

Belki de bu yüzden yalnızca cesurların işidir kanıt

ORHAN OĞULCAN TUNCER

Hacettepe Üniversitesi Matematik Bölümü

✉ otuncer@hacettepe.edu.tr



İngiliz Matematikçi Sir Michael Francis Atiyah'ın (1929-2019) sözleriyle,

“Kanıt, matematiği bir arada tutan yapıştırıcıdır.”

Bu ifadeyle Atiyah, etkileyici bir metafor yapmanın ötesinde, matematiğin en önemli yapıtaşının kanıt olduğuna işaret ediyordu. Elbette bu demek değil ki matematik yalnızca kanıttan ibarettir ya da bir matematikçi gününün her saatini önerme kanıtlayarak geçirir. Neticede matematik, teknik hesaplamalar yapmaktan karşıt örnekler oluşturmaya, algoritmalar bulmaktan özel durumlar incelemeye ya da modeller yapmaya kadar çok çeşitli uğraşlar da barındıran bir disiplindir. Yine de matematiği diğer disiplinlerden ayıran temel unsur, kanıt ve mantıksal gerekçelendirmeye sıkı sıkıya bağlı olmasıdır.

Kanıt, yalnızca bir sonucun doğruluğunu garanti altına almak için değil, aynı zamanda düşünce sürecindeki mantıksal yolculuğu aktarmak için de kullanılır. Bu sebeple matematik ve mantığı birbirinden tamamen ayırmak imkansızdır. Bu ilişkiyi belki de en iyi açıklayan, Filozof ve Matematikçi Bertrand Russell (1872-1970)'in şu sözleridir:

“Tarihsel olarak bakıldığında, matematik ve mantık tamamen farklı alanlar olarak görülmüştür. Matematik, bilimle ilişkilendirilirken; mantık, Antik Yunan’la bağdaştırılmıştır. Ancak her iki alan da modern zamanlarda önemli bir gelişim göstermiştir: mantık daha matematiksel bir nitelik kazanmış, matematik ise daha mantığa dayalı hâle gelmiştir. Sonuç olarak artık bu ikisi arasında kesin bir çizgi çekmek tamamen imkânsız olmuştur; gerçekte, ikisi bir ve aynıdır. Aralarındaki fark, çocuk ile yetişkin arasındaki fark gibidir: mantık, matematiğin gençliğidir; matematik ise mantığın olgunluk çağıdır.”

Bu yazının içinde birkaç önermenin bazı iyi bilinen kanıtlarından bahsedeceğiz. Ele alacağımız önermelerin kanıtları basit ve kolay anlaşılır olacaklar. Ancak bazı kanıtlar çok daha karmaşık olup sayfalarca hatta ciltlerce süren mantıksal ilerlemeler gerektirebilir. Dolayısıyla matematikte bir önermeyi kanıtlamak için, uzun ve soyut bir düşünme sürecine, sabırlı bir akıl yürütmeye ve kimi zaman detaylar içinde kaybolmadan ilerleyebilecek zihinsel bir dayanıklılığa hazır olmak gereklidir, ama tabii ki yeterli değildir. Nitekim bu zihinsel çabanın zorluğunu Charles Darwin şu şekilde ifade eder: “Soyut bir düşünce zincirini uzun süre takip etme gücüm sınırlı; bu yüzden metafizik ya da matematikte asla başarılı olamazdım.”

O halde esas sorumuza gelmiş bulunmaktayız: Matematiksel kanıt *tam olarak* nedir?

Russell herhangi bir önermeyi kanıtlamaya yeltenen bir matematikçinin asla muhakeme sürecinin tamamını kağıda dökemeyeceğini, bunun yerine uygun şekilde eğitilmiş bir zihni ikna etmeye yetecek kadar bir kanıt özeti ile yetinilmesi gerektiğini söylemiştir. Çünkü her önerme, daha önceki tanım ve önermelere dayanır. Onlar da başka tanım ve önermelere... Bir kanıtın, dayandığı tüm tanım ve kabulleri baştan sona eksiksiz biçimde içermesini şart koşmak, hem pratikte mümkün değildir hem de gereksiz bir çaba olur. Kendi önerilerini pek de ciddiye almadığı apaçık olan Russell, Alfred North Whitehead ile birlikte yazdığı *Principia Mathematica* kitabında, matematiğin tümünü en küçük ayrıntıları bile göz ardı etmeden temel mantıksal ilkelere indirgemeye çalışmıştır. Öyle ki $1 + 1 = 2$ ifadesini mantıksal ilkelerle elde etmeleri yüzlerce sayfa sürmüştür.

Dolayısıyla biz bu yazıda Russell’ın ilk önerisini dikkate alarak aklımıza mukayet olmaya çalışacağız. Bu bağlamda bir kanıt, bir önermenin doğruluğuna itiraz edilemeyecek şekilde ikna eden, mantık kuralları çerçevesinde inşa edilmiş tutarlı bir akıl yürütme olarak tanımlayabiliriz.¹

Alternatif olarak matematiksel bir kanıtın ne *olmadığını* da tartışabiliriz. Kanıt, sezgiye ya da sağduyuya yapılan başvurularla kurulmaz. “Bana mantıklı geliyor” ya da “herkes böyle düşünüyor” gibi ifadeler matematiksel geçerlilik taşımaz. Aynı şekilde, bir öğretmenin ya da otoritenin sözü de tek başına bir kanıt sayılmaz. Kanıt, yalnızca kuralları açık ve tutarlı biçimde tanımlanmış mantıksal bir sistem içinde geçerlidir.

Sonuç olarak, kanıt matematiksel düşüncenin omurgasıdır. Öğrenciler için bu, sadece kuralları uygulamak değil, bu kuralları neden uyguladığımızı sorgulamak anlamına gelir. Bir problemi çözmekle yetinmek değil, o çözümün neden ve nasıl çalıştığını görmek demektir. Matematiksel kanıt, sadece bilgi değil; düşünce üretmenin, paylaşmanın ve eleştirmenin en rafine yollarından biridir. Ve bu yönüyle matematik, yalnızca bir bilim değil, aynı zamanda bir düşünme biçimidir.

Şimdi yukarıda tartıştıklarımızı somut hale getirecek ve örneklerle destekleyeceğiz. Ayrıca bazı temel kanıt tekniklerinden bahsedeceğiz.

1. Belli durumlar için sağlanması yeterli değil.

Bir önermenin doğruluğunu göstermek üzere çıkılan yolda en sık yapılan hatalardan biri, önermenin birkaç özel durumda sağlandığını görüp bunu genel geçer bir doğru olarak kabul etmektir. Oysa matematikçiler için bu tür örnekler, ancak nihai kanıt inşa etmede yol gösterici olabilir; kendileri başlı başına bir kanıt sayılmaz. Bir örnek ele alalım:

İddia 1.

n , 1’den büyük bir tam sayı olsun. Eğer n asal sayı ise $2^n - 1$ de asal sayıdır.

Bu iddianın doğruluğu için ne dersiniz? Bunu görmek için bariz ve oldukça mantıklı olan bir yöntem birkaç asal sayı için yukarıdaki önermenin doğru olup olmadığını incelemektir.

- $n = 2$ asal sayısı için $2^n - 1 = 3$ olup 3 asal sayı olduğundan önerme gerçekleşir.
- $n = 3$ asal sayısı için $2^n - 1 = 7$ olup 7 asal sayı olduğundan önerme gerçekleşir.
- $n = 5$ asal sayısı için $2^n - 1 = 31$ olup 31 asal sayı olduğundan önerme gerçekleşir.
- $n = 7$ asal sayısı için $2^n - 1 = 127$ olup 127 asal sayı olduğundan önerme gerçekleşir.

Buraya kadar işler çok yolunda gidiyor. Dolayısıyla birçoğunuz önermenin doğru olduğunu düşünmeye başlamış bile olabilirsiniz. Şimdi $n = 11$ asal sayısını ele alalım. Bu durumda $2^{11} - 1 = 2047$ olup $2047 = 23 \cdot 89$ yazılabildiğinden, n asal olmasına rağmen $2^n - 1$ asal olmaz. Dolayısıyla birkaç durum için sağlanan bu önermeyi her n asal sayısı için doğru kabul edemeyiz. Yine de yalnızca 5. denemede önermenin sağlanmadığını görmüş olduk ve daha fazla deneme yapmamıza gerek kalmadı.

Şimdi başka bir örnek ele alalım:

İddia 2.

n negatif olmayan bir tam sayı olsun. Bu durumda $n^2 + n + 41$ bir asal sayıdır.

Bir önceki iddiayı incelerken yaptığımız gibi bir noktadan başlayarak denemeler yapalım. n bir negatif olmayan tam sayı olduğundan 0’dan başlamak uygun olacaktır.

- $n = 0$ için $0^2 + 0 + 41 = 41$ olup 41 bir asal sayıdır.
- $n = 1$ için $1^2 + 1 + 41 = 43$ olup 43 bir asal sayıdır.
- $n = 2$ için $2^2 + 2 + 41 = 47$ olup 47 bir asal sayıdır.
- $n = 3$ için $3^2 + 3 + 41 = 53$ olup 53 bir asal sayıdır.

¹Tabii bu tanım başka başka sorular doğurmaktadır. Ancak bunların detayına girmeyeceğiz.

- $n = 4$ için $4^2 + 4 + 41 = 61$ olup 61 bir asal sayıdır.
- $n = 5$ için $5^2 + 5 + 41 = 71$ olup 71 bir asal sayıdır.
- $n = 6$ için $6^2 + 6 + 41 = 83$ olup 83 bir asal sayıdır.
- $\vdots$
- $n = 39$ için $39^2 + 39 + 41 = 1601$ olup 1601 bir asal sayıdır.

Dolayısıyla 0 ile 39 arasındaki tüm tam sayılar için önerme gerçekleşmektedir. Yine de bu, önermenin doğru olduğu anlamına gelmez! Zira $n = 40$ için $40^2 + 40 + 41 = 1681 = 41 \cdot 41$ olup asal değildir. Bir önceki örneğin aksine burada önermenin doğru olmadığı sonucuna ulaşmak için 41 deneme yapmamız gerekti. Peki bu denemeyi nereye kadar yapabiliriz?

2. Yalnızca bir aksine örnek yeterlidir.

Bir önceki bölümde İddia 1’de verilen önermeyi ve İddia 2’de verilen önermeyi sağlamayan en az birer örnek olduğunu görmüş olduk. Buna matematikte *aksine örnek* (ya da karşı örnek, ters örnek; ing. counterexample) adı verilir. O halde, bir önermeyi kanıtlamak için istisnasız her durumu kapsayacak bir gerekçe ortaya koymak gerekirken, önermenin yanlışlığını göstermek için *yalnızca bir aksine örnek* yeterlidir. İddia 1’de $n = 11$ aksine örnek iken, İddia 2’de $n = 40$ aksine örnektir. Tabii ki başka aksine örnekler vermek mümkündür.

Dolayısıyla bir önermenin doğruluğunu kanıtlamak sayfalarca sürebilirken, tek satırlık bir aksine örnek önermenin yanlış olduğunu göstermeye yeterlidir. Ancak aksine örnek bulmak her zaman görüldüğü kadar kolay olmayabilir. Bu durumu bir örnekle görelim.

Euler² şu varsayımda bulunmuştur: *En az üç pozitif tam sayının küpleri toplanarak başka bir pozitif tam sayının kübü elde edilebilir.* Örneğin $3^3 + 4^3 + 5^3 = 27 + 64 + 125 = 216$ olup $216 = 6^3$ yazılabilir. Dolayısıyla bu örnekte üç tane pozitif tam sayının kübü toplanarak başka bir pozitif tam sayının kübü elde edilmiş oldu. Daha sonra Euler, iki tane pozitif tam sayının kübü toplanarak bir tam küp elde edilemeyeceğini kanıtladı³.

Bu durumu bir üst kuvvete taşırsak; dördüncü kuvvetlerinin toplamı bir başka tam sayının dördüncü kuvvetini verecek şekilde dört tane tam sayı bulabiliriz. Örneğin $30^4 + 120^4 + 272^4 + 315^4 = 353^4$ yazılabilir. Euler, üç tane tam sayının dördüncü kuvveti toplanarak başka bir tam sayının dördüncü kuvveti elde edilemeyeceğini iddia etti. Hatta varsayımını şu şekilde genelledi: $n \geq 2$ olmak üzere, *en az n tane pozitif tam sayının n -inci kuvvetleri toplanarak başka bir pozitif tam sayının n -inci kuvveti elde edilebilir.* Bir başka deyişle bir pozitif tam sayının n -inci kuvveti n ’den daha az pozitif tam sayının n -inci kuvvetlerinin toplamı olarak yazılamaz.

Euler’in bu iddiası 200 yıl boyunca ne kanıtlanabildi ne de çürütülebildi. Ta ki 1966 yılında iki matematikçi $27^5 + 84^5 + 110^5 + 133^5 = 144^5$ olduğunu gösterene kadar. Bu örnekle birlikte bir pozitif tam sayının 5. kuvvetinin dört tane pozitif tam sayının 5. kuvvetlerinin toplamı olarak yazılabildiği gösterilmiş oldu. Dolayısıyla Euler’in iddiasının $n = 5$ için yanlış olduğu aksine örnek ile kanıtlandı. Daha sonra bilgisayar gücüyle birlikte daha ilginç bir örnek olarak $95800^4 + 217519^4 + 414560^4 = 422481^4$ olduğu gösterildi. Dolayısıyla bir pozitif tam sayının 4. kuvvetinin üç tane pozitif tam sayının 4. kuvvetlerinin toplamı olarak yazılabildiği gösterilmiş oldu, ki bu Euler’in iddiasının $n = 4$ için de yanlış olduğu anlamına gelmekteydi.

Kıssadan hisse: Bazen önerme çürütmek, kanıtlamaktan daha zordur!

3. Nasıl başlayacağını bilmek...

Buraya kadar bir önermenin nasıl kanıtlanamayacağını ve nasıl çürütülebileceğini gördük. Şimdi ise bir önermenin nasıl kanıtlanabileceği hakkında konuşacağız.

Daha önce de söylediğimiz gibi, matematiksel bir kanıt yalnızca bir sonucun doğru olduğunu söylemek değildir; o sonucun neden doğru olduğunu, nasıl doğru olduğunu mantıklı, adım adım bir akıl yürütmeye göstermektir. Matematikte birçok kanıt tekniği mevcuttur. Ancak bu tekniklerin hepsini bilmek, karşılaştığınız her önermeyi kolayca kanıtlayabileceğiniz anlamına gelmez. Matematiği bu kadar ilgi çekici

²Leonhard Euler (1707–1783), modern matematiğin birçok alanının temellerini atan, üretkenliği ve derinliğiyle tanınan İsviçreli bir matematikçidir.

³Bu Fermat’ın son teoreminin bir özel halidir.

kılan şeylerden biri de budur. Bu nedenle, bu yazıda size kanıt yapmaya dair eksiksiz bir *reçete* sunmayı vaat etmediğimi belirtmek isterim! Yine de matematiksel kanıt sürecinde işleri kolaylaştırabilecek bazı yöntemlerden ve temel fikirlerden yazının ilerleyen bölümlerinde söz edeceğim. Bu yöntemlerin hangisinin elinizdeki önermeyi kanıtlamak için uygun olduğunu anlamak zamanla gelişen bir beceridir. Biraz alışkanlık, biraz sabır ve bolca deneme yanılma gerektirir. Ve tüm bunlara rağmen, bazen hangi yöntemle ilerleyeceğiniz hemen belli olmayabilir. Çinli filozof Lao Tzu’nun sözleriyle

“Binlerce kilometrelik bir yolculuk bile tek bir adımla başlar.”

Bir kanıtı binlerce kilometrelik bir yolculuk olarak düşünürsek, bu yolu tamamlamak için ilk adımı doğru atmak oldukça önemlidir. Ancak neyse ki matematik bize kanıtın herhangi bir anında en başa dönme, farklı yaklaşımlar deneme, hatta tamamen geri çekilip başka bir yoldan ilerleme imkânı sunar.

Aşağıda, kanıt yaparken size yardımcı olabilecek bazı temel öneriler vereceğim. Bu adımlar her zaman sıralı biçimde uygulanmak zorunda değil; ama genellikle bir önermeyle baş başa kaldığınızda işe yarayan yöntemlerdir. Yine de bu önerilerin her zaman yeterli olmayacağını bilmekte fayda var!

- *Önerme açık değilse, sadeleştirin.*

Eğer önerme size karmaşık geliyorsa ya da kullanılan terimlere tam olarak hâkim değilseniz, onu kendi anlayacağınız şekilde yeniden ifade edin. Gerekirse matematiksel dili geçici olarak bırakıp, günlük bir dille “ne demek isteniyor?” sorusunu kendinize sorun. Örneğin, türevle ilgili “türev operatörü lineerdir” ifadesi kulağa teknik gelebilir; ancak bunu “türevlerin toplamı, toplamın türevidir” biçiminde sadeleştirmek faydalı olabilir.

- *Hangi varsayımların verildiğini, hipotezin ne olduğunu, bir başka deyişle kanıtlanması istenen şeyin hangi koşullar altında verildiğini belirleyin.*

Birçok kanıt girişimi, yalnızca tanımlar üzerinden ya da hiçbir varsayım kullanılmadan yapılmaya çalışılır ve bu çoğu zaman başarısız olur. Size bir öncül verildiyse, örneğin “ n bir çift tam sayı olsun. Bu durumda ...” gibi, işe oradan başlayın.

- *İstenen şeyi açıkça belirleyin.*

Kanıtlamanız gereken ifadenin tam olarak ne olduğunu netleştirin. Ne zaman “Ben ne bulmaya çalışıyordum?” sorusunu sormaya başlarsanız, büyük ihtimalle yolunuzu kaybetmişsinizdir.

- *Konuya dair bildiklerinizi gözden geçirin.*

Kanıtlamaya çalıştığınız önermenin hipoteziyle ilgili (hatta bu hipotezi doğrudan içeren) ve bulmaya çalıştığınız sonucu da ilgilendirebilecek bilinen teoremleri gözden geçirin. Önermedeki matematiksel terimlerin tanımlarını iyi bilin ya da bu tanımları tekrar okuyun. Ayrıca hipotezi ve kanıtlanacak ifadeyi (ifadedeki terimlerin tanımlarıyla birlikte) iyi bir notasyon seçerek düzgün bir şekilde ifade edin.

- *Kendinize şu soruyu sorun: Bu ifade neden doğru olmalı?*

Bu soru, kanıt yapmanın en temel noktalarından biridir. Eğer bir ifadenin neden doğru olduğunu içten içe anlayamıyorsanız, onu kanıtlamaya çalışmak çok zordur. Bu durumda kendinize örnekler oluşturun, gerekirse bir şekil çizin, özel durumlar için önermenizi test edin. Anlamadan ispatlamak neredeyse imkânsızdır. Ama eğer içsel olarak doğru olduğuna ikna olduysanız, geriye kalan şey bunu teknik bir dille anlatmak olur. Bu teknik beceriler zamanla kazanılır; ama sezgisel anlayış çoğu zaman çok daha önceden gelişir.

Eminim ki bu listeye eklenecek çok şey var. Fakat unutmayalım ki bu listenin işe yarayıp yaramadığını denemeden, çabalamadan, vakit ayırmadan göremezsiniz. Bu listeye ünlü Fransız besteci ve piyanist Maurice Ravel’in şu sözüyle de bir katkıda bulunabiliriz:

“Kopyalayın. Eğer içinizde biraz özgünlüğünüz varsa, bu kopyaladıkça ortaya çıkar. Eğer yoksa, sorun değil.”

Gerçekten öğrenmenin ve gelişimin en doğal yollarından biri taklit etmek, kopyalamaktır. Benzer önermelerin kanıtlarını incelemek ve bu kanıtlarda izlenen yolları uyarlayarak elinizdeki önermeyi kanıtlamaya çalışmak oldukça öğreticidir. Eğer içinizde bir parça özgünlük varsa, bu zaten ortaya çıkacaktır. Yoksa bile

sorun değil, bunun bir öğrenme basamağı olduğunu bilip devam etmek gerekir. Son olarak, bu belki gereksiz bir tavsiye gibi görünebilir; ancak bence en önemlisi: YAZIN! Yazmadan matematik olmaz. Elinizde zaten yazılı bir şey varsa bile, onu tekrar yazın. Her çalıştığınızda gerekirse bir daha yazın. Çünkü düşünce, ancak kâğıda döküldüğünde gerçekten şekillenir.

Şimdi birkaç tane nispeten basit önermeyi sözlü bir şekilde anlatır gibi kanıtlamaya çalışacağım.

Teorem 1.

n bir pozitif tam sayı olmak üzere, $1 + 2 + \dots + n = \frac{n(n+1)}{2}$.

Kanıt. Teoremin ifadesini birlikte anlamaya çalışalım. n sayısının bir pozitif tam sayı olduğu verilmiş. Yani n sayısının $\mathbb{Z}^+ = \{1, 2, 3, \dots\}$ kümesinden *keyfi* bir sayı olduğu biliniyor. Bu durumda n sayısına kadar olan tüm pozitif tam sayıların toplamının, n sayısı ile 1 fazlasının çarpımının yarısına eşit olduğu iddia ediliyor. Birkaç örnekle durumu daha iyi anlamaya çalışalım:

$$\begin{aligned} n = 1 \text{ için } 1 &= \frac{1 \cdot 2}{2}, \\ n = 2 \text{ için } 1 + 2 &= 3 = \frac{2 \cdot 3}{2}, \\ n = 3 \text{ için } 1 + 2 + 3 &= 6 = \frac{3 \cdot 4}{2}, \\ n = 4 \text{ için } 1 + 2 + 3 + 4 &= 10 = \frac{4 \cdot 5}{2}. \end{aligned}$$

Yukarıdaki örnekler teorem için bir kanıt vermese de teoremin ifadesini anlamak için önemlidir. Şimdi verilen önermenin her n pozitif sayısı için doğru olduğunu kanıtlayalım.

$$1 + 2 + \dots + (n-1) + n = S$$

diyelim. Açıkça görülür ki

$$n + (n-1) + \dots + 2 + 1 = S$$

sağlanır. Çünkü tam sayılar için toplama işlemi değişmelidir, yani aynı tam sayıları hangi sırada topladığımızın bir önemi yoktur. O halde

$$\begin{aligned} 1 + 2 + \dots + (n-1) + n &= S, \\ n + (n-1) + \dots + 2 + 1 &= S \end{aligned}$$

bulunur. İki denklemi taraf tarafa toplarsak

$$(n+1) + (n+1) + \dots + (n+1) + (n+1) = 2S$$

elde ederiz. Bu denklemde n tane $(n+1)$ olduğunu görebildiniz mi? Buradan $n(n+1) = 2S$ olup dolayısıyla $S = n(n+1)/2$ bulunur. Sonuç olarak $1 + 2 + \dots + n = S = n(n+1)/2$ eşitliğine ulaşılır. $\square$

Teorem 2.

$Ax^2 + Bx + C$ ikinci dereceden bir polinom olmak üzere (yani $A \neq 0$), bu polinomun gerçel sayılar üzerinde ya kökü yoktur, ya $x = -\frac{B}{2A}$ ile verilen biricik kökü vardır ya da

$$x = \frac{-B \pm \sqrt{B^2 - 4AC}}{2A}$$

ile verilen iki farklı kökü vardır.

Kanıt. İkinci dereceden tek değişkenli bir polinomun kökleri için yukarıda verilen formülü birçoğunuzun

ezbere bildiğine yemin edebilirim, ama kanıtlayamam :) Fakat bu formülün nereden geldiğini kanıtlayabilirim.

$Ax^2 + Bx + C$ polinomunun köklerini aramak, $Ax^2 + Bx + C = 0$ denkleminin çözümlerini aramak ile aynı şeydir. Burada $A \neq 0$ olması, denklemin ikinci dereceden olması için gereklidir. Aksi takdirde $Bx + C = 0$ formunda x 'in kuvvetlerine göre en fazla birinci dereceden olan bir denklem elde edilir. Peki $Ax^2 + Bx + C = 0$ denkleminin çözümlerini nasıl bulabiliriz? En genel ikinci dereceden denklem yerine çok daha basit bir denklem ele alalım: $x^2 = a^2$. Bu denklemin çözümü için ne dersiniz? İki sayının karelerinin birbirine eşit olması için bu sayıların ya aynı ya da birbirlerinin zıt işaretlisi olması gerekir, değil mi? Yani $x = a$ ya da $x = -a$ olmalıdır. Şimdi $(x + b)^2 = a^2$ ikinci derece denklemini düşünelim. Biraz önceki duruma benzer şekilde $x + b = a$ ya da $x + b = -a$ olmalıdır. Yani bu denklemin çözümleri $x = a - b$ ve $x = -a - b$ biçimindedir. Dolayısıyla eğer denklemde x 'li terimlerin bir tam karesi varsa, bu durumda denklemi nasıl çözeceğimizi daha rahat kestirebiliriz!

Tekrar $Ax^2 + Bx + C = 0$ denkleminde x 'li terimlerin bir tam karesi olmadığı açıktır. Ancak tabii ki denklemin sol tarafını tam kareye tamamlamak mümkündür. Bu işleme geçmeden önce denklemin her iki tarafını A sayısına bölelim. A sayısı sıfırdan farklı olduğundan bunu yapabiliriz. Bunu yapmamızın sebebi tam kareye tamamlama işlemini basitleştirmektir. Böylece

$$x^2 + \frac{B}{A}x + \frac{C}{A} = 0$$

denkleminde ulaşırız. Bu denklem ile orijinal denklemimizin kökleri aynıdır. Şimdi denklemin sol tarafını tam kareye tamamlayalım:

$$x^2 + \frac{B}{A}x + \frac{C}{A} = \left(x + \frac{B}{2A}\right)^2 - \frac{B^2}{4A^2} + \frac{C}{A} = 0.$$

Buradan, neden ilk denklemi A sayısına böldüğümüz daha iyi anlaşılmış olmalı. Şimdi yukarıdaki denklemi düzenleyelim:

$$\left(x + \frac{B}{2A}\right)^2 = \frac{B^2 - 4AC}{4A^2}.$$

O halde bu denklemin kökleriyle orijinal denklemin kökleri aynıdır. Şimdi bu denklemin köklerini araştıralım. Denklemin sol tarafı bir gerçel sayının karesi olduğundan negatif bir sayı olamaz. Bu sebeple eğer denklemin sağ tarafı negatifse, yani $B^2 - 4AC < 0$ ise denklemin kökü yoktur! Eğer denklemin sağ tarafı sıfırsa, yani $B^2 - 4AC = 0$ ise bu durumda

$$\left(x + \frac{B}{2A}\right)^2 = 0$$

olup bu denklemin tek kökü $x = -\frac{B}{2A}$ 'dır. Diğer yandan $B^2 - 4AC > 0$ ise bu durumda yukarıda yaptığımız basit örneklere benzer şekilde

$$x + \frac{B}{2A} = \pm \frac{\sqrt{B^2 - 4AC}}{2A}$$

bulunur. Bu eşitlik düzenlenerek teoremden verilen ifade kolayca elde edilebilir. □

Teorem 3.

X ve Y iki küme ve $f : X \rightarrow Y$ bir fonksiyon olsun. Bu durumda aşağıdaki önermeler denktir.

- (i) f birebir fonksiyondur.
- (ii) Her $A \subseteq X$ için $A = f^{-1}(f(A))$ gerçekleşir.

Kanıt. Önce verilenleri anlayalım. X ve Y diye adlandırılan iki küme verilmiş, bu kümeler üzerinde herhangi bir kısıtlama yok. Dolayısıyla elimizde keyfi iki küme var. Bir de X kümesinden Y kümesine tanımlı keyfi bir fonksiyon mevcut.

Peki istenen ne? Basitçe (i) ve (ii)'de verilen iki önermenin birbirine denk olduğunu göstermemiz

isteniyor. Bu önermelerin detaylarına girmeden önce iki önermenin denk olmasının ne demek olduğunu anlayalım. İki önermenin denk olması demek, bu önermelerin birbirlerini *gerektirmesi* demektir. Bir başka deyişle, (i) önermesinin sağlandığı durumda (ii) önermesi de sağlanmalı ve (ii) önermesinin sağlandığı durumda (i) önermesi de sağlanmalıdır. Dolayısıyla iki önermenin denkliğini göstermek için, bu önermelerden birini kabul edip bu kabul altında diğerinin doğruluğunu göstermek gerekir ve bu iş her iki önerme için de yapılmalıdır.

İlk olarak (i)'nin (ii)'yi gerektirdiğini, yani (i)'yi kabul edip (ii)'nin gerçekleştiğini, gösterelim. f birebir fonksiyon olsun. Bu durumda her $A \subseteq X$ kümesi için $A = f^{-1}(f(A))$ olduğunu kanıtlamaya çalışacağız. Şimdiki sorumuz şu: İki kümenin eşitliği ne demek? Yani $A = f^{-1}(f(A))$ demekle neyi kastediyoruz? İki kümenin eşit olması aslında her iki kümenin birbirini kapsamaması (başka bir deyişle, birbirinin alt kümesi olması) anlamına gelir⁴. O halde $A \subseteq f^{-1}(f(A))$ ve $f^{-1}(f(A)) \subseteq A$ olduğunu göstermeliyiz.

Aslında ilk kapsama, yani $A \subseteq f^{-1}(f(A))$ ifadesi her zaman sağlanır. Yani bu kapsama, f birebir değilken de doğru zaten! Bu kısmın kanıtını alıştırma sorularında ödev olarak bırakacağım. Çünkü birazdan detaylarıyla kanıtlayacağımız ikinci kapsama, bu kısmı kendi kendinize yapmanızda çok faydalı olacak.

O halde ikinci kapsamayı gösterelim. Peki, $f^{-1}(f(A)) \subseteq A$ ne demek? $f^{-1}(f(A))$ kümesindeki her bir elemanın A kümesine de ait olması demek değil mi? O halde $f^{-1}(f(A))$ kümesinden keyfi bir eleman alıp bu elemanın A kümesine de ait olduğunu gösterelim: $x \in f^{-1}(f(A))$ olsun. Sıradaki soru şu: Bir elemanın, bir kümenin ön görüntüsünde olması ne demek?⁵ Bu bile yeni bir soru doğurdu: Bir kümenin ön görüntüsü ne demek?

Hemen ön görüntünün tanımına gidelim. $g : B \rightarrow C$ bir fonksiyon ve $E \subset C$ olmak üzere, $g^{-1}(E) = \{x \in B \mid g(x) \in E\}$ kümesine E kümesinin g fonksiyonu altındaki ön görüntüsü denir. Yani E kümesinin ön görüntüsü; fonksiyon altında görüntüsü E 'de olan elemanların kümesidir. O halde $x \in g^{-1}(E)$ ise, $g(x) \in E$ olmalıdır.

Şimdi kanıtımıza devam edelim. $x \in f^{-1}(f(A))$ olduğuna göre ön görüntü tanımı gereği $f(x) \in f(A)$ olmalıdır. Buraya kadar $f(x) \in f(A)$ olduğunu gördük ve f 'nin birebir olduğunu kullanmamıza gerek kalmadı. Ve unutmayalım ki $x \in A$ olduğunu göstermemiz gerekiyor. Bir kısmınız $f(x) \in f(A)$ ise $x \in A$ olmalıdır diye düşünebilir. Ancak bu doğru değil!

Örneğin; $f : \mathbb{R} \rightarrow \mathbb{R}_{\geq 0}$ fonksiyonu $f(x) = x^2$ biçiminde tanımlansın. $A = (0, \infty) \subset \mathbb{R}$ alt kümesini düşünelim. $f(x) = 4 \in \mathbb{R}_{\geq 0}$ elemanını ele alalım. Bu durumda $f(x) \in f(A)$ olmasına rağmen $x \in A = (0, \infty)$ olmak zorunda değil! Çünkü $x = -2$ için de $f(x) = 4$ olur ve $-2 \notin (0, \infty)$.

Bu sebeple daha dikkatli ilerleyelim. $f(x) \in f(A)$ kısmında kalmıştık. Peki bu ne demek? Bir eleman bir kümenin görüntüsü kümesinde yatıyor. Görüntü kümesi tanımını hatırlayalım: $g : B \rightarrow C$ bir fonksiyon ve $D \subset B$ olmak üzere, $g(D) = \{g(x) \in C \mid x \in D\}$ kümesine D kümesinin g fonksiyonu altındaki görüntüsü adı verilir. Yani D kümesindeki elemanların g fonksiyonu altındaki görüntülerinin oluşturduğu kümeden bahsediyoruz. Dolayısıyla $y \in g(D)$ ise bu eleman $g(x)$ tipinde yazılabilir, yani $y = g(x)$ olacak şekilde $x \in D$ mevcut olmalıdır.

Dolayısıyla $f(x) \in f(A)$ demek, $f(x) = f(a)$ olacak şekilde bir $a \in A$ mevcut olması demektir. Artık birebirliği kullanma zamanı. Ne demek bir fonksiyonun birebir olması? Farklı elemanların görüntüleri farklı olmalıdır ya da denk olarak, görüntüleri aynı olan elemanlar aynıdır. f fonksiyonu birebir ve $f(x) = f(a)$ olduğundan $x = a$ olmalıdır. $a \in A$ olduğuna göre tabii ki $x \in A$ sağlanır. İşte bu!

Şimdi, (ii)'yi kabul edip (i)'nin gerçekleştiğini gösterelim. Her $A \subseteq X$ kümesi için $A = f^{-1}(f(A))$ olsun. Bu durumda f birebir midir? f 'nin birebir olması ne demektir: Görüntüleri aynı olan elemanlar aynıdır. Yani keyfi $x, x' \in X$ için $f(x) = f(x')$ ise $x = x'$ olmalıdır. O halde $f(x) = f(x')$ sağlanırken x ile x' eşit oluyor mu diye bakacağız değil mi? Diyelim ki $x, x' \in X$ için $f(x) = f(x')$ olsun. Bu aşamada kullanabileceğimiz başka bir yardımcı yok. Sadece (ii) önermesini kullanabiliriz. Görüyoruz ki (ii) önermesi kümelerin görüntü ve ön görüntülerinin içeren bir eşitlik. Ama elimizde küme yok. x ve x' elemanları var ve $f(x) = f(x')$ eşitliği var. Bu eşitlikten

$$f(\{x\}) = f(\{x'\})$$

⁴Yani A ve B kümeler olmak üzere, $A = B$ eşitliği demek $A \subseteq B$ ve $B \subseteq A$ kapsamalarının her ikisinin de sağlanması demektir.

⁵Burada f^{-1} size doğrudan fonksiyonun tersini çağırabiliriz. Ancak bilmelisiniz ki fonksiyonunun tersinin var olması için birebir ve örten olması gerekir.

olduğunu söyleyebiliriz. Artık elimizde birer elemanlı iki küme var ve bunların görüntüleri birbirine eşit. Bir fonksiyonun görüntü kümesi tabii ki değer kümesinin içinde olmalı. O halde $f(\{x\}) \subset Y$ ve $f(\{x'\}) \subset Y$ sağlanır. Dolayısıyla elimizde Y kümesinin içinde bulunan ve birbirine eşit iki küme var. Bu kümelerin ön görüntüleri de birbirine eşittir, yani

$$f^{-1}(f(\{x\})) = f^{-1}(f(\{x'\}))$$

olur. (ii)'den biliyoruz ki her $A \subseteq X$ kümesi için $A = f^{-1}(f(A))$ sağlanıyor. Bu sebeple $f^{-1}(f(\{x\})) = \{x\}$ ve $f^{-1}(f(\{x'\})) = \{x'\}$ olup $\{x\} = \{x'\}$ bulunur. Bu ise $x = x'$ demektir. O halde f fonksiyonu birebirdir. $\square$

4. -miş gibi yapmak

“Bir şeyin var olmadığını ya da sağlanmadığını nasıl kanıtlayabilirim?” sorusu öğrenciler için zaman zaman kafa karıştırıcı olabilir. Fakat matematikte böyle “olumsuz” ifadelerin de kanıtı mümkündür. Ve matematikçiler böyle önermelerin kanıtları için güzel bir strateji kullanır: -miş gibi yapmak. Mantıksal olarak bir nesnenin var olmadığını göstermek için, bu nesne varmış gibi yaparız (yani var olduğunu kabul ederiz) ve daha sonra bu kabulün yol açtığı sonuçları inceleriz. Eğer var olduğunu varsaymak ileride bir çelişkiye neden oluyorsa, bu durumda kabulümüz doğru olamaz. Dolayısıyla nesnenin varlığı imkânsız olup bu nesne yoktur diyebiliriz. Sizce de çok havalı değil mi?

Hemen bir teorem kanıtlayarak daha iyi anlamaya çalışalım.

Teorem 4.

$\sqrt{2}$ irrasyonel bir sayıdır.

Kanıt. Bir gerçel sayının irrasyonel olması rasyonel olmaması demektir. Dolayısıyla $\sqrt{2}$ sayısının rasyonel olmadığını göstereceğiz. Bir an için $\sqrt{2}$ sayısı rasyonelmiş gibi yapalım, bir başka deyişle bu sayının rasyonel olduğunu varsayalım. Bildiğimiz üzere rasyonel sayılar aslında iki tam sayının birbirine bölümü şeklinde yazılabilen kesirli sayılardır. Tabii ki payda sıfır olamaz. Eğer $\sqrt{2}$ sayısı rasyonel bir sayı ise, bu durumda

$$\sqrt{2} = \frac{a}{b}$$

olacak şekilde sıfırdan farklı ve aralarında asal a ve b tam sayıları vardır. Burada a ve b 'nin aralarında asal olması özel bir durum değildir, aksi takdirde kesirde sadeleştirme yapılarak aralarında asal hale getirilebilir. O halde $\sqrt{2} = a/b$ eşitliğinde her iki tarafın karesi alınıp düzenlenerek

$$2b^2 = a^2 \tag{1}$$

elde edilir. Demek ki a^2 tam sayısı 2'nin bir tam katıdır, bir başka deyişle a^2 bir çift tam sayıdır. Buradan a tam sayısının da çift olduğu sonucuna varırız. Çünkü tek tam sayıların karesi çift olamaz!⁶ Demek ki bir m tam sayısı için $a = 2m$ olur. Bu ifade (1) denkleminde yerine yazılırsa $2b^2 = (2m)^2 = 4m^2$ ve buradan da $b^2 = 2c^2$ elde edilir. O halde b^2 bir çift tam sayıdır. Bu da demektir ki b de bir çift tam sayıdır.

Sonuç olarak gösterdik ki a ve b 'nin her ikisi de çift tam sayıdır. Yani her ikisi de 2'ye tam bölünüyor. Bu durumda bir gariplik fark ettiniz mi? a ve b tam sayılarının aralarında asal olduğunu söylemiştik. Yani her ikisi de 2'ye bölünemez! O halde bu bir çelişkidir. Bu sebeple $\sqrt{2}$ sayısının rasyonel olduğunu kabulü yanlıştır. Bu da demektir ki $\sqrt{2}$ irrasyoneldir. $\square$

Başka bir teorem kanıtlayarak bu durumu pekiştirelim.

Teorem 5.

Sonsuz çoklukta asal sayı vardır.

⁶Kanıt. Bir tek tam sayı $2n + 1$ formundadır. $(2n + 1)^2 = 4n^2 + 4n + 1$ olup $4n^2 + 4n$ çift olduğundan 1 fazlası tektir.

Kanıt. Asal sayıların sonsuz çoklukta olduğunu kanıtlamak, aslında sonlu tane asal sayı olmadığını kanıtlamak demektir. O halde bir an için sonlu tane asal sayı varmış gibi yapalım ve bu asal sayıları $p_1, p_2, \dots, p_k$ ile gösterelim. Burada k ile tüm asal sayıların sayısı ifade edilmektedir.

Tüm asal sayıları çarpıp sonuca 1 ekleyerek

$$N = (p_1 p_2 \cdots p_k) + 1$$

sayısını oluşturalım⁷. Elde ettiğimiz N sayısı açıkça tüm asal sayılardan büyüktür, bu sebeple asal sayıların hepsinden farklı bir sayıdır. $p_1, \dots, p_k$ sayıları elimizdeki tüm asal sayılar olduğuna göre, bunlardan farklı olan N sayısı asal olamaz. Bu sebeple N sayısının, Aritmetiğin Temel Teoremi gereğince, bir asal çarpanı olmak durumundadır. Bu asal çarpan $p_1, \dots, p_k$ sayılarından biri olmak zorundadır, çünkü elimizdeki tüm asal sayılar bunlar! Diyelim ki bu asal çarpan $p_i, i \in \{1, 2, \dots, k\}$ olsun. O halde N sayısı p_i sayısının bir katı olmak zorunda. Diğer yandan açıkça $N - 1 = p_1 \cdots p_k$ sayısı da p_i sayısının bir katıdır. N ve $N - 1$ sayılarının her ikisi de p_i asalının bir katı olduğuna göre, bunların farkı da aynı asalın bir katı olmak zorundadır. Yani $N - (N - 1)$ sayısı da p_i asalının bir katıdır. Dolayısıyla 1 sayısı p_i asalının bir katı olur. Ancak bu imkansızdır, çünkü en küçük asal sayı 2'dir ve 1 sayısı 2'nin bile bir tam katı değildir. Bu bir çelişkidir! Bu sebeple sonlu tane asal sayının olduğu kabulümüz yanlıştır. Bu da demektir ki sonsuz çoklukta asal sayı vardır. $\square$

5. Doğal sayılardaki domino etkisi: Tümevarım

Bu bölümde, belirli türdeki matematiksel ifadeleri kanıtlamak için güçlü ve zarif bir yöntem olan *matematiksel tümevarım* kavramını ele alacağız. Tümevarım, temelde bir ifadenin tüm doğal sayılar için — ya da belirli bir noktadan itibaren tüm doğal sayılar için — doğru olduğu iddia edilen genel önermeleri kanıtlamak amacıyla kullanılır.

Bir P özelliğini tüm doğal sayılar için kanıtlamak istediğimizi düşünelim. Yani o P özelliğinin 0, 1, 2, ... için doğru olduğunu göstermek istiyoruz. Burada sonsuz çoklukta sayı olduğundan dolayı hepsi için tek tek P özelliğinin sağlandığını göstermek mümkün değildir. Aslında kanıtlamak istediğimiz özelliği (P) tek bir önerme olarak değil de, her n doğal sayısı için birer tane olmak üzere bir dizi önerme olarak görebiliriz:

- $n = 0$ için P özelliğinin sağlanması
- $n = 1$ için P özelliğinin sağlanması
- $n = 2$ için P özelliğinin sağlanması
- $\vdots$

Tümevarımdaki temel fikir, bu önermeler dizisindeki ilk önermeyi kanıtlamak ve ardından herhangi bir önermenin doğruluğu kabulü altında bir sonraki önermenin de doğru olduğunu göstermektir. Bu sayede dizideki tüm önermelerin doğru olduğu sonucuna varırız. Daha matematiksel bir şekilde ifade edecek olursak; eğer bir özelliğin her n doğal sayısı için doğru olduğu kanıtlanmak istenirse aşağıdakiler yapılmalıdır:

1. **Başlangıç adımı:** Bir başlangıç değeri için önermenin doğruluğunu kanıtla. Eğer kanıt tüm doğal sayılar üzerinde yapılacaksa, bu başlangıç değeri $n = 0$ olur. Eğer bir a doğal sayısı itibarıyla tüm doğal sayılar için bir ifade kanıtlanacaksa, başlangıç adımı $n = a$ olur.
2. **Tümevarım adımı:** Bir n doğal sayısı için önermenin doğru olduğunu varsayarak, $n + 1$ için de doğru olduğunu kanıtla. Burada, ifadenin belirli bir n için doğru olduğunu varsayan bu kabul, *tümevarım hipotezi* olarak adlandırılır.

Bu iki adım gerçekleştirildiğinde, elimizdeki önermenin her n (ya da her $n \geq a$) doğal sayısı için doğru olduğu sonucuna varabiliriz. Başlangıç adımında önermenin $n = 0$ (ya da $n = a$) için doğruluğunu kanıtıyoruz. Tümevarım adımından da biliyoruz ki bir n doğal sayısı için doğruysa bir sonraki için de doğru olmak zorunda. O halde, önerme $n = 0$ için doğru olduğundan $n = 1$ için de doğru olmalı. Yine tümevarım adımından $n = 1$ için doğru olan önerme, $n = 2$ için de doğru olmalı. Tekrar tümevarım adımından $n = 2$

⁷Elimizde sonlu tane asal sayı olduğundan dolayı burada yaptığımız çarpma anlamlıdır.

için doğru olan önerme, $n = 3$ için de doğru olmalı. Tümevarım adımında önermenin keyfi bir n için doğruluğu altında $n + 1$ için de doğru olduğunu gösterdiğimiz için bu böyle sonsuza kadar devam eder.

Matematiksel tümevarımı, güzel bir benzetme ile, doğal sayılardaki domino etkisi olarak düşünebiliriz. Bir sürü domino taşının uzunca dizildiğini düşünelim. Tüm domino taşlarının devrileceğinden nasıl emin olabiliriz? Bunun için iki şey gereklidir; ilk dominonun devrilmesi ve devrilen her dominonun bir sonraki dominoyu devirmesi. Aslında tümevarım adımı, “domino taşlarının birbirine yakın yerleştirilmesini, böylece bir tanesi devrilince bir sonrakinin de devrilmesini” garanti eder. Başlangıç durumu ise “ilk dominonun gerçekten itilmesi” demektir.

Teorem 6.

Her n doğal sayısı için $3, n^3 - n$ sayısını böler.

Kanıt. Her n doğal sayısı için bir ifade kanıtlamamız gerekiyor. Bu sebeple n üzerine tümevarım uygulayabiliriz.

1. *Başlangıç adımı:* $n = 0$ için önermeyi kanıtlayalım. Bu durumda $n^3 - n = 0 - 0 = 0$ olduğundan ve 3 sayısı 0 sayısını böldüğünden, bir başka deyişle 0 sayısı 3 sayısının bir tam katı olduğundan önerme gerçekleşir. Hatta benzer şekilde $n = 1$ için de $n^3 - n = 1 - 1 = 0$ olduğundan önerme gerçekleşir.
2. *Tümevarım adımı:* Şimdi keyfi bir n doğal sayısı için önermenin olduğunu, yani 3 sayısının $n^3 - n$ sayısını böldüğünü kabul edelim. Bu kabul altında önermeyi $n + 1$ için kanıtlamaya çalışacağız, yani 3 sayısının $(n + 1)^3 - (n + 1)$ sayısını böldüğünü göstereceğiz. Kabul gereği önerme n için sağlandığından dolayı, $n^3 - n$ sayısı 3'ün bir tam katıdır. Yani $n^3 - n = 3k$ olacak şekilde bir k tam sayısı vardır. Buradan

$$\begin{aligned}(n + 1)^3 - (n + 1) &= n^3 + 3n^2 + 3n + 1 - n - 1 \\ &= n^3 - n + 3n^2 + 3n \\ &= (n^3 - n) + 3(n^2 + n) \\ &= 3k + 3(n^2 + n) \\ &= 3(k + n^2 + n)\end{aligned}$$

elde edilir. O halde $(n + 1)^3 - (n + 1)$ sayısı 3'ün bir tam katıdır. Yani önerme $n + 1$ için de doğrudur.

Dolayısıyla önerme her n doğal sayısı için sağlanır. □

Teorem 7.

1'den başlayarak ilk n doğal sayının küpleri toplamı $\frac{n^2(n+1)^2}{4}$ ’e eşittir. Yani $1^3 + 2^3 + \dots + n^3 = \frac{n^2(n+1)^2}{4}$.

Kanıt. n üzerine tümevarım uygulayalım.

1. *Başlangıç adımı:* $n = 1$ başlangıç durumunu inceleyelim. Bu durumda ise $1^3 = 1 = \frac{1^2(1+1)^2}{4}$ olup önerme $n = 1$ için gerçekleşir. Daha iyi anlayabilmek için $n = 2$ durumunu da gösterelim. Bu durumda $1^3 + 2^3 = 9$ olur. Ayrıca önermedeki ifadenin sağ tarafı da $\frac{2^2(2+1)^2}{4} = 9$ olduğundan, önerme $n = 2$ için de sağlanır.
2. *Tümevarım adımı:* Şimdi önermenin n doğal sayısı için doğru olduğunu kabul edelim. Bu kabul altında, önermenin $n + 1$ için doğru olduğunu kanıtlamaya çalışacağız. Yani $1^3 + 2^3 + \dots + (n + 1)^3 = \frac{(n + 1)^2(n + 2)^2}{4}$ olduğunu göstereceğiz. Tümevarım hipotezi kullanılarak

$$1^3 + 2^3 + \dots + n^3 + (n + 1)^3 = \frac{n^2(n + 1)^2}{4} + (n + 1)^3$$

$$\begin{aligned}
&= (n+1)^2 \left(\frac{n^2}{4} + (n+1) \right) \\
&= (n+1)^2 \frac{n^2 + 4n + 4}{4} \\
&= \frac{(n+1)^2 (n+2)^2}{4}
\end{aligned}$$

bulunur. O halde önerme $n+1$ için de gerçekleşir.

Dolayısıyla önerme her $n \geq 1$ doğal sayısı için sağlanır. $\square$

Tümevarım yoluyla bir kanıt yaparken, çoğu zaman tümevarım adımında ifadenin yalnızca n için doğruluğu, $n+1$ için doğruluğunu kanıtlamaya yeter. Ancak bazen biraz daha “güçlü” bir varsayıma ihtiyaç duyulur ve bu durumda tümevarım hipotezini güçlendirmek gerekir. Tümevarımın matematiksel ifadesindeki başlangıç adımı aynen kalırken, tümevarım adımı

2'. *Güçlü tümevarım adımı*: Bir n doğal sayısına kadar tüm doğal sayılar için önermenin doğru olduğunu varsayarak, $n+1$ için de doğru olduğunu kanıtla.

ile değiştirilsin. Bu yöntem *güçlü tümevarım* adı verilir. Ancak buradaki “güçlü tümevarım” ifadesi yukarıdaki klasik (ya da zayıf) tümevarımın bir genellemesi olduğu ya da bu yöntemle daha fazla önermenin kanıtlanabileceği anlamı taşımaz; sadece tümevarım adımında kullanılan varsayımın daha güçlü olmasına atıfta bulunur. Hatta temelde zayıf tümevarım kullanılan herhangi bir kanıt, doğrudan bir şekilde güçlü tümevarım kullanan bir kanıtla dönüştürülebilir; aynı şekilde güçlü tümevarım kullanan bir kanıt da zayıf tümevarım kullanan bir kanıtla dönüştürülebilir. Sadece, tümevarım hipotezini güçlendirmenin kolaylık sağladığı durumlar vardır.

Teorem 8.

2’den büyük her n doğal sayısı ya asaldır ya da asal sayıların çarpımı şeklinde yazılabilir.

Kanıt. n üzerine güçlü tümevarım uygulayalım. Neden bunu uyguladığımız gerektiği birazdan daha açık olacak.

1. *Başlangıç adımı*: $n=2$ başlangıç durumunu inceleyelim. 2 asal sayı olduğundan bu durum açıktır. Benzer şekilde 3 asal sayı olduğundan $n=3$ için de önermenin doğruluğu açıktır. Farklı bir örnek görmek adına $n=4$ durumunu da inceleyelim. Bu durumda $4=2 \cdot 2$ olduğundan ve 2 asal sayı olduğundan önermenin $n=4$ için sağlandığı da kolayca görülür.

2' *Güçlü tümevarım adımı*: Şimdi 2’den n doğal sayısına kadar tüm doğal sayılar için önermenin doğru olduğunu kabul edelim. Bu kabul altında, önermenin $n+1$ için doğru olduğunu kanıtlayacağız. Yani $n+1$ sayısının asal sayıların çarpımı şeklinde yazıldığını göstereceğiz. Bunu iki durumda inceleyelim:

- $n+1$ bir asal sayı olsun. Bu durumda kanıtlayacak bir şey yoktur.
- $n+1$ bir asal sayı olmasın. O halde $n+1 = a \cdot b$ olacak şekilde a ve b doğal sayıları vardır ve açıkça bu doğal sayılar $1 < a, b < n+1$ eşitsizliğini sağlar. Tümevarım hipotezinden a ve b doğal sayıları asal sayıların çarpımı olarak ifade edilebilir. O halde a doğal sayısı asal sayıların çarpımı olarak $p_1 p_2 \cdots p_i$ biçiminde ve b doğal sayısı asal sayıların çarpımı olarak $q_1 q_2 \cdots q_j$ biçiminde yazılabilir. Buradan $n+1 = p_1 p_2 \cdots p_i q_1 q_2 \cdots q_j$ olup, $n+1$ sayısı asal sayıların çarpımı biçiminde yazılmış olur.

O halde önerme $n+1$ için de doğru olur.

Dolayısıyla önerme her $n \geq 2$ doğal sayısı için gerçekleşir. $\square$

Yukarıdaki kanıtta güçlü tümevarım kullanmamızın en önemli sebebi a ve b doğal sayılarının asal sayıların çarpımı biçiminde yazıldığını söyleyebilmektir. Zayıf tümevarımda yalnızca n doğal sayısının önermeyi sağladığını kabul ederken, burada n ’den daha küçük olanların da önermeyi sağladığı kabulünü kullanmamız gerekti.

6. Önermelerin başka bir yüzü

“Eğer yağmur yağarsa dışarı çıkmam” önermesini düşünelim. Bu önermenin sözüne güvenilen bir insan tarafından söylendiğini ve bu kişinin dışarı çıktığını varsayalım. O halde yağmur yağmamıştır, öyle değil mi? Çünkü yağsaydı dışarı çıkmazdı. Dolayısıyla bu önerme ile “Dışarı çıktıysam yağmur yağmamıştır” önermesinin doğruluk değeri aynıdır. İlk koşullu önermeyi $p \rightarrow q$ ile ifade edersek, ikinci önerme $q' \rightarrow p'$ ile ifade edilir. Burada p' ile p önermesinin değili (olumsuzu) gösterilir. Bu iki koşullu önermenin doğruluk değerleri aynı olduğuna göre bu önermeler denktir: $p \rightarrow q \equiv q' \rightarrow p'$. O halde $p \rightarrow q$ önermesinin doğru olduğunu kanıtlamak yerine, $q' \rightarrow p'$ önermesinin doğru olduğunu kanıtlamakta yeterli olur. Çünkü bazen $q' \rightarrow p'$ koşullu önermesini kanıtlamak daha kolay olabilir. $q' \rightarrow p'$ koşullu önermesine $p \rightarrow q$ koşullu önermesinin karşıt tersi (ya da kontrapozitif), bu yöntem kullanılarak yapılan kanıtlara da *kontrapozitif ile kanıt* adı verilir.

Çok basit bir örnekle bu durumu anlamaya çalışalım.

Teorem 9.

Eğer n^2 çift tam sayı ise, n de çift tam sayıdır.

Kanıt. Önermeyi doğrudan kanıtlamaya çalışalım. n^2 tam sayısının çift olduğu durumda n nin de çift olduğunu göstermemiz gerek. Çift tam sayıların tanımı gereği; eğer n^2 çift tam sayı ise $n^2 = 2k$ olacak şekilde bir k tam sayısı mevcuttur. Hatta bu k tam sayısı negatif olamaz. O halde elimizde $n^2 = 2k$ gibi bir eşitlik var ve buradan n sayısının durumunu incelememiz gerekiyor. Ancak bu eşitlikten n hakkında fikir elde etmeye çalışırsak her iki tarafın karekökünü almak gerekir. Bu da bize $\sqrt{n^2} = \sqrt{2k}$ gibi bir eşitlik verir ve buradan n 'nin çift ya da tek olmasına karar veremeyiz. Dolayısıyla önermeyi doğrudan kanıtlamak biraz zorlu görünüyor. Bunun yerine koşullu önermenin karşıt tersini ele alalım: “ n çift tam sayı değilse, n^2 de çift tam sayı değildir.” Bu önerme, teoremin ifadesinde verilen önermeye denktir. O halde bu önermeyi kanıtlayalım.

n çift tam sayı olmasın. O halde n tektir ve $n = 2p + 1$ olacak şekilde p tam sayısı mevcuttur. Buradan $n^2 = (2p + 1)^2 = 4p^2 + 4p + 1 = 2(2p^2 + 2p) + 1 = 2m + 1$ olup n^2 tek tam sayıdır. Dolayısıyla n^2 çift tam sayı değildir. $\square$

■ Alıştırmalar

1. Teorem 1’de verilen önermeyi tümevarım kullanarak kanıtlayınız.
2. Aşağıdaki önermeleri kanıtlayınız.

- (a) X ve Y iki küme, $f : X \rightarrow Y$ bir fonksiyon ve $A \subseteq X$ olsun. Bu durumda $A \subseteq f^{-1}(f(A))$ olur.
- (b) A ve B iki küme olsun. Bu durumda $A \cap B = A$ olması için gerek ve yeter koşul $A \subseteq B$ olmasıdır. Not: Burada “gerek ve yeter koşul” demek aslında soldaki ve sağdaki önermelerin birbirine denk olması demektir. Bakınız Teorem 3.
- (c) A ve P , $n \times n$ tipinde matrisler ve P tersinir olsun. Her $k \geq 0$ tam sayısı için $(PAP^{-1})^k = PA^kP^{-1}$ olur.
- (d) Her $x \in [0, \pi/2]$ gerçel sayısı için, $\sin x + \cos x \geq 1$ sağlanır.

Yazıyı kapatırken, belki de zaten dikkatinizi çekmiş olabilecek bir şeyden bahsetmek istiyorum: $\square$. Bu kutucuk kanıtların sonuna konulan bir imzadır. Kanıtın bittiğini ifade etmek için kullanılır. Belki de bu işaret sadece bir sonu değil, aynı zamanda bir zafer ilanını temsil ediyordur. Eski kitapları ya da makaleleri karıştırırsanız, kanıtların sonunda genellikle Latince *quod erat demonstrandum* ifadesinin baş harflerinden oluşan Q.E.D. ifadesini görürsünüz. Bu ifade, “kanıtlanması gereken şey de buydu” anlamına gelir. Q.E.D. yerine $\square$ sembolünün matematikte ilk kullanımı Paul Halmos’a atfedilir.