genellemelerin konu edilmesi planlanmakta olup, bunların değeri, temel teoremlerin kanıtını veriyor olması üzerinden sıklıkla ölçülecektir.

Yukarıda ifade edilmeye çalışılan bakış açısıyla matematikde günümüzde "Matematiksel Tümevarım" olarak bilinen kavramın klasik formu, sadece teknik açıdan değil, çok kısa da olsa izleri- ki bu izlerin çoğunun gerçekten bir iz olduğu tartışmalıdır- üzerinden anlaşılmaya çalışılacak. Bunun yanında, bu kavram farklı fakat denk bir biçimde tekrak okunarak, elde edilecek genellemeyle kalkülüsün bir çok temel teoremi bu kavram kullanılarak kanıtlanabilmektedir.

Tümevarım kavramınının önemi sadece birçok temel teoremi kanıtlıyor olmasından değil, sonraki aşamalarda doğal sayıları tanımlıyor olmasındandır. Bu kavramın son derece doğal olmasının nedenlerinden biri de "iyi sıralama ilkesi"ne bir zamanlar denk olmasındandır. Bu ilkenin kullanımıyla bazı temel teoremler bir sonraki bölümde kanıtlanacaktır.

Bu yazıda sayılarla ilgili standartlaşmış semboller herhangi bir açıklama yapılmadan kullanılacaktır. Örneğin, $\mathbb{R}$, $\mathbb{Q}$ ve $\mathbb{Z}$, sırasıyla reel sayılar, rasyonel sayılar ve tam sayılar kümesini gösterir.

Genel olarak sayıların nasıl inşa edildiği bu yazının konusu olamayacak. Buna karşı, reel sayılar sistemi doğal sayılar sistemi üzerine inşa edilebileceği gibi aksiyomatik

[5]Bu sayılara **Von Neumann doğal sayı** denilecek olunursa, sıfır, bir Von Neumann doğal sayı olup, $(\omega \setminus \{0\}, 0, s)$ üçlüsü Peano sistemi olacaktır. Yani, her Peano doğal sayı von Neumann doğal sayı olmasına karşılık, sıfır haricindeki her von Neumann doğal sayı bir Peano doğal sayıdır.

olarak tanımlanıp sonrasında doğal sayı sistemi tanımlanabilir bir sistem olduğunu ifade edelim. Bu yolla tanımlanan doğal sayılar kümesi,

$$1 \in A \text{ ve } a \in A \text{ ise } a + 1 \in A$$

koşulunu sağlayan bütün A altkümelerinin arakesiti olarak tanımlanır. $\mathbb{R}$'nin kendisi bu özelliği sağlar.

Bu yazıda kapsam dışı konulara girilerek (örneğin rasyonel sayıların reel sayılarda yoğun olmasının gösterilmesi) içeriğin saptırıldığı yönünde haklı eleştiriler olabilir, haklıdırlar da. Bunları, tümevarımla edilen sonuçların bazı temel sonuçlara uygulanma vurgusu olarak değerlendirilmesi gerektiğini düşünüyorum.

Bu giriş yazısını tümevarımla hiçbir alkası olmayan şu kelimeyle bitirmek istiyorum:

Saygılarımla.

1. İyİ Sıralama İlkesİ

İyi sıralama ilkesi[6] sayma sayılar kümesini tanımlayan Peano aksiyom sisteminin tanımlandığı zamana (1889) kadar tümevarıma denk olan kavram olarak değerlendirilebilmesine karşın, Peano-aksiyom sistemi içerisinde tümevarım bir aksiyom olarak yer alırken, iyi sıralama ilkesi bir teorem olmuştur[7].

Tümevarımın dolaylı olarak ilk uygulamasının asal sayıların sonsuz olduğunu göstermekte olduğu sıklıkla ifade edilir. Asal sayıların asaleti, sanırım, onun "parçalanamaz" olmasından gelir. Bu sayılar, sadece ve sadece kendisi ve bir sayısınca ölçülebilir sayılardır ve dolayısıyla her biri birer eksendir. Her doğal sayının bu eksenlerden sonlu tanesine olan bir izdüşümü vardır ve bir anlamda bir "taban"dır. Biraz daha açık bir ifadeyle, birden büyük her doğal sayı bazı asal sayıların çarpımı olarak yazılabiliyor. Bu, aritmetiğin temel teoremi olarak adlandırılıp, bu teoremde dahil olmak üzere, sayılarla ilgili bazı temel sonuçlar, tümevarıma denk olan *iyi sıralama ilkesi* üzerinden anlaşılmaya çalışılacak. Bu yaklaşım, tümevarımın olmazsa olmaz olduğunun bir "kanıtı" olarak da değerlendirilecektir.

$S \subset \mathbb{R}$ verilsin. Her $s \in S$ için $d \leqslant s$ eşitsizliğini sağlayan $d \in \mathbb{R}$'ye S'nin bir **alt sınırı** denir. En az bir altsınırı olan kümeye alttan sınırlı denir. d, S'nin bir altsınırı ve aynı zamanda, $d \in S$ ise d'ye S'nin **en küçük elemanı** ya da **minumumu** denir. ω'nin her alt kümesinin minumunun elemanının olmasının doğallığı aşağıdaki teoremle anlaşılabilir.

[6]İngilizce: well ordering principle.

[7]Sayma sayılar içi iyi sıralama ilkesinin ilk olarak ne zaman kullanıdığına ilişkin bir bilgiye ulaşamadım.

Teorem 1.1. *Aşağıdakiler denktir.*

a. *$\mathbb{Z}$'nin boş olmayan alttan sınırlı her altkümesinin minumumu vardır.*
b. *$\mathbb{Z}$'nin boş olmayan sonlu her altkümesinin minumumu vardır.*

Aşağıdaki teorem doğal sayılar yapısının kavramsal olarak tanımlanmadan verilmesine karşın, bu teoremin ikinci denk koşulu doğal sayılar sistemini tanımlayan en temel aksiyomlardan biridir.

Teorem 1.2. *Aşağıdakiler denktir.*

a. *$\mathbb{N}$'nin boş olmayan her alt kümesinin minumumu vardır.*
b. *$A \subset \mathbb{N}$ kümesinin $A = \mathbb{N}$ olması için gerek ve yeter koşul, $1 \in S$ ve $n \in S$ olduğunda $n+1 \in S$ olmasıdır.*

Kanıt. $a \Rightarrow b$: $A \subset \mathbb{N}$ verilsin. $1 \in A$ ve $n \in A$ olduğunda $n+1 \in A$ olmasına karşın $A \neq \mathbb{N}$ olsun. $\mathbb{N} \setminus A$ boş kümeden farklı olduğundan, $\mathbb{N} \setminus A$ kümesinin en büyük alt sınırı vardır, buna k ile gösterelim. $1 \in \mathbb{N} \setminus A$ olduğundan, $1 < k$ olur. $k-1 \notin \mathbb{N} \setminus A$ olduğundan $k-1 \in A$ olmak zorundadır. A'nın varsayılan özelliğinden de $k = (k-1)+1 \in A$ elde edilir. Bu, $k \in \mathbb{N} \setminus A$ olmasıyla çelişir.
$b \Rightarrow a$: $S \subset \mathbb{N}$ boş olmayan bir küme olsun. S'nin en büyük altsınırının olmadığını varsayalım.

$$T = \{n : \{1, 2, \cdots, n\} \subset \mathbb{N} \setminus S\}$$

olarak tanımlansın. S'nin en büyük altsınırı olmadığından $1 \in T$ olur. $n \in T$ olduğunu varsayalım, yani $\{1, 2, \cdots, n\} \subset \mathbb{N} \setminus S$ olsun. $n+1 \notin T$ olsaydı $n+1 \in S$ olur ve her $1 \leqslant i \leqslant n$ için $i \notin S$ olacağından, $n+1$, S'nin en büyük alt sınırı olurdu ki-bu çelişki olurdu. Dolayısıyla, $n+1 \in T$ olur. Varsayım gereği $T = \mathbb{N}$ olur. Buradan, her n için $\{1, 2, \cdots n\} \cap S = \varnothing$ ve dolayısıyla, n üzerinden alınarak elde edilen bileşim kümesi boş küme olur. Buradan da, S'nin boş küme olduğu görülür ve bu, bir çelişkidir. Kanıt tamamlanır. □

Tanım 1.3. *Teorem 1.2'de yer alan birinci denk koşula* **iyi sıralama ilkesi** *ve ikinci denk koşula* **tümevarım** *denir.*

2. Arşİmedyan Özellİğİ

Doğal sayıların reel sayılarda sıralamaya[8] göre, $b > 0$ doğal sayı olmak üzere her $a \in \omega$ için

$$a \leqslant kb$$

olacak biçimde bir k doğal sayısının olmasıyla her rasyonel sayının bir doğal sayıdan küçük olmasının birbirlerine denk olduğu kolayca gösterilebilir. Diğer taraftan, bu denk koşullardan ilkinin doğruluğu $k = a$ alınarak hemen elde edilebilmesine karşın, iyi sıralama ilkesine vurgu yapmak için daha uzun kanıtıyla aşağıdaki teorem verilebilir.

Teorem 2.1 (Arşimedyan özelliği)**.** [9] *$a, b \in \mathbb{N}$ verilsin. $a \leqslant nb$ olacak biçimde $n \in \mathbb{N}$ vardır.*

Kanıt. Olmadığını varsayalım. Yani, her $n \in \mathbb{N}$ için $nb < a$ olsun. Bu durumda

$$S = \{a - nb : n \in \mathbb{N}\} \subset \mathbb{N}$$

olacaktır. S'nin minumumu d, vardır. $d = a - nb$ olacak biçimde $n \in \mathbb{N}$ seçilebilir.

$$a - (n+1)b \in S$$

olduğundan,

$$a - nb \leqslant a - (n+1)b$$

olur. Bu, $b \leqslant 0$ çelişkisini verir ve kanıt tamamlanır □

Arşimedyan özelliğinin bileşim olarak söylediği, her $b \in \mathbb{N}$ için

$$\mathbb{N} = \bigcup_{n=1}^{\infty} [1, nb)$$

eşitliğidir. Bu teoremin bir sonucu olarak şu teorem hemen elde edilir.

Teorem 2.2. *Her rasyonel sayı en az bir doğal sayıdan küçüktür.*

---

[8] Peano aksiyom sisteminde $\mathbb{N}$'de $a < b$ olması $b = a + c$ olacak biçimde $c \in \mathbb{N}$'nin olması üzerinden tanımlanır. Burada geçen toplama "+" işleminden detaylı olarak bahsedilmeyecek. Ancak, bu işlemin $m + n$ tanımlandığında $m + (n+1) = (m+n) + 1$ özelliğini sağlayacak biçimde tanımlandığını ifade edelim. Buna göre, her n için $n < n + 1$ olur. $n + 1 < n$ olmadığını göstermekse biraz çaba ister! Buna karşın $2 < 1$ olmadığını göstermek zor değildir. Diğer taraftan, Zermelo-Fraenkel sistemde ω'da sıralama doğrudan kapsama üzerinden tanımlanır, ve bu durumda, $\{\varnothing, \{\varnothing\}\} \subset \{\varnothing\}$ olamayacağından, $1 + 1 < 1$ olamaz.

[9] "Arşimedian özelliği" (Archimedean property) adlandırması 1880 yılında Otto Stolz tarafından yapılmıştır. Bu özellik Öklid'in Elemanları Kitap 5'de Tanım 4 olarak yer almıştır. Reel sayılar için Archimedean özelliği şöyledir: Her $x \in \mathbb{R}$ için $x < n$ olacak biçimde $n \in \mathbb{N}$ vardır. Bunun kanıtı için iyi sıralama ilkesi yeterli değildir.

Reel sayılar sistemini tanımlayan aksiyomlardan biri "tam" (Dedekind tam) olma aksiyomudur. Yukarıda verilen teoremi kanıtlamada bu aksiyom kullanılmadı. Buna karşın, her reel sayının bir doğal sayıdan küçük olduğu göstermek için tam olma aksiyomuna ihtiyaç vardır. Tam olma aksiyomunun dediği şudur: $A \subset \mathbb{R}$ kümesi üstten sınırlı, yani her $a \in A$ için $a \leqslant x$ olacak biçimde bir $x \in \mathbb{R}$ olsun. Bu durumda

i. her $a \in A$ için $a \leqslant s$
ii. b, A'nın bir üstsını ise $s \leqslant b$

olacak biçimde $s \in \mathbb{R}$ vardır. Bu özellikteki s tek bir tane olup, buna A'nın **supremumu** denir ve $s = \sup A$ yazılır. Bir $x \in \mathbb{R}$'nin $A \subset \mathbb{R}$'nin supremumu olması için gerek ve yeter koşul, x'in A'nın bir üst sınırı olması ve her $\varepsilon > 0$ için $x - \varepsilon < a$ olacak biçimde $a \in A$ olmasıdır.

Teorem 2.3. *($\mathbb{R}$ için Arşimedyan özelliği) $\mathbb{N}$, $\mathbb{R}$'de üstten sınırsızdır.*

Kanıt. Her $n \in \mathbb{N}$ için $n \leqslant x$ olacak biçimde $x \in \mathbb{R}$ olduğunu varsayalım. $\mathbb{R}$'nin tam olması nedeniyle $\mathbb{N}$'nin supremumumu vardır, s ile gösterelim. Bu durumda $s - 1 < n$ olacak biçimde $n \in \mathbb{N}$ vardır. Buradan $s < n + 1 \leqslant s$ çelişkisi elde edilir. Kanıt tamamlanır. □

Not edelim: Bu teorem, tam olma aksiyomu kullanılmadan

"her $x > 0$ için $0 < \frac{1}{n} < x$ olacak biçimde n doğal sayısı vardır"

ifadesine denktir.

3. Araya Yerleşebilme

Teorem 2.3'in bir uygulaması olarak şu teorem verilebilir.

Teorem 3.1. *Her $x \in \mathbb{R}$ için,*

$$n - 1 \leqslant x < n$$

olacak biçimde $n \in \mathbb{Z}$ var ve tektir.

Kanıt. $0 \leqslant x$ olsun. $x < k$ olacak biçimde $k \in \mathbb{N}$ sayıları olduğundan bu eşitsizliği sağlayan k'lerin ilk elemanı vardır, bunu n ile gösterelim. Bu durumda $1 < n$ ve $x \nless n - 1$ olacaktır. Dolayısıyla,

$$n - 1 \leqslant x < n$$

olur. Tekliğin gösterilmesi açık. $x < 0$ olama durumu da benzer biçimde gösterilir. □

Tanım 3.2. *$x \in \mathbb{R}$ ve $m \in \mathbb{Z}$ sayıları $m \leqslant x < m+1$ eşitsizligini sağlıyorsa m'ye x'in* **tam değeri** *denir.*

Bir a sayısının tam değeri $[[a]]$ ile gösterilir. Dolayısıyla, $[[a]] \leqslant a < [[a]]+1$ olur.

Teorem 3.3. *a, b reel sayıları $1 < b-a$ eşitsizliğini sağlıyorsa $a \leqslant n \leqslant b$ olacak şekilde n tamsayısı vardır.*

Kanıt $b < [[a]]+1$ olsaydı, $1 < b-a \leqslant ([[a]]+1)-[[a]] = 1$ olurdu. Dolayısıyla $n = [[a]]+1$ alınarak istenilen elde edilir.

Teorem 3.4. *$\mathbb{R}$'de $x < y$ eşitsizliği verilsin. $x < r < y$ olacak biçimde r rasyonel sayısı vardır.*

Kanıt. $0 < \frac{1}{y-x} < n$ olacak biçimde n doğal sayısı seçilebilir. Buradan, $1 < ny - nx$ seçilebilir. Teorem 3.3 gereği $nx \leqslant m \leqslant ny$ olacak biçimde m doğal sayısı vardır. $r = \frac{m}{n}$ rasyonel sayısı $x \leqslant r \leqslant y$ eşitsizliğini sağlar. Kanıt tamamlanır. $\square$

Bu teorem, literatüerde "rasyonel sayılar reel sayılarda yoğundur" olarak bilinir. Aşağıdaki teoremin kanıtında $\sqrt{2}$ sayısının irrasyonel ve bir irrasyone sayı ile rasyonel sayının çarpımının irrasyone sayı olduğu kullanılacak.

Teorem 3.5. *$\mathbb{R}$'de $x < y$ eşitsizliği verilsin. $x < r < y$ olacak biçimde r irrasyonel sayı r vardır.*

Kanıt. $\mathbb{R}$'de $x < y$ olsun. Bu durumda $\sqrt{2}x \leqslant r \leqslant \sqrt{2}y$ olacak biçimde r rasyonel sayısı vardır. $q = \frac{1}{\sqrt{2}}r$ bir irrasyonel sayı olup, $x \leqslant q \leqslant y$ eşitsizliği sağlanır. $\square$

Bu teorem, literatüerde "irrasyonel sayılar reel sayılarda yoğundur" olarak bilinir.

$x \in \mathbb{R}$ için, $\mathbb{Z} \cap (-\infty, x]$ kümesinin maksimimu vardır, bunu, $[x]$ ile gösterelim. Bu durumda $nx - 1 \leqslant [nx] \leqslant nx$ eşitsizliği sağlanacağından,

$$x - \tfrac{1}{n} \leqslant \tfrac{[nx]}{n} \leqslant x$$

olur ve buradan da,

$$\lim_{n\to\infty} \tfrac{[nx]}{n} = x$$

elde edilir. Ayrıca,

$$\lim_{n\to\infty} \tfrac{1}{\sqrt{2}n}[\sqrt{2}nx] = x$$

Teorem 3.6. *Her reel sayı bir rasyonel sayılar dizisinin bir limitidir. Aynı zamanda irrasyonel sayılar dizisinin limitidir.*

Yukarıdaki teoremin kanıtı dikkate alınığına x'ya yakınsayan rasyonel sayılar dizisi artan yada azalan olarak alınabilir. Benzer durum irrasyonel sayılar dizisi içinde geçerlidir. Teorem olarak ifade edilecek olunursa:

Teorem 3.7. $x \in \mathbb{R}$ *verilsin.*

$$\sup\{r_n : n \in \mathbb{N}\} = x = \inf\{q_n : n \in \mathbb{N}\}$$

olacak biçimde artan (r_n) *ve azalan* (q_n) *rasyonel sayılar dizisi vardır. Bu ifadeki "rasyonel" kelimesi "irrasyonel" olarak da değiştirilebilir.*

Verilen $x \in [0, 1)$ için

$$[x] = \max \mathbb{Z} \cap (-\infty, x]$$

olarak tanımlanırsa her $n \in \mathbb{N}$ için

$$nx - 1 < [nx] \leqslant nx$$

ifadesinden

$$x = \lim_{n\to\infty} \tfrac{[nx]}{n} = 0$$

olur. Bunun sonucu olarak, her $p > 1$ doğal sayısı için şu teorem verilebilir. Her $x \in [0, 1)$ için

$$\alpha_n = [p^n x] - p[p^{n-1}x]$$

olmak üzere

$$x = \sum_{n=1}^{\infty} \tfrac{\alpha_n}{p^n}$$

yazılabilir. Benzer biçimde,

$$\beta_n = p[[p^{n-1}x]] - [[p^n x]]$$

olmak üzere

$$x = \sum_{n=1}^{\infty} \tfrac{\beta_n}{p^n}$$

elde edilir. Böylece şu teorem ifade edilebilir.

Teorem 3.8. *Her* $p > 1$ *doğal sayısı için*

$$[0, x] = \{\sum_{n=1}^{\infty} \tfrac{r_n}{p^n} : r_n \in \{0, 1, \cdots, p-1\}\}$$

olur.

4. Bölünme

Arşimedyan özelliği kullanılarak her $b \in \mathbb{N}$ için
$$\mathbb{N} = \bigcup_{n=1}^{\infty} [1, nb)$$
olduğu gösterilmişti. İyi sıralama ilkesi kullanılarak her $b \in \mathbb{N}$ için
$$\omega = \bigcup_{k=0}^{\infty} [kb, (k+1)b)$$
olduğu görülebilir. Dolayısıyla, verilen $a \in \omega$ için $a \in [kb, (k+1)b)$ olacak biçimde $k \in \omega$ bulunabilir, ve dolayısıyla,
$$a = kb + r,\ 0 \leqslant r = a - kb < b$$
yazılabilir.

Teorem 4.1 (Bölme Algoritması)**.** *$b > 0$ olmak üzere verilen a, b tam sayıları verilsin.*
$$a = qb + r,\ 0 \leqslant r < b$$
olacak biçimde q,r tam sayıları vardır ve tektir.

Kanıt. $S = \{a - qb : q \in \mathbb{Z}, a - qb \geqslant 0\}$ kümesi $0 \leqslant a - (-|a|)b \in S$ olduğundan, S, boş kümeden farklıdır ve dolayısıyla, minumumu vardır, buna r diyelim. Buradan, bazı tam sayı q için $a = qb + r$ ve $0 \leqslant r$ olur. $b \leqslant r$ olsaydı,
$$a - (q+1)b = (a - qb) - b = r - b \geqslant 0$$
olacağından,
$$a - (q+1)b \geqslant a - qb$$
olur ve buradan da $0 \geqslant b$ çelişkisi olurdu. Dolayısıla, $r < b$ olmak zorundadır. Tekliği göstermek için: Bazı q' ve r' tamsayıları için
$$a = qb + r = q'b + r',\ 0 \leqslant r' < b$$
olması durumunda,
$$b > |r - r'| = b|q - q'|$$
ifadesi sağlanır ve dolayısıyla, $|q - q'| < 1$ olur. Buradan da $q = q'$ elde edilir. Bunun kullanılmasıyla da $r = r'$ elde edilir. Böylece, teklik de gösterilmiş olur. $\square$

Bu teoremde q'ya **bölüm** ve r'ye **kalan** denir. Teeorem de kalanın sıfır, yani $r = 0$ olması durumunda b'ye a'nın bir **böleni** (**katı**) denir ve bu durumda $b|a$ gösterimi kullanılır. b sayısı $a_1, a_2 \cdots, a_n$ sayılarının her birinin bir ortak katıysa, b'ye bu sayıların bir **ortak böleni** denir. Bu sayıların ortak böleni sonlu olacağında, ortak bölenlerin en büyüğü vardır ve buna, **ortak bölenlerin en büyüğü** denir ve $gcd(a_1, a_2, \cdots, a_n)$ ile gösterilir. Bu sayı sıfırdan büyüktür. Her pozitif sayı kendisi ve 1 tarafından bölünebilir.

Teorem 4.2. *a ve b, her ikisi birden sıfır olmayan tamsayılarsa*

$$gcd(a, b) = ax + by$$

olacak biçimde x, y tamsayıları vardır.

Kanıt. $S = \{au+bv : u, v \in \mathbb{Z}, au+bv > 0\}$ kümesi, $|a|$ ya da $|b|$ elemanlarından en az birini içereceğinden, S boş kümeden farklıdır. Dolayısıyla, S'nin minumumu vardır, bunu d ile gösterelim. Bazı $u, v \in \mathbb{Z}$ için

$$d = au + bv$$

olur. Bölme algoritması kullanılarak, $a = qd + r$ olacak biçimde q ve $0 \leqslant r < d$ sayıları bulunabilir. $0 < r$ olma durumunda,

$$r = a - qd = a - q(ax + by) = a(1 - qx) + b(-qy) \in S$$

olacağından $r \geqslant d$ olur ki, bu çelişkidir. Dolayısıyla $r = 0$ ve buradan da $d|a$ olur. Benzer biçim de, $d|b$ olur. Kanıt tamamlanır □

Bu teoremin sonuçlarından biri,

$$\{ax + by : x, y \in \mathbb{Z}\} = gcd(a, b)\mathbb{Z}$$

olmasıdır[10]. Yani, $ax + by = k$ denkleminin çözümünün olması için gerek ve yeter koşul, $gcd(a, b)|k$ olmasıdır.

Yine bu teorem varsayımları altında $gcd(a, b) = 1$ ise a ve b sayıları **aralarında asal** denir.

Teorem 4.3. *a ve b her ikisi birden sıfır olmayan sayılar olmak üzere, bu sayıların aralarında asal olması için gerek ve yeter koşul, $ax + by = 1$ olacak biçimde x ve y tamsayılarının olmasıdır.*

Aşağıdaki teoremden aralarında asal sayı üretmek zor değil.

Teorem 4.4. *a ve b her ikisi birden sıfır olmayan tam sayılarsa,*

$$gcd(a, b) = d$$

olma durumunda,

[10] a, b, c tamsayılar olmak üzere, $\mathbb{Z}$'de $ax+by = c$ biçimindeki denklemlere **Diophantine denklemi** denir.

$$gcd(\tfrac{a}{d}, \tfrac{b}{d}) = 1$$

olur.

Bu teoremin bir uygulaması olarak:

Teorem 4.5. *r, sıfırdan farklı bir sayı ise*

$$r = \tfrac{a}{b}$$

olacak biçimde aralarında asal olan a ve b tamsayıları vardır ve bu yazılım, tektir.

Kanıt. $\mathbb{Q}$, rasyonel sayılar kümesini göstermek üzere, bir önceki teorem kullanılarak,

$$\mathbb{Q} = \{\tfrac{a}{b} : a, b \in \mathbb{Z}, b \neq 0, gcd(a, b) = 1\}$$

olduğu olduğu gösterilebilir.

$$\tfrac{a}{b} = \tfrac{c}{d},\ gcd(a, b) = 1 \text{ ve } gcd(c, d) = 1$$

olsun.

$$ax + by = 1 \text{ ve } cu + dv = 1$$

olacak biçimde x, y, u, v tamsayıları seçilebilir. Birinci eşitlik d ile çarpılarak, ikinci eşitlik b ile çapılarak ve $ad = bc$ eştliği kullanılarak, $b|d$ ve $d|b$ elde edilir. Buradan $|b| = |d|$ elde edilerek, istenilen kanıtlanır. □

Teorem 4.6. *Bir doğal sayının karekökünün doğal sayı olması için gerek ve yeter koşul, karekökünün rasyonel sayı olmasıdır.*

Kanıt. İfadenin bir tarafı açık. $n \in \mathbb{N}$ ve $\sqrt{n}$ doğal sayı olmamasına karşın rasyonel sayı olsun. Bu durumda $\sqrt{n} = \frac{p}{q}$, olacak biçinde aralarında asal olan p ve q doğal sayılar varsır. $px + qy = 1$ olacak biçimde x ve y seçelim. Bu eşitlik p ile çarpılarak ve

$$p^2 = nq^2$$

eşitliği kullanılarak $\frac{p}{q} = \sqrt{n}$'nin doğal sayı olduğu sonucu elde edilir. Bu çelişki kanıtı tamamlar.

Bunun bir sonucu olarak $\sqrt{2}$,$\sqrt{3}$, $\sqrt{5}$ sayılarının rasyonel olmadığı gösterilebilir. Teorem 4.4'nin başka bir sonucu olarak şu teorem verilebilir.

Teorem 4.7. *$\mathbb{Q}$'dan $\mathbb{Z} \times \mathbb{Z}$'ye birebir fonksiyon vardır.*

Kanıt. $\mathbb{Q}$'dan $\mathbb{Z}^2$'ye,

$$\tfrac{a}{b} \to \left(\tfrac{a}{gcd(a,b)}, \tfrac{b}{gcd(a,b)}\right)$$

kuralıyla birebir fonksiyon birebirdir. □

Teorem 4.8. *a, b ve c tam sayılar olmak üzere, $a|bc$ ve $gcd(a,b)=1$ ise $a|c$ olur.*

Kanıt. $ax+by=1$ olacak biçimde x, y tam sayıları vardır. $a|ac$ ve $a|bc$ olması nedeniyle $a|(acx+bcy)$ olur.

$$c = 1.c = (ax+by)c = acx+bcy$$

olacağından, $a|c$ elde edilir. □

5. Asal sayılar

Her sayı "önemli"dir. Bazı sayılarsa aşağıdaki anlamda asildir!

Tanım 5.1. *Kendisi ve 1'den başka böleni olmayan 1'den büyük tam sayıya* **asal** *denir.*

Teorem 4.8'in bir sonucu olarak şu teorem verilebilir.

Teorem 5.2. *a ve b doğal sayılar, p asal sayı ve $p|ab$ ise $p|a$ ya da $p|b$ olur.*

Bu teorem, Öklid'in Elemanları'nın VII. Kitabı'nın 30. Önerme'si olup, " Euclid's lemma" olarak bilinir.

Teorem 5.3 (Aritmetiğin Temel teoremi)**.** *Her doğal sayı bazı asal sayıların tek bir biçimde çarpımıdır.*

Kanıt. Asal sayıların çarpımı olarak yazılabilen doğal sayıların kümesini S ile gösterelim. $S=\mathbb{N}$ olduğunu göstermek istiyoruz. Olmasın, yani $T=\mathbb{N}\setminus S$ boş kümeden farklı olsun. T'nin minumumu, d, vardır. $2<d$ olacağı açık. d, asal olamaz. Dolayısıla

$$d = mn$$

olacak biçimde $2 \leqslant m,n$ sayıları vardır. $m,n<d$ olacağından $m,n \in S$ ve dolayısıyla $d \in S$ olur. Bu çelişki kanıtı tamamlar □

Bu teoremin bir sonucu olarak asal olmayan her sayının bir asal sayı tarafından bölüneceği sonucu elde edilir. Bu, Öklid'in Elemanı'nın 12. Kitabı'nın 31. Önermesi'dir.

Teorem 5.4. *Aşağıdakiler denktir.*

i. *p asal ve a, b pozitif sayılar olmak üzere, $p|ab$ ise $p|a$ ya da $p|b$ olur.*
ii. *p_i ve q_i'ler $p_1 \leqslant p_2 \cdots \leqslant p_n$ ve $q_1 \leqslant q_2 \cdots \leqslant q_k$ eşitsizliğini ve*

$$p_1p_2\cdots p_n = q_1q_2\cdots q_k$$

eşitliğini sağlayan asal sayılarsa $n = k$ ve her i için $p_i = q_i$ olur.

Kanıt. $i \Rightarrow ii$: p_i ve q_i'ler (ii)'deki gibi verilsin. $p_1|q_1q_2\cdots q_k$ olduğundan (i)'den $p_1|q_j$ olacak biçimde j vardır, dolayısıyla

$$p_i = q_j \geqslant q_1$$

olur. Benzer biçimde $q_1 \leqslant p_1$ olur. Buradan $p_1 = q_1$ elde edilir. Bu yöntemin en fazla sonlu kez uygulanmasıyla, $n < k$ olma durumunda,

$$1 = q_{n+1}\cdots q_k$$

çelişkisi elde edilir, ve dolayısıyla, $k \leqslant n$ olmak zorundadır. Benzer biçimde, $n \leqslant k$ ve dolayısıyla $n = k$ olur. Yine aynı yöntemin uygulanmasıyla istenilen gösterilmiş olur. $ii \Rightarrow i$: $p|ab$ ise $ab = kp$ olacak biçim k pozitif tamsayısı bulunabilir. Teorem 5.3 gereği,

$$a = p_1p_2\cdots p_n \text{ ve } b = q_1q_2\cdots q_m$$

olacak biçimde p_i ve q_i asal sayıları bulunabilir. k'nın da asal sayıların çarpımı olarak yazılabildiği ve (ii) devreye sokularak $p = p_i$ ya da $p = q_j$ olacak biçimde i ya da j bulunabilir. Birinci durumda $p|a$ ve ikinci durumun olması durumunda $p|b$ olur. Kanıt tamamlanır. □

Bu teoremin (ii)'si Öklid'in Elemanları'nın IX kitabının 14. Önermesi'dir. Bu teoremde verilen (ii), doğal sayılarda bir teoremdir.

Teorem 5.4'ün, yani "a ve b, doğal sayılar, p asal ve $p|ab$ ise $p|a$ ya da $p|b$ olur." ifadesinin doğrudan kanıtı aşağıdaki gibi verilebilir. Bu kanıt, [3]'den alınmıştır.

Teoremin ifadesini sağlamayan asal sayıların kümesini U ile gösterelim. U'nın boş küme olduğunu göstemek, kanıtı tamamlar. Olmadığunu varsayalım.

$$p = \min U$$

diyelim.

$$U(p) = \{a \in \mathbb{N} : \exists a, b \in \mathbb{N}, p|ab, p \not| a, p \not| b\}$$

kümesi boş kümeden farklıdır.

$$a = \min U(p)$$

diyelim.

$$U(p, a) = \{b \in \mathbb{N} : p|ab, p \not| a, p \not| b\}$$

kümesi de boş kümeden farklıdır. $b \in U(p, a)$ seçelim.

$$ab = (a - p)b + pb$$

olduğundan,

$$p|(a-p)b \Leftrightarrow p|ab$$

olur. Aşağıdaki durumlardan biri olmalı:

i. $a > p$: $0 < a-p < a$ ve a, minumum olduğundan $a-p \notin U(p)$ olur. Buradan, bir $b \in \mathbb{N}$ için

$$p \not| (a-p)b,\ p|(a-p),\ p|b$$

ifadelerinden biri gerçekleşir. İkincisi ve üçünüsü olamaz. Dolayısıyla,

$$ab = (a-p)b + pb$$

olur. $p|ab$ ve $p|pb$ olması nedeniyle de birincisi de olamaz.

ii. $a = p$: Bu durumda $p|a$ çelişkisi olur.

iii. $a < p$: Bu durumda $1 < a$ olmak zorunda-gerçekten de $a = 1$ olsaydı $p|ab$, yani $p \not| b$ olurdu- dolayısıyla $q|a$ olacak biçimde q asal sayısı vardır. $p \leqslant q$ olsaydı, $a = qt$ olacak biçimde bir t doğal sayısı olacağından

$$pt \leqslant qt = a < p$$

çelişkisi olurdu, dolayısıyla $q < p$ olmak zorunda. $q \notin U$, yani Öklid lemmasını q sağlar. $p|ab$ olduğundan $ab = pk$ olacak biçimde k vardır. $q|a$ olduğundan $q|ab$ ve dolayısıyla $q|pk$ olur. q, Öklid lemmasını sağladığından $q|p$ ya da $q|k$ olur. Birinci durum gerçekleşemeyeceğinden $q|k$ dır.

$$p\tfrac{k}{q} = \tfrac{a}{q}$$

olmasından $p|\frac{a}{q}b$ olur. Yani,

$$p|(\tfrac{a}{q},\ p|(\tfrac{a}{q})b \text{ ve } p \not| b$$

olması ve a'nın minumum olması nedeniyle

$$p|\tfrac{a}{q}b$$

olur. Buradan da, $p|\frac{a}{q}$-ki buradan $p|a$ olur- ya da $p|b$ olur. Bu çelişkidir.

Kanıt tamamlanır, yani her asal sayı için Öklid Lemması gerçeleşr. □

Teorem 5.4 ve sonrasındaki açıklama sonucu olarak şu teorem elde edilir.

Teorem 5.5. *p_i ve q_j'ler $p_1 \leqslant p_2 \leqslant \cdots \leqslant p_n$, $q_1 \leqslant q_2 \leqslant \cdots \leqslant q_n$ eşitsizliğini ve*

$$p_1p_2\cdots p_n = q_1q_2\cdots q_k$$

eşitliğini sağlayan asal sayılarsa $n = k$ ve her i için $p_i = q_i$ olur.

Teorem 5.4'ün (i)'si bir teorem olduğundan, denklik üzerinden (ii) de bir teoremdir. Bu teoremin (i)'sini tekrar ifade ederek doğrudan da bir kanıtı verilebilir.

Teorem 5.6. *Her doğal sayı asal sayıların çarpımı olarak yazılabilir.*

Kanıt. Her doğal sayının bazı asal sayıların çarpımı olarak yazılabildiği zaten Teorem 5.3'de ifade edilmişti. Yazılımın tek olduğunu gösterilecek. Olmadığını varsayalım. Bu durumda en az iki farklı biçimde asal sayıların çarpımı olarak yazılabilen doğal sayıların kümesi boşkümeden farklıdır. Bu kümeyi U ile gösterelim. İyi sıralama ilkesi gereği U'nın maksimumu vardır, bunu n ile gösterelim. Bu durumda, $m \neq k$ ve

$$n = p_1 p_2 \cdots p_r = q_1 p_2 \cdots q_s$$

olacak biçimde p_i ve q_j asal sayıları vardır.

$$p_1 \leqslant p_2 \leqslant \cdots \leqslant p_r \text{ ve } q_1 \leqslant p_2 \leqslant \cdots \leqslant p_s$$

olduğunu varsayabiliriz.

Her j için, $p_i \neq p_j$ olur: Gerçekten de bazı j'ler için $p_i = q_j$ olsaydı,

$$\tfrac{n}{p_1} = p_2 p_3 \cdots p_r = q_1 \cdots q_{j-1} q_{j+1} \cdots q_s,$$

$\frac{n}{p_1} < n$ ve n, U'nun minumumu olacağından, $r - 1 = s - 1$ ve

$$p_2 = q_1, \cdots p_j = q_{j-1}, p_{j+1} = q_{j+1}, \cdots, p_r = q_s$$

olur. Buradan da $p_1 = q_j$ olur ki, bu n'nin asallar olarak tek bir biçimde yazılamaz olmasıyla çelişir. Ayrıca, $p_1 \neq q_1$ olur. $p_1 < q_1$ olduğunu varsayabiliriz.

$$m = n - q_1 p_2 \cdots q_s = p_1(p_1 p_2 \cdots p_r - q_2 q_3 \cdots q_s) = (q_1 - p_1)(q_1 q_3 \cdots q_s)$$

$m | p_1$ olduğundan, $m = (q_1 - p_1)(q_1 q_3 \cdots q_s)$ sayısın asalların çarpımı olarak yazılabileceğinden ve bu yazılımın tek olması nedeniyle bu asallardan en az biri p_1 olmak zorundadır. $q_2, q_3, \cdots q_s$'lerin her biri p_1'den farklı olması ve ayrıca,

$$p_1 | (q_1 - p_1)(q_1 q_3 \cdots q_s)$$

olmasından,

$$q_1 - p_1 = p_1 t_1 \cdots t_k$$

olacak biçimde t_i asal sayıları vardır. Yani, $p_1 | (q_1 - p_1)$ olur. Buradan, $p_1 | q_1$ elde edilir ki bu, $p_1 = q_1$ olmasını verir. Bu çelişki kanıtı tamamlar. □

Bu teoremin bir uygulaması olarak:

Teorem 5.7. $n \in \mathbb{N}$ *verilsin.* $\sqrt{n}^{\frac{1}{n}}$, *rasyonelse doğal sayıdır da.*

Kanıt. $\sqrt{n}^{\frac{1}{n}}$ doğal sayı olmayan bir rasyonel sayı olsun. p ve q aralarında asal olmak üzere, $\sqrt{n}^{\frac{1}{n}} = \frac{p}{q}$ olacak biçimde aralarında asal p ve q doğal sayılarını seçelim. Bu sayıların asal sayıların çarpımı olarak yazılımı

$$p = p_1 p_2 \cdots p_r,\ q = q_1 q_2 \cdots q_s$$

olsun. Her i ve j için $p_i \neq p_j$ olacaktır. Ayrıca, n asal sayıların çarpımı olarak yazılabildiğinden,

$$n = t_1 t_2 \cdots t_k$$

olacak biçimde t_i asal sayılar vardır. Buradan,

$$t_1 t_2 \cdots t_k q_1^n q_2^n \cdots q_s^n = p_1^n p_2^n \cdots p_s^n$$

$q_i \neq p_j$ olması nedeniyle Teorem 5.6'dan her i için $t_i \in \{p_j : 1 \leqslant j \leqslant n\}$ olacaktır, dolayısıyla, $q_1^n q_2^n \cdots q_s^n$, bazı p_i asal sayıların çarpımı olacaktır. Bu bir çelişki olup, kanıtı tamamlar. □

Bu bölümde verilen teoremlerin kanıtlarında iyi sıralama ilkesi mümkün olduğu kadar doğrudan kullanılmaya çalışıldı. Her doğal sayının sonlu tane asal sayıya izdüşümünün olduğu da kanıtlandı. Sıra, hep aklımızda olan asal sayıların sayıların sonsuz olduğunu göstermeye geldi.

Teorem 5.8 (Asal Sayıların Sonsuzluğu)**.** *Asal sayılar kümesi sonsuzdur.*

Kanıt. Olmadığını varsayalım. Bu durumda, bütün asal sayıların listesi

$$p_1, p_2, \cdots, p_n$$

olarak verilebilir. Ayrıca,

$$P = p_1 p_2 \cdots p_n + 1$$

sayısı asal olmayacaktır. Dolayısıyla, P, en az bir p asal sayısı-ki $p = p_i$ biçimindedir-tarafından bölünebilir. Yani, $p_i | P$ olur. Buradan $p_i | 1$ çelişkisi elde edilir. □

Bu teorem Öklid'in Elemanları Kitap IX, Önerme 20'dir. Bu teoremin kanıtı doğudan iyi sıralama ilkesi kullanılarak verilebilir mi?

6. Sonlu Küme

Bir önceki bölümde iyi sıralama ilkesi'nden kopmamak istemediğimiz verilen teoremlerin kanıtlarındaki kullanımından anlaşılmıştır. Bu bölümde de aynı biçimde devam edilecek. Esas amaç belli; bu ilkeye denk olan tümevarım yapısını tanımak.

X ve Y kümelerinin aralarında birebir ve örten fonksiyon olma durumunda

$$|X| = |Y|$$

gösterimi kullanılır. $|X| = |X|$ ve $|X| = |Y|$ ve $|Y| = |Z|$ olduğunda $|X| = |Z|$ olduğu açık. Bu bölümde $n \in \mathbb{N}$ için

$$S_n = \{0, 1, \cdots, n-1\}$$

olarak gösterilecek[11].

Aşağıdaki teorem ve kanıtı hemen hemen açık. Ama, iyi sıralama ilkesi kullanılarak kanıtı verilecek.

Teorem 6.1. *Her $n, m \in \mathbb{N}$ için $|S_n| = |S_m|$ olması için gerekli ve yeterli koşul $n = m$ olmasıdır.*

Kanıt. $n = m$ için $S_n = S_m$ olacağından $|S_n| = |S_m|$ olur. $A = \{n : \exists m \in \mathbb{N}, n \neq m, |S_n| = |S_m|\}$ kümesinin boşkümeden farklı olduğunu varsayalım. İyi sıralama ilkesi gereği $k = \min A$ vardır. $1 \notin A$ olduğu kolaylıkla gösterilebilir. $1 < k$ olur. $k \in A$ olması nedeniyle $k \neq m$ ve $|S_k| = |S_m|$ olacak biçimde m vardır. Buradan, $|S_{k-1}| = |S_{m-1}|$ olduğu kolaylıkla gösterilir. $k-1 \neq m-1$ olması $k-1 \notin A$ olmasıyla çelişir. Kanıt tamamlanır. □

Tanım 6.2. *Bir $n \in \mathbb{N}$ için $|X| = |S_n|$ olan kümeye sonlu küme denir. Ayrıca, X'n kardinalitesi n denir ve $|X| = n$ yazılır.*

Sonlu olmayan bir küme vardır. Bunun için şunu kanıtlamalıyız.

Teorem 6.3. *$n \in \mathbb{N}$ verilsin. $|\mathbb{N}| = |\mathbb{N} \setminus \{n\}|$ olur.*

Kanıt. $f(k) = k\chi_{\mathbb{N}\setminus\{1\}}(k) + n\chi_{\{1\}}(k)$ kuralıyla tanımlı $f : \mathbb{N} \to \mathbb{N} \setminus \{1\}$ fonksiyonu birebir ve örtendir.

Teorem 6.4. *$\mathbb{N}$ kümesi sonlu değildir.*

Kanıt. $\mathbb{N}$'nin sonlu olduğunu varsayalım. Bu durumda $A = \{n : n = |\mathbb{N}|\}$ kümesi boş kümeden farklıdır. İyi sıralama ilkesi gereği $k = \min A$ vardır. $\{0\}$ ile $\mathbb{N}$ arasına birebir ve örten fonksiyonun olmayacağından $1 \notin A$ olur. $f : S_k \to \mathbb{N}$ birebir ve örten fonksiyon olsun. Bu durumda,

$$g : S_{k-1} \to \mathbb{N} \setminus \{f(n-1)\},\ g(n) = f(n)$$

olarak tanımlanan fonksiyon birebir ve örten, ve dolayısıyla

$$|S_{k-1}| = |\mathbb{N} \setminus \{f(n-1)\}| = |\mathbb{N}| = |S_k|$$

ve dolayısıyla, $k - 1 = k$ çelişkisi ende edilir. □

[11] ZF sisteminde her $n \in \omega$ için $n = \{0, 1. \cdots, n-1\}$ olarak tanımlanır.

Tanım 6.5. $|\mathbb{N}| = \aleph_0$.

Teorem 6.6. *$S \subset \mathbb{N}$ olmak üzere $f : S \to \mathbb{N}$ fonksiyonu birebir ve örten ise $\mathbb{N}$'den S'ye birebir, örten ve artan fonksiyon vardır.*

Kanıt. $g(1) = \min f(S)$ ve $g(n+1) = \min f(S) \setminus \{g(1), g(2), \cdots, g(n)\}$ kuralıyla tanımlı $g : S \to \mathbb{N}$ fonksiyonu istenilen niteliktedir.

Teorem 6.7. *$S \subset \mathbb{N}$ için $|S| = \aleph_0$ olması için gerekli ve yeterli koşul, S'nin üstten sınırsız olmasıdır.*

Kanıt. S, üstten sınırsız olsun. İyi sıralama ilkesi gereği,

$$f(1) = \min S$$

vardır. $f(n)$ tanımlandığında, $f(n)$, S'nin bir üst sınırı olamayacağından,

$$f(n+1) = \min S \setminus \{f(1), \cdots, f(n)\}$$

tanımlanabilir. Ayrıca, f artan ve her i için $i \leqslant f(i) < f(i+1)$ olur. $\{f(i) : i \in \mathbb{N}\}$ kümesinin üst sınırı yoktur.

$$S = \{f(i) : i \in \mathbb{N}\}$$

olur. (olmadığını varsayalım. İyi sıralılama ilkesi gereği,

$$s = \min S \setminus \{f(i) : i \in \mathbb{N}\}$$

seçilebilir. Bu durumda her i için $s \geqslant f(i) \geqslant i$ çelişkisi olur.) Dolayısıyla, $\mathbb{N}$ ile S arasında $i \to f(i)$ birebir ve örten fonksiyon vardır.

$f : S \to \mathbb{N}$ birebir ve örten fonksiyon olsun. Teorem 6.6 gereği bu fonksiyon artan olarak da seçilebilir. S'nin üst sınırının olduğunu varsayalım, s ile gösterelim. Bu durumda, $f(s)$, $f(S)$'nin bir üst sınırı ve dolayısıyla, s, $\mathbb{N}$'nin üst sırı olur ki, bu çelişkidir. □

Teorem 6.8. *X sonlu olmayan bir küme olmak üzere, X'den $\mathbb{N}$'ye tanımlı birebir fonksiyon varsa $|X| = \aleph_0$ olur.*

Teorem 6.9. $|\mathbb{N}^n| = \aleph_0$.

Kanıt. $p_1, p_2, \cdots, p_n$, birbirlerinden farklı asal sayılar olsun. $\mathbb{N}$'den $\mathbb{N}$'ye

$$f(k_1, k_2, \cdots, k_n) = p_1^{k_1} p_1^{k_2} \cdots p_n^{k_n}$$

kuralıyla tanımlı fonksiyon birebirdir. Teorem 6.8 gereği istenilen elde edilir □

Ayrıca, $f : \mathbb{N}^2 \to \mathbb{N}$, $f(n, m) = 2^n(2m-1)$ birebir ve örten fonksiyondur.

Teorem 6.10. *Her n için $|\mathbb{Z}^n| = \aleph_0$.*

Bunun yanında, $f(n) = n\chi_{\mathbb{N}}(n) + (2|n| + 1)\chi_{\mathbb{Z}\setminus\mathbb{N}}(n)$ kuralıyla tanımlı fonksiyon birebir örtendir.

Teorem 6.11. $|\mathbb{Q}| = \aleph_0$.

Kanıt. $\mathbb{Q}$'dan $\mathbb{Z}^2$'ya birebir fonksiyon olduğu ifade edilmişti. $|\mathbb{Z}^2| = \aleph_0$ olmasından ve Teorem 6.8'nin uygulanmasıyla istenilen elde edilir. $\square$

P, asal sayılar kümesi olsun. P'nin üst sınırı olmadığından $\mathbb{N}$'den P'ye birebir, örten ve artan fonksiyon vardır. Dolayısıyla, her i için $p_i < p_{i+1}$ olmak üzere,

$$P = \{p_i : i \in \mathbb{N}\}$$

yazılabilir. Bunun kullanımıyla aşağıdaki teoremin kanıtı verilebilir.

Teorem 6.12. *$\wp(\mathbb{N})^<$, $\mathbb{N}$'nin sonlu altkümelerinin kümesi olsun.*

$$|\wp(\mathbb{N})^<| = |\mathbb{N}|$$

olur.

Kanıt. Asal sayılar kümesini, her i için $p_i < p_{i+1}$ olmak üzere $\{p_i : i \in \mathbb{N}\}$ ile gösterelim. $S = \{n_1, n_2, \cdots, n_k\} \subset \mathbb{N}$ için,

$$f(\{n_1, \cdots, n_k) = p_{n_1}^{n_1} p_{n_2}^{n_2} \cdots p_{n_k}^{n_k}$$

kuralıyla tanımlı $f : \wp(\mathbb{N})^< \to \mathbb{N}$ fonksiyonu birebirdir. $f(\wp(\mathbb{N})^<)$, üstten sınırsı olduğundan, Teorem 6.7'den istenilen elde edilir. $\square$

Teorem 6.13. *Her $1 \leqslant i \leqslant n$ için $|X_i| = \aleph_0$, A sonlu ve $1 \leqslant j \leqslant n$ verilsin.*

$$|\prod_{i=1}^{n} X_i| = |\bigcup_{i=1}^{n} X_i| = |X_j \setminus A| = |X_j \cup A| = \aleph_0.$$

Konumuz dışı olan seçim aksiyomu kullanılarak şu teorem verilebilir.

Teorem 6.14. *Her $i \neq j$ için $X_i \cap X_j = \varnothing$ ve her i için $|X_i| = \aleph_0$ ise*

$$|\bigcup_{i=1}^{\infty} X_i| = \aleph_0$$

olur. **Kanıt**. *Her i için $|X_i| = |\mathbb{N} \times \{i\}|$ olması dikkate alınarak*

$$|\bigcup_{i=1}^{\infty} X_i| = |\bigcup_{i=1}^{\infty} \mathbb{N} \times \{i\}| = |\mathbb{N}^2| = \aleph_0$$

elde edilir.

7. Dedekind Doğal sayı

Şu ana kadar doğal sayılar üzerine birçok iş yapılmasına karşın onun ne olduğundan hiçmi hiç bahsedilmedi. Örneğin, "bir" sayısının ne olduğu hiç tartışma konusu bile olmadı. Dedekind, 1888'de bu konuyu ele alarak doğal sayıları tanımlamadı. Bu tanımlama sürecinde Dedekind'in "küme" kavramını nasıl ele aldığı konumuz olmayacak.

Dedekind, doğal sayılar kümesinin tanımlayabilmek için

$$f : S \to S,\ f(S) \neq S$$

özelliğinde birebir bir fonksiyon f'ye ihtiyaç duydu. Günümüzde, bu özellikteki bir S kümesine **Dedekind sonsuz** küme denir[12].

Dedekind sonsuz olmayan kümeye **Dedekind sonlu** küme denir[13].

Tanım 7.1. *$f : S \to S$, birebir ama örten olmayan bir fonksiyon olsun.*

$$1 \in S \setminus f(S)$$

verilsin.

$$\mathcal{N} = \{K \subset S : f(K) \subset K, 1 \in K \setminus f(K)\}$$

olmak üzere,

$$\mathbb{N} = \textstyle\bigcap_{K \in \mathcal{N}} K$$

kümesine f'nin 1'e göre **Dedekind doğal sayılar kümesi** *denir.*

En az bir Dedekind sonsuz kümenin olması durumunda aşağıdaki teorem gerçekleşir.

Teorem 7.2. *Aşağıdaki koşulları sağlayan bir $(\mathbb{N}, f, 1)$ üçlüsü vardır.*

i. $f : \mathbb{N} \to \mathbb{N}$ *birebir bir fonksiyondur.*
ii. $1 \in \mathbb{N} \setminus f(\mathbb{N})$.
iii. $K \subset \mathbb{N}$, $f(K) \subset \mathbb{N}$ *ve* $1 \in K \setminus f(K)$ *ise* $K = \mathbb{N}$

olur.

[12] 1638'de Galileo, doğal sayılar kümesiyle elemanları bir doğal sayının karesi olan kümenin birbirlerine eşit olmamasına karşılık bu iki küme arasında birebir bir eşlemenin olduğunu farkediyor. Bu "tuhaf" durum, Dedekind sonsuz küme kavramının ilk sinyallerini veriyordu. Bu gözlem Dedekind ve Cantor dönemine kadar, yani yaklaşık 200 yıl beklemeye başlıyordu.

[13] Her sonlu küme Dedekind sonlu küme olmasına karşın ZF-sisteminde Dedekind sonlu ve sonsuz olan bir küme vardır. Diğer taraftan ZFC sisteminde Sonlu ve Dedekind sonlu küme kavramları çakışır. Bu kavramların incelenmesi bu yazının konusu olmayacak. Diğer taraftan çarpıcı olması açısından bir X kümesinin sonlu olması için gerekli ve yeterli koşulun $\wp(\wp(X))$ kümesinin Dedekind sonlu olması olduğunu ifade edelim. Burada, $\wp(X)$, X kümesinin kuvvet kümesini, yani X'in altkümelerinin kümesini gösteriyor.

Bu teoremde tanımlanan $\mathbb{N}$ aşağıdaki anlamda tektir.

Teorem 7.3. *$(\mathbb{N}, f, a)$ ve $(\mathbb{M}, g, b)$ üçlüleri Teorem 7.2'nin koşullarını sağlasın.*

i. $\alpha : \mathbb{N} \to \mathbb{M}$ *birebir ve örten.*
ii. $\alpha(b) = a$
iii. *Her* $n \in \mathbb{N}$ *için* $\alpha(f(n)) = g(\alpha(n))$

olacak biçimde α fonksiyonu vardır.

Bu teoremindeki anlamda Teorem ???'de yer alan $(\mathbb{N}, f, 1)$ tekbir tane olup, bu üçlüye **Dedekind doğal sayı sistemi** denir. "Tümevarım bu sistemin neresinde?" sorusunun yanıtı, (*iii*) olacaktır.

$(\mathbb{N}, f, 1)$ Dedekind doğal sayı sisteminde bir $n \in \mathbb{N}$ ile 1'in toplamı

$$n + 1 = f(n)$$

ve bir m için, n ile $m + 1$ sayılarının toplamı

$$n + (m + 1) = (n + m) + 1$$

özelliğini sağlayacak biçimde tanımlanarak, her $n, m \in \mathbb{N}$ için n ve m'nin toplamı $n+m$ tanımlanır. Benzer biçimde **çarpma** işlemi,

$$n1 = n \text{ ve } m(m + 1) = (nm) + m$$

özelliklerini sağlayacak biçimde tanımlanır. Detaylar bu yazının konusu olmayacaktır.

Şu teoremi de verelim.

Teorem 7.4. *Dedekind doğal sayılar kümesi* $\mathbb{N}$*, sonsuz ve Dedekind sonsuz kümedir.*

8. Tümevarım ve Peano Aksiyomları

Birçok temel teoremin kanıtında kullanılan iyi sıralama ilkesi doğal sayılar sisteminin tanımlanmasına ihtiyaç duyulmadan verildi. Benzer durum tümevarım için de geçerli. Bu iki kavram tanımlanmadan kullanılan doğal sayılar sisteminde birbirlerine denk olmasına karşın, tümevarım, doğal sayıların Peano sistemi olarak tanımlanmasındaki aksiyomlardan biri olarak verilerek, iyi sıralama ilkesi bir sonuç olarak verilebiliyor. Buna karşın, doğal sayıların sisteminin küme teorik olarak tanımlanması durumunda bu iki kavram birbirlerine denk olmasının yanında, bu sistem Peano aksiyomlarını sağlamaktadır.

Giriş kısmında "verilen miktardan daha fazlası vardır" ifadesini doğal sayılar için anlamaya çalışlım. $\{1\}$ miktarı verilsin. Bu miktardan daha fazlası olduğuna göre bu miktarı kapsayan ama onunla aynı olmayan bir miktar vardır, bunu B ile gösterelim.

Sonra B miktarından daha fazla miktarı içeren bir miktar vardır. Bu böyle devam etsin gitsin, "sonsuza" kadar. Bu miktarlar topluluğu bütünü (bileşimini) M_∞ ile gösterelim. M_∞ miktarı 1'i içeriyor ama 2'yi içerdiğinin bir delili yok! Olması nasıl sağlanabilir? Ya da sağlanmaması durumunda bazı şeyler kontrol dışına çıkabilir mi? "daha fazlası"yı "hemen sonraki" olarak değiştirsek, bu kez "verilen miktarın" "hemen sonrası"nı tanımlama problemi oluşacaktır. Bunun içinde verilen miktarı sadece bir sayıdan olduğu varsayılırsa, bir sayının hemen sonrası tanımlanabilecek gibi durum olduğundan, "verilen miktardan daha fazlası vardır" ifadesini "verilen sadece bir sayıdan oluşan bir miktardan hemen sonraki sayıdan oluşan miktar vardır" diye değiştirilirse de iki sayısının yukarıdaki anlamda içerildiğinin yine garantisi olmayacaktır. O problemi çözmek içinde şu yapılabilir: "verilen miktardan daha fazlası vardır" yerine "sadece bir sayısından oluşan bir miktar vardır" ve "verilen sadece bir sayıdan oluşan bir miktardan hemen sonraki sayıdan oluşan miktar vardır" alınırsa ne iki sayısı, ne üç sayısı kaçabilecektir. Kuş uçurtulmayacaktır!

Doğal sayıları aksiyomatik olarak tanımlama gereği duymadan tümevarım şöyle ifade edilebilir[14]: $A \subset \mathbb{N}$ olmak üzere bir $n \in \omega$ için

$$S = \{n, n+1, \cdots\} \cap A$$

diyelim. $n \in S$ ve $k \in S$ olduğunda $k+1 \in S$ oluyorsa $S = \mathbb{N}$ olur. İyi sıralama ilkesinden tümevarım elde edilebilir: S, tümevarım koşullarını sağlamasına karşın $S \neq \mathbb{N}$ olduğunu varsayalım. $k = \mathbb{N} \setminus S$ vardır. $1 \in S$ olduğundan $1 < k$ olur. $k-1 \notin \mathbb{N} \setminus S$ ve dolayısıyla $k-1 \in S$ olur. S'nin sağladığı ikinci koşuldan $k = (k-1)+1 \in S$ olur. Bu çelişkidir.

Matematiksel Tümevarım Peano Aksiyomlarından biridir. Bu aşamada, konuyu dağıtmadan, bu kavramı tanım olarak verip, bunun ilerisi ve sonrası için arayışlar sürdürülebilir. Yukarıda yapılan açıklamalar aşağıda verilen aksiyom sisteminin geri plandaki nedenini daha fazla yorumlatabilmenin yolunu açacaktır.

Peano axiom sistemi üç tanımsız şey üzerine kurulmuş bir akiyom sistemidir. Giriş paragraflarının birinde kullanılan "düne kadar" denilen zaman 1889'dır. Bu tarihte Peano doğal sayıları üç tanımsız terim olan **sıfır**, **sayı** ve **ardılı** ile beş aksiyom ile tanımlamıştır. Bu aksiyomlar semboller kullanılmadan şöyle ifade edilebilir:

i. Sıfır bir sayıdır.
ii. Her sayının bir ardılısı vardır.
iii. Farklı iki sayının ardılıları aynı olamaz.

[14] Tümevarım kavramının ne olduğu farklı seviyelerde ifade edildiğinin farkındayız.

iv. Sıfır bir sayının ardılısı değildir.
v. Tümevarım sağlanır!

Sıfır, sayılar ve ardılılar sırasıyla, 0, ω ve S ile gösterilsin. n bir sayı ise $n \in \omega$ yazalım. Bu durumda Peano Aksiyomları şöyle ifade edilebilir.

Tanım 8.1 (Peano Aksiyomları, 1889)**.** *Aşağıdaki aksiyomları sağlayan* $(0, =, \in, \omega, s)$ *beşlisine* **Peano beşlisi** *denir*[15].

a. $0 \in \omega$.
b. $n \in \omega$ *ise* $s(n) \in \omega$.
c. $n, m \in \omega$ *ve* $s(n) = s(m)$ *ise* $n = m$ *olur.*
d. $s(n) = 0$ *olacak biçimde* $n \in \omega$ *yoktur.*
e. *(Tümevarım)* S*,* $0 \in S$ *ve* $n \in S$ *olsuğunda* $s(n) \in S$ *olacak biçimde* ω*'nın bir topluluğu ise* $S = \omega$ *olur.*

Burada verilen son aksiyom, ω'nın sayılardan başka herhangi birşey içermeyeceğinin garantisidir. Bu yapı üzerinden tanımlanan aritmetik işlemler ve sıralamalar bildiğimiz gibi olup, o kavramların tanımlanmaları konumuz dışıdır.

Tanım 8.2. *Her* $n \in \mathbb{N}$ *için* n*'ye* **Peano sayısı** *denir.*

Tanım 8.3. $\mathbb{N} = \omega \setminus \{0\}$.

Pratiklik açısından doğal sayılar kümesi denilince kastedilen $\mathbb{N}$ olacaktır ama bu çok önemli bir ayrıntı değildir; yani, ω'ya da doğal sayılar kümesi denilmesi sorun olmaz.

Teorem 8.4 (İyi Sıralama İklesi)**.** *Doğal sayılar kümesinin boş olmayan her altkümesinin en büyük alt sınırı vardır.*

Kanıt. $S \subset \mathbb{N}$ boş olmayan bir küme olsun. S'nin en büyük altsınırının olmadığını varsayalım.

$$T = \{n : \{1, 2, \cdots, n\} \subset \mathbb{N} \setminus S\}$$

olarak tanımlansın. S'nin en büyük altsınırı olmadığından $1 \in T$ olur. $n \in T$ olduğunu varsayalım, yani $\{1, 2, \cdots, n\} \subset \mathbb{N} \setminus S$ olsun. $n + 1 \in T$ olsaydı $n + 1 \in S$ olur ve her $1 \leqslant i \leqslant n$ için $i \notin S$ olacağından, $n + 1$, S'nin en büyük alt sınırı olurdu ki-bu çelişki olurdu. Dolayısıyla, $n + 1 \in T$ olur. Tümevarım gereği $T = \mathbb{N}$ olur. Buradan,

[15] Dedekind, bu aksiyomları 1887 yılında *Essays on the theory of numbers. I: Continuity and irrational numbers. II: The nature and meaning of numbers* adlı eserinde de gözlemiştir. Bu nedenle bu aksiyom topluluğuna Dedekind-Peano Aksiyomları da denir.

her n için $\{1, 2, \cdots n\} \cap S = \varnothing$ ve dolayısıyla n üzerinden bileşilmeri de boş küme olur. Buradan, S'nin boş küme elde edilir ve bu, çelişkidir. $\square$

İyi sıralama ilkesi üzerinden tümevarım elde edilmişti. Dolayısıyla, bu teoremi de dikkate alarak, kitabi olarak değil ama alaylı bir ifadeyle, tümevarım ve iyi sıralama ilkesinin, yazının ilk satırlarında da belirtildiği gibi birbirine denk olduğu söylenebilir. Bu durum gözönüne alınarak şu sorulabilir:

Soru: Peano aksiyomlar sisteminde tümevarı aksiyomu yerine iyi sıralama ilkesi bir aksiyom olarak alınarak doğal sayılar sistemi tanımlanabilir mi?

9. Tümevarımın Temel İzleri

Tümevarım yönteminin izleri farklı eksenlerde aranabilir ve elbet de bu "izlerin" seviyeleri bazı anlamlarda tartışmalı olabilir. Bu izlerin bazıları bulanık, bazıları daha belirgin ve elbette bazıları tartışmasız bir biçimde güncel (modern)dir.

Bazı matematik tarihçilerine göre, bu izler Platon'un Diyalogları'nda (MÖ 370) vardır, çünkü bu, tümevarımın temel bileşenlerinden oluşan "bir sonraki"ni tartışmaktadır. Aynı bakış açısıyla Öklid'in elemanları Kitap IX, Önerme 20'nin (asal sayıların sonsuzluğu) kanıtı tümevarım yöntemini içermektedir. Bir başka iz, Hintli matematikçi Bhaskaracharya'nın (1114-1185) kuadradik denklemleri ($ax^2 + bx + c = 0$ biçimindeki denklemler) çözmek için "dairesel yöntem" (cyclic method) olarak adlandırılan yöntemde yer almaktadır.

"Tümevarım yöntemiyle bir teorem yazın ve kanıtlayın" sorusuna verilecek yanıtların çok büyük bir kısmının, "verilen herhangi bi n doğal sayısı için,

$$1 + 2 + \cdots + = \frac{n(n+1)}{2}$$

eşitliği doğrudur" üzerine olacağı tahmin edilebilir. Bu eşitliğin ilk olarak Carl Friedrich Gauss'un (1777-1855) bir ilkokul ögrencisiyken verdiği yaygın olarak bilinse de bu eşitlik, Gauss'dan yüzlerce yıl önce Levi ben Gerson'un[16] temel eseri olan Maasei Hoshev'de (The art of the calculator) n'nin bir çift sayı olma durumu için verilmiştir[1].

[16]Levi ben Gerson (1288-1344) Güney Fransa'nın Bagnols-sur-Ceze köyünde doğmuş ve yaşamının büyük bir kısmını Orange'de geçirmiş matematikçi ve anstronomdur. Temel eseri olan Maasei Hoshev (The art of the calculator), 1321'de yayınlanmış olup, kombinatörük formüller ve tümevarım yöntemiyle kanıtlanan matematiksel ifadeler içermektedir. Bu eserdeki sonuçların bir kısmı bu eserden sonra yaklaşık 200 yıl başka yerlerde yer almamış olmasına rağmen bu esere uzun yıllar referans verilmemis ve etki bırakmamıştır. [1]'de "Levi ben Gerson'un çalışmalarını okuyan olmuş mudur?" başlığla bir bölüm vardır. Bu eser, 1620 yılında, Fransa'nın İstanbul elçisi Achille Harlay de Sancy tarafından Paris'e getirilmiştir.

Bunun kanıtı için Gauss ve Gerson'un kullandığı yöntem aynı olup, bu yöntem tümevarım yöntemiyle tamamıyla farklıdır. Her ne kadar bu eşitliğin doğruluğu Maasei Hoshev'de n'nin çift sayı olma durumu için verilmiş olsa da bu, n'nin tek olma durumunda da verilebilir. Diğer taraftan, günümüzde, bu eşitliğin doğruluğunun gösterilmesi tümevarımın uygulandığı en klasik örneklerden biridir.

Tümevarım yönteminin ilk ne zaman kullanıldığına ilişkin sorunun daha belirgin bir izi

$$1^3 + 2^3 + \cdots + 10^3 = (1 + 2 + \cdots + n)^2$$

eşitliğine dayanmaktadır. Bu eşitliğin gösterilmesinde Al-Karaji[17] tarafından kullanılan yöntemin tümevarımın ilk atası olduğu düşünülmektedir. Bu eşitlik Aryabhata[18] tarafından biliniyor olmasının ötesinde Yunanlılar tarafından da bilindiği sanılmaktadır. Bu eşitliğin gösterilmesinde uygulanan yöntem [1], 9.3.4'de bulunabilir. Al-Karaji'nin kullandığı yöntem, "k'dan $k - 1$'e geçiş" biçiminde olup, bu yaklaşım güncel tümevarımgiller kavramının temel bileşenlerinden biridir.

Günümüz matematik diliyle "k'den $k - 1$'e geçiş yöntemi" şu biçimde de ifade edilebilir.

Teorem 9.1. *$n \in \mathbb{N}$, $f : \{1, 2, \cdots, n\} \to X$ bir fonksiyon ve $a \in X$ verilsin.*

i. *$f(n) = a$.*

ii. *$1 < k \leqslant n$ ve $f(k) = a$ ise $f(k - 1) = a$*

koşulları sağlanıyorsa her $1 \leqslant i \leqslant n$ için $f(i) = 1$ olur.

Maasei Hoshev'de temel olarak bu yöntem ve aşağıda verilen bazı öncül teoremler kullanılarak,

$$1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^3$$

eşitliğinin doğruluğu kanıtlanır.

Teorem 9.2 (Maasei Hoshev, Önerme 30)**.** *Verilen herhangi bir n doğal sayısı için,*

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

[17]Karaj'da doğmuş ve 953-1029 yilları arasında yaşmış İranlı matematikçi ve mühendis. Temel eserleri :Al-Badi' fi'l-hisab (Wonderful on calculation), Al-Fakhri fi'l-jabr wa'l-muqabala (Glorious on algebra), and Al-Kafi fi'l-hisab (Sufficient on calculation) Tümevarım yöntemini ilk kullanan kişi olarak da bilinir. Bunun yanında, Mısır Pramitleri'nin inşa edilme nedenini anlayabilirim ama yaklaşık 1000 yıl önce 1'den 10'a kadar olan sayıların toplamının karesinin o sayıların küplerinin toplamına eşit olduğunu gösteren Abu Bakral-Karaji'nin derdi neydi, anlayamadım.

[18]Hintli matematikçi ve astronum (476-550). Trigonometrik fonksiyonları tanımlamış, ikinci derece denklemlerini çözmüş, π sayısının yaklaşık değerini hesap etmiş ve π'nin irrasyonel olduğunu sezinlemiştir.

olur.

Bir sonraki teoremin orjinal bir kanıtı [1], s. 340'da bulunabilir.

Teorem 9.3 (Maasei Hoshev, Önerme 41)**.** *Verilen herhangi bir n doğal sayısı için,*

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

olur.

Yukarıda verilen iki teorem birleştirilerek sayıların küplerinin toplamıyla ilgili aşağıdaki sonuç elde edilir.

Teorem 9.4 (Maasei Hoshev, Önerme 41)**.** *Verilen herhangi bir n doğal sayısı için,*

$$1^3 + 2^3 + \cdots + n^3 = (1+2+\cdots+n)^2$$

olur[19].

Yukarıda verilen bakış açısıyla tümevarım tekniğini kullanan bilinen ilk matematikçilerin al-Karaji ve Levi Ben Gerson olduğu söylenebilir.

10. Sayıların Kuvvetinin Toplamı

Bir önceki atlbölümde 1'den n'ye kadar olan sayıların toplamının $\frac{n(n+1)}{2}$ olduğunun gösterilmesinin tümevarımın temel uygulamalarından biri olduğu ifade edilmişti. Doğal olarak, verilen bir k ve n doğal sayısı için 1'den n'ye kadar olan sayıların k'ıncı kuvvetlerinin toplamının ne olacağı sezinlenerek, bu sezginin doğruluğu yine tümevarımla gösterilebilir. Bu toplamın ne olduğundan bahsedilerek kanıtın tümevarımla gösterilmesi okuyucuya bırakılacak.

a bir reel sayı ve n bir tam sayı olmak üzere,

$$(a+1)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}$$

olması ve her k doğal sayısı için

$$\sum_{i=1}^{n}(i+1)^k - \sum_{i=1}^{n} i^k = -1 + (i+1)^k$$

eşitliği kullanılarak,

$$\sum_{i=1}^{n} i, \sum_{i=1}^{n} i^2, \cdots \sum_{i=1}^{n} i^k$$

toplamları "biliniyorsa", bu bilininirlik üzerinden,

$$\sum_{i=1}^{n} i^{k+1}$$

[19]Bu eşitlik Nicomachus teoremi olarak da bilinir.

toplamı da "bilinebilir". Ve dolayısıyla, $\sum_{i=1}^{n} i^1$ bilinidiğinden, tümevarımla her k için $\sum_{i=1}^{n} i^k$ hesaplanabilir. Dikkat edilirse k'dan $k+1$'e geçiş yapıldı.

Yeri gelmişken sayıların k'nıcı kuvvetlerinin toplamının ne olduğunu verebilecek şu teoremi verelim.

Teorem 10.1. *Verilen k ve n doğal sayıları için*

$$(n+1)\sum_{i=1}^{n} i^k = \sum_{i=1}^{n} i^{k+1} + \sum_{p=1}^{n}(\sum_{i=1}^{p} i^k)$$

olur.

Günümüzde tümevarımla kanıtlanabilecek bu teoremi, $n = 4$, $k = 1, 2, 3$ için Ibn al-Haytkam[20] vermiştir. Bu teoremin kanıtında yukarıda behsedilen al-Karaji yöntemi kullanılabilir.

Teorem 10.2 (Ibn al-Haytham)**.** *Her n doğal sayısı için,*

- $\sum_{i=1}^{n} i^2 = \frac{n^3}{3} + \frac{n^2}{6} + \frac{n}{6}$,
- $\sum_{i=1}^{n} i^3 = \frac{n^4}{4} + \frac{n^3}{2} + \frac{n^2}{4}$,
- $\sum_{i=1}^{n} i^4 = (\frac{n}{5} + \frac{1}{5})n(n + \frac{1}{2})[(n+1)n - \frac{1}{3}]$,

olur.

11. Sayıların Kuvvetinin Toplamı

Tanım 11.1. *Her doğal sayı n,*

$$B_n = \sum_{k=0}^{n}[\frac{1}{k+1}\sum_{v=0}^{k}(-1)^v(v+1)^n\binom{k}{v}]$$

sayısına **Bernoulli sayı** denir.

Teorem 11.2 (Faulhaber-Bernoulli formülü)**.** *Verilen n ve p doğal sayıları için,* $0 \leqslant k \leqslant p$ *için*

$$\sum_{k=1}^{n} k^p = \frac{1}{p+1}\sum_{j=0}^{p}\binom{p+1}{j}B_j n^{p+1-j}$$

Bu teoremle bağlantılı Türkçe kaynaklardan biri [2]'dir.

[20] Avrupa'da Alhazen olarak bilinen Ibn al-Haytham Irak'ın Basra kentinde doğmuş doğmuş ve yaşamının büyük bir kısmını Mısır'da geçirmiş matematikçidir. En önemli eseri, toplam 7 kitapta toplanmış olan *Kitab al-Manazir* (Optik) kitabı olup, bu kitap 13.Yüzyılın başlarında Latince'ye çevrilmiştir. Literatüerde "Alhazen Problemi" olarak bilinen problem vardır.

12. Tümevarımın Modern İzİ

Tümevarım yönteminin izleri farklı eksenlerde aranabilir ve elbet de bu "izlerin" seviyeleri bazı anlamlarda tartışmalı olabilir. Bazı matematik tarihçilerine göre, bu izler Platon'un Diyalogları'nda (MÖ 370) vardır, çünkü bu, tümevarımın temel bileşenlerinden oluşan "bir sonraki"ni tartışmaktadır. Aynı bakış açısıyla Öklid'in elemanları Kitap IX, Önerme 20'nin (asal sayıların sonsuzluğu) kanıtı tümevarım yöntemini içermektedir. Bir başka iz, Hintli matematikçi Bhaskaracharya'nın (1114-1185) kuadradik denklemleri ($ax^2 + bx + c = 0$ biçimindeki denklemler) çözmek için "dairesel yöntem" (cyclic method) olarak adlandırılan yöntemde yer almaktadır.

Şu ana kadar tam tamına tümevarım yöntemi kullanılarak herhangi bir teorem kanıtlanmadı. Güncel anlamda tümevarım tekniğinin kanıt olarak kullanıldığı ilk teorem binom teoremidir.

$0 \leqslant k \leqslant n$ için,

$$\tbinom{n}{k} = \tfrac{n!}{(n-k)!}$$

gösterimi kullanılı. Her $n \in \omega$ için

$$\tbinom{n}{0} = \tbinom{n}{n} = 1$$

olur. Ayrıca,

$$\tbinom{n}{k-1} + \tbinom{n}{k} = \tbinom{n+1}{k}$$

olduğu kolaylıkla gösterilebilir. Bu veriler altında Paskal ilk kez tümevarım yöntemini kullanarak aşağıdaki teoremi kanıtlamıştır.

Teorem 12.1 (Binom Teoremi, Pascal)**.** *a, b reel sayıları ve $n \in w$ verilsin.*

$$(a+b)^n = \sum_{k=0}^{n} \tbinom{n}{k} a^{n-k} b^k$$

olur.

Kanıt. Kanıt için $b = 1$ almak genelliği bozmayacaktır. $n = 0$ için istenilen açık. n için ifadenin doğruluğunu kabul edelim, yani

$$(a+b)^n = \sum_{k=0}^{n} \tbinom{n}{k} a^{n-k}$$

olsun. Bu durumda,

$$(a+1)^{n+1} = (a+1)(a+1)^n = a(a+1)^n + (a+1)^n = \sum_{i=0}^{n} \tbinom{n}{i} a^{i+1} + \sum_{i=0}^{n} \tbinom{n}{i} a^i$$

olması kullanılarak,

$$(a+1)^n = \sum_{k=1}^{n} (\tbinom{n}{k-1} + \tbinom{n}{k}) a^k + a^0 + a^{n+1}$$

elde edilir.

$$1 = \binom{n+1}{0} = \binom{n+1}{n+1} \text{ ve } \binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$$

olması kullanılarak,

$$(a+1)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^k$$

elde edilir. Yani, doğruluğu gösterilmeye çalışılan eşitlik $n+1$ için doğrudur. Böylece kanıt tamamlanır.

References

[1] V. J. Katz, A history of Mathematics, 3. Edition,
[2] T. Terzioğlu, Sayıların Güçlerini Toplamak, Matematik Dünyasi, Sayı:1, ???-???, 2004.
[3] K. Rogers, Classroom Notes: Unique Factorization. Amer. Math. Monthly 70 (1963). 547-548.
[4] W. L. Duren, Jr., Mathematical induction in sets, Amer. Math. Monthly 64 (1957) 19-22. 99-114
[5] S. Sertöz, Ökli'in Elemanları, TÜBİTAK 2019. (Çeviri.)