# Sayılar Kuramına Giriş

Mustafa Topkara

# İçindekiler

# Bölüm 1

# Sayı sistemleri

Şimdiye kadarki matematik eğitim hayatımız boyunca birçok farklı 'şey' için *sayı* kelimesini kullandık. Her seferinde, bu sayı dediğimiz şeylerin aynı cinsten olanlarını *sayı kümesi* adını verdiğimiz topluluklarda bir araya topladık. Bu sayı kümelerinin en ünlüleri şunlardı:

| | | |
|---|---|---|
| $\mathbb{N}$ | Doğal sayılar | $0, 1, 2, 3, 4, \ldots$ |
| $\mathbb{Z}$ | Tamsayılar | $\ldots, -2, -1, 0, 1, 2, \ldots$ |
| $\mathbb{Q}$ | Rasyonel sayılar | örn. $8$ , $-\frac{1}{2}$ , $\frac{3}{7}$ |
| $\mathbb{R}$ | Gerçel sayılar | örn. $\frac{6}{7}$ , $\sqrt{5}$ , $\frac{\pi}{4}$ |
| $\mathbb{C}$ | Karmaşık sayılar | örn. $\sqrt{2}$ , $2+3i$ , $\frac{3}{5}-\sqrt{2}i$ |

Ayrıca bu listedeki sayı kümelerinin her birinin kendinden öncekileri içerdiğini de gördük: bir tamsayı her zaman aynı zamanda bir rasyonel sayıydı, bir gerçel sayı her zaman bir karmaşık sayıydı... Yani özetle:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \ .$$

Peki bu kadar birbirinden farklı 'şey'lerin hepsi için *sayı* kelimesini kullanmamımızın, birbirine çok da benzemeyen bütün bu kümelere sayı kümesi dememizin nedeni nedir?

Bu soruya hakkıyla cevap verebilmek için önemli bir noktayı hatırlamamız gerekiyor: bu kümeleri neredeyse hiçbir zaman tek başlarına dü-

şünmüyoruz aslında. Her zaman, bu kümeler üzerinde tanımlı *işlemleri* de bu kümelerle birlikte hayal ettik ve öğrendik. Her bir küme için temel işlemlerimiz toplama ve çarpma ile, bu işlemlerin bir bakıma tersi olarak düşünülebilecek çıkartma ve bölme işlemleri; bu sayı kümelerin hepsinin üzerinde yukarıdaki içerme ilişkisi ile en azından tanımlı oldukları durumlarda uyumlu olarak mevcut: doğal sayılarda $4 \times 3$ işlemi 12 doğal sayısını verirken 4 ve 3 gerçel sayılarini çarptığımızda da bu sefer 12 gerçel sayısına sonuç olarak ulaşıyoruz. Bu kümeleri üzerindeki işlemlerle birlikte düşündüğümüzde *sayı sistemi* olarak adlandıracağız.

Her ne kadar bu sayı sistemleri uyumlu işlemlere sahip olsalar da en yaygın kullanımlarında anlamları büyük değişiklikler gösterir:

- Doğal sayıların temel kullanımı nesnelerin sayısını vermektir. (Matematiksel olarak, sonlu kümelerin büyüklüklerine karşılık gelirler.) Yine bir diğer temel kullanımları sıralama işlemindedir: bir yarışı kaçıncı bitirdiğinizi doğal sayılarla belirtirsiniz.
- Negatif sayılar ile doğal sayıları tamamlayarak tamsayıları elde ederiz ve artık eksilmeyi de sayılarla ifade edebilir, tutarlı bir şekilde çıkartma yapabiliriz.
- Rasyonel sayılar temel olarak parçalı büyüklükleri ve oransal büyükleri ifade etmemizi mümkün kılar.
- Gerçel sayılarla rasyonel sayıların 'aralarını tamamlarız' ve artık uzunlukları ve diğer geometrik büyüklükleri sayılarla ifade edebiliriz.
- Karmaşık sayıların birçok kullanımı olmakla birlikte, belki de en doğrudan gözlenebileni tüm polinomların kökünün var olmasını, bu sayede bütün polinomların lineer çarpanlara ayrılmasını sağlamasıdır.

Gördüğümüz üzere, sayı sistemleri pek çeşitli işlevleri yerine getirirler. Bu sistemler arasında doğal sayılar, diğerlerine zemin oluşturan kurucu bir işleve sahiptir. Tamsayılar, neredeyse doğal sayıların sadeliğine sahip

olmakla birlikte önemli bir işlemsel eksiği de kapatır. Ayrıca tamsayılar, rasyonel sayıları anlamanın da temelini oluşturur.

Bu derste ağırlıklı olarak bu üç sayı sistemi üzerinde duracağız ve tamsayılar nasıl küme olarak diğer ikisinin ortasında kalıyorsa burada da bu sayı sistemlerini anlama yolunda merkezi bir rol üstlenecek. Çalışmalarımızın önemli bir kısmını tamsayılar üzerinde geçekleştireceğiz.

***Soru* 1.** Sayı kavramı bu sistemler ile kısıtlı mıdır?

# Bölüm 2

# Tamsayılar sistemi ve temel özellikleri

## 2.1 İşlemler

Tamsayılar sistemi üzerindeki işlemler, şu temel özelliklere sahipler:

**i.** *Toplamanın bileşme özelliği*. İlk özelliğimiz, özetle birkaç sayıyı toplarken güvenle parantez kaydırma yapabileceğimizi, dolayısıyla toplamalar arasında işlem sıralamasını değiştirebileceğimizi söylüyor:
Her $a, b, c \in \mathbb{Z}$ için $a + (b + c) = (a + b) + c$.

**ii.** 0, toplamada *etkisiz eleman*dır:
Her $a \in \mathbb{Z}$ için $a + 0 = 0 + a = a$.

**iii.** Her elemanın *toplamsal ters*i vardır:
Her $a \in \mathbb{Z}$ için öyle bir $b \in \mathbb{Z}$ vardır ki $a + b = b + a = 0$.
(bu $b$ sayısı $-a$ olarak gösterilir.)

**iv.** Toplama işlemi *değişmeli*dir:
Her $a, b \in \mathbb{Z}$ için $a + b = b + a$.

Soyut cebir dilinde ilk üç özellik, tamsayıların toplama işlemi ile bir *grup* oluşturduğu anlamına gelir. Dördüncü özellik eklendiğiyse bu yapı bir *abelyan grup* olarak isimlendirilir. Aşağıda, tamsayılar üzerinde çarpmanın sahip olduğu özelliklerle devam edeceğiz:

**v.** *Çarpmanın bileşme özelliği:*
Her $a, b, c \in \mathbb{Z}$ için $a(bc) = (ab)c$.

**vi.** *Çarpmanın toplama üzerinde dağılma özelliği* ile çarpma ve toplama işlemlerini birbiriyle nasıl ilişkilendiğini görüyoruz:
Her $a, b, c \in \mathbb{Z}$ için $a(b + c) = ab + ac$ ve $(a + b)c = ac + bc$.

**vii.** *Çarpmanın değişme özelliği:*
Her $a, b \in \mathbb{Z}$ için $ab = ba$.

**viii.** *Çarpımsal birim eleman:* Her $a \in \mathbb{Z}$ için $1a = a$

**ix.** Her $a, b \in \mathbb{Z}$ için, eğer $ab = 0$ ise $a = 0$ veya $b = 0$ sağlanır.

İlk sekiz özellik birlikte düşünüldüğünde bize soyut cebir dilinde tamsayıların toplama ve çarpmaya göre *birim elemanlı değişmeli halka* olduğunu söyler. Ek olarak, son ve dokuzuncu özellik de sağlandığından soyut cebirde tamsayılar sistemi bir *tamlık bölgesi* olarak adlandırılır. Bu kavramların üzerinde bu derste durmayacağız, cebir derslerinde bu özellikler ve adlandırmalar derinlemesine tartışılacak. Biz ise bu özellikleri sadece dersin bu noktasında bir arada listeliyoruz ve sayı kuramı ile uğraşırken bu özellikleri ispatlarda ve heaplamalarda güvenle kullanabileceğimizi kendimize hatırlatıyoruz.

Bu noktada, tamsayılar sisteminde her sayının çarpımsal tersin varolmadığına da dikkat çekelim. Bu nedenle tamsayılar üzerinde bölmeyi bir işlem olarak göremiyoruz, fakat tamsayılar üzerinde farklı tür ve ilginç özelliklere sahip (eğitimimizin önceki dönemlerinde *kalanlı bölme* adını da verdiğimiz) bir çeşit bölmeyi daha sonra inceleyeceğiz.

Toplama ve çarpmayla ilgili kimi özellikler bu yukarıdaki temel özelliklerlerden çıkarsanabilir. Örnek olarak, şimdi iki özelliği ispatlayalım.

**Önerme 2.1.** *Tamsayıların toplamsal tersi tektir. Bir başka deyişle, Madde iii'teki eşitlikleri sağlayan tek bir b sayısı vardır.*

***Kanıt.*** Verilen bir $a$ tamsayısı için $b$ ve $c$ tamsayıları

$$a + b = b + a = 0$$
$$a + c = c + a = 0$$

eşitliklerini sağlıyor olsun. Bu durumda,

$$a + b = a + c$$

olur. İki tarafa soldan b eklersek

$$b + (a + b) = b + (a + c)$$

elde edilir. Şimdi, Madde i ile

$$(b + a) + b = (b + a) + c$$
$$0 + b = 0 + c$$

elde ederiz. Burada da Madde ii kullanarak

$$b = c$$

sonucuna ulaşırız, ki ispatlamaya çalıştığımız şey de buydu. □

Bir $a$ sayısının toplamsal tersi $-a$ olarak gösterilir. Her sayının tek bir toplamsal tersi olduğundan, çıkartma işlemini toplamayı kullanılarak herhangi $a, b$ tamsayıları için şöyle tanımlarız:

$$a - b := a + (-b)\ .^{1}$$

Bu açıdan, çıkartma işlemi toplamaya göre ikincildir: Toplama aracılığıyla ve toplamanın özellikleri kullanılarak tanımlanabilir.

[1] Burada := sembolü tanım vermek için kullanılıyor. Bu sembolü kullandığımızda, sol taraftaki ifadeyi sağ taraftaki olarak tanımlıyoruz demektir.

***Soru* 1.** Her $a \in \mathbb{Z}$ için $-a = (-1)a$ olduğunu ispatlayın.

***Soru* 2.** Her $a \in \mathbb{Z}$ için $-(-a) = a$ olduğunu ispatlayın.

**Önerme 2.2.** *Her $a \in \mathbb{Z}$ için*

$$0a = 0$$

*sağlanır. (Bir diğer deyişle,* 0 çarpımsal yutan eleman*dır.)*

***Kanıt***. Bir $a$ tamsayısı alalım. Bu durumda,

$$\begin{aligned} 0 &= 0 + 0 \\ 0a &= (0 + 0)a \\ 0a &= 0a + 0a \\ 0a - 0a &= (0a + 0a) - 0a \\ 0 &= 0a + (0a - 0a) \\ 0 &= 0a + 0 = 0a \end{aligned}$$

sonucu elde edilir. □

***Soru* 3.** Önerme 2.2'nin yukarıdaki ispatında, tamsayılar sisteminin özelliklerinin hangileri hangi aşamalarda kullanıldı?

## 2.2 Sıralama

Tamsayıları sadece işlemlerle değil, ayrıca aralarında bir sıralama ilişkisi içinde görmeye alışığız. Tamsayılarda eşitsizlikleri $\leqslant$ sembolüyle göstereceğiz ve *küçük-eşittir* olarak okuyacağız. Önce, sıralamanın yönünü belirleyen çok basit bir kabulü burada not edelim:

- $0 \leqslant 1$.

Şimdi bu sıralamanın temel özelliklerini de burada listeleyelim:

I. Her $a \in \mathbb{Z}$ için $a \leqslant a$. *(Yansıma)*

II. Her $a, b \in \mathbb{Z}$ için eğer $a \leqslant b$ ve $b \leqslant a$ ise $a = b$. *(Antisimetri)*

III. Her $a, b, c \in \mathbb{Z}$ için, eğer $a \leqslant b$ ve $b \leqslant c$ ise $a \leqslant c$. *(Geçişkenlik)*

Herhangi bir ilişkinin matematikte *sıralama* adını hak etmesi için zaten bu üç özelliği sağlaması gerekir.

Burada eşitsizliğin *kapsayıcı* halini, yani eşitliğe de izin veren halini kullandık. Eşitsizliğin *dışlayıcı* halini $<$ ile göstereceğiz ve '*küçüktür*' olarak okuyacağız. Eşitsizliğin dışlayıcı halini, kapsayıcı halini kullanarak şöyle tanımlayabiliriz: Her $a, b \in \mathbb{Z}$ için eğer

$$a \leqslant b \text{ ve } a \neq b$$

ise $a < b$ olsun.

***Soru* 4.**

$$a < b \iff \neg(b \leqslant a)$$

olduğunu ispatlayın.

Sıradaki özellik, bir tamsayıya 1 eklersek *ardışık* tamsayıyı elde edeceğimizi söylüyor, yani verilen bir tamsayı ve ve bu sayının 1 fazlası arasında başka bir tamsayı olmadığını:

IV. Her $m \in \mathbb{Z}$ için, $m < n < m + 1$ eşitsizliği her $n \in \mathbb{Z}$ tamsayısı için yanlıştır.

Bu özelliği matematiğin sembolik dilinde şöyle de yazabiliriz:

$$\forall m \in \mathbb{Z},\ \forall n \in \mathbb{Z}\ \neg(m < n < m + 1)$$

Burada $\neg$ sembolü, 'değil' anlamındadır, yani kendisinden sonra gelen ifadenin mantıksal tersini alır, o ifadenin yanlış olduğunu söyler. Sıradaki özellikler, sıralama ve tamsayılar üzerindeki işlemler arasındaki ilişkilerle ilgili:

V. Her $a, b, c \in \mathbb{Z}$ için, eğer $a \leqslant b$ ise $a + c \leqslant b + c$.

VI. Her $a, b \in Z$ için, eğer $a, b > 0$ ise $ab > 0$.

***Soru* 5.** $-1 \leqslant 0$ olduğunu gösterin.

***Soru* 6.** Her $a$ tamsayısı için

$$a \geqslant 0 \iff -a < 0$$

olduğunu gösterin.

**Önerme 2.3.** *Her $a, b, c \in Z$ için,*

***(a)*** *Eğer $c > 0$ ise; $a \leqslant b$ ancak ve ancak $ac \leqslant bc$ ise.*

***(b)*** *Eğer $c < 0$ ise; $a \leqslant b$ ancak ve ancak $bc \leqslant ac$ ise.*

***Kanıt.*** **(a).** İspatlamamız gereken iddiayı sembolik dilde yazalım:

$$\forall a, b, c \in \mathbb{Z}\ [c > 0 \implies (a \leqslant b \iff ac \leqslant bc)].$$

Başka bir deyişle; eğer $c$ pozitif ise $a, b$ ve $c$ tamsayıları için $a \leqslant b$ koşulu ile $ac \leqslant bc$ koşulunun mantıksal olarak birbirine denk olduğunu, yani biri doğru olduğunda diğerinin de doğru olduğunu göstermeliyiz. Böyle çift yönlü gerektirmeleri ispatlamanın yaygın bir yolu, çift yönlü gerektirmenin iki yönünün doğruluğunu ayrı ayrı göstermektir:

- *Düz yön ($\implies$):* Eğer $a \leqslant b$ ise $ac \leqslant bc$.
- *Ters yön ($\impliedby$)*: Eğer $ac \leqslant bc$ ise $a \leqslant b$.

$a, b, c \in \mathbb{Z}$ ve $c > 0$ olsun. Sırayla bu iki yönü ispatlayalım:

( $\Longrightarrow$ ). Eğer $a \leqslant b$ olduğuğnu kabul edersek

$$\begin{aligned} 0 &\leqslant b - a \\ 0 &\leqslant (b-a)c \\ 0 &\leqslant bc - ac \\ ac &\leqslant bc \end{aligned}$$

sonucuna ulaşırız.

( $\Longleftarrow$ ). Şimdi de $ac < bc$ doğru kabul edelim. Bu koşul altında, $a < b$ olmak zorunda olduğunu göstermek istiyoruz. *Çelişkiyle ispat* (bir diğer adıyla *olmayana ergi*) yöntemini kullanmak üzere, bu önermenin yanlış olduğunu varsayalım: $a < b$ yanlış olsun, yani $b \leqslant a$ olsun. [2]

Bu durumda, $b \leqslant a$ eşitsizliğinden,

$$\begin{aligned} 0 &\leqslant a - b \\ 0 &\leqslant (a-b)c \\ 0 &\leqslant ac - bc \\ bc &\leqslant ac \end{aligned}$$

sonucuna ulaşırız, bu da apaçık bir şekilde $ac < bc$ kabulüyle çelişir. Dolayısıyla, $a < b$ *varsayımının yanlış oluğu* varsayımının çekişkiye yol açtığı sonucuna ulaşırız. Sonuç olarak, $a < b$ olduğunu çelişkiyle ispat yöntemiyle göstermiş olduk.

**(b)**. Egzersiz.

***Soru 7.*** Önerme 2.3 (b) şıkkını ispatlayın.

□

[2] Eğer bu varsayım bizi apaçık bir yanlışa sürüklerse, bunun tek bir sebebi olabilir: $a < b$ 'nin yanlış olduğu varsayımımızın yanlış olması. Dolayısıyla, bu varsayımın yanlış olduğunu göstererek $a < b$ eşitsizliğinin doğru olduğunu göstermiş oluruz.

# Bölüm 3

# Doğal sayıların iki önemli özelliği

## 3.1 Matematiksel tümevarım ilkesi

Belirsiz bir doğal sayıyı $n$ harfi ile gösterelim; yani $n$, herhangi bir doğal sayı değeri alabilsin.

Bu belirsiz $n$ doğal sayısı ile ilgili bir önermeyi $P$ ile gösterelim.[1] Örneğin $P$ önermesi, bu sayının çift olup olmadığıyla ilgili olsun:

$$P(n) : n \text{ bir çift sayıdır.}$$

Bu haliyle bu $P$ önermesinin doğru ya da yanlış olduğuyla ilgili bir şey söylenemez. Eğer $P$ yerine sayı değerleri koyarsak doğru ya da yanlış önermeler elde ederiz:

$$\begin{aligned}
P(1) &: 1 \text{ bir çift sayıdır.} && \rightarrow \text{ yanlış} \\
P(2) &: 2 \text{ bir çift sayıdır.} && \rightarrow \text{ doğru} \\
P(3) &: 3 \text{ bir çift sayıdır.} && \rightarrow \text{ yanlış} \\
P(4) &: 4 \text{ bir çift sayıdır.} && \rightarrow \text{ doğru} \\
&\vdots && \vdots
\end{aligned}$$

[1] Daha doğrusu, bu haliyle $P$ bir önerme değil formüldür, $n$ yerine bir sayı koyduğumuzda önerme haline gelir

Ya da $n$ belirsizini bir niceleyici ile ($\forall$ ya da $\exists$ ile) *bağlayarak* doğruluk değerine sahip bir önerme elde edebiliriz:

$\forall n \in \mathbb{N}\ P(n)$ : Her $n$ tamsayısı için $n$ çift sayıdır. $\rightarrow$ yanlış

$\exists n \in \mathbb{N}\ P(n)$ : Bir $n$ tamsayısı vardır ki $n$ çift sayıdır. $\rightarrow$ doğru

İlk önerme her tamsayının çift olduğunu iddia ediyor, ki bu yanlıştır. İkinci önermeyse en az bir tamsayının çift olduğunu iddia ediyor, ki bu doğrudur.

Matematikte bildiğimiz özdeşliklerin önemli bir bölümü aslında "Her $n$ için $P(n)$" formundadır. Örneğin, 0'dan $n$'e kadar olan sayıların toplamının $\frac{n(n+1)}{2}$ olduğunu söylerken [2] asıl kastettiğimiz bunun *her* $n$ doğal sayısı için doğru olduğudur, yani

$$\forall n \in \mathbb{N} \quad 0 + 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

olduğudur. Burada, her bir $n$ doğal sayısı için ayrı ayrı değerlendirebileceğimiz

$$P(n) : 0 + 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

önermelerinin *hepsinin, her bir n doğal sayısı için* doğru olduğu iddiası vardır. Bu tür önermeleri ve özdeşlikleri ispatlamak için *matematiksel tümevarım* yöntemi oldukça yararlıdır. Önce bu ilkeyi formüle edelim:

**Matematiksel Tümevarım İlkesi.** Her $n$ doğal sayısı için $P(n)$ önermesi verilsin. Eğer

i. $P(0)$ doğru ise, ve

ii. Her $k \in \mathbb{N}$ için, $P(k)$ doğru olduğunda $P(k+1)$ doğru ise [3]

her $n$ doğal sayısı için $P(n)$ doğrudur.

[2] Dikkat edin, bu ifade pozitif $n$ tamsayıları için 1'den $n$'ye kadar sayıların toplamının $\frac{n(n+1)}{2}$ olması ile denktir!

[3] Yani, sembolik olarak yazarsak: $\forall k \in \mathbb{N}\ \ P(k) \implies P(k+1)$.

Yukarıdaki ilk maddeye *taban durum*, ikinci maddeye ise *gerektirme adımı* da denir. Sebebi, ilk maddedeki taban durumundan başlayıp ikinci maddedeki gerektirme adımlarıyla bütün doğal sayı basamaklarını aşağıda açıklandığı gibi tırmanmamızdır.

Matematiksel tümevarımın çalışma prensibi şu şekildedir: Taban durum zaten bize $P(0)$'ın doğru olduğunu söylüyor. Gerektirme adımı ise her $k$ doğal sayısı için "$P(k)$ doğruysa $P(k+1)$ doğrudur" diyor. Bu ifadeyi $k = 0, 1$ ve 2 için yazalım:

$P(0)$ doğruysa $P(1)$ doğrudur.
$P(1)$ doğruysa $P(2)$ doğrudur.
$P(2)$ doğruysa $P(3)$ doğrudur.
$\vdots$

Bu durumda, $P(0)$'ın doğru olduğunu bildiğimizden ilk satırı kullarak $P(1)$'in doğru olduğu sonucuna ulaşırız. Fakat şimdi de de $P(1)$'in doğru olduğunu bildiğimizden ikinci sayırı kullarak $P(2)$'nin de doğru olduğu sonucunu elde ederiz. Fakat bu da üçüncü satırdaki gerektirmeyi kullandığımızda bize $P(3)$'ün doğru olduğunu verir. Böyle devam ederek bütün $n$ doğal sayıları için $P(n)$ önermesinin doğru olması gerektiğini görüyor musunuz? Taban durum, bize en baştaki, sıfırıncı önermenin doğru olduğunu söyledi; gerektirme adımı ise bu *doğruluğu* her bir $P(k)$ önermesinden bir sonrakine taşıyarak bütün $P(n)$ önermelerine yayılmasını sağladı.

Tümevarımın nasıl kullanıldığını bir örnek üzerinden görelim:

**Önerme 3.1.** *Her $n$ doğal sayısı için, 1'den $2n+1$'e kadar tüm tek sayıların toplamı $(n+1)^2$ olur.*

***Kanıt.*** Önce bir $n$ doğal sayısı için $P(n)$ önermesini açıkça yazalım:

$$P(n) : 1 + 3 + 5 + \cdots + (2n+1) = (n+1)^2,$$

ya da toplamsal notasyonu kullanırsak

$$P(n) : \sum_{i=0}^{n} (2i+1) = (n+1)^2.$$

Önce tümevarımın taban durumunu gösterelim:

$$\sum_{i=0}^{0}(2i+1) = 2.0 + 1 = 1 = (0+1)^2$$

olduğundan $P(0)$ doğrudur.

Şimdi de gerektirme adımını ispatlamalıyız. Bunun için, $P(k)$ önermesini doğru kabul ediyoruz. Yani,

$$\sum_{i=0}^{k}(2i+1) = (k+1)^2$$

doğru olsun. Bu durumda;

$$\begin{aligned}
\sum_{0=1}^{k+1}(2i+1) &= 1+3+5+\cdots+(2k+1)+[2(k+1)+1] \\
&= \left[\sum_{i=0}^{k}(2i+1)\right] + (2k+3) \\
&= (k+1)^2 + 2k + 3 \\
&= k^2 + 2k + 1 + 2k + 3 \\
&= k^2 + 4k + 4 \\
&= (k+2)^2 \\
&= [(k+1)+1]^2
\end{aligned}$$

sonucuna ulaşırız, ki bu bize tam olarak

$$P(k+1) : \sum_{0=1}^{k+1}(2i+1) = [(k+1)+1]^2$$

önermesini verir. Böylece gerektirme adımını da ispatlamış olduk.

Sonuç olarak, tümevarım ile her $n$ doğal sayısı için $P(n)$ önermesini ispatlamış olduk. □

Matematiksel tümevarımı rahatlıkla tamsayıların doğal sayılara 'benzeyen' altkümelerine uyarlayabiliriz. Burada benzerlikten kastımız, bu altkümenin 0 yerine başka bir $n_0$ tamsayısından başlaması ve elemanlarının buradan birer birer artarak devam etmesi.

**Teorem 3.2** (Genelleşmiş tümevarım). *Bir $n_0$ tamsayısı verilmiş olsun ve Her $n \geqslant n_0$ tamsayısı için $P(n)$ önermesi verilsin. Eğer*

*i. $P(n_0)$ doğru ise, ve*

*ii. Her $k \geqslant n_0$ tamsayısı için, $P(k)$ doğru olduğunda $P(k+1)$ doğru ise*

*her $n \geqslant n_0$ tamsayısı için $P(n)$ doğrudur.*

***Kanıt.*** (Anafikir) Her $n$ doğal sayısı için $Q(n)$ önermesini

$$Q(n) = P(n + n_0)$$

olarak tanımlayalım. Bu durumda $Q(n)$ önermelerine matematiksel tümevarımı uygularsak istediğimiz sonucu elde ederiz. □

***Soru* 1.** Yukarıdaki ispatı tamamlayın.

Tümevarımın bu versiyonunun koşulları daha esnek olduğundan, sıradaki önermede göreceğimiz gibi birçok durumda doğrudan kullanıma daha uygundur:

**Önerme 3.3.** *Her $n \geqslant 5$ tamsayısı için*

$$2^n > n^2$$

*sağlanır.*

***Kanıt.*** Önce taban durumu kontrol edelim. $n = 5$ için

$$2^5 = 32 > 25 = 5^2$$

olduğundan önerme $n = 5$ için sağlanır.

Şimdi önermenin bir $k \geqslant 5$ tamsayısı için doğru olduğunu, yani

$$2^k > k^2$$

eşitsizliğinin sağlandığını varsayalım ve $k+1$ için gösterelim:

$$\begin{aligned}
2^{k+1} &= 2.2^k \\
&> 2k^2 && \text{(tümevarım varsayımından } 2^k > k^2\text{)} \\
&= k^2 + k^2 \\
&= k^2 + k.k \\
&> k^2 + 3k && (k \geqslant 5 > 3 > 0) \\
&= k^2 + 2k + k \\
&> k^2 + 2k + 1 && (k \geqslant 5 > 1) \\
&= (k+1)^2.
\end{aligned}$$

Böylece gerektirme adımını da ispatlamış oluyoruz.

Sonuç olarak, tümevarımla eşitsizliğin tüm $n \geqslant 5$ tamsayıları için geçerli olduğunu göstermiş olduk. □

## 3.2 İyi sıralama ilkesi

Doğal sayıları, tamsayıların bir altkümesi olarak görebiliriz ve bu durumda tamsayılar üzerindeki sıralama, doğal sayılar üzerinde alışık olduğumuz tam sıralamayı verir.

*Tam* sıralamanın ne anlama geldiğini hatırlayalım: verilen herhangi iki farklı elemanı büyüklük/küçüklük açısından birbiriyle her zaman karşılaştırabiliyoruz ve birinin diğerinden küçük olduğunu söyleyebiliyoruz.

Peki daha çok sayıda eleman arasından hangisinin en küçük olduğuna karar verebilir miyiz? Tam sıralılık ve geçişkenlik ilkelerini kullanarak, tam sıralı herhangi bir sistemde *sonlu* sayıda elemanı olan herhangi bir altkümesinin en küçük elemanını saptayabiliriz. Peki, boş olmayan bir altkümenin *en küçük elemanı* her koşulda bulunabilir mi? Bu konuyu tartışmak için en küçük elemana isim verecek bir tanım yapalım:

**Tanım 3.4.** Üzerinde sıralama olan bir sayı sisteminin $A$ adında bir altkü-

mesini alalım. Eğer bir $m \in A$ sayısı

$$\text{Her } a \in A \text{ için } m \leqslant a$$

koşulunu sağlıyorsa (yani $m$ sayısı $A$ kümesinin bütün elemanlarından küçük-eşit ise) $m$ sayısı $A$ kümesinin *minimum elemanıdır* (ya da kısaca, *minimumudur*) denir ve $m = \min A$ ile gösterilir.

Bir kümenin minimumunun, o kümenin elemanı olması gerektiğine dikkat edelim. Yukarıdaki tartışma ile, tam sıralı bütün sayı sistemleride (yani $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$) *sonlu* altkümelerin minimumlarının var olduğunu gördük. Fakat bu sayı sistemlerinin *bazı* altkümeleri için minimum bulunamayabilir! En basiti, $\mathbb{Z}, \mathbb{Q}$ veya $\mathbb{R}$ kümelerinin tamamını alırsak, bunların minimumları yoktur. Örnek olarak, tamsayılar için bu durumu ispatlayalım:

**Önerme 3.5.** *$\mathbb{Z}$ kümesinin minimum elemanı yoktur.*

***Kanıt***. Çelişkiyle ispat yapmak üzere, $\mathbb{Z}$ kümesinin minimumu olduğunu varsayalım.

$$m = \min \mathbb{Z}$$

olsun. Fakat bu durumda

$$m - 1 < m \text{ ve } m - 1 \in \mathbb{Z}$$

elde ederiz, ki bu da $m$ sayısının $\mathbb{Z}$ kümesinin minimumu olması ile çelişir. Sonuç olarak, $\mathbb{Z}$ sisteminin minimumu yoktur. □

Benzeri ispat ile $\mathbb{Q}$ ve $\mathbb{R}$ kümelerinin de minimumları olmadığını görebiliriz. Buradaki ispatta, $\mathbb{Z}$ kümesinin *alttan sınırlı* olmamasını kullandık: bu sayede kümenin elemanları çok çok küçülebildiğinden minimum elemanın olmadığını gördük. [4]

Peki, bir sayı sisteminde bir küme eğer alttan sınırlı ise her zaman minimumunu bulabilir miyiz? Şimdi göreceğiz ki $\mathbb{Q}$ ve $\mathbb{R}$ sayı sistemlerinde bir altküme alttan sınırlı olsa bile bir minimum bulunmayabilir.

[4] Bir sayı sisteminin $A$ adlı bir altkümesi için, eğer bir $b$ sayısı her $a \in A$ için $b \leqslant a$ şartını sağlıyorsa bu $b$ sayısına $A$ kümesinin bir *alt sınırı* diyoruz. Bir alt sınırı olan kümelere de *alttan sınırlı* diyoruz. Bir alt sınır, minimumun aksine kümenin elemanı olmayabilir.

**Örnek 3.1.** $A = \{x \in \mathbb{Q} : 0 < x < 1\} \subset \mathbb{Q} \subset \mathbb{R}$ kümesinin $\mathbb{Q}$ ya da $\mathbb{R}$ sayı sisteminde minimum elemanı olmadığını görelim.

Çelişkiyle ispat yapmak üzere, $A$ kümesinin bir minimum elemanı olduğunu varsayalım ve bu sayıyı $m \in A$ ile gösterelim. Fakat bu durumda, $0 < m < 1$ ve $m \in \mathbb{Q}$ olduğundan $\frac{m}{2}$ sayısı da

$$0 \leqslant \frac{m}{2} \leqslant 1, \frac{m}{2} \in \mathbb{Q}$$

şartlarını sağlar ve dolayısıyla $A$ kümesinin elemanıdır, fakat aynı zamanda da $\frac{m}{2} < m$ eşitsizliğini sağladığından $m$ sayısının $A$ kümesinin minimum elemanı olduğu varsayımıyla çelişki oluşturur. Böylece, olmayana ergi (çelişkiyle ispat) yöntemiyle $A$ kümesinin bir minimum elemanı olmadığını görüyoruz.

Böylece elimizdeki sayı sistemlerinin kimi altkümelerinin minimumu olmadığını gördük, doğal sayılar dışında! Bir sıralı kümede her altkümenin minimum elemanının varsa o kümeye *iyi sıralı* denir. Aşağıdaki teorem, doğal sayıların iyi sıralı olduğunu söylüyor:

**Teorem 3.6** (İyi sıralama ilkesi)**.** *Doğal sayılar kümesinin boştan farklı her altkümesinin minimumu vardır.*

***Kanıt.*** Doğal sayılar kümesinin boştan farklı bir altkümesini alalım ve bu kümeye $A$ diyelim. Önce ispatı iki duruma ayıralım:

**Durum 1:** $0 \in A$ olsun. Bu durumda $\min A = 0$ olur ve ispat biter.

**Durum 2:** $0 \notin A$ olsun. Çelişkiyle ispat yapmak üzere, $A$ kümesinin bir minimum elemanı olmadığını varsayalım.

Şimdi tümevarım uygulamak üzere, her $n$ doğal sayısı için $P(n)$ önermesini

$$P(n) : \{1, 2, \ldots, n\} \cap A = \varnothing$$

olarak tanımlayalım. Başka bir deyişle, $P(n)$ önermesi bize 0'dan $n$'ye kadar olan hiçbir doğal sayının $A$ kümesinin elemanı olmadığını söylüyor.

Taban durumu,

$$P(0) : \{0\} \cap A = \varnothing$$

olduğundan 0'ın $A$ kümesinin elemanı olmamasına denktir, ki içinde bulunduğumuz durumda bunun doğru olduğunu biliyoruz.

Şimdi gerektirme adımını göstermek üzere $P(k)$ önermesini, yani $A$ kümesinin $0, 1, 2, \ldots, k$ sayılarından hiçbirini içermediğini varsayalım. Bu durumda

$$\{0, 1, 2, \ldots, k, k+1\}$$

kümesinin $A$ kümesi ile boştan farklı kesişmesi ancak $k+1 \in A$ olması durumunda mümkün olurdu. Fakat bu durumda da $\min A = k+1$ olurdu ve bu da $A$ kümesinin minimum elemanı olmadığı varsayımıyla çelişirdi, o yüzden de

$$\{0, 1, 2, \ldots, k, k+1\} \cap A = \varnothing$$

olmak zorunda. Böylece $P(k+1)$ önermesini göstermiş olduk ve gerektirme adımının ispatını tamamladık.

Sonuç olarak, tümevarım ile her $n$ doğal sayısı için $P(n)$ önermesini, yani her $n \in \mathbb{N}$ için $\{1, 2, \ldots, n\} \cap A = \varnothing$ olduğunu gösterdik, fakat bu durumda her $n \in \mathbb{N}$ için $n \notin A \subset \mathbb{N}$ sonucuna da ulaşmış oluruz ki bu da $A$ kümesinin boş küme olduğu anlamına gelir. Fakat en başta $A$ kümesini boştan farklı seçmiştik, dolayısıyla bir çelişkiye ulaştık ve baştaki $A$ kümesinin minimumu olmadığı varsayımının yanlış olduğunu çelişkiyle ispat yöntemiyle göstermiş olduk. □

# Bölüm 4

# Bölünürlük

Bundan sonra, aksi belirtilmediği sürece 'sayı' dendiğinde 'tamsayı' kastedilecek.

Tamsayılarda neredeyse hiçbir sayının [1] çarpımsal tersi yoktur, yani genel olarak bir $d$ tamsayısı verildiğinde

$$1 = m.d$$

denklemini sağlayan $m$ tamsayısı bulunamaz. Bu durumdan kaynaklı olarak tamsayılarda rasyonel sayılarda ya da gerçel sayılarda olduğu gibi bir bölme yoktur. Başka bir deyişle, rastgele $n$ ve $d$ tamsayıları verildiğinde

$$n = m.d$$

denklemini sağlayacak bir $m$ tamsayısı her zaman yoktur. Böyle $m$ tamsayılarının bulunabildiği durumlara bu yüzden ayrı bir isim vereceğiz:

**Tanım 4.1.** Verilen $n$ ve $d$ tamsayıları için, eğer

$$n = m.d$$

denklemi sağlanacak şekilde $m$ tamsayısı varsa $d$ tamsayısı $m$ tamsayısını *böler* denir ve bu durum

$$d \mid n$$

[1] 1 ve -1 dışında

şeklinde ifade edilir.

Bu durum,

- $n$ sayısı $d$ sayısına *bölünür*,
- $d$ sayısı $n$ sayısını *böler*,
- $d$ sayısı $n$ sayısının bir *bölenidir*, ya da
- $n$ sayısı $d$ sayısının bir *katıdır*

şeklide de ifade edilebilir. Eğer bir $d$ sayısı $m$ sayısını bölmüyorsa bu durum $d \nmid n$ şeklinde yazılır.

**Örnek 4.1.** **(a)** $12 = 3.4$ olduğundan 3 ve 4 tamsayıları 12'yi böler. Bu durumu $3 \mid 12$ ve $4 \mid 12$ şeklinde ifade ederiz.

**(b)** Ayrıca $12 = 2.6$ olduğundan $2 \mid 12$ ve $6 \mid 12$ ifadeleri de doğrudur.

**(c)** Fakat $12 = 5.m$ denklemini sağlayacak $m \in \mathbb{Z}$ bulunmadığından 5 sayısı 12'yi bölmez: bunu $5 \nmid 12$ şeklinde ifade ederiz.

Şimdi de bazı temel bölünürlük özelliklerini gözlemleyeceğiz.

**I.** Her sayı kendisini böler ve 1 her sayıyı böler, yani her $n \in \mathbb{Z}$ için $n \mid n$ ve $1 \mid n$.

***Kanıt.*** Her $n$ tamsayısı için $n = 1.n$ olduğundan $n \mid n$ ve $1 \mid n$ sağlanır. □

**II.** Her sayı sıfırı böler, yani her $n \in \mathbb{Z}$ için $n \mid 0$.

***Kanıt.*** Her $n$ tamsayısı için $0 = 0.n$ olduğundan $n \mid 0$ sağlanır. □

Dikkat! Buradan "0 sayısı 0'ı böler" sonucu da çıkmaktadır, fakat yine de "öyleyse 0'ın 0'a bölümü kaçtır?" sorusu sorulamaz. Çünkü, *bölünebilme* iki sayı arasındaki bir *ilişki* (aslında, bir *bağıntı*) olarak tanımlandı fakat daha önce de belirttiğimiz gibi, tamsayılar üzerinde bir bölme işlemi tanımlamadık. Dolayısıyla hiçbir tamsayının bir diğerine bölümünden burada bahsedemiyoruz. [2]

**III.** Eğer bir $n$ tamsayısı için $0 \mid n$ ise $n = 0$ olması gerekir. [3]

***Kanıt.*** Eğer $0 \mid n$ ise $n = 0.m$ olacak şekilde bir $m$ tamsayısı vardır. Fakat önceki bölümde her $m$ sayısı için $0.m = 0$ olduğunu görmüştük. □

**IV.** Eğer $d \mid m$ ve $m \mid n$ ise $d \mid n$.

***Kanıt.*** $d \mid m$ ve $m \mid n$ olduğundan

$$m = d.k \text{ ve } n = m.l$$

eşitliklerini sağlayan $k$ ve $l$ tamsayıları vardır. Buradan

$$\begin{aligned} n &= m.l \\ &= (d.k).l \\ &= d.(kl) \end{aligned}$$

sonucunu elde ederek $d \mid n$ olduğunu görürüz. □

**V.** Eğer $d \mid n$ ve $d \mid m$ ise her $a, b \in \mathbb{Z}$ için $d \mid an + bm$.

***Kanıt.*** $d \mid n$ ve $d \mid m$ olduğundan

$$n = d.k \text{ ve } m = d.l$$

[2] İleride tamsayılar üzerinde ayrı bir çeşit işlem olarak bölmeden bahsedeceğiz fakat o zaman da zaten 0 ile bölmeye izin vermeyeceğiz.

[3] Başka bir deyişle, 0 sadece 0'ı böler.

eşitliklerini sağlayan $k$ ve $l$ tamsayıları vardır. Dolayısıyla

$$\begin{aligned} an + bm &= a(d.k) + b(d.l) \\ &= d.ak + d.bl \\ &= d.(ak + bl) \end{aligned}$$

olduğundan $d \mid an + bm$ sonucuna ulaşırız. □

**VI.** Eğer $d \mid n$ ise her $a \in \mathbb{Z}$ için $ad \mid an$ sağlanır.

***Kanıt.*** Egzersiz. □

***Soru* 1.** Üstteki Özellik **VI.**'yı ispatlayın.

**VII.** Eğer $a \neq 0$ ve $ad \mid an$ ise $d \mid n$.

***Kanıt.*** $a, d$ ve $n$ tamsayıları için $ad \mid an$ olduğunu kabul edelim. Bu durumda

$$an = k.ad$$

olacak şekilde bir $k$ tamsayısı vardır. Öyleyse

$$\begin{aligned} 0 &= a.kd - a.n \\ 0 &= a.(kd - n) \end{aligned}$$

sağlanır. Bu durumda, $a \neq 0$ olduğundan, Kısım 2.1 Özellik **ix.** ile $kd - n = 0$ olması gerektiğini görüyoruz. Bu durumda da $n = k.d$ olduğundan $d \mid n$ sonucuna ulaşırız. □

**VIII.** Eğer $d, n > 0$ ve $d \mid n$ ise $d \leqslant n$ sağlanır.

***Kanıt.*** $d \mid n$ olduğundan bir $k \in \mathbb{Z}$ için $n = k.d$ olur. Şimdi, $0 < d$ ve $0 = 0.d \leqslant k.d = n$ olduğundan Önerme 2.3(a)'nın ters yönünü kullanarak $0 \leqslant k$ sonucuna varırız.

Şimdi de $k \neq 0$ olduğunu olmayana ergi (çelişkiyle ispat) yöntemiyle gösterelim. Eğer $k = 0$ olsaydı $n = k.d = 0.d = 0$ olurdu fakat $n > 0$ olduğundan $n \neq 0$ olduğunu biliyoruz. Sonuç olarak, $k \neq 0$ sonucuna ulaşırız.

Bu durumda $k \geqslant 0$ ve $k \neq 0$ olduğundan $k > 0$ olduğunu görürüz. Aynı zamanda $k \in \mathbb{Z}$ olduğundan $k \geqslant 1$ olduğu sonucuna varıyoruz. Öyleyse

$$\begin{aligned} n &= kd \\ &= [(k-1)+1]d \\ &= (k-1)d + d \end{aligned}$$

eşitliğini elde ederiz. Şimdi, $k-1 \geqslant 0$ ve $d > 0$ olduğundan $(k-1)d \geqslant 0$ olduğunu gözlemleyebiliriz. Bunun sonucu olarak da aradığımız

$$n = \underbrace{(k-1)d}_{\geqslant 0} + d \geqslant d$$

eşitsizliği elde edilir. □

**IX.** $d, n$ tamsayıları için $d \mid n \iff (-d) \mid n$.

***Kanıt.*** ( $\Longrightarrow$ ) $d \mid n$ olsun. Bu durumda bir $m \in \mathbb{Z}$ için $m.d = n$ sağlanır. Buradan da $n = m.d = (-m).(-d)$ eşitliği elde edilir. Bu da bize $(-d) \mid n$ sonucunu verir.

( $\Longleftarrow$ ) Şimdi de $(-d) \mid n$ olduğunu varsayalım. Bu durumda bir $m \in \mathbb{Z}$ için $m.(-d) = n$ sağlanır. Buradan da $n = m.(-d) = (-m).d$ eşitliğini elde ederiz. Bu da bize $(-d) \mid n$ sonucunu verir. □

> ***Soru 2.*** $d, n$ tamsayıları için $d \mid (-n) \iff d \mid n$ olduğunu gösterin.

**X.** Eğer $d \mid 1$ ise $d = 1$ veya $d = -1$.

***Kanıt***. Eğer $d \mid 1$ ise Özellik **III.**'ten $d \neq 0$ olduğunu biliyoruz. İspatı iki duruma ayırarak $d \mid 1$ şartını sağlayan $d$ değerlerini arayalım:

Durum 1: $d > 0$ olsun. Bu durumda Özellik **VIII.** ile $d \leqslant 1$ olduğunu görüyoruz. Dolayısıyla $0 < d \leqslant 1$ olduğundan ve 1 her sayıyı böldüğünden $d = 1$ olması gerektiği sonucuna ulaşıyoruz.

Durum 2: $d < 0$ olsun. Bu durumda Özellik **IX.** ve Durum 1 ile $d \mid 1$ şartının sadece $d = -1$ durumunda sağlandığını görüyoruz. □

***Soru*** **3.** Her $n$ sayısı için $n \mid (-n)$, $(-n) \mid n$ ve $-1 \mid n$ olduğunu gösterin.

# Bölüm 5

# Bölme algoritması

Önceki bölümün başında, tamsayılar üzerinde rasyonel ve gerçel sayı sistemlerdeki anlamıyla bir bölme işlemi olmadığı üzerine tartışmıştık. Bir başka ifadeyle, bize verilen herhangi $a$ ve $b \neq 0$ tamsayıları için

$$a = bq$$

olacak şekilde bir $q$ tamsayının her zaman bulunamayacağını gözlemlemiştik. Bununla birlikte bir 'hata payı' ile birlikte bir çeşit bölmeyi tamsayılarda da yapabiliyoruz. Her ne kadar tamsayılarda 'tam' bir bölme yapamasak da, göreceğiz ki $r$ sayısı 'küçük' olacak şekilde

$$a = bq + r$$

eşitliğini sağlayacak belirli $q$ ve $r$ tamsayıları bulmak her zaman mümkün. Bu sayılar üzerindeki tam şartları ve $r$ sayısının 'küçük' olmasından ne anladığımızı aşağıdaki teoremde netleştireceğiz. Bu bahsedilen $q$ ve $r$ değerlerinin belirlenmesine, ve bu sayıların varlığını ve tekliğini veren teoreme *bölme algoritması*[1] adı verilir. İlkokulda öğrendiğimiz kalanlı bölme, $a$ ve $b$ doğal sayı iken bu $q$ ve $r$ sayılarını bulmak için bir yöntemdi.

**Theorem 5.1** (Bölme algoritması). *Verilen $a$ ve $b$ tamsayıları için $b > 0$ sağlansın. Bu durumda, öyle $q$ ve $r$ tamsayıları vardır ki*

$$a = bq + r \text{ ve } 0 \leqslant r < b$$

[1] ya da, Öklid bölmesi

*sağlanır. Bu özellikleri sağlayan $q$ ve $r$ tamsayıları tektir.*

***Kanıt***. Verilen $a$ ve $b$ tamsayıları için

$$R = \{a - nb : n \in \mathbb{Z}, a - nb \geqslant 0\}$$

kümesini tanımlayalım.

Öncelikle kümenin elemanlarının her biri 0'dan büyük-eşit tamsayılar olduğundan $R \subseteq \mathbb{N}$ olduğunu gözlemliyoruz.

Şimdi de $R$ kümesinin boş olmadığını gösterelim. Bunun için, $a \geqslant 0$ ve $a < 0$ durumlarını ayrı ayrı düşünelim:

- Eğer $a \geqslant 0$ ise $n = 0$ için $a - nb$ sayısı $a - 0b = a \geqslant 0$ şartını sağlayacağından $a \in R$ olur.
- Diğer yandan, eğer $a < 0$ ise $-a > 1$ olduğunu görürüz. İki tarafa 1 eklersek $1 - a > 2 > 0$ olduğu sonucuna ulaşırız. Bu gözleme ek olarak $b > 0$ olduğunu hatırlayarak; $n = a$ için $a - nb$ ifadesinin $a - ab = (1 - a)b > 0$ şartını sağladığı, dolayısıyla $a - ab \in R$ olduğu sonucuna varırız.

Birleştirirsek; hem $a \geqslant 0$ hem $a < 0$ durumunda $R$ kümesinin en az bir elemanı olduğunu gördük, dolayısıyla $R \neq \varnothing$ olduğunu göstermiş olduk.

İyi sıralama ilkesi bize $R$ kümesinin bir en küçük elemanı olduğunu söylüyor. Bu en küçük elemana

$$r = \min R$$

adını verelim. Bu $r$ sayısı $R$ kümesinin bir elemanı olduğundan bir $q$ sayısı için $r = a - qb$ olduğunu biliyoruz. Bu eşitliği

$$a = bq + r$$

biçiminde de yazabiliriz.

Bulduğumuz $r$ sayısı $R \subseteq \mathbb{N}$ kümesinin elemanı olduğundan $r \geqslant 0$ şartını sağlar. Şimdi de $r < b$ olduğunu göstermeliyiz. Çelişkiyle ispat (olmayana

ergi) yöntemini kullanmak üzere $r \geqslant b$ olduğunu varsayalım. Bu durumda $r - b \geqslant 0$ olur. Fakat aynı zamanda $r = a - qb$ olduğundan

$$r - b = a - qb - b = a - (q+1)b$$

sağlanır ve dolayısıyla $r - b \in R$ olması gerektiği görülür. Fakat bu, $r - b < r$ olduğundan $r$ sayısının $R$ kümesinin en küçük elemanı olduğu bilgisiyle çelişir. Sonuç olarak, $r \geqslant b$ varsayının çelişkiye yok açtığını ve dolayısıyla $r < b$ olduğunu göstermiş olduk.

Böylece, aradığımız özelliklere sahip $q$ ve $r$ tamsayılarının varlığını göstermiş olduk. Teoremin ispatını tamamlamak için şimdi de bu özelliklere sahip bu sayılar dışında başkaları olamayacağını göstermeliyiz. Diğer bir ifadesiyle, bu özelliklere sahip sayıların yukarıdaki $q$ ve $r$ sayılarına eşit olmak zorunda olduğunu ispatlamalıyız.

Birtakım $q'$ ve $r'$ sayıları için de

$$a = bq' + r' \text{ ve } 0 \leqslant r' < b$$

şartları sağlanıyor olsun. Bu durumda $r' \in R$ olması gerektiğini görüyoruz. Buradan da, $r = \min R$ olduğundan $r' \geqslant r$, yani $r' - r \geqslant 0$ sonucu çıkıyor. Öyleyse

$$\begin{aligned} bq + r &= bq' + r' \\ bq - bq' &= r' - r \\ b(q - q') &= r' - r \geqslant 0 \end{aligned}$$

sonucunu elde ederiz. Dolayısıyla

$$b \mid r' - r \ , \ b > 0, \ r' - r \geqslant 0$$

özelliklerinin sağlandığını gözlemleyebiliyoruz.

Buradan çelişki yöntemiyle $r' - r = 0$ olduğunu ispatlayacağız. $r' - r \neq 0$ olduğunu varsayalım. Bu durumda $r' - r \geqslant 0$ olduğundan $r' - r > 0$ elde ederiz. Ek olarak $b > 0$ ve $b \mid r' - r$ de sağlandığından Bölüm 4 Özellik **VIII.** ile $b \leqslant r' - r$ sonucuna ulaşırız. Fakat buradan da, $r \geqslant 0$ olduğundan

$$b \leqslant r' - r \leqslant r' < b$$

sonucu çıkar, ki bu da bize $b \neq b$ çelişkisini verir. Sonuç olarak, $r' - r = 0$ olduğunu ispatlamış oluyoruz. Bu da $r' = r$ olduğunu verir.

Bu bilgi ile $bq + r = bq' + r'$ eşitliği $bq + r = bq' + r$ haline gelir. Buradan da

$$\begin{aligned} bq + r &= bq' + r \\ bq - bq' &= r - r \\ b(q - q') &= 0 \end{aligned}$$

eşitliği elde edilir. Buradan da $b \neq 0$ olduğunu bildiğimizden $q - q' = 0$, yani $q = q'$ sonucuna ulaşırız.

Böylece, teoremdeki özellikleri sağlayan $q$ ve $r$ dışında tamsayılar olamayacağını göstermiş olduk. □

# Bölüm 6

# En büyük ortak bölen

Elimizde iki tamsayı varken, bu sayıların ikisinin de böleni olan en büyük tamsayıyı bu iki sayının *en büyük ortak böleni* olarak tanımlayacağız. Fakat daha önce (iyi sıralılık ile ilgili tartışmada) gördük ki bir kümenin en küçük ya da en büyük elemanı her zaman olmayabilir. Bu yüzden, sayıların en büyük ortak bölenini tanımlamak için bu sayının varlığını da garantilecek biraz daha uzun bir yok izleyeceğiz.

Öncelikle, bir $n$ tamsayısı verildiğinde bu sayının *bölen kümesini*

$$\mathcal{B}(n) = \{k \in \mathbb{Z} : k \mid n\}$$

yani o sayının tüm bölenlerinden oluşan küme olarak tanımlayalım. Ayrıca, bir sayının *mutlak değerinin*

$$|m| = \begin{cases} m, & \text{eğer } m \geqslant 0 \text{ ise} \\ -m, & \text{eğer } m < 0 \text{ ise} \end{cases}$$

şeklinde tanımlandığını hatırlayalım. Bölüm 4 içinde gördüğümüz özellikler mutlak değer kavramıyla birleştirildiğinde aşağıdaki sonuç elde edilir. İspatın yazımını okuyucuya bırakıyoruz.

**Sonuç 6.1.** [1] *Her $k, n \in \mathbb{Z}$ için $k \mid n \iff |k| \mid |n|$.*

[1] Matematikte, önceki önerme ve tanımlardan görece rahat bir şekilde elde edilen önermeleri burada yaptığımız gibi *sonuç* (ing. *corollary*) adıyla ifade etmek yaygındır.

***Kanıt.*** Egzersiz. (*İpucu:* Bölüm 4 Özellik **VIII.** ile Özellik **IX.** ve Soru 2 bir araya getirilerek ispat yapılabilir.) □

***Soru* 1.** Sonuç 6.1'i ispatlayın.

**Lemma 6.2.** [2] *Her $n$ tamsayısı için $\mathcal{B}(n)$ sonludur.*

***Kanıt.*** Sonuç 6.1 ile, eğer $k \in \mathcal{B}(n)$ ise $|x| \leqslant |n|$ olduğunu görüyoruz. Bu da bize

$$\mathcal{B}(n) \subseteq \{-|n|, |n|+1, \ldots, -1, 0, 1, \ldots, |n|-1, |n|\}$$

içerme ilişkisini veriyor. Sağdaki küme sonlu olduğundan $\mathcal{B}(n)$ kümesi de sonludur. □

Verilen $m$ ve $n$ tamsayılarının *ortak bölen kümesini*

$$\mathcal{OB}(m,n) := \{k \in \mathbb{Z} : k \mid m, k \mid n\}$$

olarak tanımlayalım. Tanım gereği

$$\mathcal{OB}(m,n) = \mathcal{B}(m) \cap \mathcal{B}(n)$$

olduğunu, dolayısıyla kesişimde $m$ ve $n$ sayılarından en az biri sıfırdan farklı iken kesişimdeki kümelerin en az biri sonlu olduğundan ortak bölen kümesini de sonlu olduğunu görüyoruz.

Her tamsayının 1 ile bölündüğünü biliyoruz. Dolayısıyla her $n$ ve $m$ tamsayı çifti için $1 \in \mathcal{OB}(m,n)$ olduğunu, dolayısıyla ortak bölen kümesinin her zaman boştan farklı olduğunu da biliyoruz.

Tamsayılar kümesinin $S$ adında bir altkümesi verildiğinde eğer bir $M \in S$ sayısı kümenin tüm diğer elemanlarından büyük-eşitse, yani

$$\forall k \in S \quad M \geqslant k$$

[2] Matematik yazımında, kendinden sonraki daha önemli önermelerden önce bu daha önemli önermelerin ispatında kullanılmak üzere ön hazırlık olarak verilen, kendi başına önemi sıklıkla daha az olan önermeler *lemma* olarak isimlendirilir. Türkçe yazımda 'lemma' için bazen *yardımcı önerme* ya da *yardımcı teorem* ifadesi de kullanılır.

özelliğine sahipse bu elemana $S$ kümesinin *maksimumu* denir ve

$$M = \max S$$

ile gösterilir. (Bu tanım üzerinde sıralama olan bütün kümelerde kullanılabilir.)

Tamsayılar kümesinin boştan farklı her sonlu altkümesinin bir *en büyük elemanı* vardır. Bunun ispatını, alınan altkümenin eleman sayısı üzerine tümevarımla ispatlamak mümkün. Bu ispatı egzersiz olarak bırakıyoruz.

***Soru* 2.** Tamsayıların boştan farklı her sonlu altkümesinin bir maksimumu olduğunu gösterin.
(Not: Bu önerme bütün *tam sıralı* kümeler için geçerlidir.)

Böylece, iki tamsayının en büyük ortak bölenini tanımlamakta bir sorun olmadığını görmüş olduk.

**Tanım 6.3.** En az biri sıfırdan farklı $m$ ve $n$ tamsayılarının *en büyük ortak böleni*

$$\text{ebob}(m, n) := \max \mathcal{OB}(m, n)$$

olarak tanımlanır.

Ek olarak, her zaman 1 sayısı ortak bölen kümesinin elemanı olduğundan her zaman

$$\text{ebob}(m, n) \geqslant 1$$

eşitsizliğinin sağlandığını, yani en büyük ortak bölenin her zaman pozitif olduğunu da görüyoruz. Bu nedenle, en büyük ortak bölen bulunmaya çalışırken sadece pozitif bölenleri düşünebiliriz. Ayrıca Bölüm 4 Soru 2 ile, $n$ ve $|n|$ sayılarının bölenleri aynı olduğundan sadece pozitif sayılar için en büyük ortak bölenleri düşünmemiz yeterli olacak.

**Örnek 6.1.** $\text{ebob}(6, 9)$ değerini bulalım. 6'nın pozitif bölenlerinin 1,2,3 ve 6 olduğunu; 9'un pozitif bölenlerinin ise 1,3 ve 9 olduğunu görüyoruz. Bu iki sayının ortak bölenleri 1 ve 3 olduğundan en büyük ortak bölenlerinin

$$\text{ebob}(6, 9) = 3$$

olduğu sonucuna ulaşıyoruz.

Bu örnekteki gibi, elimizdeki sayılar küçükse bu sayıların tüm bölenlerini yazıp en büyük ortak böleni belirlemek zor olmaz. Peki büyük sayılar için daha verimli bir yöntem mevcut mu? Böyle bir yöntemi bir sonraki bölümde, *Öklid algoritması* adıyla göreceğiz.

**Önerme 6.4.** *Verilen $m$ ve $n$ pozitif tamsayıları için*

$$\text{ebob}(m,n) = m \iff m \mid n.$$

***Kanıt.*** ( $\Longrightarrow$ ) $\text{ebob}(m,n) = m$ olsun. Bu durumda tanım gereği $m$ sayısı $n$ sayısının bir bölenidir, dolayısıyla $m \mid n$ sonucuna ulaşırız.

( $\Longleftarrow$ ) $m \mid n$ olduğunu kabul edelim. Bu durumda, $\text{ebob}(m,n) \mid m$ olduğundan Bölüm 4 Özellik **VIII.** ile $\text{ebob}(m,n) \leqslant m$ olduğunu görürüz. Diğer yandan $m \mid m$ ve kabul nedeniyle $m \mid n$ olduğundan $m$ sayısı $m$ ve $n$ sayılarının bir ortak bölenidir, dolayısıyla

$$m \leqslant \max \mathcal{OB}(m,n) = \text{ebob}(m,n)$$

olduğunu da elde ederiz. Bu iki eşitsizliği bir araya getirerek $\text{ebob}(m,n) = m$ olduğu sonucuna varırız. □

İki sayı verildiğinde, her zaman 1 ve -1 sayılarının verilen sayıların ortak böleni olacağını biliyoruz. İki sayının -1 ve 1 dışında ortak böleni olmaması, en büyük ortak bölenlerinin 1 olmasına denk. Bu durumu aşağıdaki tanımda isimlendirelim:

**Tanım 6.5.** Eğer $m$ ve $n$ tamsayıları için $\text{ebob}(m,n) = 1$ ise $m$ ve $n$ sayıları *aralarında asaldır* denir.

Bir $n$ sayısı ve bu sayının böleni olan sıfırdan farklı bir $d$ sayısı verildiğinde,

$$n = x.d$$

denklemini sağlayan tek bir $x$ sayısı vardır (neden?). Bu sayıyı $n$ sayısının $d$ sayısına *bölümü* olarak adlandıracağız ve $n : d$ ile göstereceğiz.

Bir tamsayının diğer bir tamsayıya bölümüyle ilgili şu noktalara dikkat edelim:

– Hiçbir $n$ sayısı için $n : 0$ tanımlı değildir.

– $d$ sayısı sıfırdan farklı olsa da, eğer $d$ sayısı $n$ sayısının bir böleni değilse $n : d$ tanımlı değildir. Örneğin, $5 : 3$ tanımlı değildir.

Aşağıdaki önerme, sayıların en büyük ortak bölenlerinden 'kurtularak' aralarında asal hale getirebileceğimizi söylüyor.

**Önerme 6.6.** *Sıfırdan farklı herhangi iki $m, n$ tamsayısı için, $d = \text{ebob}(m, n)$ olmak üzere $m : d$ ve $n : d$ sayıları aralarında asaldır.*

***Kanıt.*** Öncelikle,

$$m = (m : d).d \text{ ve } n = (n : d).d \tag{6.1}$$

denklemlerinin sağlandığına dikkat çekelim.

Şimdi, bir $e \geqslant 1$ sayısının $m : d$ ve $n : d$ sayılarının bir pozitif ortak böleni olduğunu, yani belli $x$ ve $y$ tamsayıları için

$$m : d = x.e \text{ ve } n : d = y.e$$

denklemlerini sağladığını varsayalım. Bu durumda, bu denklemleri yukarıdaki Denklemler 6.1 ile birleştirirsek

$$m = x.e.d \text{ ve } n = y.e.d$$

denklemlerine ulaşırız. Bunları ise

$$m = (e.d).x \text{ ve } n = (e.d).y$$

şeklinde yeniden yazarak $e.d$ çarpımının $m$ ve $n$ sayılarının bir ortak böleni olduğunu görürüz, dolayısıyla $e.d \leqslant \text{ebob}(m, n) = d$ eşitsizliğini elde ederiz. Diğer yandan, Bölüm 4 Özellik **VIII.** ile $e.d \geqslant d$ sonucuna ulaşırız. Bu iki eşitsizliği birleştirdiğimizde $e.d = d$ sonucuna ulaşırız. Böylece $e = 1$ olduğunu, yani $m : d$ ve $n : d$ sayılarının tek pozitif ortak böleninin 1 olduğunu görürüz. Bu da $m : d$ ve $n : d$ sayılarının aralarında asal olduğu anlamına gelir. □

## 6.1 Bezout Özdeşliği

Elimizde $m$ ve $n$ tamsayıları olsun. Bu sayıların herhangi $x$ ve $y$ sayılarıyla çarpılıp bu çarpımların toplanmasıyla oluşan sayılara, yani belli $x, y \in \mathbb{Z}$ için

$$x.m + y.n$$

biçiminde yazılabilen sayılara $m$ ve $n$ sayılarının *doğrusal bileşimi* [3] denir. Az sonra ispatlayacağımız Bezout özdeşliği, iki sayının en büyük ortak böleninin her zaman bu iki sayının doğrusal bileşimi olarak yazılabileceğini söyler. Örneğin, $\text{ebob}(12, 30) = 6$ olduğunu gözlemleyelim. Bu 6 sayısını 12 ve 30 sayılarının doğrusal bileşimi olarak

$$6 = 3.12 + (-1).30$$

biçiminde yazabiliriz. Bahsi geçen $x$ ve $y$ sayılarının tek bir şekilde belirlenmediğinde dikkat edin: 12 ve 30 için en büyük ortak bölen

$$6 = (-2).12 + 1.30$$

şeklinde de elde edilebilir.

**Teorem 6.7** (Bezout özdeşliği). [4] *Verilen sıfırdan farklı $m$ ve $n$ tamsayıları için*

$$\text{ebob}(m, n) = x.m + y.n$$

*olacak şekilde $x$ ve $y$ tamsayıları vardır.*

***Kanıt***. Elimizdeki $m$ ve $n$ tamsayıları için $S$ kümesini

$$S = \{k.m + l.n \ : \ k, l \in \mathbb{Z},\ k.m + l.n > 0\},$$

yani $m$ ve $n$ sayılarının tüm *pozitif* doğrusal bileşimleri kümesi olarak tanımlayalım. Bu küme pozitif tamsayılardan oluşur, dolayısıyla doğal sayıların bir altkümesidir. Ek olarak $k = m,\ l = n$ için $k.m + l.n$ ifadesi

$$m.m + n.n = m^2 + n^2 > 0$$

[3] ya da, *lineer kombinasyonu.* (ing. *linear combination*)

[4] Bu önerme *Bezout lemması* olarak da isimlendirilir.

şartını sağladığından $m^2+n^2 \in S$ elde ederiz ve $S$ kümesinin boş olmadığını görürüz. Böylece İyi Sıralama İlkesi (Teorem 3.6) ile $S$ kümesinin bir en küçük elemanı olduğunu biliyoruz. Bu elemanı

$$d := \min S$$

olarak tanımlayalım. Bu sayı $S$ kümesinin elemanı olduğundan belli $x, y \in \mathbb{Z}$ sayıları için

$$d = x.m + y.n$$

formundadır. İlerleyen kısımda $d$ sayısının $m$ ve $n$ sayılarının en büyük ortak böleni olduğunu göstererek ispatı tamamlayacağız. Bunun için ilk olarak $d \mid m$ olduğunu gösterelim.

Bölme algoritması (Teorem 5.1) ile

$$m = qd + r, \ 0 \leqslant r < b$$

sağlanacak şekilde $q$ ve $r$ tamsayılarının olduğunu biliyoruz. Buradan

$$\begin{aligned} r &= m - qd \\ &= m - (xm + yn)d \\ &= m - xmd - ynd \\ &= (1 - xd).m + (-y).n \end{aligned}$$

olduğunu, yani $r$ 'nin $m$ ve $n$ sayılarının bir doğrusal bileşimi olarak yazılabileceğini elde ederiz.

Bu durumda, eğer $r$ pozitif olsaydı $S$ kümesinin bir elemanı olurdu, fakat bu mümkün değildir çünkü $r < d$ olduğundan $d = \min S$ sayısının minimalliği ile çelişirdi. Dolayısıyla $r$ sayısı pozitif olamaz. Öyleyse $r \geqslant 0$ olduğundan $r = 0$ olmak zorundadır. Bu ise $m = qd$ eşitliğini, dolayısıyla da $d \mid m$ olduğu sonucunu bize verir.

Yukarıdaki yöntemi $n$ sayısı için tekrarlayarak $d \mid n$ olduğunu da gösterebiliriz. Böylece, $d$ sayısının $m$ ve $n$ sayılarının bir ortak böleni olduğunu görüyoruz.

Şimdi, $m$ ve $n$ sayılarının pozitif ortak böleni olan bir $k$ sayısı alalım. Bu durumda Bölüm 4 Özellik **V.** ile $k \mid x.m + y.n$ olması gerektiğini görüyoruz.

Bu durumda da, yine aynı bölümdeki Özellik **VIII.** ile $k \leqslant d$ sonucuna ulaşırız, ki bu da bize tam olarak $d$ sayısının $m$ ve $n$ sayılarının en büyük pozitif ortak böleni olduğunu, yani

$$\text{ebob}(m, n) = d = x.m + y.n$$

olduğunu verir.

□

**Sonuç 6.8.** *Eğer $d$ sayısı sıfırdan farklı $m$ ve $n$ sayılarının bir ortak böleni ise $d \mid \text{ebob}(m, n)$ sağlanır.*

***Kanıt.*** Egzersiz.

***Soru* 3.** Yukarıdaki ispatı Bezout özdeşliğini kullanarak yapın.

□

**Sonuç 6.9.** *$m$ ve $n$ sayıları aralarında asaldır ancak ve ancak*

$$x.n + y.m = 1$$

*olacak şekilde $x, y \in bZ$ sayıları varsa.*

***Kanıt.*** Egzersiz. □

# Bölüm 7

# Öklid algoritması

Bu bölümde, verilen iki sayının en büyük ortak bölenini belirlemenin bir yöntemini geliştireceğiz. Bezout özdeşliği ile, $m$ ve $n$ tamsayıları verildiğinde

$$x.m + y.n = \text{ebob}(m, n)$$

olacak şekilde $x$ ve $y$ tamsayılarının var olduğunu görmüştük, fakat bu sayıların nasıl bulunacağını hala bilmiyoruz. Öğreneceğimiz yöntem, bu sayıların belirlenmesini de sağlayacak. Yöntemimiz bölme algoritmasına dayanacak. Yöntemin kendisinden önce, bu yöntemin belkemiğini oluşturacak önermeyi ispatlayalım.

**Önerme 7.1.** *Verilen $m$ tamsayısı ve $n > 0$ tamsayısı için $q$ ve $r$ sayıları*

$$m = qn + r, \ 0 \leqslant r < n$$

*şartlarını sağlansın. Bu durumda,*

$$\text{ebob}(m, n) = \text{ebob}(n, r)$$

*sağlanır.*

***Kanıt***. Bir $k$ sayısı $m$ ve $n$ sayılarının bir ortak böleni olsun. Bu durumda

$$r = m - qn = 1.m + (-q).n$$

olduğundan Bölüm 4 Özellik **V.** ile $k$ sayısı, $r$ 'nin de bir bölenidir. Dolayısıyla, $k$ sayısı $n$ ve $r$ sayılarının bir ortak bölenidir.

Diğer yandan, eğer $k$ sayıyı $n$ ve $r$ sayılarının bir ortak böleniyse

$$m = qn + r = q.n + 1.r$$

olduğundan yine aynı özellik ile $k$ sayısı $m$ 'yi böler, dolayısıyla $k$ sayısı $m$ ve $n$ sayılarının bir ortak böleni olur.

Birleştirirsek, $m$ ve $n$ sayılarının ortak bölen kümesi ile $n$ ve $r$ sayılarının ortak bölen kümesinin eşit olduğunu, yani

$$\mathcal{OB}(m,n) = \mathcal{OB}(n,r)$$

olduğunu görürüz. Bu da en büyük ortak bölenlerin eşit olduğu, yani

$$\text{ebob}(m,n) = -max\mathcal{OB}(m,n) = max\mathcal{OB}(n,r) = \text{ebob}(n,r)$$

olduğu sonucunu verir. □

Verilen $m$ ve $n \neq 0$ tamsayıları için, bu sayıların en büyük ortak bölenlerinin bulunmasına yarayan *Öklid algoritmasını* şimdi şu şekilde tarif edebiliriz:

Adım 1. Bölme algoritması ile $m$ sayısını $n$ sayısına bölerek $m = q_0 n + r_1,\ 0 \leqslant r_1 < n$ özelliklerini sağlayan $q_0$ ve $r_1$ sayılarını elde edin. Eğer $r_1 = 0$ ise algoritmayı sonlandırın. Eğer $r \neq 0$ ise Adım 2'ye geçin.

Adım 2. Bölme algoritması ile $n$ sayısını $r_1$ sayısına bölerek $n = q_1 r_1 + r_2,\ 0 \leqslant r_2 < r_1$ özelliklerini sağlayan $q_1, r_2$ sayılarını elde edin. Eğer $r_2 = 0$ ise algoritmayı sonlandırın. Eğer $r_2 \neq 0$ ise Adım 3'e geçin.

Adım 3. Elimizde $r_{i-1}$ ve $r_i$ sayı çifti varken, bölme algoritması ile $r_{i-1}$ sayısını $r_i$ sayısına bölerek $r_{i-1} = q_i r_i + r_{i+1},\ 0 \leqslant r_{i+1} < r_i$ özelliklerini sağlayan $q_i, r_{i+1}$ sayılarını elde edin. Eğer $r_{i+1} = 0$ ise algoritmayı sonlandırın, aksi takdirde Adım 3'ü $r_i$ ve $r_{i+1}$ sayı çifti için tekrarlayın.

Bu algoritma verilen $m$ ve $n > 0$ sayılarına uygulandığında elimizde bölme algoritmasının tekrar tekrar uygulanmasıyla

$$\begin{aligned}
m &= q_0 n + r_1, & 0 < r_1 < n \\
n &= q_1 r_1 + r_2, & 0 < r_2 < r_1 \\
r_1 &= q_2 r_2 + r_3, & 0 < r_3 < r_2 \\
&\vdots & \vdots \\
r_{k-2} &= q_{k-1} r_{k-1} + r_k, & 0 < r_k < r_{k-1} \\
r_{k-1} &= q_k r_k + r_{k+1}, & 0 = r_{k+1}.
\end{aligned}$$

özelliklerini sağlayan

$$n > r_1 > r_2 > r_3 > \cdots > r_{k-2} > r_{k-1} > r_k > r_{k+1} = 0$$

sayılarını elde ederiz. Her bir $r_{i+1}$ sayısı $r_i$ sayısından küçük olduğundan ve her bir $r_i$ sayısı doğal sayı olmak zorunda olduğundan bu sayılar sonlu sayıda adımda, mesela yukarıda gösterildiği gibi bir $k$ doğal sayısı için $k+1$ adımda sonlanmak zorundadır. Bunun ispatını aşağıdaki soru ile egzersiz olarak bırakıyoruz.

***Soru* 1.** Yukarıdaki prosedürde tanımlanan sayılarla, her $i > 0$ tamsayısı için $r_i \leqslant n - i$ olduğunu $i$ üzerine tümevarım ile ispatlayın.
(Bunun sonucu olarak, eğer $r_n$ tanımlı olursa $0 \leqslant r_n \leqslant n - n = 0$ yani $0 = r_n$ olacağını, dolayısıyla algoritmanın en fazla $i = n$ adımda biteceğini görüyoruz.)

Burada bizim açımızdan kritik nokta, Önerme 7.1 ile

$$\begin{aligned}
\text{ebob}(m,n) &= \text{ebob}(n,r_1)\\
&= \text{ebob}(r_1,r_2)\\
&= \text{ebob}(r_2,r_3)\\
&\vdots\\
&= \text{ebob}(r_{k-2},r_{k-1})\\
&= \text{ebob}(r_{k-1},r_k)\\
&= \text{ebob}(r_k,r_{k+1})\\
&= \text{ebob}(r_k,0)\\
&= r_k
\end{aligned}$$

olduğunu gözlememiz. Böylece, algoritmada bulduğumuz son sıfırdan farklı $r_k$ sayısının bize $m$ ve $n$ sayılarının en büyük ortak böleni olduğunu görüyoruz. Şimdi bu algoritmayı bir örnek üzerinde çalıştıralım.

**Örnek 7.1.** Öklid algoritması kullanarak 624 ve 82 sayılarının en büyük ortak bölenini bulalım:

$$\begin{aligned}
624 &= 7.82 + 50\\
82 &= 1.50 + 32\\
50 &= 1.32 + 18\\
32 &= 1.18 + 14\\
18 &= 1.14 + 4\\
14 &= 3.4 + \textcircled{2}\\
4 &= 2.2 + 0\ .
\end{aligned}$$

Böylece, $\text{ebob}(624,82) = 2$ olduğunu göstermiş olduk.

**Örnek 7.2.** Şimdi de Öklid algoritması kullanarak 624 ve 84 sayılarının en

büyük ortak bölenini bulalım:

$$\begin{aligned} 624 &= 7.84 + 36 \\ 84 &= 2.36 + \textcircled{12} \\ 36 &= 3.12 + 0\ . \end{aligned}$$

Bu işlemler sonunda $\text{ebob}(624, 84) = 12$ olduğunu görmüş olduk. Bu bölme algoritması işlemlerini 'tersten işleterek' Bezout özdeşliğindeki katsayıları da belirleyebiliriz:

$$\begin{aligned} \text{ebob}(624, 84) &= 12 \\ &= 84 - 2.36 \\ &= 84 - 2.(624 - 7.84) \\ &= 84 - 2.624 + 14.84 \\ &= (-2).624 + 15.84\ . \end{aligned}$$

***Soru* 2.** Örnek 7.1'deki hesaplamarı kullanarak

$$\text{ebob}(624, 82) = 2 = x.624 + y.82$$

olacak şekilde $x, y \in \mathbb{Z}$ katsayılarını belirleyin.

# Bölüm 8

# Asal sayılar

Bize herhangi bir sayı verildiğinde, o sayının kendisinin ve 1'in her zaman verilen sayının böleni olacağını biliyoruz. Eğer 1'den büyük bir sayının bu sıradan bölenler dışında 'ilginç' bölenleri yoksa bu sayıya özel bir isim vereceğiz.

**Tanım 8.1.** Verilen bir $p > 1$ sayısının 1 ve $p$ dışında pozitif böleni yoksa bu sayıya *asal sayı* denir. Eğer 1'den büyük bir sayı asal değilse o sayıya *bileşik sayı* denir.

İlk birkaç asal sayıyı $2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$ şeklinde listeleyebiliriz.

**Önerme 8.2.** *Bir $n$ sayısı $n > 1$ koşulunu sağlıyor olsun. Bu $n$ sayısı bileşiktir ancak ve ancak $n = kl$ olacak şekilde $k, l > 1$ sayıları varsa.*

***Kanıt.*** Bir $n$ sayısı için $n > 1$ olsun.

($\Longrightarrow$) Eğer $n$ bileşik ise öyle bir $k$ sayısı vardır ki $1 \neq k \neq n$ ve $k \mid n$ sağlanır. Öyleyse bir $l \in \mathbb{Z}$ için $n = kl$ olduğunu görürüz. Ayrıca $k > 0$ ve $kl = n > 0$ olduğundan $l > 0$ olduğunu görürüz. Şimdi, eğer $l = 1$ olsaydı $n = k$ olurdu ve fakat $k < n$ olduğunu bildiğimizden bu mümkün değildir. Öyleyse $l > 0$ ve $l \neq 1$ olduğundan $l > 1$ sonucuna ulaşırız.

( $\Longleftarrow$ ) Eğer $n = kl$ olacak şekilde $k, l > 1$ sayıları varsa $l \neq 1$ olduğundan $k \neq n$ sonucuna ulaşırız. Öyleyse $k$ sayısı $n$ sayısının 1 ve $n$ dışında bir pozitif bölenidir, sonuç olarak $n$ bir asal sayı değildir. Öyleyse, $n > 1$ olduğunu bildiğimizden $n$ bir bileşik sayıdır. □

Bir sayının asal olup olmadığını göstermek genel olarak pek kolay değildir. Asal sayı tanımından yola çıkarak şu yöntemi izleyebiliriz: Bir $n$ sayısı verildiğinde *her* $1 < k < p$ sayısı için $k \mid n$ olup olmadığını (mesela bölme algoritmasını kullanarak) kontrol ederiz. eğer böyle bir $k$ sayısı için $k \mid n$ sağlanıyorsa $n$ sayısı bileşiktir, eğer böyle *hiçbir* $k$ için $k \mid n$ sağlanmıyorsa $n$ asaldır.

Bahsettiğimiz yöntem, bölünürlüğü $n$ sayısından küçük sayıların her biri için teker teker denemeyi gerektirdiğinden özellikle büyük $n$ sayıları için uzun süreler alabilir. Sıradaki önerme bu arayışı görece erkenden sonlandırmamıza yardımcı olur:

**Önerme 8.3.** *Bir $n > 1$ tamsayısı verilsin ve bir $m$ sayısı için $1 < m < n$ ve $m^2 > n$ sağlansın. Bu durumda, $n$ bir asal sayıdır ancak ve ancak $1 < k < m$ şartını sağlayan her $k$ sayısı için $k \nmid n$ ise.*

***Kanıt.*** ( $\Longrightarrow$ ) Bir $n > 1$ sayısı ve $m^2 > n$ şartını sağlayan bir $m > 1$ sayısı alalım, öyle ki her $k \leqslant m$ için $k \nmid n$ sağlansın. Bu koşullar altında $n$ sayısının asal olduğunu göstermek için, $m \leqslant k < n$ şartını sağlayan tüm $k$ sayıları için de $k \nmid n$ olduğunu göstermeliyiz.

Çelişki yöntemiyle ispat yapmak üzere, $m \leqslant k < n$ şartını sağlayan bir $k$ sayısı için $k \mid n$ olduğunu kabul edelim, yani bir sayısı için $n = k.l$ olsun. Böyle bir $l$ sayısının 1'den büyük olması gerektiğini görüyoruz (nasıl?). Eğer bu $l$ sayısı $m$ sayısından büyük-eşit olsaydı

$$n = k.l \underbrace{\geqslant}_{(l \geqslant m)} k.m \underbrace{\geqslant}_{(k \geqslant m)} m.m = m^2 > n$$

eşitsizliğini ve dolayısıyla $n \neq n$ çelişkisini elde ederdik. Fakat $l \leqslant m$ olsaydı da bu durumda önkabulümüz nedeniyle $l \nmid n$ olurdu, ki bu da $n = k.l$

ile çelişirdi. Sonuç olarak, $m < k < n$ şartını sağlayan bütün $k$ sayıları için de $k \nmid n$ olduğunu, dolayısıyla $n$ sayısının asal olduğunu görmüş olduk.

($\Longleftarrow$) Eğer $p$ sayısı asal ise $1 < k < n$ şartını sağlayan her $k$ sayısı için $k \nmid n$ olur. Dolayısıyla $m < n$ olduğundan her $1 < k < m$ sayısı için de $k \nmid n$ sağlanır. □

**Örnek 8.1.** Önerme 8.3 ile 37 sayısının asal olduğunu gösterelim. $37 < 7^2 = 49$ olduğundan bu önerme ile; eğer $1 < k < 7$ şartını sağlayan $k$ sayıları, yani $2, 3, 4, 5, 6$ sayıları 37'yi bölmüyorsa 37 sayısı asaldır. Bölme algoritması ile bu şartı kontrol edelim:

- $37 = 18.2 + 1$ ve $r = 1 \neq 0$ olduğundan $2 \nmid 37$ olduğunu görüyoruz.
- $37 = 12.3 + 1$ ve $r = 1 \neq 0$ olduğundan $3 \nmid 37$.
- Eğer $4 \mid 37$ olsaydı $2 \mid 4$ olduğundan Bölüm 4 Özellik **IV.** ile $2 \mid 37$ olurdu, ki bunun sağlanmadığını gördük.
- $37 = 7.5 + 2$ ve $r = 2 \neq 0$ olduğundan $5 \nmid 37$
- $2 \mid 6$ olduğundan, yukarıda 4 için yapılan açıklama 6 için de geçerlidir, dolayısıyla $6 \nmid 37$.

Böylece 37'nin bir asal sayı olduğunu göstermiş olduk.

**Not.** Gerçel sayıları da tartışmaya dahil ederek önermeyi şu şekilde ifade edebiliriz: "Bir $n > 1$ sayısı asaldır ancak ve ancak $1 < k < \sqrt{n}$ şartını sağlayan her $k$ sayısı için $k \nmid n$ ise." Buradaki $\sqrt{n}$ sayısının genelde tamsayı olmadığına dikkat edelim.

Sıradaki önerme, bir asal sayıyı bir çarpımın böleni olduğundaki davranışı ile sınıflandırmamızı sağlıyor.

**Önerme 8.4.** *Bir $p > 1$ sayısı verilmiş olsun. Bu $p$ sayısı asaldır ancak ve ancak her $m, n \in \mathbb{Z}$ için $p \mid mn$ iken $p \mid m$ veya $p \mid n$ sağlanıyor ise.*

***Kanıt.*** Bir $p > 1$ sayısı alalım.

($\Longrightarrow$) $p$ sayısının asal olduğunu kabul edelim. Herhangi $m, n$ tamsayıları için $p \mid mn$ olsun, yani bir $k$ sayısı için $pk = mn$ sağlansın. Şimdi, ya $p \mid m$ ya da $p \nmid n$ sağlanır. Eğer $p \mid m$ sağlanıyor ise zaten sonuca ulaşmış oluruz.

Diğer yandan, eğer $p \nmid n$ ise $p$ sayısının tek pozitif bölenleri 1 ve $p$ olduğundan ve $p$ sayısı $m$ sayısının böleni olmadığından $\text{ebob}(p, m) = 1$, yani $p$ ve $m$ sayılarının aralarında asal olduğu sonucuna ulaşırız. Bu durumda, Bezout özdeşliği (Teorem 6.7) ile

$$1 = xm + yp$$

olacak şekilde $x, y \in \mathbb{Z}$ sayılarının olduğunu görüyoruz. Bu özdeşliğin iki tarafını da $n$ sayısıyla çarpalım ve $pk = mn$ eşitliğini hatırlayalım:

$$\begin{aligned} n &= n(xm + yp) \\ &= x(nm) + nyp \\ &= xpk + nyp \\ &= p(xk + ny). \end{aligned}$$

Böylece $p \mid n$ olduğunu görmüş olduk ve istediğimiz sonuca ulaştık.

($\Longleftarrow$) Herhangi iki $m, n$ sayısı verildiğinde, eğer $p \mid mn$ ise $p \mid m$ veya $p \mid n$ olsun. Şimdi, $k \mid p$ olmak üzere bir $k > 0$ sayısı alalım, yani bir $l$ sayısı için $p = kl$ olsun. Bu $l$ sayısının da pozitif olduğunu görüyoruz. Bu durumda, $p \mid p = kl$ olduğundan, varsaydığımız özellik nedeniyle $p \mid k$ veya $p \mid l$ olur. Eğer $p \mid k$ ise $p \leqslant k$ olması gerekir, fakat aynı zamanda $k \mid p$ olduğundan $k \leqslant p$ olduğunu da görürüz, böylece $k = p$ elde ederiz. Diğer yandan, eğer $p \mid l$ sağlanıyorsa bu sefer de aynı şekilde $l = p$ olduğunu görürüz. Bu durumda da

$$p = kl = k.p$$

olduğundan $k = 1$ sonucunu elde ederiz. Birleştirirsek, $p$ sayısının rastgele pozitif böleni olan $k$ sayısının 1 veya $p$ olması gerektiğini, dolayısıyla $p$ sayısının asal olduğunu görüyoruz. □

Bu önermenin bir yönü şunu söylüyor: "Eğer bir asal sayı *iki* sayının çarpımını bölüyorsa, bu iki sayıdan birini böler". Aşağıdaki önerme ile bu bilgiyi daha çok sayının çarpımına genelliyoruz.

**Önerme 8.5.** *$p$ bir asal sayı; $a_1, a_2, \dots a_n$ birer tamsayı ve $p \mid a_1 a_2 \dots a_n$ olsun. Bu durumda, $p$ sayısı $a_1, a_2, \dots, a_n$ sayılarından birini böler.*
*(Bir başka deyişle, bir $i \in \{1, 2, \dots, n\}$ için $p \mid a_i$ sağlanır.)*

***Kanıt***. Çarpımda yer alan çarpan sayısı, yani $n$ sayısı üzerine tümevarım kullanacağız. Bir $p$ asal sayısı alalım.

Taban durum. $n = 1$ için: Eğer $p \mid a_1$ ise ispatlanacak bir şey kalmıyor, $p$ sayısı tek çarpan olan $a_1$ sayısını böler.

Gerektirme adımı. Önermenin $n = k$ için doğru olduğunu varsayalım, yani eğer $p$ asalı $k$ tane sayının çarpımını bölüyorsa bu sayılardan birini böldüğünü varsayalım. Şimdi aynı şeyin $k+1$ sayının çarpımı için de doğru olduğunu göstermeliyiz.

$a_1, a_2, \dots, a_k, a_{k+1}$ sayıları için $p \mid a_1 a_2 \dots a_k a_{k+1}$ olsun. Bu durumda

$$p \mid (a_1 a_2 \dots a_k).a_{k+1}$$

olduğundan, Önerme 8.4 ile $p \mid a_1 a_2 \dots a_k$ veya $p \mid a_{k+1}$ olduğunu varsayalım. Eğer $p \mid a_{k+1}$ ise ispatı bitirmiş oluruz. Eğer $p \nmid a_{k+1}$ ise $a \mid a_1 a_2 \dots a_k$ olmalıdır. Fakat bu durumda da gerektirme adımı varsayımıyla bir $i \in \{1, 2, \dots, k\}$ için $p \mid a_i$ sağlanır. Böylece gerektirme adımını da ispatlamış oluruz.

Böylece tümevarım ile önermedeki iddiayı kanıtlamış olduk. □

## 8.1 Aritmetiğin temel teoremi

Bu kısımda göreceğimiz teorem, adından da anlaşılacağı üzere doğal sayıların çarpımsal yapısıyla ilgili büyük öneme sahip: Teoremimiz bize, bütün doğal sayıların asal sayılardan çarpma yoluyla elde edilebileceğini söyleyecek. Yani asal sayıları temel yapı taşları olarak kullanarak bütün doğal

sayıların oluşturulabileceğini, ya da tersinden düşünürsek herhangi bir bir doğal sayıyı asal sayıların çarpımı olarak yazabileceğimizi göreceğiz. Ek olarak, bu tarifin tek olduğunu da ispatlayacağız: yani bir sayıyı doğal sayıların çarpımı olarak yazarken hangi asal sayıların kullanılacağı ve her bir asal sayının sayının kaçar kere çarpımda kullanılacağı da tek bir şekilde belirlenecek.

Bu önemli teoremin ispatı için tümevarımın biraz daha güçlü bir versiyonunu kullanmak işimizi kolaylaştıracak.

**Önerme 8.6** (Güçlü tümevarım)**.** *Bir $n_0$ sayısı verilmiş olsun ve her $n \geqslant n_0$ tamsayısı için $P(n)$ önermesi verilsin. Eğer*

*i. $P(n_0)$ doğru ise, ve*

*ii. Her $m > n_0$ tamsayısı için, $n_0 \leqslant k < m$ şartını sağlayan her $k$ tamsayısı için $P(k)$ doğru olduğunda $P(m)$ doğru ise*

*her $n \geqslant n_0$ tamsayısı için $P(n)$ doğrudur.*

***Kanıt***. Egzersiz. (*İpucu: $Q(n) = P(n_0) \wedge P(n_0+1) \wedge \ldots P(n-2) \wedge P(n-1)$* üzerinde $n \geqslant 1$ için genelleşmiş tümevarım (bkz. Teorem 3.2) uygulayın.) □

Güçlü tümevarımda da, önceki versiyonlarında olduğu gibi ilk şarta taban durumu, ikinci şarta gerektirme adımı diyeceğiz.

Bu noktada, pozitif tamsayılarda bölünürlüğün sıralama benzeri bir özellik gösterdiğini göreceğiz. Sonrasında bu özelliğe ihtiyacımız olacak.

**Önerme 8.7.** *$m$ ve $n$ pozitif tamsayıları için eğer $m \mid n$ ve $n \mid m$ ise $n = m$ sağlanır.*

***Kanıt***. $m, n > 0$ olduğundan, $m \mid n$ olması bize $m \leqslant n$ eşitsizliğini verir. Aynı şekilde $n \mid n$ olduğundan $n \leqslant m$ eşitsizliğini elde ederiz. Birleştirirsek, $m = n$ sonucuna ulaşırız. □

Sıradaki önerme bize asal sayıların 'ilginç bir biçimde' çarpım şeklinde yazılamayacağını söylüyor.

**Önerme 8.8.** *Eğer bir $p$ asal sayısı ve $a_1a_2\dots a_n$ pozitif tamsayıları için $p = a_1a_2\dots a_n$ ise*

- *Bir $i \in \{1,2,\dots,n\}$ için $a_i = p$ olur.*
- *Her $j \neq i, 1 \leqslant j \leqslant n$ için $a_j = 1$ sağlanır.*

***Kanıt***. Önerme 8.5 ile, bir $i, 1 \leqslant i \leqslant n$ için $p \mid a_i$ olması gerektiğini görüyoruz. Diğer yandan, $p = a_1\dots a_{i-1}a_{i+1}\dots a_n.a_i$ olduğundan $a_i \mid p$ olduğunu da görüyoruz. Sonuç olarak, Önerme 8.7 ile $a_i = p$ sonucuna ulaşıyoruz.

Elde ettiğimiz eşitliği kullanarak

$$p = a_1\dots a_{i-1}a_{i+1}\dots a_n.a_i$$
$$p = a_1\dots a_{i-1}a_{i+1}\dots a_n.p$$
$$1 = a_1\dots a_{i-1}a_{i+1}\dots a_n$$

Sonucuna ulaşıyoruz. Her bir $a_1,\dots,a_{i-1},a_{i+1},\dots,a_n$ pozitif olduğundan bu eşitlik bize her bir $j \neq i, 1 \leqslant j \leqslant n$ için $a_i = 1$ olduğunu verir. (Bu gerektirmeyi bir soru olarak okuyucuya bırakıyoruz.)

***Soru* 1.** $b_1, b_2\dots, b_m$ pozitif sayıları için $b_1b_2\dots b_m = 1$ olsun. Bu durumda her $j, 1 \leqslant j \leqslant m$ için $b_j = 1$ olması gerektiğini ispatlayın.

□

Bu önermenin doğrudan bir sonucu olarak asal sayıların diğer asalları çarpımı olarak yazılamayacağını aşağıda elde ediyoruz.

**Sonuç 8.9.** *Eğer bir $p$ asalı ve $p_1, p_2, ..., p_n$ asalları için*

$$p = p_1p_2...p_n$$

*ise $n = 1$ ve $p_1 = p$ olur.*

***Kanıt.*** $p$ asalı verilsin ve $p_1, p_2, \ldots, p_n$ asalları için

$$p = p_1 p_2 \ldots p_n$$

olsun. Öyleyse, Sonuç 8.8 ile biri dışında bütün $p_i$ sayılarının 1'e eşit olması gerektiğini görüyoruz. Fakat her bir $p_i$ asal olduğundan $p_i \neq 1$ olduğunu biliyoruz. Öyleyse tek bir $p_i$ vardır, yani $n = 1$ olur. Bu durumda $p = p_1$ elde ederiz. □

Bir $n > 1$ sayısının $p_1, p_2, \ldots, p_n$ asal ayıları için

$$n = p_1 p_2 \ldots p_n \tag{8.1}$$

biçiminde yazımına o sayının bir *asal çarpan ayrışması* diyelim. Bu durumda, 1'den büyük bir sayının asalların çarpımı olarak yazılabilmesi, bir asal çarpan ayrışması olması ile aynı anlama geliyor. Elbette, bir sayının asal çarpan ayrışmasında asalların yerini değiştirirsek biraz daha farklı görünen bir ayrışma elde ederiz. Örneğin, 12 sayısını

$$12 = 2.2.2 = 2.3.2$$

olarak birbirinden biraz farklı şekillerde asalların çarpımı olarak yazabiliyoruz, fakat iki çarpımda da ikişer tane 2, birer tane 3 kullanıldığını ve aradaki farkın sadece asalların sıralaması olduğunu görüyoruz. Bu yüzden, asal çarpan ayrışmasını asalların aralarında yer değiştirmelerine izin vermeyecek şekilde tarif edeceğiz.

Bir $n > 1$ sayısı alalım. Eğer $p_1, p_2, \ldots, p_s$ asalları ve $q_1, q_2, \ldots, q_t$ asalları için

$$n = p_1 p_2 \ldots p_s, \quad p_1 \leqslant p_2 \leqslant \ldots \leqslant p_s$$
$$n = q_1 p_2 \ldots q_t, \quad q_1 \leqslant q_2 \leqslant \ldots \leqslant q_t$$

koşulları sağlandığında eşitliklerdeki asalların sayısı ve sırasıyla asallar eşitse, yani

$$s = t \text{ ve her } i, 1 \leqslant i \leqslant s \text{ için } p_i = q_i$$

sağlanıyorsa $n$ sayısının asal sayı ayrışması tektir [1] diyeceğiz.

Bir $p$ asalı zaten halihazırda yukarıda Denklem 8.1'deki biçimde yazılmış olarak görülebilir: Çarpımda tek bir asal kullanılmıştır, yani $n = 1$'dir; ayrıca $p_1 = p$ alırız. Yukarıdaki Sonuç 8.9 ile asalların asal çarpan ayrışmasının tek olduğunu görüyoruz. Bunu da kullanarak, ana teoremimizi artık ispatlayabiliriz.

**Teorem 8.10** (Aritmetiğin Temel Teoremi)**.** *1'den büyük her sayısı asal çarpan ayrışması vardır ve bu ayrışma tektir.*

***Kanıt***. Teoremimizi $n \geqslant 2$ sayısının asal çarpan ayrışması üzerine güçlü tümevarım ile yapacağız.

Taban durumu: $n = 2$ sayısı bir asal olduğundan asal çarpan ayrışması vardır. Bu ayrışmanın tek olduğunu da Sonuç 8.9 ile biliyoruz.

Gerektirme adımı: Bir $m > 2$ sayısı alalım ve $2 \leqslant k < m$ şartını sağlayan bütün $k$ sayılarının asal çarpan ayrışmasının var ve tek olduğunu kabul edelim. Bu önkabulle $m$ sayısının da asal çarpan ayrışmasının var olduğunu ve bu ayrışmanın tek olduğunu göstermeye çalışacağız.

Elimizdeki $m$ sayısı ya asaldır ya da bileşiktir. İlk durumda, yani eğer $m$ sayısı asal ise Sonuç 8.9 ile ispat bitmiş olur. Diğer durumu, yani $m$ sayısının bileşik olduğunu kabul edelim.

Söz konusu $m$ sayısının bölen kümesi sonlu olduğundan bu kümenin bir altkümesi olan asal bölenleri kümesi de sonludur, dolayısıyla $m$ sayısının en büyük asal bölenini her zaman seçebilirim. Bu asal en büyük asal böleni $p$ ile gösterelim. Bu durumda, $m$ sayısını bir $k$ sayısı için

$$m = k.p$$

biçiminde yazabiliriz ve bu $k$ sayısının $m$ bileşik olduğundan ve $p > 1$ olduğundan $1 < k < m$ şartını sağladığını görüyoruz. Bu durumda, gerektirme adımı varsayımı gereği $k$ sayısının tek bir asal çarpan ayrışması olduğunu, yani asalların çarpımı olarak belli bir $s$ sayısı için $p_1, p_2, \ldots, p_s$ asal

[1] ya da, *sıralama dışında tektir*

sayılarının çarpımı olarak tek bir şekilde

$$k = p_1 p_2 \dots p_s, \quad p_1 \leqslant p_2 \leqslant \dots \leqslant p_s$$

biçiminde yazılabildiğini biliyoruz. Bu durumda, $m$ sayısının bir asal çarpan ayrışmasını

$$m = k.p = p_1 p_2 \dots p_s.p$$

şeklinde elde ederiz. Bu asal çarpan ayrışmasının tek olduğunu göstermek üzere, $m$ sayısının $q_1, q_2, \dots q_{t-1}, q_t$ asal sayılar olmak üzere

$$m = q_1 q_2 \dots q_{t-1} q_t, \quad q_1 \leqslant q_2 \leqslant \dots \leqslant p_s$$

şeklinde bir asal çarpan ayrışmasını alalım. Bu durumda

$$p \mid m = q_1 q_2 \dots q_{t-1} q_t$$

olduğundan Önerme 8.5 ile bir $i, 1 \leqslant i \leqslant t$ için $p \mid q_i$ olması gerektiği sonucuna ulaşıyoruz. Ayrıca $q_i$ asal ve $p \neq 1$ olduğundan $p = q_i$ olduğunu görüyoruz. Ek olarak, $q_t \mid m$ ve $p$ sayısı $m$ sayısının maksimum asal böleni olduğundan

$$p = q_i \leqslant q_t \leqslant p$$

eşitsizlikleriyle $q_t$ sayısını iki $p$ değeri arasına sıkıştırarak $p = q_t$ eşitliğini elde ediyoruz. Buradan da

$$p_1 p_2 \dots p_s.p = q_1 q_2 \dots q_{t-1} q_t$$
$$p_1 p_2 \dots p_s.p = q_1 q_2 \dots q_{t-1}.p$$
$$p_1 p_2 \dots p_s = q_1 q_2 \dots q_{t-1}$$

Eşitliğin solundaki değerin $m$ ile eşit olduğunu görüyoruz. Böylece $m$ sayısının asal çarpan ayrışmasının tekliğinden

$$s = t - 1 \text{ ve her } i \in \{1, 2, \dots, t-1\} \text{ için } q_i = p_i$$

olduğunu, ve böylece $m$ sayısının asal çarpan ayrışmasının tek olduğunu görüyoruz.

Böylece, gerektirme adımının da ispatını tamamlıyor ve her $n \geqslant 2$ sayısının asal çarpan ayrışmasının tek olduğunu güçlü tümevarım ile göstermiş oluyoruz. □

# Bölüm 9

# Pozitif bölen sayısı ve toplamı

Bu bölümde, bir sayının pozitif bölen kümesiyle ilgili2 iki fonksiyonu inceleyeceğiz. Bir $n$ sayının bölenleri kümesini $\mathcal{B}(n)$ ile gösterdiğimizi hatırlayalım. Bu notasyondan ilham alarak, bir $n$ sayısının pozitif bölenleri kümesini

$$\mathcal{B}^+(n) := \{k \in \mathbb{Z} : k \mid n \text{ ve } k > 0\}$$

şeklinde ifade edeceğiz. Bu kümenin eleman sayısını $\tau(n)$ ile gösterelim, [1] yani

$$\tau(n) := |\mathcal{B}^+(n)|$$

olsun. Bu tanımla $\tau$, sıfırdan farklı tamsayılar kümesinden pozitif tamsayılara bir fonksiyon olarak düşünülebilir. Bir sayı sisteminin sıfırdan farklı elemanlarından oluşan altkümesini o sayı sisteminin adının sağ üstüne bir $*$ sembolü koyarak, pozitif elemanlardan oluşan altkümesini ise $+$ koyarak göstermek yaygındır. Örneğin sıfırdan farklı tamsayılar kümesi $\mathbb{Z}^*$ ile, pozitif tamsayılar kümesi ise $\mathbb{Z}^+$ ile gösterilir. Bu notasyonla $\tau$, $\mathbb{Z}^*$ kümesinden $\mathbb{Z}^+$ kümesine, yani;

$$\tau : \mathbb{Z}^* \to \mathbb{Z}^+$$

formunda bir fonksiyon olarak görülebilir.

[1] buradaki $\tau$ sembolü, yunan alfabesindeki küçük 'tau' harfidir.

**Örnek 9.1.** $n = 72$ sayısını alalım ve $\tau(72)$ sayısının kaç olduğunu hesaplayalım. Önce, bu sayının pozitif bölen kümesinin

$$\mathcal{B}^+ = \{1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72\}$$

olduğunu gözlemliyoruz. Böylece, $\tau(72) = 12$ olduğu sonucuna ulaşıyoruz.

Örnekte gördüğümüz üzere, elimizde 72 gibi görece küçük bir sayı varsa ve pozitif bölenlerini teker teker listelemek kolaysa bu sayının pozitif bölen sayısını buradan elde edebiliyoruz. Peki elimizde 'büyük' bir sayı varsa ne yapabiliriz? Aritmetiğin Temel Teoremi'ne dayanarak geliştireceğimiz bir yöntem ile, eğer verilen bir sayının asal çarpan ayrışmasını biliyorsak bu sayının bütün pozitif bölenleri kümesini tarif etmenin sistematik bir yolunu geliştireceğiz. Böylece, bir açık formülle pozitif bölen sayısını yani $\tau$ değerini hesaplayabileceğiz.

Verilen bir $n$ sayısının pozitif bölenleri ile ilgili bir diğer önemli değer, o sayının tüm pozitif bölenlerinin toplamıdır ve $\sigma(n)$ ile gösterilir [2]. Yukarıdaki $\tau$ için olduğu gibi, $\sigma$ da

$$\sigma : \mathbb{Z}^* \to \mathbb{Z}^+$$

formunda bir fonksiyon olarak düşünülebilir. Toplam sembolünü kullanarak $\sigma(n)$ için

$$\sigma(n) := \sum_{k \in \mathcal{B}^+(n)} k = \sum_{\substack{k|n \\ k>0}} k$$

ifadesini yazabiliriz.

**Örnek 9.2.** Yine $n = 72$ sayısını ele alalım. $\sigma(72)$ değerini

$$\sigma(72) = 1 + 2 + 3 + 4 + 6 + 8 + 9 + 12 + 18 + 24 + 36 + 72$$

şeklinde elle hesaplamak mümkün.

Yine, 'büyük' sayılar için elle teker teker bölenleri belirleyip toplamak çetrefilli bir hal alır. Yukarıdaki $\tau$ fonksiyonu için geliştireceğimizi söylediğimiz yöntem, eğer elimizde ilgilendiğimiz sayının asal çarpan ayrışması

[2] buradaki $\sigma$ sembolü, yunan alfabesindeki küçük 'sigma' harfidir.

varsa bu sayının pozitif bölenler toplamı yani $\sigma$ değeri için de bir formül geliştirmemizi sağlayacak. Fakat yöntemimizi geliştirmek için öncelikle, bir $mn$ çarpımının bölenleri ile $m$ ve $n$ sayılarının bölenleri arasındaki ilişkiyi inceleyeceğiz. Burada elde edeceğimiz sonuçlar, daha sonra $\tau$ ve $\sigma$ fonksiyonlarının hesabı konusunda işimize yarayacak.

## 9.1 Bölenin çarpanlara ayrılması

Bu kısımda şu soruları inceleyeceğiz: bir $k$ sayısı eğer bir $mn$ çarpımını bölüyorsa, $m$ sayısının bir böleni ve $n$ sayısının bir böleni şeklinde çarpanlara ayrılır mı? Başka bir deyişle,

$$u \mid m, v \mid n \text{ ve } k = uv$$

olacak şekilde $u$ ve $v$ sayıları var mıdır? Eğer varsa, bu sayılar tek bir şekilde mi belirlenir? Bir örnek üzerinden bu soruyu inceleyelim:

**Örnek 9.3.** Öncelikle $m = 12, n = 30, k = 20$ sayıları için

$$k = 20 \mid 360 = 12.30 = mn$$

şartının sağlandığını gözlemleyelim. Burada, $k = 20$ sayısını $m = 12$ ve $n = 20$ sayılarının bölenlerinin çarpımı olarak, yani $u \mid m, v \mid n$ ve $k = uv$ olacak şekilde

$$u = 2,\ v = 10 \quad \text{veya} \quad u = 4,\ v = 5$$

olmak üzere iki farklı şekilde ayırabildiğimizi görüyoruz. Yani, aradığımız ayrışma var olmakla birlikte tek değil.

**Örnek 9.4.** Bu sefer, aralarında asal $m$ ve $n$ sayıları alalım: $m = 9$ ve $n = 20$ olsun. Bölen olarak da $k = 15$ sayısını alabiliriz çünkü

$$k = 15 \mid 180 = 9.20 = mn$$

şartı sağlanır. Bu durumda, aradığımız şartlar sağlanacak şekilde $k = 15$ sayısının sadece

$$u = 3, v = 5$$

için $k = 15 = 3.5 = uv$ şeklinde çarpanlara ayrılabildiğini görüyoruz. $mn = 180$ sayısının bütün bölenleri için benzeri ayrışmanın tek bir şekilde var olduğunu deneyerek gözlemleyebilirsiniz.

Üstteki örnekteki durumun bütün aralarında asal $m, n$ sayı çiftleri için sağlanacağını göreceğiz. Fakat öncesinde ihtiyacımız olacak bazı önermeleri ispatlamalıyız.

**Lemma 9.1.** *Verilen $u, v$ ve $k$ sayıları için eğer $u$ ve $v$ aralarında asal ve $u \mid k, v \mid k$ ise $uv \mid k$ sağlanır.*

***Kanıt.*** Verilen $u$ ve $v$ sayıları için $u \mid k$ ve $v \mid k$ olduğundan

$$k = au, \ k = bv$$

olacak şekilde $a$ ve $b$ sayıları vardır. Ayrıca $u$ ve $v$ aralarında asal olduğundan, Bezout özdeşliği ile

$$1 = xu + yv$$

olacak şekilde $x$ ve $y$ sayıları olduğunu biliyoruz. Eşitliğin iki yanını $k$ ile çarparak

$$k = k(xu + yv)$$
$$k = kxu + kyv$$

olduğunu görüyoruz. Burada $k = bv, \ k = au$ eşitliklerini kullanarak

$$k = bvxu + auyv$$
$$k = uv.(xb + ya)$$

eşitliğine ulaşırız, ki bu da bize $uv \mid k$ sonucunu verir. □

**Önerme 9.2.** *Eğer $m$ ve $n$ sayıları aralarında asal ise her $k \in \mathbb{Z}$ sayısı için*

$$\text{ebob}(k, mn) = \text{ebob}(k, m)\,\text{ebob}(k, n)$$

*sağlanır.*

***Kanıt.*** Öncelikle, yazacağımız ifadeleri kısaltmak için

$$d = \text{ebob}(k, mn)$$
$$d_1 = \text{ebob}(k, m)$$
$$d_2 = \text{ebob}(k, n)$$

şeklinde bir isimlendirme yapalım. Bu isimlendirme ile, ispatlamamız gerekenin $d = d_1 d_2$ olduğunu gözlemleyelim. Hem $d$ hem de $d_1 d_2$ pozitif olduğundan, bu sayıların her ikisinin de birbirinin böleni olduğunu göstermek eşit olduklarını göstermek için yeterlidir.

Bezout özdeşliği ile, belli $x_1, y_1, x_2, y_2$ sayıları için

$$d_1 = x_1 k + y_1 m$$
$$d_2 = x_2 k + y_2 n$$

eşitliklerinin sağlanacağını biliyoruz. Bu eşitliklerin her iki tarafını birbiriyle çarparak

$$\begin{aligned} d_1 d_2 &= (x_1 k + y_1 m)(x_2 k + y_2 n) \\ &= x_1 x_2 k^2 + x_1 y_2 kn + x_2 y_1 km + y_1 y_2 mn \\ &= (x_1 x_2 k + x_1 y_2 n + x_2 y_1 m).k + y_1 y_2 .mn \end{aligned}$$

sonucunu elde ederiz. Böylece $d_1 d_2$ sayısının $k$ ve $mn$ sayılarının bir doğrusal bileşimi olduğunu görüyoruz. Bu da Ödev 3 Soru 1'de elde ettiğimiz sonuç ile bize

$$d = \text{ebob}(k, mn) \mid d_1 d_2$$

olduğu sonucunu verir.

Diğer taraftan, $d_1 \mid k = \text{ebob}(k, m)$ ve $d_2 \mid k = \text{ebob}(k, n)$ olduğunu biliyoruz. Ayrıca $m$ ve $n$ aralarında asal olduğundan ve $d_1 \mid m$ ve $d_2 \mid n$ olduğundan $d_1$ ve $d_2$ de aralarında asaldır (neden?). Dolayısıyla Lemma 9.1 ile $d_1 d_2 \mid k$ sonucuna ulaşıyoruz. Ek olarak $d_1 \mid m$ ve $d_2 \mid n$ olduğundan $d_1 d_2 \mid mn$ olduğunu da görüyoruz. Böylece $d_1 d_2$ sayısının $k$ ve $mn$ sayılarının bir ortak bölenidir, yani $d_1 d_2 \in \mathcal{OB}(m, n)$ olur. Bu durumda, Sonuç 6.8 ile aradığımız

$$d_1 d_2 \mid d = \text{ebob}(k, mn)$$

sonucunu elde ediyoruz. □

**Önerme 9.3.** *Eğer $m, n$ ve $k$ pozitif sayıları için $m, n$ aralarında asal ve $k \mid mn$ ise*

$$u \mid m, v \mid n \text{ ve } k = uv$$

*olacak şekilde $u$ ve $v$ pozitif sayıları vardır ve bu sayılar tek bir şekilde belirlenir.*

***Kanıt***. Verilen $m$ ve $n$ sayıları aralarında asal ve $k \mid mn$ olduğundan, Önerme 6.4 ve Önerme 9.2 ile

$$k = \text{ebob}(k, mn) = \text{ebob}(k, m)\,\text{ebob}(k, n)$$

olduğunu görüyoruz. Şimdi, $u$ ve $v$ sayılarını

$$u := \text{ebob}(k, m), \;\; v := \text{ebob}(k, n)$$

olarak tanımlarsak önermedeki $u \mid m, v \mid n$ ve $k = uv$ şartlarının sağlandığını görürüz.

Bu sayıların tek bir şekilde belirlendiğini göstermek üzere, $u'$ ve $v'$ pozitif sayıları için de bu özelliklerin sağlandığını, yani

$$u' \mid m, v' \mid n \text{ ve } k = u'v'$$

olduğunu varsayalım. Bu durumda, $k = u'v'$ eşitliğinden $u' \mid k$ olduğunu görüyoruz. Aynı zamanda $u' \mid m$ olduğundan $u'$ sayısı $k$ ve $m$ sayılarının bir ortak bölenidir, dolayısıyla $u' \mid \text{ebob}(k, m) = u$ sağlanır. Öyleyse $u'$ ve $u$ pozitif olduğundan Bölüm 4 Özellik **VIII.** ile $u' \leqslant u$ sonucuna ulaşırız. Aynı şekilde $v' \leqslant v$ sonucu da elde edilir.

Olmayana ergi yöntemini kullanmak üzere $u \neq u'$ olduğunu varsayalım. Bu durumda $u > u'$ olmalıdır. Fakat bu durumda $v \geqslant v'$ eşitsizliğini de kullanarak

$$k = uv > u'v \geqslant u'v' = k$$

olduğu, yani $k > k$ dolayısıyla da $k \neq k$ olduğu çelişkisine ulaşırız. Dolayısıyla $u = u'$ olmak zorundadır. Benzer şekilde $v = v'$ olduğu da gösterilebilir. □

**Not.** Bu sonuçtaki $u$ ve $v$ sayılarının ispatta görüldüğü üzere

$$u = \text{ebob}(k, m), \;\; v = \text{ebob}(k, n)$$

şeklinde belirlendiğini vurgulayalım.

## 9.2 Asal çarpan ayrışmasından $\tau$ ve $\sigma$ hesabı

Sıradaki teorem, $\tau$ ve $\sigma$ fonksiyonlarının aralarında asal sayı çiftleri için *çarpımsal* olduğunu ifade ediyor:

**Önerme 9.4.** *Eğer $m$ ve $n$ pozitif sayıları aralarında asal ise $mn$ sayısı için $\tau$ ve $\sigma$ fonksiyonlarının değerleri*

$$\tau(mn) = \tau(m)\tau(n) \;\; \textit{ve} \;\; \sigma(mn) = \sigma(m)\sigma(n)$$

*olur.*

***Kanıt***. Önerme 9.3 ile, $m$ ve $n$ sayıları aralarında asal olduklarından

$$\mathcal{B}^+(mn) = \{kl : k \in \mathcal{B}^+(m), l \in \mathcal{B}^+(n)\} \tag{9.1}$$

olduğunu ve bu kümenin elemanlarının $k_1, k_2 \in \mathcal{B}^+(m), \;\; l_1, l_2 \in \mathcal{B}^+(n)$ için

$$\text{eğer } k_1 l_1 = k_2 l_2 \text{ ise } k_1 = l_1, \;\; k_2 = l_2$$

şartını sağlardığını görüyoruz. Dolayısıyla

$$\tau(mn) = |\mathcal{B}^+(mn)| = |\mathcal{B}^+(m)|.|\mathcal{B}^+(n)| = \tau(m)\tau(n)$$

eşitliğinin sağlandığını gözlemliyoruz.

Şimdi de $\sigma(mn)$ değerini hesaplayalım. Bunun için; $a_1, a_2, \ldots, a_s$ değerleri birbirinden farklı, $b_1, b_2, \ldots, b_t$ değerleri birbirinden farklı olmak üzere $m$ ve $n$ sayılarının pozitif bölen kümelerini

$$\mathcal{B}^+(m) = \{k_i : i = 1, 2, \ldots, s\} = \{k_1, k_2, \ldots, k_s\}$$
$$\mathcal{B}^+(n) = \{l_j : j = 1, 2, \ldots, t\} = \{l_1, l_2, \ldots, l_t\}$$

olarak ifade edelim. Bu durumda Denklem 9.1 ile ve çarpmanın toplama üzerinde dağılma özelliğini kullanarak

$$\begin{aligned}
\sigma(mn) = \quad & k_1l_1 + k_1l_2 + \cdots + k_1l_t \\
& + k_2l_1 + k_2l_2 + \cdots + k_2l_t \\
& \quad \vdots \qquad \vdots \qquad\quad \vdots \\
& + k_sl_1 + k_sl_2 + \cdots + k_sl_t \\
= \quad & k_1(l_1 + l_2 + \cdots + l_t) \\
& + k_2(l_1 + l_2 + \cdots + l_t) \\
& \quad \vdots \qquad \vdots \\
& + k_s(l_1 + l_2 + \cdots + l_t) \\
= {} & (k_1 + k_2 + \cdots + k_s)(l_1 + l_2 + \cdots + l_t) \\
= {} & \sigma(m)\sigma(n)
\end{aligned}$$

eşitliğini elde ederiz. □

**Not.** Toplama sembolü ile, yukarıdaki ispattaki hesabı daha sade biçimde

$$\sum_{i=1}^{s}\sum_{j=1}^{t} k_il_j = \left(\sum_{i=1}^{s} k_i\right)\left(\sum_{j=1}^{t} l_j\right)$$

ile ifade edebiliriz.

Üstteki önermeyi çok sayıda aralarında asal sayının çarpımı için genelleyebiliriz:

**Sonuç 9.5.** *Pozitif $n_1, n_2, \ldots, n_t$ sayıları verilmiş olsun. Eğer $1 \leqslant i < j \leqslant t$ şartını sağlayan her $i, j$ çifti için $n_i$ ve $n_j$ aralarında asal ise*

$$\tau(n_1n_2\ldots n_t) = \tau(n_1)\tau(n_2)\ldots\tau(n_t)$$
$$\sigma(n_1n_2\ldots n_t) = \sigma(n_1)\sigma(n_2)\ldots\sigma(n_t)$$

*sağlanır.*

***Kanıt.*** Egzersiz. Her iki eşitlik için de $t \geqslant 2$ üzerinde tümevarım uygulayın. Ayrıca şu önermeyi ispatlayıp kullanmanız gerekecek:
"Eğer $k$ ile $m$ sayıları ve $k$ ile $n$ sayıları aralarında asal ise $k$ ve $mn$ sayıları aralarında asaldır." □

**Lemma 9.6.** *$m$ ve $n$ sayıları aralarında asaldır ancak ve ancak ortak asal bölenleri yoksa.*

***Kanıt.*** ( $\Longrightarrow$ ) $m$ ve $n$ sayıları aralarında asal olsun. Bu durumda, 1 dışında ortak pozitif bölenleri yoktur. Dolayısıyla hiçbir asal sayıl $m$ ve $n$ sayılarının ortak pozitif böleni değildir.

( $\Longleftarrow$ ) "Eğer $m$ ve $n$ sayılarının ortak asal böleni yok ise bu sayılar aralarında asaldır" önermesi yerine buna denk olan *karşıt-ters*ini, yani "Eğer $m$ ve $n$ aralarında asal değil ise bu sayıların ortak asal böleni vardır" ifadesini ispatlayacağız. Bunun için, $m$ ve $n$ sayılarının aralarında asal olmadıklarını kabul edelim. Bu durumda bir $k > 1$ sayısı bu iki sayının bir ortak bölenidir. Aritmetiğin Temel Teoremi ile, $k > 1$ olduğundan bir $p$ asalı için $p \mid k$ olduğunu görüyoruz. Bu durumda, aynı zamanda $k \mid m$ olduğundan bölünürlüğün geçişkenliğinden (Bölüm 4 Özellik **IV.**) $p \mid m$ olduğunu elde ederiz. Aynı şekilde $p \mid n$ de elde edilir. Sonuç olarak, $p$ asalı $m$ ve $n$ sayılarının bir ortak asal bölenidir. □

Sıradaki lemmadaki bir sayının kuvvetleri toplamıyla ilgili özdeşliği herhangi bir $r \neq 1$ gerçel sayısı için

$$1 + r + r^2 + \cdots + r^s = \frac{1 - r^{s+1}}{1 - r}$$

formunda hatırlıyor olabilirsiniz. Biz ise bu bölmeyi, bütün $n \neq 1$ tamsayıları için $n - 1 \neq 0$ ve göstereceğimiz üzere $n - 1 \mid n^{t+1} - 1$ olduğundan, bu şartları sağlayan tamsayılar için tanımlı ":" ile gösterdiğimiz bölme ile yazacağız.

**Lemma 9.7.** *Herhangi bir $n \neq 1$ tamsayısı ve $s > 0$ tamsayısı için*

$$\sum_{i=0}^{s} n^i = 1 + n + n^2 + \cdots + n^s = (n^{s+1} - 1) : (n - 1)$$

*sağlanır.*

***Kanıt.*** Verilen sayılar için şu çarpmayı inceleyelim:

$$\begin{aligned}(1-n)(1+n+n^2+\cdots+n^s) =& 1.(1+n+n^2+\cdots+n^s) - n.(1+n+n^2+\cdots+n^s)\\ =& 1+n+n^2+\cdots+n^s\\ & -n-n^2-\cdots-n^s-n^{s+1}\\ =& 1-n^{s+1}\ .\end{aligned}$$

Buradan $1-n \mid 1-n^s$ olduğunu ve $1-n \neq 0$ olduğundan

$$1+n+n^2+\cdots+n^s = (1-n^{s+1}) : (1-n)$$

sonucunu elde ederiz. Bu da lemmada verilen denklem ile denktir. □

**Sonuç 9.8.** *Verilen bir $p$ asal sayısı ve $s$ pozitif sayısı için $p^s$ sayısında $\tau$ ve $\sigma$ fonksiyonlarının değerleri*

$$\tau(p^s) = s+1 \tag{9.2}$$
$$\sigma(p^s) = (p^{s+1}-1) : (p-1) \tag{9.3}$$

*olur.*

***Kanıt.*** Eğer $m \mid p^s$ ise $m$ sayısının tek asal böleni $p$ olabilir; çünkü bir $q$ asalı için $q \mid m$ ise, aynı zamanda $m \mid p^s$ olduğundan $q \mid p^s$ elde ederiz. Fakat Aritmetiğin Temel Teoremi'nden $p^s$ sayısını bölen tek asalın $p$ olduğunu bildiğimizden $p = q$ sonucuna ulaşırız. Dolayısıyla, $p^s$ sayısının her pozitif böleninin bir $e$ sayısı için $m = p^e, e \geqslant 0$ biçiminde olması gerektiği sonucuna ulaşırız. Eğer $0 \leqslant e \leqslant s$ ise $p^s = p^e p^{s-e}$ olduğundan $p^e \mid p^s$ olduğunu görürüz. Eğer $e > s$ ise $p^e = p^s p^{e-s} > p^s$ olduğundan $p^e \nmid p^s$ olduğunu görürüz. Sonuç olarak, pozitif bölen kümesinin tam olarak $\tau(p^s) = s+1$ elemanlı $\mathcal{B}(p^s) = \{p^e : 0 \leqslant e \leqslant s\}$ kümesi olduğu sonucuna ulaşıyoruz. Buradan da Lemma 9.7 ile pozitif bölenler toplamının

$$\sigma(p^s) = 1+p+p^2+\cdots+p^s = (p^{s+1}-1) : (p-1)$$

olduğunu görüyoruz. □

Sıradaki önerme ile artık bir sayının asal çarpan ayrışması verildiğinde bu sayının pozitif bölen kümesini açık bir şekilde yazabilecek ve pozitif bölen sayısını ve pozitif bölenler toplamını, yani $\tau$ ve $\sigma$ fonksiyonlarının değerlerini rahatlıkla hesaplayabileceğiz.

**Teorem 9.9.** *Bir $m > 1$ sayısı, birbirinden farklı $p_1, p_2, \ldots, p_t$ asalları ve pozitif $s_1, s_2, \ldots, s_t$ sayıları için*

$$m = p_1^{s_1} p_2^{s_2} \ldots p_t^{s_t}$$

*olarak verisin. Bu durumda $mn$ sayısı için $\tau$ ve $\sigma$ fonksiyonlarının değerleri*

$$\begin{aligned}
\tau(m) &= \prod_{i=1}^{t} (s_i + 1) \\
&= (s_1 + 1)(s_2 + 1) \ldots (s_t + 1) \ , \\
\sigma(m) &= \prod_{i=1}^{t} (p_i^{s_i+1} - 1) : (p_i - 1) \\
&= [(p_1^{s_1+1} - 1) : (p_1 - 1)].[(p_2^{s_2+1} - 1) : (p_2 - 1)] \ldots [(p_t^{s_t+1} - 1) : (p_t - 1)]
\end{aligned}$$

*olur.*

***Kanıt.*** Verilen $m = p_1^{s_1} p_2^{s_2} \ldots p_t^{s_t}$ sayısının farklı asallardan elde edilen çarpanlarını şu şekilde isimlendirelim:

$$n_1 := p_1^{s_1}, \ n_2 := p_2^{s_2}, \ \ldots, \ n_t := p_t^{s_t}$$

olsun. Bu isimlendirmeyle $m$ sayısı

$$m = n_1 n_2 \ldots n_t$$

olarak ifade edilebilir. Lemma 9.6 sayesinde $i \neq j$ için $n_i, n_j$ sayı çiftinin aralarında asal olduğunu görüyoruz, çünkü $n_i$ sayısının tek asal böleni $p_i$, $n_j$ sayısının tek asal böleni $p_j$ sayısıdır ve $i \neq j$ için bu asallar farklıdır. Öyleyse Sonuç 9.5 ve Sonuç 9.8 ile aradığımız

$$\begin{aligned}
\tau(m) &= \tau(n_1)\tau(n_2) \ldots \tau(n_t) \\
&= \tau(p_1^{s_1})\tau(p_2^{s_2}) \ldots \tau(p_t^{s_t}) \\
&= (s_1 + 1)(s_2 + 1) \ldots (s_t + 1)
\end{aligned}$$

ve

$$\begin{aligned}\sigma(m) &= \sigma(n_1)\sigma(n_2)\dots\sigma(n_t)\\ &= \sigma(p_1^{s_1})\sigma(p_2^{s_2})\dots\sigma(p_t^{s_t})\\ &= [(p_1^{s_1+1}-1):(p_1-1)].[(p_2^{s_2+1}-1):(p_2-1)]\dots[(p_t^{s_t+1}-1):(p_t-1)]\end{aligned}$$

sonuçlarını elde ederiz. □

**Örnek 9.5.** Tekrar bölümünün başında Örnek 9.1 ve Örnek 9.2'de incelediğimiz $n = 72$ için $\tau$ ve $\sigma$ fonksiyonlarını, bu sefer yukarıda elde ettimiz yöntemleri uygulayarak hesaplayalım. Öncelikle $n = 72$ sayısının asal çarpan ayrışmasına ihtiyacımız var:

$$72 = 8.9 = 2^3.3^2 \quad .$$

Dolayısıyla;

$$\begin{aligned}\tau(72) &= (3+1)(2+1)\\ &= 4.3 = 12\ .\\ \sigma(72) &= [(2^{3+1}-1):(2-1)].[(3^{2+1}-1):(3-1)]\\ &= (15:1).(26:2)\\ &= 15.13 = 195\ .\end{aligned}$$

**Örnek 9.6.** Bu sefer $\tau$ ve $\sigma$ fonksiyonlarını $n = 36000$ için hesaplayalım. Bunun için önce bu sayının asal çarpan ayrışmasını elde edelim.

$$36000 = 36.10^3 = 2^2.3^2.2^3.5^3 = 2^5.3^2.5^3\ .$$

Şimdi Teorem 9.9 ile fonksiyonlarımızın değerlerini hesaplayabiliriz:

$$\begin{aligned}\tau(36000) &= (5+1)(2+1)(3+1) = 6.3.4 = 72\ .\\ \sigma(36000) &= [(2^{5+1}-1):(2-1)].[(3^{2+1}-1):(3-1)].[(5^{3+1}-1):(5-1)]\\ &= (63:1).(26:2).(624:4)\\ &= 63.13.156 = 127764\ .\end{aligned}$$

# Bölüm 10

# Mersenne asalları ve mükemmel sayılar

## 10.1 Mersenne asalları

Bir $a$ pozitif sayısı alalım. Herhangi bir $n$ pozitif sayısı için $a^n - 1$ ile $a$ sayısının aralarında asal olduklarını görmek zor değildir: Eğer bir $k$ sayısı $a$ ve $a^n - 1$ sayılarının ortak böleni ise $k \mid [a^{n-1}.a - 1(a^n - 1)] = 1$ sağlanır, dolayısıyla $a$ ve $a^n - 1$ sayılarının tek pozitif ortak böleni 1'dir.

Şu soruyu düşünelim: $m = a^n - 1$ formundaki bir sayı ne zaman asal olur? Eğer $a = 1$ veya $n = 1$ ise sorunun ilginç olmadığını fark ediyoruz: Eğer $a = 1$ ise $m = 0$ olur. Eğer $n = 1$ ise de $m = a - 1$ sağlanıyor, yani eğer $a$ sayısı bir asalın bir fazlasıyla $m$ asal oluyor. Bu yüzden bundan sonrası için $a \geqslant 2$ ve $n \geqslant 2$ olduğunu kabul edelim.

Öncelikle, böyle bir $m$ sayısının

$$m = a^n - 1 = (a - 1)(a^{n-1} + a^{n-2} + \cdots + a + 1) \tag{10.1}$$

şeklinde çarpanlara ayrıldığını hatırlayalım. Eğer $n \geqslant 2$ ise

$$a^{n-1} + a^{n-2} + \cdots + a + 1 \geqslant a + 1 \geqslant 2$$

olduğunu görüyoruz. Dolayısıyla eğer aynı zamanda $a-1 \geqslant 2$ ise Denklem 10.1 ile $m$ sayısı bir bileşik sayı olur. Öyleyse $m = a^n - 1$ sayısının asal sayı olmasının tek yolu, $a = 2$ olması. Bu yüzden bundan sonra sadece $a = 2$, yani $m = 2^n - 1$ durumunu inceleyeceğiz.

Şimdi de $n$ sayısının bileşik olduğunu, yani $k, l > 1$ için $n = kl$ olduğunu varsayalım. Bu durumda $m$ sayısını $m = 2^{kl} - 1 = (2^k)^l - 1$ olarak yazabiliriz. Eğer $b = 2^k$ dersek $m$ sayısının $m = b^l - 1$ formunda olduğunu görürüz. Bu da bize $m$ sayısının

$$m = b^l - 1 = (b-1)(b^{l-1} + b^{l-2} + \cdots + b + 1) \tag{10.2}$$

şeklinde çarpanlara ayrılmasını verir. Bu durumda $k \geqslant 2$ olduğundan $b = 2^k \geqslant 2^2 = 4$, dolayısıyla $b - 1 \geqslant 4 - 1 = 3 > 1$ olduğunu görüyoruz. Ayrıca

$$b^{l-1} + b^{l-2} + \cdots + b + 1 \geqslant b + 1 > 1$$

olduğunu da gözlemliyoruz. Sonuç olarak, Denklem 10.2 ile $m$ sayısının 1'den büyük iki sayının çarpımı olarak yazıldığını, yani bir bileşik sayı olduğunu görüyoruz.

Üstteki paragrafta eğer $n$ sayısı bileşikse $m = 2^n - 1$ sayısının asal olamayacağını gördük. Yani böyle bir sayı ancak $n$ sayısı asal ise asal olabilir. Yukarıda ulaştığımız sonuçları şu önerme ile özetleyelim.

**Önerme 10.1.** *Eğer $a > 2$ ise veya $n$ sayısı bileşik ise $a^n - 1$ sayısı bileşiktir.*

Bu önermenin $a > 1, n > 1$ durumundaki karşıt-tersini de düşünmek faydalıdır:

**Sonuç 10.2.** *1'den büyük $a$ ve $n$ sayıları için, eğer $m = a^n - 1$ sayısı asal ise $a = 2$ ve $n$ sayısı asal olmalıdır.*

Bahsettiğimiz bu özel biçime sahip asallara ayrı bir isim vereceğiz:

**Tanım 10.3.** Eğer $p$ asal sayısı için $q = 2^p - 1$ sayısı asal ise bu $q$ sayısına bir *Mersenne asalı* denir.

İlk birkaç Mersenne asalını şöyle listeleyebiliriz:

$$2^2 - 1 = 3$$
$$2^3 - 1 = 7$$
$$2^5 - 1 = 31$$
$$2^7 - 1 = 127$$

Burada muhtemelen aklımıza gelen ilk soru şu olur: Herhangi bir $p$ asalı için $q = 2^p - 1$ sayısı her zaman asal mıdır? Bu sorunun yanıtının olumsuz olduğunu, $2^{11} - 1$ sayısının

$$2^{11} - 1 = 2047 = 23.89$$

şeklinde çarpanlara ayrıldığını gözlemleyerek görüyoruz. Yani, bir $p$ asalı için $2^p - 1$ sayısı bir Mersenne asalı olabileceği gibi bileşik bir sayı da olabilir.

## 10.2 Mükemmel sayılar

Bir sayının kendinden küçük (yani kendisi hariç) pozitif bölenlerine o sayının *özbölenleri* diyelim. Örneğin, 6 sayısının özbölenlerinin 1,2 ve 3; 12 sayısının özbölenlerinin ise $1, 2, 3, 4, 6$ olduğunu gözlemleyelim.

$$6 = 1 + 2 + 3$$

olduğunu yani 6 sayısının özbölenleri toplamına eşit olduğunu da görüyoruz. Fakat bu özellik bütün sayılar için sağlanmaz. Örneğin 12 için

$$12 \neq 16 = 1 + 2 + 3 + 4 + 6$$

olur.

**Tanım 10.4.** Eğer bir sayı özbölenlerinin toplamına eşit ise o sayıya *mükemmel sayı* denir.

Yukarıda gördük ki 6 bir mükemmel sayıdır ama 12 değildir.

$$28 = 1 + 2 + 4 + 7 + 14$$

olduğundan 28 de bir mükemmel sayıdır.

Bir pozitif sayının özbölenleri toplamına o sayının kendisini eklersek o sayının bütün pozitif bölenleri toplamını elde ederiz. Bir başka deyişle, bir $n$ pozitif sayısının bütün özbölenleri toplamı $\sigma(n) - n$ olur. Dolayısıyla bir $n$ sayısı mükemmel sayıdır ancak ve ancak $n = \sigma(n) - n$ ise. Eşitliğin iki tarafına $n$ ekleyerek şu sonucu elde ediyoruz:

**Önerme 10.5.** *Pozitif bir $n$ sayısı mükemmel sayıdır ancak ve ancak $\sigma(n) = 2n$ ise.*

Sıradaki önerme mükemmel sayılar ile Mersenne asalları arasında güçlü bir ilişki olduğuna işaret ediyor:

**Teorem 10.6.** *Eğer $q = 2^p - 1$ bir Mersenne asalı ise $2^{p-1}(2^p - 1)$ bir mükemmel sayıdır.*

***Kanıt.*** Verilen $q = 2^p - 1$ sayısı bir Mersenne asalı olduğundan $p$ sayısının asal olduğunu biliyoruz. $p > 1$ olduğundan $q = 2^p - 1$ asal sayısı tektir, dolayısıyla $q$ asalı 2'den farklıdır. Bu durumda, $n = 2^{p-1}(2^p - 1)$ sayısı için

$$n = 2^{p-1}.q^1$$

bir asal çarpan ayrışmasıdır. Buradan, Teorem 9.9 ile

$$\begin{aligned}
\sigma(n) &= [(2^{(p-1)+1} - 1) : (2 - 1)].[(q^{1+1} - 1) : (q - 1)] \\
&= (2^p - 1).[\underbrace{(q^2 - 1)}_{(q-1)(q+1)} : (q - 1)] \\
&= (2^p - 1)(q + 1) \\
&= (2^p - 1)2^p \\
&= 2.2^{p-1}(2^p - 1) \\
&= 2n
\end{aligned}$$

sonucuna ulaşırız. Bu da Önerme 10.5 ile $n$ sayısının bir mükemmel sayı olduğunu verir. □

Bu teorem diyor ki, ne zaman elimizde bir Mersenne asalı varsa bu sayıdan bir mükemmel sayı elde ederiz. Peki bunun tersi de doğru mudur? Eğer elimizde bir mükemmel sayı varsa buradan bir Mersenne asalı elde edebilir miyiz? Sıradaki teorem bunun da, en azından çift mükemmel sayılar için doğru olduğunu söylüyor.

**Teorem 10.7.** *Eğer bir $n$ sayısı çift ve mükemmel sayı ise, bir $q = 2^p - 1$ Mersenne asalı için bu $n$ sayısı*

$$n = 2^{p-1}(2^p - 1)$$

*biçimindedir.*

***Kanıt***. Öncelikle, Aritmetiğin Temel Teoremi ile $n$ sayısının 2'den ve birbirinden farklı $p_1, p_2, \ldots, p_s$ asalları ve pozitif $k, k_1, k_2, \ldots, k_s$ sayıları için

$$n = 2^k.p_2^{k_2}p_2^{k_2}\ldots p_s^{k_s}$$

şeklinde yazılabileceğini biliyoruz. Bu ifadenin $2^k$ dışında kalana kısmını

$$q := p_2^{k_2}p_2^{k_2}\ldots p_s^{k_s}$$

olarak isimlendirelim. Bu isimlendirme ile $n$ sayısını

$$n = 2^k.q \tag{10.3}$$

olarak ifade ediyoruz.

Şimdi, $n$ sayısının bir mükemmel sayı olduğunu kullanarak $\sigma(n)$ değerini

$$\sigma(n) = 2n = 2.2^k q = 2^{k+1}q \tag{10.4}$$

olarak hesaplayalım.

Elimizdeki $q$ sayısı tek sayıların çarpımı olduğundan bir tek sayıdır ve dolayısıyla 2 asalı ile bölünmediğinden Sonuç 9.6 sebebiyle $2^k$ ve $q$ sayıları aralarında asaldır. Öyleyse, Önerme 9.4 ve Teorem 9.9 ile $\sigma(n)$

değeri

$$\begin{aligned}\sigma(n) &= \sigma(2^k.q)\\ &= \sigma(2^k).\sigma(q)\\ &= [(2^{k+1}-1):(2-1)].\sigma(q)\\ &= (2^{k+1}-1).\sigma(q)\end{aligned}$$

olarak hesaplanabilir. Burada $\sigma(n)$ için Denklem 10.4'te elde ettiğimiz ifadeyi kullanalım ve denklemin sol tarafından $q$ sayısını çıkarıp ekleyelim:

$$\begin{aligned}2^{k+1}q - q + q &= (2^{k+1}-1).\sigma(q)\\ (2^{k+1}-1)q + q &= (2^{k+1}-1).\sigma(q)\\ q &= (2^{k+1}-1).\sigma(q) - (2^{k+1}-1)q\\ q &= (2^{k+1}-1).[\sigma(q)-q]\ . \qquad (10.5)\end{aligned}$$

Bu denklemle $\sigma(q)-q$ sayısının $q$ sayısını böldüğünü görüyoruz. Ayrıca $k \geqslant 1$ olduğundan $2^{k+1}-1 \geqslant 2^2-1 = 3 > 1$ olduğunu da gözlemleyelim. Dolayısıyla, $\sigma(q)-q < q$ olmalıdır, yani bu sayı $q$'nun bir özböleni, başka bir deyişle $q$'nun kendisinden farklı bir bölenidir.

Şimdi, $q$ sayısının $\sigma(q)-q$ ve $q$ dışındaki bütün pozitif bölenlerinin toplamını $b$ ile isimlendirelim. Bu durumda

$$\begin{aligned}\sigma(q) &= b + [\sigma(q)-q] + q\\ \sigma(q) &= b + \sigma(q)\\ 0 &= b\end{aligned}$$

eşitliğine ulaşırız. Başka bir deyişle, $q$ sayısının $\sigma(q)-q$ ve $q$ dışındaki tüm pozitif bölenlerinin toplamı 0'dır, yani $q$'nun kendisinden ve $\sigma(q)-q$'dan başka pozitif böleni yoktur. Böylece; $1 \mid q$ ve $1 \neq 1$ olduğunu bildiğimizden 1 sayısının $q$'nun bir özböleni olduğunu, dolayısıyla da $q$ sayısının tek özböleni $\sigma(q)-q$ olduğundan

$$\sigma(q) - q = 1$$

olması gerektiğini görüyoruz. Ayrıca $q$ sayısının 1 ve kendisi dışında pozitif böleni olmadığından $q$ sayısının asal olduğu sonucuna da ulaşıyoruz. Şimdi

$\sigma(q) - q = 1$ eşitliğini Denklem 10.5'te kullanırsak $q$ asalı için

$$q = 2^{k+1} - 1$$

ifadesini elde ederiz. Buradan da Sonuç 10.2 ile $p = k + 1$ sayısının asal olduğunu görüyoruz. Sonuç olarak, Denklem 10.3'te ifadeleri yerlerine koyarsak, $n$ sayısını bir $p$ asalı ve $q = 2^p - 1$ Mersenne asalı için

$$n = 2^{p-1}(2^p - 1)$$

olarak ifade etmiş olduk.

□

# Bölüm 11

# Kalandaşlık

Bir pozitif $n$ sayısı alalım. Bu sayıyı kullanarak tamsayılar üzerinde bir $\sim$ bağıntısını şöyle tanımlayalım: Herhangi $a$ ve $b$ tamsayıları için

$$a \sim b \iff n \mid b - a \tag{11.1}$$

olsun. Başka bir deyişle, eğer $n$ sayısı iki sayının farkını bölüyorsa bu iki sayı $\sim$ ile bağıntılı olsun.

**Örnek 11.1.** $n = 5$ için;

| | |
|---|---|
| $8 \sim 23$ | çünkü $5 \mid 23 - 8 = 15$ |
| $16 \not\sim 43$ | çünkü $5 \nmid 43 - 16 = 27$ |
| $23 \sim 8$ | çünkü $5 \mid 8 - 23 = -15$ |
| $42 \sim 42$ | çünkü $5 \mid 42 - 42 = 0$ . |

Bu şekilde tanımlı $\sim$ bağıntısı, aşağıdaki önermeyle ispatlayacağımız üzere birtakım temel özellikleri taşır.

**Önerme 11.1.** *Her $n > 0$ sayısı için $\sim$ yukarıda tanımlı bağıntı olmak üzere*

*(a)* ***Yansıma:*** *Her $a \in \mathbb{Z}$ için $a \sim a$ .*

*(b)* ***Simetri:*** *Her $a, b \in \mathbb{Z}$ için, eğer $a \sim b$ ise $b \sim a$.*

*(c)* ***Geçişkenlik:*** *Her $a, b, c \in \mathbb{Z}$ için, eğer $a \sim b$ ve $b \sim c$ ise $a \sim c$.*

***Kanıt.*** (a) Herhangi bir $n$ sayısı ve $a \in \mathbb{Z}$ için $n \mid 0 = a - a$ olduğundan $a \sim a$ elde ederiz.

(b) Verilen $a$ ve $b$ sayıları için $a \sim b$ sağlansın. Bu durumda $n \mid b - a$ olduğunu elde ederiz. Buradan da $n \mid -(b-a) = a - b$ olduğunu görüyoruz, dolayısıyla $\sim$ bağıntısının tanımından $b \sim a$ sonucuna ulaşıyoruz.

(c) Şimdi de $a \sim b$ ve $b \sim c$ olduğunu kabul edelim. Bu, $n \mid b-a$ ve $n \mid c-b$ olduğu anlamına gelir. Buradan Bölüm 4 Özellik **V.** ile $n \mid (b-a)+(c-b) = c-a$ olduğunu elde ederiz. Bu da bize aradığımız $a \sim c$ sonucunu verir. □

Bir küme üzerinde Önerme 11.1'deki üç şartı sağlayan bağıntılara matematikte *denklik bağıntısı* dendiğini hatırlayalım.

**Sonuç 11.2.** *Her $n$ pozitif sayısı için, $\mathbb{Z}$ üzerinde Denklem 11.1 ile tanımlı $\sim$ bağıntısı bir denklik bağıntısıdır.*

Tamsayılar üzerindeki bu önemli denklik bağıntısı, kendine özel bir adı ve gösterimi hak ediyor:

**Tanım 11.3.** Bir $n$ pozitif sayısı verilmiş olsun. Eğer $a, b$ sayıları için $n \mid b - a$ ise '$a$ sayısı $b$ ile *modülo $n$'de kalandaştır*' denir ve bu ilişki

$$a \equiv b \pmod{n}$$

ile gösterilir.

**Örnek 11.2.** Bu tanım ve gösterim ile Örnek 11.1'deki ilişkileri şöyle ifade edebiliriz:

$$\begin{aligned} 8 &\equiv 23 \pmod 5 \\ 16 &\not\equiv 43 \pmod 5 \\ 23 &\equiv 8 \pmod 5 \\ 42 &\equiv 42 \pmod 5 \ . \end{aligned}$$

***Soru* 1.** Modülo 1'de bütün sayıların kalandaş olduğunu, yani her $a, b \in \mathbb{Z}$ için

$$a \equiv b \pmod 1$$

olduğunu gösterin.

Sıradaki önerme, 'kalandaş' kelimesini neden kullandığımızı açıklıyor: İki sayının modülo $n$'de kalandaş olması, tam olarak bu sayıların $n$ ile bölme algoritmasıyla bölündüklerinde aynı kalanı vermeleri anlamına gelir.

**Önerme 11.4.** *Bir $n$ pozitif sayısı verilmiş olsun. $a$ ve $b$ sayıları modülo $n$'de kalandaştır ancak ve ancak bölme algoritması ile $n$ sayısına bölündüklerinde kalanlar eşit ise.*

***Kanıt.*** ( $\Longrightarrow$ ) $a$ ve $b$ sayılarının modülo $n$'de kalandaş olduklarını, yani $a \equiv b \pmod n$ olduğunu kabul edelim. Bu,

$$n \mid b - a$$

olduğu anlamına gelir. Diğer yandan, bölme algoritması ile $a$ ve $b$ sayıları $0 \leqslant r_1, r_2 < n$ olmak üzere belli $q_1, q_2, r_1$ ve $r_2$ sayıları için

$$a = q_1 n + r_1 \quad \text{ve} \quad b = q_2 n + r_2$$

olarak ifade edilsin. Bu iki bilgiyi birleştirirsek

$$n \mid b - a = (q_2 n + r_2) - (q_1 n + r_1) = (q_2 - q_1)n + (r_2 - r_1)$$

olduğunu görüyoruz. Bu ifadede $n \mid (q_2 - q_1)n$ olduğu açıktır, dolayısıyla Bölüm 4 Özellik **V.** ile

$$n \mid (q_2 - q_1)n + (r_2 - r_1) - (q_2 - q_1)n = r_2 - r_1$$

olduğu sonucuna ulaşıyoruz, ki bu da bize $n \mid |r_2 - r_1|$ olduğunu da gösteriyor. Diğer yandan,

$$\begin{aligned} 0 &\leqslant\ r_2 < n, \\ -n &< -r_1 \leqslant 0 \end{aligned}$$

olduğundan, eşitsizlikleri toplayarak

$$-n < r_2 - r_1 < n$$

olduğunu görüyoruz ve böylece $0 \leqslant |r_2 - r_1| < n$ eşitsizliklerini elde ediyoruz. Eğer $|r_2 - r_1| > 0$ olsaydı, $n \mid |r_2 - r_1|$ olduğundan Bölüm 4 Özellik **VIII.** ile $|r_2 - r_1| \geqslant n$ olması gerekirdi, fakat bunun doğru olmadığını şimdi gördük. Sonuç olarak $|r_2 - r_1| = 0$ ve dolayısıyla $r_1 = r_2$ olmak zorundadır.

($\Longleftarrow$) $a$ ve $b$ sayılarının $n$ sayısına bölme algoritmasıyla bölündüklerinde aynı kalanı verdiklerini, yani $0 \leqslant r < n$ olmak üzere belli $q_1, q_2$ ve $r$ sayıları için

$$a = q_1 n + r \text{ ve } b = q_2 n + r$$

olduğunu kabul edelim. Bu durumda

$$b - a = (q_2 n + r) - (q_1 n + r) = q_2 n + r - q_1 n - r = (q_2 - q_1)n$$

olduğunu, dolayısıyla da $n \mid b - a$ olduğunu görüyoruz. Bu da kalandaşlığın tanımıyla $a$ ve $b$ sayılarının modülo $n$'de kalandaş oldukları, yani

$$a \equiv b \pmod{n}$$

olduğu anlamına gelir. □

## 11.1 Kalandaşlık ve işlemler

Bu kısımda, temel işlemlerimiz ile kalandaşlığın şu anlamda uyumlu olduğunu göstereceğiz: "Eğer kalandaş olan sayılara temel işlemler uygulanırsa, sonuçlar da kalandaş olur." Bu kısım boyunca, bir $n > 1$ sayısının verili olduğunu varsayalım.

**Teorem 11.5.** *Herhangi $a_1, a_2, b_1, b_2$ sayıları için, eğer $a_1 \equiv a_2 \pmod{n}$ ve $b_1 \equiv b_2 \pmod{n}$ ise*

**i.** $a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$

**ii.** $a_1.b_1 \equiv a_2.b_2 \pmod{n}$

*sağlanır.*

***Kanıt***. $a_1 \equiv a_2 \pmod{n}$ ve $b_1 \equiv b_2 \pmod{n}$ olduğunu kabul edelim, yani $n \mid a_2 - a_1$ ve $n \mid b_2 - b_1$ olsun.

**(i.)** Bölüm 4 Özellik **V.** ile

$$n \mid (a_2 - a_1) + (b_2 - b_1) = (a_2 + b_2) - (a_1 + b_1)$$

olduğunu görüyoruz. Bu da aradığımız $a_1 + b_1 \equiv a_2 + a_2 \pmod{n}$ sonucu ile denktir.

**(ii.)** Öncelikle $a_2b_2 - a_1b_1$ ifadesinden $a_2b_1$ sayısını çıkarıp geri ekleyerek

$$a_2b_2 - a_1b_1 = a_2b_2 - a_2b_1 + a_2b_1 - a_1b_1 = a_2(b_2 - b_1) + b_1(a_2 - a_1)$$

eşitliğini elde edelim. Bu, bize $a_2b_2 - a_1b_1$ ifadesinin $a_2 - a_1$ ve $b_2 - b_1$ sayılarının bir doğrusal bileşimi olarak yazılabileceğini gösteriyor. Dolayısıyla, $n \mid a_2 - a_1$ ve $n \mid b_2 - b_1$ olduğundan, yine Bölüm 4 Özellik **V.** ile

$$n \mid a_2(b_2 - b_1) + b_1(a_2 - a_1) = a_2b_2 - a_1b_1$$

olduğunu görüyoruz. Bu da bize ulaşmaya çalıştığımız

$$a_1a_2 \equiv b_1b_2 \pmod{n}$$

sonucunu veriyor. □

***Soru*** **2.** Bu özellikleri kullanarak kalandaşlık ile çıkartma işleminin yukarıdaki anlamda uyumlu olduğunu, yani eğer $a_1 \equiv a_2 \pmod{n}$ ve $b_1 \equiv b_2 \pmod{n}$ ise

$$a_1 - b_1 \equiv a_2 - a_2 \pmod{n}$$

olduğunu gösterin.

***Soru* 3.** Eğer $a_1 \equiv a_2 \pmod{n}$ ise her $k \in \mathbb{Z}^+$ için

$$a_1^k \equiv a_2^k \pmod{n}$$

olduğunu gösterin.
(Öneri: Çarpmayla kalandaşlığın uyumu ile ilgili önermeyi kullanın ve $k$ üzerinde tümevarım uygulayın.)

## 11.2 Kalandaşlık sınıfları ve modüler aritmetik

Geçen kısımda olduğu gibi bu kısım boyunca da bir $n > 1$ sayısının verilmiş olduğunu varsayalım.

Bu bölümün başlarında, Sonuç 11.2 ile kalandaşlığın bir denklik bağıntısı olduğunu görmüştük. Bir denklik bağıntısı verildiğinde, belli bir elemanla bu bağıntıya göre denk olan bütün elemanlardan oluşan kümeye bu elemanın 'denklik sınıfı' dendiğini hatırlayalım. Buradan hareketle, her bir $a \in \mathbb{Z}$ sayısı için $a$ ile kalandaş olan bütün sayıların oluşturduğu kümeye modülo $n$'de $a$ sayısının *kalandaşlık sınıfı*, ya da kısaca *kalan sınıfı* diyeceğiz. Bir $a$ sayısının kalan sınıfını

$$\overline{a} = \{x \in \mathbb{Z} : \ x \equiv a \pmod{n}\}$$

ile göstereceğiz. Bu yazımın bir zayıflığı var: buradaki gibi $\overline{a}$ şeklinde bir ifadeyle karşılaştığımızda, tek başına bu ifadeden hangi $n$ sayısı için modülo $n$'deki kalan sınıfından bahsedildiğini anlamak mümkün değil. Dolayısıyla, bu notasyonu kullandığımız her yerde hangi $n$ sayısı için kalandaşlıktan ve kalan sınıflarından bahsettiğimizin bağlamdan açık olması gerekiyor.

**Örnek 11.3.** Modülo 5'teki kimi denklik sınıflarını yazalım:

$$\overline{1} = \{\ldots, -9, -4, 1, 6, 11, \ldots\}$$
$$\overline{3} = \{\ldots, -7, -2, 3, 8, 13, \ldots\}$$
$$\overline{10} = \{\ldots, -10, -5, 0, 5, 10, 15, \ldots\}\ .$$

Bu noktada eğer Önerme 11.4'ü hatırlayacak olursak, modülo $n$'de tam olarak $n$ tane kalan sınıfı olduğunu ve bunları

$$\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-2}, \overline{n-1}$$

olarak listeleyebileceğimizi görürüz. Bunlar bir denklik bağıntısının tüm farklı denklik sınıfları olduğundan; ikili kesişimlerinin boş küme verdiğini ve hepsinin bileşiminin tamsayılar kümesini oluşturduğunu, başka bir deyişle $\mathbb{Z}$'nin bir 'parçalanışını' verdiklerini biliyoruz.

Modülo $n$'de kalan sınıfları kümesini $\mathbb{Z}_n$ ile göstereceğiz. Bu kümeyi açık şekilde

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-2}, \overline{n-1}\}$$

olarak yazabiliriz. Bu kümenin tam olarak $n$ elemandan oluştuğuna, yani $|\mathbb{Z}_n| = n$ olduğuna dikkat edelim.

Kalandaşlık ve kalan sınıfı kavramları, tanımlarından da anlaşılacağı üzere birbirlerine sıkı sıkıya bağlıdır. Bu bağı şu şekilde ifade edebiliriz:

*'İki sayı modülo n'de kalandaştır ancak ve ancak modülo n'de kalan sınıfları aynıysa.'*

Ayrıca bu koşullar, bir sayının diğerinin kalan sınıfının elemanı olmasıyla da denktir. Bu söylediklerimizi sembolik yazımla şöyle toparlayabiliriz:

$$a \equiv b \pmod{n} \iff \overline{a} = \overline{b} \iff a \in \overline{b} \iff b \in \overline{a}\ .$$

**Örnek 11.4.** Modülo 5'te 1 ve 6 sayılarının kalandaş olduğunu, yani

$$1 \equiv 6 \pmod{5}$$

olduğunu rahatlıkla görüyoruz. Aynı bilgiyi, kalandaşlık sınıfları ile yukarıdaki ifadeye denk olacak şekilde

$$\begin{aligned} &\overline{1} = \overline{6}, \\ &1 \in \overline{6}, \quad \text{veya} \\ &6 \in \overline{1} \end{aligned}$$

ile de ifade edebiliriz.

Görüyoruz ki, bir kalan sınıfının her bir elemanı o kalan sınıfını 'temsil etmek' için kullanılabilir: eğer $b \in \overline{a}$ ise $\overline{b}$ denklik sınıfını $\overline{a}$ olarak da yazabiliriz, çünkü $\overline{a} = \overline{b}$ olduğunu biliyoruz. [1]

Eğer $a_1, a_2, \ldots, a_n$ sayılarının her biri farklı kalan sınıflarından ise (yani herhangi ikisi modülo $n$'de kalandaş değilse) bu sayıların her birinin kalan sınıfı diğerlerininkilerden farklıdır ve dolayısıyla tam $n$ tane olduklarından bize bütün kalan sınıflarını verirler, yani

$$\mathbb{Z}_n = \{\overline{a_1}, \overline{a_2}, \ldots, \overline{a_{n-1}}, \overline{a_n}\}$$

olur. Bu şekilde, her bir kalan sınıfından birer 'temsilci' seçilerek oluşturulan $\{a_1, a_2, \ldots, a_{n-1}, a_n\}$ şeklindeki kümeye bir *tam temsilciler kümesi* denir. Örneğin, modülo $n$'de 0'dan $n-1$'e kadar sayıların bir tam temsilciler kümesi oluşturduğunu görüyoruz.

**Örnek 11.5.** Modülo 5'te $\{0, 1, 2, 3, 4\}$ bir tam temsilciler kümesidir. Aynı şekilde

$$\{1, 2, 3, 4, 5\}, \quad \{-3, -2, -1, 0, 1\}, \quad \{17, 18, 19, 20, 21\}$$

kümeleri de birer tam temsilciler kümesidir. Aslında, herhangi ardışık beş tamsayı, modülo 5'te bir tam temsilciler kümesi oluşturur. Ardışık sayılardan oluşmayan bir tam temsilciler kümesi de, örneğin $\{15, 6, -3, 23, 54\}$ biçiminde kurulabilir.

Kalan sınıflarının kullanışlı olmasının asıl nedeni, tamsayılar üzerindeki temel işlemleri $\mathbb{Z}_n$ üzerinde de tanımlamanın mümkün olmasıdır. Şimdi iki kalan sınıfının, örneğin belli $a$ ve $b$ sayıları için $\overline{a}$ ve $\overline{b}$'nin toplamını nasıl tanımlamanın doğal ve kullanışlı olacağı üzerine düşünelim. Muhtemelen ilk akla gelecek fikirlerden biri bu kalan sınıflarının temsilcilerini toplamak ve kalan sınıflarının toplamını, bu toplamın temsil ettiği kalan sınıfı olarak tanımlamak olurdu. Matematiksel dilde yazacak olursak, $\overline{a}$ ve $\overline{b}$ kalan sınıflarının toplamını

$$\overline{a} + \overline{b} := \overline{a + b} \tag{11.2}$$

[1] Bu anlamda, kalan sınıfları çok demokratiktirler: her bir elemanı bütün sınıfı temsil edebilir.

olarak tanımlamak akla yatkın görünüyor[2]. Fakat biraz dikkatli bakarsak bu tanımda potansiyel bir sorun olduğunu görürüz: Tanımladığımız toplamanın sonucu, topladığımız kalan sınıflarının temsilcilerine bağlı görünüyor. Fakat biliyoruz ki aynı denklik sınıfını farklı sayılar temsil edebilir. Dolayısıyla Denklem 11.2 ile $\mathbb{Z}_n$ üzerinde 'gerçekten' bir işlem tanımlayabilmemiz için, aynı denklik sınıfını temsil eden farklı sayılar aldığımızda da sonucun değişmemesi gerekli. Buradaki gibi, denklik sınıfları üzerinde bir işlem (ya da fonksiyon) tanımlarken bu işlemin sonucunun temsilciye bağlı olmayıp gerçekten de sadece denklik sınıfına bağlı olmasına *iyi-tanımlılık* denir. Denklem 11.2 ile gerçekten bir toplama tanımlayabilmemiz için, bu işlemin tanımı için önerdiğimiz kuralın iyi-tanımlı olması gerekir.

**Önerme ve tanım 11.6.** $\mathbb{Z}_n$ üzerinde

$$\overline{a} + \overline{b} := \overline{a+b} \ ,$$
$$\overline{a}.\overline{b} := \overline{a.b}$$

denklemleriyle tanımlanan 'toplama' ve "çarpma' işlemleri iyi-tanımlıdır, yani eğer $a_1, a_2, b_1, b_2$ sayıları için $\overline{a_1} = \overline{a_2}$ ve $\overline{b_1} = \overline{b_2}$ sağlanıyorsa

$$\overline{a_1 + b_1} = \overline{a_2 + b_2} \text{ ve } \ \overline{a_1.b_1} = \overline{a_2.b_2}$$

sağlanır.

***Kanıt***. Teorem 11.5 tam olarak aradığımız sonucu kalandaşlık dilinde ifade etmektedir. □

Kalan sınıfları kümesi yani $\mathbb{Z}_n$ üzerinde tanımlı bu toplama ve çarpma işlemleri, tamsayılar ve diğer sayı sistemlerinden aşina olduğumuz aşağıdaki önermede özetlenen temel özelliklere sahiptir:

[2]Burada, $\overline{a} + \overline{b}$ şeklinde bir toplamanın daha önce tanımlı olmadığına dikkat çekelim. Denklem 11.2'deki eşitliğin solundaki ve sağındaki '+' sembolleri aynı toplamayı göstermiyor: eşitliğin solundaki, $\overline{a}$ ve $\overline{b}$ arasındaki '+' sembolü yeni tanımlamaya niyetlendiğimiz, $\mathbb{Z}_n$ üzerinde bir işlem adayını belirtirken; eşitliğin sağındaki $a$ ve $b$ sayıları arasındaki '+' ise ilkokulda öğrendiğimiz tamsayılar üzerindeki toplama işlemini gösteriyor. Biz burada $\mathbb{Z}$ üzerindeki toplamayı kullanarak $\mathbb{Z}_n$ üzerinde bir toplama tanımlamaya çalışıyoruz.

**Önerme 11.7.** [3]*Her* $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$ *için aşağıdaki özellikler sağlanır:*

*i.* $\overline{a} + (\overline{b} + \overline{c}) = (\overline{a} + \overline{b}) + \overline{c}$ *(toplamsal bileşme)*

*ii.* $\overline{a} + \overline{0} = \overline{0} + \overline{a} = \overline{a}$ *(toplamsal etkisiz eleman)*

*iii.* $\overline{a} + \overline{-a} = \overline{-a} + \overline{a} = \overline{0}$ *(toplamsal ters)*

*iv.* $\overline{a} + \overline{b} = \overline{b} + \overline{a}$ *(toplamsal değişme)*

*v.* $\overline{a}.(\overline{b}.\overline{c}) = (\overline{a}.\overline{b}).\overline{c}$ *(çarpımsal bileşme)*

*vi.* $\overline{a}.\overline{b} = \overline{b}.\overline{a}$ *(çarpımsal değişme)*

*vii.* $\overline{1}.\overline{a} = \overline{a}.\overline{1} = \overline{1}$ *(çarpımsal birim eleman)*

*viii.* $\overline{a}.(\overline{b} + \overline{c}) = \overline{a}.\overline{b} + \overline{a}.\overline{c}$
$(\overline{a} + \overline{b}).\overline{c} = \overline{a}.\overline{c} + \overline{b}.\overline{c}$ *(dağılma)*

***Kanıt***. Her maddenin ispatı, kalan sınıfları üzerinde ilgili işlemin tanımı ve tamsayılarda ilgili özellik kullanılarak rahatlıkla yapılabilir. Örnek olarak, (i) özelliğini ispatlayalım:

$$\begin{aligned}
\overline{a} + (\overline{b} + \overline{c}) &= \overline{a} + \overline{b + c} \\
&= \overline{a + (b + c)} \\
&= \overline{(a + b) + c} \\
&= \overline{a + b} + \overline{c} \\
&= (\overline{a} + \overline{b}) + \overline{c} \ .
\end{aligned}$$

□

[3]Eğer bir küme üzerinde bu önermede listelenen özelliklere sahip toplama ve çarpma gibi iki işlem varsa, üzerindeki işlemlerle bu kümeye soyut cebirde *birim elemanlı değişmeli halka* denir.

Önermedeki Özellik (iii) ile, $\mathbb{Z}_n$ üzerinde çıkartma işleminin de toplama aracılığıyla

$$\overline{a} - \overline{b} := \overline{a} + \overline{-b}$$

şeklinde tanımlı olduğunu düşünebiliriz.

Böylece $\mathbb{Z}_n$ kümesinin üzerinde de bildiğimiz sayı sistemlerinin üzerinde olduğu gibi 'güzel ve uyumlu' özelliklere sahip işlemler tanımlı olduğunu görüyoruz. Dolayısıyla her bir $n$ pozitif sayısı için $\mathbb{Z}_n$ de bir 'sayı sistemi' olarak görülebilir. Bu sayı sistemini *modülo n'de sayılar* olarak isimlendirebiliriz.

Modülo $n$'de sayıların sahip olmadığı önemli bir özelliğe dikkat çekelim: Tamsayılarda olduğu gibi, $\mathbb{Z}_n$'de de genel olarak sayıların çarpımsal tersi yoktur. Fakat sonraki kısımda göreceğiz ki, $n$ sayısı asal olduğunda bu durum önemli ölçüde değişecek.

Bu sayı sistemleri üzerinde yapılan hesaplar ya da aynı hesapların kalandaşlık bağıntısı ile ifadeleri, yaygın olarak *modüler aritmetik* olarak adlandırılır.

***Soru* 4.** *Yutan eleman*: Her $\overline{a} \in \mathbb{Z}_n$ için $\overline{0}.\overline{a} = \overline{0}$ olduğunu gösterin.

## 11.3 Çarpımsal ters ve sıfır-bölenleri

Önceki kısımlarda olduğu gibi bu kısım boyunca da bir $n > 0$ sayısının verili olduğunu varsayıyoruz.

Modülo $n$'deki sayılarda, yani $\mathbb{Z}_n$'de şu soruyu düşünelim: Modülo $n$'de hangi sayıların çarpımsal tersi vardır? Başka bir ifadeyle, hangi $\overline{a} \in \mathbb{Z}_n$ kalan sınıfları için

$$\overline{x}.\overline{a} = \overline{1}$$

olacak şekilde bir $\overline{x} \in \mathbb{Z}_n$ bulunabilir? [4] Tamsayılarda sadece 1 ve -1'in çarpımsal tersleri olduğunu görüyoruz. Fakat, örneğin $\mathbb{Z}_9$'da ilk anda göze

[4] Bu özelliğe sahip olan kalan sınıflarının, tam olarak $\mathbb{Z}_n$ içindeki birim elemanın, yani $\overline{1}$'in bölenleri olduğunu gözlemleyelim.

çarpmayan kimi elemanların çarpımsal tersi olabiliyor:

$$\overline{2}.\overline{5} = \overline{10} = \overline{1}$$

olduğundan $\mathbb{Z}_9$'da $\overline{2}$'nin (ve tabii $\overline{5}$'in de) çarpımsal tersinin olduğunu gözlemliyoruz.

***Soru* 5.** (a) $\mathbb{Z}_n$'de $\overline{n-1}$'in çarpımsal tersinin olduğunu gösterin.

(b) Hiçbir zaman sıfır kalan sınıfının, yani $\overline{0}$'nin çarpımsal tersi olmadığını gösterin.

Tam olarak $\mathbb{Z}_n$'in hangi elemanlarının çarpımsal tersi oldu sorusunun cevabını sıradaki önermeyle veriyoruz.

**Önerme 11.8.** *Bir $\overline{a} \in \mathbb{Z}_n$ kalan sınıfının çarpımsal tersi vardır (yani $\overline{x}.\overline{a} = \overline{1}$ olacak şekilde bir $\overline{x} \in \mathbb{Z}_n$ bulunabilir) ancak ve ancak $a$ ve $n$ sayıları aralarında asal ise (yani* $\text{ebob}(n, a) = 1$ *ise).*

***Kanıt.*** ($\Longrightarrow$) Verilen $\overline{a} \in \mathbb{Z}_n$ için çarpımsal tersin var olduğunu varsayalım, yani bir $\overline{x} \in \mathbb{Z}_n$ için $\overline{x}.\overline{a} = \overline{1}$ olsun. Bu durumda, $\mathbb{Z}_n$'de çarpmanın tanımından $\overline{xa} = \overline{1}$ olduğunu görüyoruz, bu da bize $xa \equiv 1 \pmod{n}$, yani $n \mid 1 - xa$ olduğunu söylüyor. Bu ise, bir $y \in \mathbb{Z}$ için $1 - xa = yn$ olduğu sonucunu veriyor. Bu denklemi düzenlersek

$$1 = x.a + y.n$$

eşitliğini elde ediyoruz. Buradan da Sonuç 6.9 ile $a$ ve $n$ sayılarının aralarında asal olduklarını elde ediyoruz.

($\Longleftarrow$) Elimizdeki $a$ ve $n$ sayılarının aralarında asal olduklarını varsayalım. Bu durumda, yine Sonuç 6.9 ile

$$1 = x.a + y.n$$

olacak şekilde $x$ ve $y$ sayılarının var oluğunu elde ederiz. İki taraftaki ifadelerin kalan sınıflarına bakarak ve $\mathbb{Z}_n$'de elde ettiğimiz eşitliği düzen-

leyerek

$$\begin{aligned}\overline{1} &= \overline{x.a + y.n} \\ &= \overline{x}.\overline{a} + \overline{y}.\underbrace{\overline{n}}_{\overline{0}} \\ &= \overline{x}.\overline{a}\end{aligned}$$

sonucunu elde ediyoruz, ki bu da bize $\overline{a}$ için $\mathbb{Z}_n$'de $\overline{x}$ gibi bir çarpımsal tersin var olduğunu söylüyor. □

Bu önermeyle görüyoruz ki, $\mathbb{Z}_n$ içinde çarpımsal tersi olan elemanlar tam olarak $n$ ile aralarında asal olan sayılarla temsil edilen kalan sınıflarıdır. Bu durumda, elimizde bir tam temsilciler sınıfı varsa (örneğin, $\{0, 1, \ldots, n-1\}$), bu sayılar içinde kaçı $n$ ile aralarında asalsa $\mathbb{Z}_n$ içinde o kadar çarpımsal tersi olan eleman bulunur.

Şimdi de bir $p$ asalı için modülo $p$'de sayıların çarpımsal tersleri üzerine düşünelim. Sıfır kalan sınıfının, yani $\overline{0}$'nin hiçbir zaman çarpımsal tersi olamadığını biliyoruz. Tam temsilci kümesi olarak $\{0, 1, \ldots, p-2, p-1\}$ kümesini seçerek $\mathbb{Z}_p$'yi

$$\mathbb{Z}_p = \{\overline{0}, \overline{1}, \ldots, \overline{p-2}, \overline{p-1}\}$$

olarak ifade edelim. Şimdi, her $k \in \{1, 2, \ldots, p-2, p-1\}$ için $0 < k < p$ olduğunu ve dolayısıyla $p$ asal olduğundan ebob$(p, k) = 1$ olduğunu görüyoruz. Dolayısıyla da $\mathbb{Z}_p$'de Önerme 11.8 ile böyle bir $k$ seçimi için $\overline{k}$ kalan sınıfının çarpımsal tersinin var olduğu sonucuna ulaşıyoruz. Bu gözlemimizi aşağıdaki sonuç ile ifade edelim:

**Sonuç 11.9.** *Eğer $p$ asal ise $\mathbb{Z}_p$'de $\overline{0}$ dışında bütün kalan sınıflarının çarpımsal tersi vardır.*

Yine $\mathbb{Z}_n$ içinde kimi elemanlar, tamsayılarda gözlemlenmeyen ikinci bir ilginç özellik sergileyebiliyor. Biliyoruz ki $a$ ve $b$ tamsayıları sıfırdan farklı ise $a.b$ çarpımı sıfır olamaz. Fakat, örneğin $\mathbb{Z}_6$'da, $\overline{2} \neq \overline{0}$ ve $\overline{3} \neq \overline{0}$ olmasına karşın

$$\overline{2}.\overline{3} = \overline{6} = \overline{0}$$

elde edebiliyoruz. Bu davranışı sergileyen sayılara aşağıdaki tanımla özel bir isim veriyoruz:

**Tanım 11.10.** Eğer bir $\overline{a} \in \mathbb{Z}_n$ kalan sınıfı, sıfır kalan sınıfından farklıysa (yani $\overline{a} \neq \overline{0}$ ise) ve $\overline{x} \neq \overline{0}$ olmak üzere bir $\overline{x} \in \mathbb{Z}_n$ için

$$\overline{x}.\overline{a} = \overline{0}$$

ise $\mathbb{Z}_n$'de $\overline{a}$ bir *sıfır-bölenidir* denir.

Tanımın hemen öncesinde gördük ki $\mathbb{Z}_6$'da $\overline{2}$ ve $\overline{3}$ birer sıfır-bölenidir. Tanım gereği $\overline{0}$ kalan sınıfının sıfır-böleni olarak kabul edilmediğine dikkat edin. Yukarıda Sonuç 11.9 ile gördük ki, $p$ asal sayısı için $\mathbb{Z}_p$'de hiç sıfır-böleni yoktur.

Sıradaki önerme, $\mathbb{Z}_n$ içindeki sıfır-bölenlerini tam olarak tarif ediyor.

**Önerme 11.11.** *Bir $\overline{a} \in \mathbb{Z}_n$ kalan sınıfı için $\overline{a} \neq \overline{0}$ olsun. $\overline{a}$ bir sıfır-bölenidir ancak ve ancak $a$ ve $n$ aralarında asal değilse.*

***Kanıt.*** ($\Longrightarrow$) Önermenin bu yönünü şöyle ifade edebiliriz:

$$\text{“}\overline{a} \text{ sıfır-böleni} \implies a \text{ ve } n \text{ aralarında asal değil”.}$$

Bu önerme, gördüğümüz gibi $P \implies Q$ biçiminde. Biz bu önermenin yerine, mantıksal denki olan $\neg Q \implies \neg P$ önermesini, yani bu önermenin *karşıt-tersi* [5] olan

$$\text{“}a \text{ ve } n \text{ aralarında asal} \implies \overline{a} \text{ sıfır-böleni değil”}$$

önermesini ispatlamayı tercih ediyoruz.

$a$ ve $n$ sayılarının aralarında asal olsun. Öyleyse Önerme 11.8 ile $\overline{a}.\overline{y} = \overline{1}$ olacak şekilde bir $\overline{y} \in \mathbb{Z}_n$ kalan sınıfının var olduğunu biliyoruz. Bir

[5] ya da, *kontrapozitifi*

$\overline{x} \in \mathbb{Z}$ için $\overline{x}.\overline{a} = \overline{0}$ olduğunu kabul edelim. Bu denklemin iki tarafını $\overline{y}$ ile çarparsak

$$\overline{x}.\underbrace{\overline{a}.\overline{y}}_{\overline{1}} = \overline{0}.\overline{y}$$
$$\overline{x}.\overline{1} = \overline{0}$$
$$\overline{x} = \overline{0}$$

sonucuna ulaşırız. Yani $\overline{a}$'yı $\overline{0}$ dışında bir $\overline{x}$ ile çarparak $\overline{0}$ elde etmek mümkün değildir. Bir başka deyişle, göstermek istediğimiz üzere, $\overline{a}$ bir sıfır-böleni değildir.

($\Longleftarrow$) $a$ ve $n$ sayıları aralarında asal olmasın, yani bir $d > 1$ sayısı için $\text{ebob}(n, a) = d$ olsun. Öyleyse, $d \mid n$ ve $d \mid a$ olacağından, belli $k, l \in \mathbb{Z}$ sayıları için

$$n = kd \quad \text{ve} \quad a = ld$$

sağlanır. Şimdi, $n > 0$ ve $d > 1$ olduğundan $0 < k < n$ olduğunu görüyoruz. Buradan da $k \not\equiv n \pmod{n}$ sonucuna ulaşıyoruz. Bu da

$$\overline{k} \neq \overline{n} = \overline{0}$$

olmasıyla, yani $\overline{k}$'nın sıfır sınıfından farklı olmasıyla denktir. Diğer yandan,

$$\overline{k}.\overline{a} = \overline{k.a} = \overline{k.ld} = \overline{l.kd} = \overline{l.n} = \overline{l}.\overline{n} = \overline{l}.\overline{0} = \overline{0}$$

olduğunu görüyoruz ve $\overline{a}$'nın bir sıfır-böleni olduğu sonucuna ulaşıyoruz. □

**Örnek 11.6.** $\mathbb{Z}_6$'yı

$$\mathbb{Z}_6 = \{\overline{0}, \overline{12}, \overline{3}, \overline{4}, \overline{5}\}$$

şeklinde yazalım ve

$$1 = \text{ebob}(1, 6) = \text{ebob}(5, 6),$$
$$2 = \text{ebob}(2, 6) = \text{ebob}(4, 6),$$
$$3 = \text{ebob}(3, 6)$$

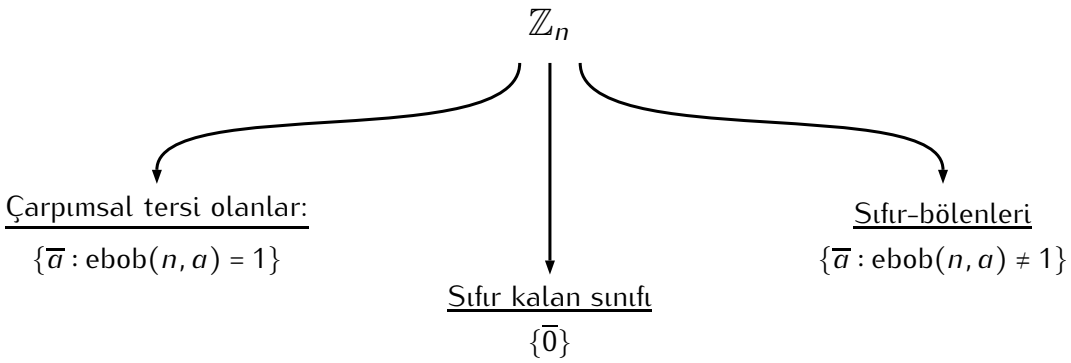
olduğunu gözlemleyelim. Görüyoruz ki, temsilcilerden 1 ve 5 sayıları 6 ile aralarında asaldır; 2,3 ve 4 ise değildir. Buna göre $\mathbb{Z}_6$'nın elemanları şöyle üç gruba ayrılır:

i. Sıfır kalan sınıfı: $\overline{0}$

ii. Çarpımsal tersi olanlar: $\overline{1}, \overline{5}$

iii. Sıfır-bölenleri: $\overline{2}, \overline{3}, \overline{4}$.

Yukarıdaki örnekteki ayrım, bütün $n > 1$ seçimleri için geçerlidir: Modülo $n$'deki sayılar kümesinin elemanları, temsilcilerinin $n$ sayısı ile aralarında asal olup olmamasına göre iki altkümeye ayrılırlar. Sıfır kalan sınıfı, tek elemanlı üçüncü bir altküme oluşturur. Bu ayrışmayı bir diagram ile gösterelim.



# Bölüm 12

# Sayı tabanları

## 12.1 Sayının bir tabanda ifadesi

Bir $b > 1$ sayısı alalım. Herhangi bir $n$ pozitif sayısı seçelim ve aşağıdaki yinelemeli prosedürü kullanarak $a_0, a_1, \ldots, a_m$ ve $q_0, q_1, \ldots, q_m$sayılarını oluşturalım:

**I.** (Başlangıç adımı) Bölme algoritmasıyla $n$ sayısını $b$ ile bölelim ve bölüme $q_0$, kalana $a_0$ diyelim, yani

$$n = q_0.b + a_0,\ 0 \leqslant a_0 < b$$

olsun.

**II.** (Yineleme adımı) Son olarak elde edilen bölüm değeri $q_i$ olsun. Eğer $q_i = 0$ ise prosedürü sonlandıralım. Eğer $q_i \neq 0$ ise $q_i$ sayısını $b$ ile bölelim ve bölümü $q_{i+1}$, kalanı $a_{i+1}$ olara isimlendirelim, yani

$$q_i = q_{i+1}.b + a_{i+1},\ 0 \leqslant a_{i+1} < b \tag{12.1}$$

olsun. Bu adımı tekrarlayalım.

Verilen bir sayı için bahsi geçen $a_i$ ve $q_i$ sayılarının nasıl elde edildiğini bir örnek üzerinden gözlemleyelim

**Örnek 12.1.** $b = 5$ ve $n = 366$ için yukarıda tarif edilen prosedürü işletelim:

$$\begin{aligned} 366 &= 73.5 + 1 & q_0 &= 73, \ a_0 = 1 \\ 73 &= 14.5 + 3 & q_1 &= 14, \ a_1 = 3 \\ 14 &= 2.5 + 4 & q_2 &= 2, \ a_2 = 4 \\ 4 &= 0.5 + 2 & q_3 &= \textcircled{0}, \ a_3 = 2 \end{aligned}$$

Böylece $a_3 = 2, a_2 = 4, a_1 = 3, a_0 = 1$ değerlerini elde ediyoruz. Yukarıdan aşağıya doğru her bir adımdaki $q_i$ değeri için bir alttaki ifadeyi kullanırsak

$$\begin{aligned} 366 &= 73.5 + 1 \\ &= (14.5 + 3).5 + 1 = 14.5^2 + 3.5 + 1 \\ &= (2.5 + 4).5^2 + 3.5 + 1 = 2.5^3 + 4.5^2 + 3.5 + 1 \\ &= 2.5^3 + 4.5^2 + 3.5^1 + 1.5^0 \end{aligned}$$

eşitliğine ulaşırız.

Bu örnekte, tarif edilen prosedür aracılığıyla elde ettiğimiz $a_i$ sayılarını katsayı olarak kullanarak $n = 366$ sayısını $b = 5$ sayısının üslerinin bir doğrusal bileşimi olarak yazabildiğimizi gördük. Ayrıca, bölme algoritması sayesinde her bir $a_i$ için $0 \leqslant a_i < b$ sağlandığından $n$ sayısının bu gösteriminde katsayılarımızın negatif olmaması ve 'küçük' olması gibi avantajlara da sahibiz. Öyleyse şu soruyu soralım: Bir $b > 1$ sayısı verildiğinde, her $n$ pozitif sayısı için böyle bir gösterim var mıdır? Eğer varsa, bu gösterim tek midir? Bu soruları hakkıyla yanıtlamak için biraz hazırlık yapmamız gerekecek.

Yineleme adımındaki Denklem 12.1 ile, her $i$ için

$$q_{i+1}.b = q_i - a_{i+1} \leqslant q_i$$

ve $b > 1$ olduğundan $q_{i+1} < q_i$ eşitsizliğini elde ediyoruz, yani $q_i$ sayıları gittikçe küçülüyor. Diğer yandan her bölmede bölünen ve bölen pozitif olduğundan $q_{i+1} \geqslant 0$ olduğunu da görüyoruz. Böylece, $q_i$ sayıları her adımda

azaldığından ve $q_i$ değerleri sıfırın altına düşemeyeceğinden bu yinelemeli prosedürün sonlu adımda, örneğin bir $m \in \mathbb{N}$ sayısı için $q_m = 0$ olacak şekilde $a_m = q_{m-1} \neq 0$ değerlerine ulaşarak sonlanacağını görüyoruz.

Eğer $q_0 = q_1.b + a_1$ değerini $n = q_0.b + a_0$ denkleminde yerine koyarsak

$$\begin{aligned} n &= (q_1.b + a_1).b + a_0 \\ &= q_1.b^2 + a_1.b + a_0 \end{aligned}$$

denklemine ulaşıyoruz. Yine bu ifadede $q_1 = q_2.b + a_2$ değişikliğini yaparsak

$$\begin{aligned} n &= (q_2.b + a_2).b^2 + a_1.b + a_0 \\ &= q_2.b^3 + a_2.b^2 + a_1.b + a_0 \end{aligned}$$

eşitliğini elde ediyoruz. Sıradaki lemma ile bu gözlemimizi genelleyecek ve tümevarım kullanarak ispatlayacağız.

**Lemma 12.1.** *Bir $b > 1$ sayısı ve $n$ pozitif sayısı verildiğinde, yukarıda tarif edilen $a_0, \ldots, a_m$ ve $q_0, \ldots, q_m$ sayıları ve her $1 \leqslant k \leqslant m$ için*

$$\begin{aligned} n &= q_{k-1}.b^k + a_{k-1}.b^{k-1} + \cdots + a_2.b^2 + a_1.b + a_0 \\ &= q_{k-1}.b^k + \sum_{i=0}^{k-1} a_i.b^i \end{aligned}$$

*sağlanır.*

***Kanıt***. İspatı $k$ üzerinde tümevarımla yapacağız.

$k = 1$ için ispatlamaya çalıştığımız denklem $n = q_0.b + a_0$ biçimini alır, ki bunun doğru olduğunu $q_0$ ve $a_0$ sayılarının başlangıç adımındaki tanımından biliyoruz.

Şimdi de gerektirme adımı için denklemin $k$ sayısı için doğru olduğunu, yani

$$n = q_{k-1}.b^k + \sum_{i=0}^{k-1} a_i.b^i$$

eşitliğinin sağlandığını varsayalım ve aynı ifadenin $k$ yerine $k+1$ konduğunda da doğru olacağını gösterelim. $q_i$ sayılarının tanımından

$$q_{k-1} = q_k.b + a_k$$

olduğunu biliyoruz. Bunu $n = q_{k-1}.b^k + \sum_{i=0}^{k-1} a_i.b^i$ ifadesinde yerine koyarsak

$$\begin{aligned} n &= (q_k.b + a_k).b^k + \sum_{i=0}^{k-1} a_i.b^i \\ &= q_k.b^{k+1} + a_k.b_k + \sum_{i=0}^{k-1} a_i.b^i \\ &= q_k.b^{k+1} + \sum_{i=0}^{k} a_i.b^i \\ &= q_{(k+1)-1}.b^{k+1} + \sum_{i=0}^{(k+1)-1} a_i.b^i \end{aligned}$$

eşitliğine ulaşırız. Bu da tam olarak ispatlamaya çalıştığımız ifadenin $k+1$ için doğru olduğunu gösterir. □

Şimdi her sayı için Örnek 12.1'deki gibi bir gösterimin tek bir şekilde var olduğunu gösterebiliriz.

**Teorem 12.2.** *Bir $b > 1$ sayısı verilmiş olsun. Her $n$ pozitif sayısı için*

$$\begin{aligned} n &= a_m.b^m + a_{m-1}.b^{m-1} + \cdots + a_2.b^2 + a_1.b + a_0 \\ &= \sum_{i=0}^{m} a_i.b^i \ , \end{aligned}$$

*$a_m \neq 0$ ve her $i = 0, 1, \ldots, m$ için $0 \leqslant a_i < b$ olacak şekilde $m \geqslant 0$ ve $a_0, a_1, \ldots, a_{m-1}, a_m$ sayıları vardır ve tektir.*

***Kanıt***. Bu gösterimin varlığı için Lemma 12.1'de elde ettiğimiz eşitliği $k = m$ için hesaplamak yeterlidir. Bu şekilde, bölümün başında tanımlanan $a_i$ ve $q_i$ sayılarını kullanarak

$$\begin{aligned} n &= q_{m-1}.b^m + \sum_{i=0}^{m-1} a_i.b^i \\ &= a_m.b^m + \sum_{i=0}^{m-1} a_i.b^i \\ &= \sum_{i=0}^{m} a_i.b^i \end{aligned}$$

eşitliğini elde ederiz. Tanım gereği $i = 0, 1, \ldots, m$ için $0 \leqslant a_i < b$ eşitsizliklerinin sağlandığını zaten biliyoruz.

Bu sayıların tek bir şekilde belirlendiğini görmek için, $\tilde{m} \geqslant 0$ ve $i = 0, 1, \ldots, \tilde{m}$ için $0 \leqslant \tilde{a}_i < b$ olmak üzere belli $\tilde{m}, \tilde{a}_0, \tilde{a}_1, \ldots, \tilde{a}_{\tilde{m}}$ sayıları için

$$n = \sum_{i=0}^{\tilde{m}} \tilde{a}_i . b^i$$

eşitliğinin sağlandığını varsayalım.

Eğer $m \neq \tilde{m}$ ise $n$ için gösterimleri aynı uzunluğa getirmek için şöyle bir düzenleme yapıyoruz: bir $M$ sayısını $m$ ve $\tilde{m}$ sayılarının büyük olanı, yani $M = \max\{m, \tilde{m}\}$ olarak tanımlayalım ve $m < i \leqslant M$ veya $\tilde{m} < i \leqslant M$ için katsayıları sıfır olarak tanımlayalım. Yani her $m < i \leqslant M$ için $a_i := 0$, her $\tilde{m} < i \leqslant M$ için $\tilde{a}_i = 0$ olsun.

Bu durumda $n$ sayısını hem $a_i$ katsayıları hem de $\tilde{a}_i$ katsayılarıyla

$$\begin{aligned} n &= a_M . b^M + a_{M-1} . b^{M-1} + \cdots + a_2 . b^2 + a_1 . b + a_0 \\ n &= \tilde{a}_M . b^M + \tilde{a}_{M-1} . b^{M-1} + \cdots + \tilde{a}_2 . b^2 + \tilde{a}_1 . b + \tilde{a}_0 \end{aligned}$$

şeklinde aynı miktarda katsayı kullanarak ifade edebiliyoruz. Bu iki eşitliği birbirinden çıkararak

$$0 = (a_M - \tilde{a}_M) . b^M + (a_{M-1} - \tilde{a}_{M-1}) . b^{M-1} + \cdots + (a_1 - \tilde{a}_1) . b + (a_0 - \tilde{a}_0)$$

eşitliğine ulaşırız. Şimdi her $i = 0, 1, \ldots, M$ için $c_i$ sayısını $c_i = a_i - \tilde{a}_i$ olarak tanımlayalım ve yukarıdaki eşitliği

$$0 = c_M . b^M + c_{M-1} . b^{M-1} + \cdots + c_1 . b + c_0$$

biçiminde tekrar yazalım. Buradaki $c_i$ katsayıları tam olarak $a_i$ ve $\tilde{a}_i$ katsayılarının farkı olarak tanımlandığından, $a_i = \tilde{a}_i$ şartı ile $c_i = 0$ şartı denktir, dolayısıyla $a_i$ ve $\tilde{a}_i$ sayılarının eşit olduğunu göstermek için $c_i = 0$ olduğunu göstermemiz yeterlidir.

Çelişkiyle ispat yapmak üzere, kimi $i$ indeksleri için $c_i \neq 0$ olduğunu varsayalım. Söz konusu $c_i$ katsayılarının sıfırdan farklı olduğu en küçük

indeks $i = s$ olsun. Bu durumda, $c_s \neq 0$ olmak üzere

$$\begin{aligned} 0 &= c_M.b^M + c_{M-1}.b^{M-1} + \cdots + c_{s+1}.b^{s+1} + c_s.b^s \\ &= (c_M.b^{M-s} + c_{M-1}.b^{M-s-1} + \cdots + c_{s+1}.b + c_s).b^s \end{aligned}$$

eşitliğini elde ederiz. Sağdaki çarpımda $b^s \neq 0$ olduğundan

$$c_M.b^{M-s} + c_{M-1}.b^{M-s-1} + \cdots + c_{s+1}.b + c_s = 0$$

olması gerektiğini görüyoruz. Burada $c_s$ sayısını eşitliğin solunda yalnız bırakarak ve sonrasında sağ taraftaki ifadeyi $b$ parantezine alarak

$$\begin{aligned} c_s &= -c_M.b^{M-s} - c_{M-1}.b^{M-s-1} - \cdots - c_{s+1}.b \\ c_s &= (-c_M.b^{M-s-1} - c_{M-1}.b^{M-s-2} - \cdots - c_{s+1}).b \end{aligned}$$

eşitliğine ulaşıyoruz. Bu da bize $b \mid c_s$ olduğunu gösteriyor. Diğer yandan, $c_s = a_s - \tilde{a}_s$ olarak tanımlandığından ve $0 \leqslant a_s, \tilde{a}_s < b$ olduğundan

$$-b < c_s < b$$

olduğunu görüyoruz. Bu da $b \mid c_s$ ile birlikte düşünüldüğünde bize $c_s = 0$ olması gerektiğini söylüyor ki $c_s \neq 0$ olduğunu biliyoruz, dolayısıyla $c_i$ sayılarının sıfırdan farklı olabileceği varsayımından bir çelişkiye ulaştık. Böylece her bir $i$ için $c_i = 0$ olduğunu, bunun sonucu olarak da $a_i = \tilde{a}_i$ olduğunu göstermiş olduk. □

Bu teorem ile, her $n$ pozitif sayısının yukarıda tarif edilen $0 \leqslant a_i < b$ sayıları tarafından tek bir şekilde belirlendiğini görüyoruz.

**Tanım 12.3.** Bir $b > 1$ sayısı ve her $i = 0, 1, \ldots, m$ için $0 \leqslant a_i < b$ şartını sağlayan $a_m, a_{m-1} \ldots, a_1, a_0$ sayıları verilmiş olsun. Bu özelliği sağlayan sayılar için $(a_m a_{m-a} \ldots a_1 a_0)_b$ ifadesini

$$\begin{aligned} (a_m a_{m-a} \ldots a_1 a_0)_b &:= a_m.b^m + a_{m-1}.b^{m-a} + \cdots + a_1.b + a_0 \\ &= \sum_{i=0}^{m} a_i.b^i \end{aligned}$$

sayısı olarak tanımlıyoruz. Bir $n$ pozitif sayısı için eğer $n = (a_m a_{m-a} \ldots a_1 a_0)_b$ ise $(a_m a_{m-a} \ldots a_1 a_0)_b$ ifadesi, $n$ sayısının *$b$ tabanında gösterimi* olarak adlandırılır.

Sayıların alışageldiğimiz yazımının, sayıların 10 tabanında gösterimine karşılık geldiğine dikkat edelim. Örneğin 366 sayısı için

$$366 = (366)_{10}$$

olduğunu görüyoruz. Yine aynı sayının 5 tabanındaki gösterimini Örnek 12.1'de

$$366 = (2431)_5$$

olarak elde ettiğimizi de gözlemleyelim. Sayıların 2 tabanında gösterimi (özellikle bilgisayar biliminde) büyük öneme sahiptir. Yine 366 sayısını ele alacak olursak, bu sayının 2 tabanında gösterimini bölümün başındaki prosedürü bu sefer 2 ile bölmeler kullanarak elde edebiliz. Bu gösterime ulaşmanın bir diğer yolu ise, bu sayıyı 2'nin üslerinin toplamı olarak yazmaktır:

$$\begin{aligned} 366 &= 256 + 64 + 32 + 8 + 4 + 2 \\ &= 2^8 + 2^6 + 2^5 + 2^3 + 2^2 + 2^1 \\ &= 1.2^8 + 0.2^7 + 1.2^6 + 1.2^5 + 0.2^4 + 1.2^3 + 1.3^2 + 1.2^1 + 0.2^0 \\ &= (101101110)_2 \ . \end{aligned}$$

## 12.2 Polinomlar

Bir $x$ *belirsizi*[1] ve tamsayıları kullanarak yazabileceğimiz; $a_0, a_1, \ldots, a_m \in \mathbb{Z}$ olmak üzere

$$p(x) = a_m.x^m + a_{m-1}.x^{m-1} + \cdots + a_1.x + a_0$$

biçimindeki ifadelere *tamsayı katsayılı polinomlar* denir. Eğer $p(x)$ polinomu bir fonksiyon olarak kullanılırsa, yani $x$ yerine tamsayı değerleri konularak tamsayı değerleri elde edilirse, buradaki $x$ belirsizi değişken görevi görür. Bir $p(x)$ polinomundan bu şekilde elde edilen $p : \mathbb{Z} \to \mathbb{Z}$ biçimindeki fonksiyonlara *polinom fonksiyon* denir.

[1] ing. *indeterminate*.

Tamsayılar üzerinde bütün polinomlar kümesi $\mathbb{Z}[x]$ ile gösterilir ve *tamsayı katsayılı polinom halkası*[2] olarak isimlendirilir.

Her $n$ pozitif sayısı için benzeri bir şekilde $\mathbb{Z}_n$ *katsayılı polinomları* da tanımlayabiliriz: $\overline{a_m}, \overline{a_m - 1}, \ldots, \overline{a_1}, \overline{a_0} \in \mathbb{Z}_n$ olmak üzere

$$P(x) = \overline{a_m}.x^m + \overline{a_m - 1}.x^{m-1} + \cdots + \overline{a_1}.x + \overline{a_0}$$

biçiminde ifadelere $\mathbb{Z}_n$ *katsayılı polinomlar* diyeceğiz. Bütün $\mathbb{Z}_n$ katsayılı polinomlardan oluşan kümeyi $\mathbb{Z}_n[x]$ ile göstereceğiz ve $\mathbb{Z}_n$ *katsayılı polinom halkası* olarak adlandıracağız. Yine $\mathbb{Z}_n$ katsayılı polinomlardan da belirsize değişken muamelesi yapılarak birer

$$p : \mathbb{Z}_n \to \mathbb{Z}_n$$

biçiminde fonksiyon elde edilebilir.

**Örnek 12.2.** $\mathbb{Z}_5$ katsayılı bir $P(x) \in \mathbb{Z}_5[x]$ polinomu

$$P(x) = \overline{3}x^3 - x^2 + \overline{2}$$

olarak tanımlanabilir ($x^2$ teriminin katsayısının $\overline{-1}$ olduğunu düşünebiliriz.)

Bu polinomdan elde edilen polinom fonksiyon, $x = \overline{2}$'de şu şekilde hesaplanabilir:

$$\begin{aligned} P(\overline{2}) &= \overline{3}.\overline{2}^3 - \overline{2}^2 + \overline{2} \\ &= \overline{3}.\overline{8} - \overline{4} + \overline{2} \\ &= \overline{3}.\overline{3} - \overline{4} + \overline{2} \\ &= \overline{9} - \overline{4} + \overline{2} \\ &= \overline{9 - 4 + 2} = \overline{7} = \overline{2}\ . \end{aligned}$$

Eğer elimizde tamsayı katsayılı bir $p(x) \in \mathbb{Z}[x]$ polinomu varsa, katsayıların kalan sınıflarına geçerek bu polinomdan $\overline{p}(x)$ ile göstereceğimiz bir

[2] Bu kümenin *halka* olarak isimlendirilmesinin sebebi, üzerinde belli temel özelliklere sahip toplama ve çarpmanın tanımlı olmasıdır. Halkalar ve özel olarak polinom halkaları üzerine soyut cebir alanında derinlemesine çalışılır.

$\mathbb{Z}_n$ katsayılı polinom elde edebiliriz. Daha net bir şekilde yazacak olursak, eğer $p(x) \in \mathbb{Z}[x]$ polinomu

$$p(x) = a_m.x^m + a_{m-1}.x^{m-1} + \cdots + a_1.x + a_0$$

olarak tanımlanmışsa $\overline{p}(x) \in \mathbb{Z}_n[x]$ polinomu

$$\overline{p}(x) = \overline{a_m}.x^m + \overline{a_{m-1}}.x^{m-1} + \cdots + \overline{a_1}.x + \overline{a_0}$$

olarak tanımlanır.

**Örnek 12.3.** Tamsayı katsayılı

$$p(x) = 3x^2 - 4x + 7 \in \mathbb{Z}[x]$$

polinomu verilsin. Bu polinomdan elde edilen $\mathbb{Z}_6$ katsayılı $\overline{p}(x)$ polinomu

$$\begin{aligned}\overline{p}(x) &= \overline{3}x^2 + \overline{(-4)}x + \overline{7} \\ &= \overline{3}x^2 + \overline{2}x + \overline{1}\end{aligned}$$

olarak ifade edilebilir.

Tamsayı katsayılı polinom fonksiyonlar ile onlardan elde edilen $\mathbb{Z}_n$ katsayılı polinom fonksiyonlar arasındaki ilişki, sıradaki önerme tarafından veriliyor.

**Önerme 12.4.** *Tamsayı katsayılı bir $p(x)$ polinomu ve bir $c \in \mathbb{Z}$ sayısı verilsin. Bu $p(x)$ polinomundan elde edilen $\mathbb{Z}_n$ katsayılı polinom $\overline{p}(x)$ ile, $c$ sayısının modülo $n$'de kalan sınıfı $\overline{c}$ ile gösterilmek üzere*

$$\overline{p}(\overline{c}) = \overline{p(c)}$$

*sağlanır.*

***Kanıt.*** $p(x)$ polinomu belli $a_0, a_1, \ldots, a_m \in \mathbb{Z}$ sayıları için

$$p(x) = a_m.x^m + a_{m-1}.x^{m-1} + \cdots + a_1.x + a_0$$

olarak verilmiş olsun. Bu durumda, kalan sınıfları için toplama ve çarpmanın tanımından

$$\begin{aligned}\overline{p(c)} &= \overline{a_m.c^m + a_{m-1}.c^{m-1} + \cdots + a_1.c + a_0} \\ &= \overline{a_m}.\overline{c}^m + \overline{a_{m-1}}.\overline{c}^{m-1} + \cdots + \overline{a_1}.\overline{c} + \overline{a_0} \\ &= \overline{p}(\overline{c})\end{aligned}$$

sonucunu elde ederiz. □

## 12.3 Bölünürlük kuralları

Eğitim hayatımızın daha erken aşamalarında, muhtemelen 'tam bölünebilme kuralları' adı altında öğrendiğimiz kimi bölünürlük kurallarını derinlemesine anlayacak ve bu kuralları ispatlayabilecek kuramsal donanıma ulaşmış bulunuyoruz. Bu kuralların en ünlülerinden biri olan 9'a bölünürlük kuralını, geliştirmiş bulunduğumuz çerçevede bir önerme olarak aşağıda ifade edelim ve ispatlayalım.

**Önerme 12.5.** *Bir $n$ sayısı 10 tabanında $0 \leqslant a_0, \ldots, a_m < 10$ sayıları ile*

$$n = (a_m a_{m-1} \ldots a_1 a_0)_{10}$$

*biçiminde ifade edilmiş olsun. Bu durumda*

$$n \equiv a_m + a_{m-1} + \cdots + a_1 + a_0 \pmod 9$$

*sağlanır.*

***Kanıt.*** Tamsayı katsayılı bir $p(x) \in \mathbb{Z}[x]$ polinomununu $a_0, \ldots, a_m$ sayılarını katsayı olarak kullanarak

$$p(x) = a_m.x^m + a_{m-1}.x^{m-1} + \cdots + a_1 x + a_0$$

olarak tanımlayalım. Verilen $n$ sayısı 10 tabanında

$$\begin{aligned}n &= (a_m a_{m-1} \ldots a_1 a_0)_{10} \\ &= a_m.10^m + a_{m-1}.10^{m-1} + \cdots + a_1.10 + a_0\end{aligned}$$

olarak ifade edildiğinden, bu polinom için

$$n = p(10)$$

eşitliğinin sağlandığını gözlemleyelim. Şimdi, herhangi bir $a$ tamsayısının modülo 9'daki kalan sınıfı $\overline{a}$ ile gösterilmek üzere, Önerme 12.4 kullanılarak $\mathbb{Z}_9$'da

$$\begin{aligned}
\overline{n} &= \overline{p(10)} \\
&= \overline{p}(\overline{10}) \\
&= \overline{p}(\overline{1}) \\
&= \overline{a_m}.\overline{1}^m + \overline{a_{m-1}}.\overline{1}^{m-1} + \cdots + \overline{a_1}.\overline{1} + \overline{a_0} \\
&= \overline{a_m} + \overline{a_{m-1}} + \cdots + \overline{a_1} + \overline{a_0} \\
&= \overline{a_m + a_{m-1} + \cdots + a_1 + a_0}
\end{aligned}$$

eşitliğine ulaşıyoruz. Bu da tam olarak ispatlamaya çalıştığımız

$$n \equiv a_m + a_{m-1} + \cdots + a_1 + a_0 \pmod{n}$$

kalandaşlığının kalan sınıfları dilinde ifadesidir. □

**Sonuç 12.6.** *Bir $n = (a_m a_{m-1} \ldots a_1 a_0)_{10}$ sayısı 9 ile bölünür ancak ve ancak $a_m + a_{m-1} + \cdots + a_1 + a_0$ sayısı 9 ile bölünür ise.*

***Kanıt.*** Önerme 12.5 ile $n \equiv a_m + a_{m-1} + \cdots + a_1 + a_0 \pmod 9$ olduğunu hatırlayalım. Dolayısıyla, $n \equiv 0 \pmod 9$ ile $a_m + a_{m-1} + \cdots + a_1 + a_0 \equiv 0 \pmod 9$ ifadeleri mantıksal olarak denktir. Öyleyse

$$\begin{aligned}
9 \mid n &\iff n \equiv 0 \pmod 9 \\
&\iff a_m + a_{m-1} + \cdots + a_1 + a_0 \equiv 0 \pmod 9 \\
&\iff 9 \mid a_m + a_{m-1} + \cdots + a_1 + a_0
\end{aligned}$$

mantıksal denkliklerini elde ederiz. □

**Örnek 12.4.** $n = 63485467$ sayısının 9 ile bölme algoritmasıyla bölündüğünde kalan olarak kaçı vereceğini Önerme 12.5 ile hesaplayalım. Bu

önerme ile

$$63485467 \equiv 6+3+4+8+5+4+6+7 \pmod 9$$
$$63485467 \equiv 43 \pmod 9$$

olduğunu elde ederiz. Bu aşamada 43'ü 9'a bölerek kalanı hesaplamak zor olmasa da, biz Önerme 12.5'i tekrar uygulayalım:

$$43 \equiv 4+3 \pmod 9$$
$$43 \equiv 7 \pmod 9 \ .$$

Böylece 63485467'nin 9 ile bölümünün 7 kalanını verdiğini, özel olarak da 63485467'nin 9'a bölünmediğini yani $9 \nmid 63485467$ sonucunu elde etmiş olduk.

# Bölüm 13

# Fermat'nın küçük teoremi

**Lemma 13.1.** *Verilen bir $a$ sayısı ve $p$ asalı için $p \nmid a$ olsun.*[1] *Bu durumda modülo $p$'deki kalandaşlık sınıfları kümesi*

$$\mathbb{Z}_p = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}, \overline{pa}\}$$

*olur.*

***Kanıt.*** Öncelikle

$$\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}, \overline{pa} \in \mathbb{Z}_p$$

kalandaşlık sınıflarını düşünelim. Eğer $\mathbb{Z}_p$'nin bu elemanlarının hepsinin birbirinden farklı olduğunu ispatlayabilirsek, bu listede tam olarak $p = |\mathbb{Z}_p|$ adet kalandaşlık sınıfı olduğunu ve dolayısıyla $\mathbb{Z}_p$'nin bütün elemanlarının bu listeden ibaret olduğunu göstermiş oluruz.

Olmayana ergi yöntemi kullanmak üzere bu listedeki iki kalandaşlık sınıfının eşit olduğunu, yani $1 \leqslant k < l \leqslant p$ şartını sağlayan $k$ ve $l$ sayıları için $\overline{ka} = \overline{la}$ eşitliğinin sağlandığını varsayalım. Bu durumda,

$$ka \equiv la \pmod{p}$$

[1] $p$ sayısı asal olduğundan bu koşul $p$ ve $a$ sayılarının aralarında asal olmalarıyla denktir..

kalandaşlığını elde ederiz. Bu da bize

$$p \mid (la - ka) = a(l - k)$$

bölünürlük ilişkisini verir. Burada $p$ bir asal olduğundan Önerme 8.4 ile $p \mid a$ veya $p \mid l - k$ olması gerektiği sonucuna ulaşırız. Fakat ebob$(p, a) = 1$ ve $p$ asal olduğundan $p \nmid a$ olduğunu; $0 < l - k < p$ olduğundan ise $p \nmid l - k$ olduğunu görüyoruz. Dolayısıyla bir çelişkiye ulaşmış olduk. □

**Lemma 13.2.** *Her $p$ asalı için $p$ ile $n = (p-1)! = 1.2. \ldots .(p-1)$ aralarında asaldır.*

***Kanıt.*** Verilen $p$ sayısı asal olduğundan, $p$ ile $n$ sayılarının aralarında asal olması ile $p \nmid n$ birbirine denktir, dolayısıyla $p \nmid n$ olduğunu göstermemiz yeterlidir.

Olmayana ergi yöntemi kullanmak üzere $p \mid n$ olduğunu varsayalım. Bu durumda

$$p \mid 1.2. \ldots .(p-1)$$

olacağından Önerme 8.5 ile, $0 < i < p$ şartını sağlayan bir $i$ sayısı için $p \mid i$ sonucu çıkar, ki bu da Bölüm 4 Özellik **VIII.** ile çelişir. □

**Teorem 13.3** (Fermat'nın Küçük Teoremi)**.** *Bir $p$ asal sayısı ve bir $\overline{a} \in \mathbb{Z}_p$ kalandaşlık sınıfı için, eğer $\mathbb{Z}_p$'de $\overline{a} \neq \overline{0}$ ise*

$$\overline{a}^{p-1} = \overline{1}$$

*sağlanır.*

***Kanıt.*** Lemma 13.1 ile

$$\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}, \overline{pa} \in \mathbb{Z}_p$$

kalandaşlık sınıflarının her birinin farklı olduğunu ve modülo p'de tüm kalandaşlık sınıflarının bunlardan ibaret olduğunu biliyoruz. Burada, $\overline{pa}$ ile sıfır kalandaşlık sınıfı, yani $\overline{0}$ ifade edildiğinden

$$\{\overline{1}, \overline{2}, \ldots, \overline{p-1}\} = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\}$$

küme eşitliği sağlanır. Bu gösterimdeki elemanların çarpımları eşittir, dolayısıyla

$$\begin{aligned}
\overline{1}.\overline{2}.\ \ldots\ .\overline{p-1} &= \overline{a}.\overline{2a}.\ \ldots\ .\overline{(p-1)a} \\
\overline{1.2.\ \ldots\ .(p-1)} &= \overline{1.2a.\ \ldots\ .(p-1)a} \\
\overline{(p-1)!} &= \overline{(p-1)!a^{p-1}} \\
\overline{(p-1)!} &= \overline{(p-1)!}.\overline{a}^{p-1}
\end{aligned}$$

sonucunu elde ederiz. Lemma 13.2 ile $(p-1)!$ ile $p$ aralarında asal olduğundan $\overline{(p-1)!}$ kalandaşlık sınıfının $\mathbb{Z}_p$'de tersi vardır, dolayısıyla yukarıdaki eşitlikte bu ifadeyi denklemin iki tarafından sadeleştirebilir ve aradığımız

$$\overline{1} = \overline{a}^{p-1}$$

kalandaşlık sınıfları eşitliğini elde ederiz. □

Bu teoremi, kalandaşlık bağıntısı diliyle de ifade etmek yaygındır:

**Sonuç 13.4.** *Her $p$ asalı ve $p \nmid a$ şartını sağlayan $a$ sayısı için*

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

*sağlanır.*

Bu sonuçtaki kalandaşlığın her iki tarafını da $a$ ile çarptığımızda, Fermat'nın Küçük Teoremi'nin çok kullanışlı bir diğer görünümünü elde ederiz:

**Sonuç 13.5.** *Her $p$ asalı ve $p \nmid a$ şartını sağlayan $a$ sayısı için*

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

*sağlanır.*

# Bölüm 14

# Pisagor üçlüleri

**Tanım 14.1.** Eğer $a, b$ ve $c$ pozitif sayıları için

$$a^2 + b^2 = c^2$$

eşitliği sağlanıyor ise $(a, b, c)$ bir *Pisagor üçlüsüdür* denir.

Verilen herhangi üç sayının pozitif ortak bölen kümesini

$$\begin{aligned}\mathcal{OB}^+(a, b, c) &= \{d \in \mathbb{Z}^+ : d \mid a, d \mid b, d \mid c\} \\ &= \mathcal{B}^+(a) \cap \mathcal{B}^+(b) \cap \mathcal{B}^+(c)\end{aligned}$$

olarak tanımlayalım. İki sayının ortak bölen kümesi için olduğu gibi, bu sayılardan en az biri sıfırdan farklı ise $\mathcal{OB}^+(a, b, c)$ kümesi sonludur ve dolayısıyla bir maksimum elemanı vardır. Bu maksimumu $a, b, c$ sayılarının en büyük ortak ortak böleni olarak tanımlayalım ve

$$\text{ebob}(a, b, c) := \max \mathcal{OB}^+(a, b, c)$$

ile gösterelim.

**Tanım 14.2.** Eğer $(a, b, c)$ şeklinde bir Pisagor üçlüsü için $\text{ebob}(a, b, c) = 1$ ise, $(a, b, c)$ bir *ilkel Pisagor üçlüsüdür* denir.

Her $(a, b, c)$ Pisagor üçlüsü için, $d = \text{ebob}(a, b, c)$ olmak üzere $(a : d, b : d, c : d)$ bir ilkel Pisagor üçlüsü olur. Demek ki her Pisagor üçlüsünü bir ilkel pisagor üçlüsünden, terimlerinin hepsini bir pozitif sayıyla çarparak elde edebiliriz. Yani bütün Pisagor üçlülerini bulmak için ilkel Pisagor üçlülerini bulmamız yeterlidir.

**Lemma 14.3.** *Eğer $(a, b, c)$ bir ilkel Pisagor üçlüsü ise $a, b$ ve $c$ sayılarının herhangi ikisi aralarında asaldır.*

***Kanıt.*** $(a, b, c)$ bir ilkel Pisagor üçlüsü olsun ve olmayana ergi yöntemi kullanmak üzere, $a$ ve $b$ sayılarının aralanda asal olmadıklarını varsayalım. Bu durumda bir $p$ asalı için $p \mid a$ ve $p \mid b$ sağlanır. Bu durumda $p \mid a^2$ ve $p \mid b^2$ olduğunu, bunun sonucu olarak da $p \mid a^2 + b^2 = c^2$ olduğunu görüyoruz. Fakat bu da $p$ asal olduğundan $p \mid c$ olduğu sonucunu ve dolayısıyla da $\text{ebob}(a, b, c) \neq 1$ olduğunu verir, bu ise $(a, b, c)$ Pisagor üçlüsünün ilkelliğiyle çelişir (egzersiz).

Aynı yöntemle, $a$ ile $c$'nin ve $b$ ile $c$'nin de aralarında asal oldukları gösterilebilir. □

**Lemma 14.4.** *Eğer $(a, b, c)$ bir ilkel Pisagor üçlüsü ise $a$ ve $b$ sayılarının biri çift diğeri tektir.*

***Kanıt.*** Bir $(a, b, c)$ ilkel Pisagor üçlüsü için $a$ ve $b$ sayılarının ikisinin birden çift ya da ikisinin birden tek olamayacağını gösterelim.

Buradaki $a$ ve $b$ sayılarının ikisinin birden çift olamayacağını Lemma 14.3 ile hemen görüyoruz: Eğer $a$ ve $b$ çift olsaydı aralarında asal olmazlardı.

Şimdi $a$ ve $b$ sayılarının ikisinin birden tek olamayacağını gösterelim. Olmayana ergi yöntemi kullanmak üzere, ikisinin de tek olduğunu varsayalım. Bu durumda $a = 2k+1, b = 2l+1$ olacak şekilde $k$ ve $l$ sayıları vardır.

Öyleyse

$$\begin{aligned} c^2 &= a^2 + b^2 \\ &= (2k+1)^2 + (2l+1)^2 \\ &= 4k^2 + 4k + 1 + 4l^2 + 4k + 1 \\ &= 4(k^2 + k + l^2 + l) + 2 \end{aligned}$$

eşitliğini elde ederiz. Bu da modülo 4'te

$$c^2 \equiv 2 \pmod 4$$

kalandaşlığını verir. Fakat modülo 4'te hiçbir sayının karesi 2 ile kalandaş olamayacağından, bu bir çelişki verir. [1] □

Bu lemmanın sonucu olarak, herhangi bir $(a, b, c)$ ilkel Pisagor üçlüsü için $c^2 = a^2 + b^2$ olduğundan $c^2$ sayısının her zaman tek olduğunu, buradan da $c$ sayısının bir tek sayı olacağını elde ederiz.

**Lemma 14.5.** *Eğer aralarında asal olan $m$ ve $n$ pozitif sayılarının çarpımı bir $x$ pozitif sayısının karesine eşitse, yani* $\text{ebob}(m, n) = 1$ *ise ve bir $x$ sayısı için*

$$mn = x^2$$

*sağlanıyorsa,*

$$m = u^2, n = v^2$$

*olacak şekilde $u$ ve $v$ pozitif sayıları vardır.*

***Kanıt***. Lemmada varsayıldığı gibi, $m, n$ ve $x$ sayıları için $\text{ebob}(m, n) = 1$ ve $x^2 = mn$ eşitlikleri sağlansın. Bu durumda $x \mid mn$ ve $\text{ebob}(m, n) = 1$ olduğundan, Önerme 9.3 ile

$$x = uv, u \mid m, v \mid n$$

[1] Modülo 4'te hiçbir sayının karesinin 2 ile kalandaş olamayacağını görmek için, $\mathbb{Z}_4$'te

$$\overline{0}^2 = \overline{0}, \qquad \overline{1}^2 = \overline{1}, \qquad \overline{2}^2 = \overline{0}, \qquad \overline{3}^2 = \overline{1}$$

olduğunu gözlemleyelim.

olacak şekilde $u$ ve $v$ pozitif sayılarının var olduğunu görüyoruz.

Buradaki $m$ ve $n$ sayıları aralarında asal ve $u \mid m$ olduğundan $u$ ve $n$ sayıları da aralarında asal olur. Dolayısıyla, $u^2$ ve $n$ sayıları da aralarında asaldır. [2] Şimdi,

$$u^2 \mid u^2v^2 = x^2 = mn$$

olduğunu gözlemliyoruz ve $\text{ebob}(u^2, n) = 1$ olduğundan $u^2 \mid m$ olduğu sonucuna varıyoruz (neden? egzersiz). Aynı şekilde $v^2 \mid n$ olduğunu da gösterebiliriz.

Bölüm 4 Özellik **VIII.** ile $u^2 \leqslant m$ ve $v^2 \leqslant n$ olduğunu görüyoruz. Eğer $u^2 \neq m$ veya $v^2 \neq n$ olsaydı

$$x^2 = (uv)^2 = u^2v^2 < mn = x^2$$

çelişkisini elde ederdik. Böylece $u$ ve $v$ sayıları için

$$m = u^2, n = v^2$$

olduğu sonucuna ulaşıyoruz.

Yukarıdaki $u^2 \mid m$ ve $v^2 \mid n$ ifadelerini birleştirerek $u^2v^2 \mid mn = x^2$ olduğunu da görüyoruz. □

Yukarıdaki ispatta egzersiz olarak bıraktığımız özelliği bir soru olarak formüle edelim:

***Soru* 1.** Eğer $m, n$ ve $k$ sayıları için

$$k \mid mn \quad \text{ve} \quad \text{ebob}(k, n) = 1$$

ise $k \mid m$ olduğunu gösterin.

[2] Bunu görmek için, $u^2$ ve $n$'nin aralarında asal olmadıklarını varsayalım. Bu durumda bir $p$ asalı için $p \mid u^2$ ve $p \mid n$ sağlanır. Bu durumda $p \mid u$ olduğunu da görürüz. Dolayısıyla $p$ asalının $u$ ve $n$ sayılarının bir ortak böleni olduğu sonucu çıkar, ki bu da $u$ ve $n$'nin aralarında asal olmasıyla çelişir.

**Teorem 14.6.** *$a$ sayısı çift olmak üzere bütün $(a, b, c)$ ilkel Pisagor üçlüleri, tam olarak*

$$u > v > 0,\ \text{ebob}(u, v) = 1 \quad ve \quad u \not\equiv v \pmod 2$$

*şartlarını sağlayan belli $u$ ve $v$ sayıları için*

$$\begin{aligned} a &= 2uv\ , \\ b &= u^2 - v^2\ , \\ c &= u^2 + v^2 \end{aligned}$$

*olarak ifade edilen sayılardan oluşur.*

***Kanıt***. İlk olarak, $a$ sayısı çift olmak üzere bir $(a, b, c)$ ilkel Pisagor üçlüsü alalım ve teoremde verilen özelliklere sahip $u$ ve $v$ sayıları bulunabileceğini gösterelim.

Öncelikle; Lemma 14.4 ve sonrasındaki açıklama ile $b$ ve $c$ sayılarının tek olduğunu görüyoruz. Öyleyse $c + b$ ve $c - b$ sayıları çifttir, yani 2 ile bölünürler. Dolayısıyla, $m$ ve $n$ pozitif tamsayılarını

$$m := (c + b) : 2 \qquad n := (c - b) : 2$$

olarak tanımlayabiliriz. Burada $c > b > 0$ olduğunu bildiğimizden

$$m > n > 0$$

olduğunu da görüyoruz. Ek olarak, bu $m$ ve $n$ sayılarının aralarında asal olduklarını da görebiliriz. Çünkü aksi takdirde bir $p$ asalı hem $m$ hem $n$ sayısını bölerdi, bu durumda da

$$p \mid m + n = c \quad \text{ve} \quad p \mid m - n = b$$

olmasını gerektirirdi. Fakat Lemma 14.3 ile $b$ ve $c$ sayılarının aralarında asal olduklarını, dolayısıyla bunun doğru olamayacağını biliyoruz.

Şimdi $mn$ çarpımını hesaplayalım:

$$\begin{aligned} mn &= [(c+b):2].[(c-b):2] \\ &= [(c+b)(c-b)]:4 \\ &= (c^2-b^2):4 \\ &= a^2:4 \\ &= (a:2)^2 \ . \end{aligned}$$

Böylece, $mn$ çarpımının bir sayının karesine eşit olduğunu görmüş olduk. Ek olarak $m$ ve $n$ sayılarının aralarında asal olduklarını da bildiğimizden, Lemma 14.5 ile

$$m = u^2, \ n = v^2$$

olacak şekilde $u$ ve $v$ pozitif sayılarının var olduğunu görüyoruz. Bu şekilde tanımlı $u$ ve $v$ sayıları için

$$c = m + n = u^2 + v^2 \quad \text{ve} \quad b = m - n = u^2 - v^2$$

olduğunu hemen görüyoruz. Ayrıca

$$\begin{aligned} a^2 &= c^2 - b^2 \\ &= (c+b)(c-b) \\ &= 2m.2n \\ &= 4u^2v^2 \\ &= (2uv)^2 \end{aligned}$$

olduğundan ve $a > 0, 2uv > 0$ olduğunu bildiğimizden

$$a = 2uv$$

sonucuna da ulaşırız. Böylece $a, b$ ve $c$ sayılarının $u$ ve $v$ sayıları için istediğimiz formda olduklarını görüyoruz. Ayrıca $m > n$ olduğundan $u > v$ de sağlanır. Bu $u$ ve $v$ sayıları aralarında asaldır; çünkü eğer aralarında asal olmasalardı bir $p$ asalı için $p \mid u$ ve $p \mid v$ sağlanırdı, bu da $p \mid u^2 = m$ ve $p \mid v^2 = n$ olmasını gerektirirdi ki bu sonuç $m$ ve $n$ sayılarının aralarında

asal olmasıyla çelişirdi. Dolayısıyla $u$ ve $v$ ile ilgili göstermemiz gereken koşullardan sadece $u \not\equiv v \pmod 2$ olduğu kaldı. Bu koşul ise

$$u + v \equiv 1 \pmod 2$$

kalandaşlığı ile, yani $u + v$ sayısının tek olması ile denktir. Bu sonuca ulaşmak için önce

$$(u + v)^2 = u^2 + v^2 + 2uv = m + n + 2uv = c + 2uv$$

olduğunu gözlemleyelim. Buradaki $c$ sayısının tek olduğunu biliyoruz, dolayısıyla $2uv$ çift olduğundan $(u+v)^2$ sayısının, buradan da $u+v$ sayısının tek olduğunu görüyoruz.

Şimdi de $u > v > 0, \text{ebob}(u, v) = 1$ ve $u \not\equiv v \pmod 2$ koşullarını sağlayan bütün $u, v$ sayı çiftleri için

$$a = 2uv, \;\; b = u^2 - v^2, c = u^2 + v^2$$

şeklinde tanımlı $(a, b, c)$ sayılarının $a$ çift olmak üzere birer ilkel Pisagor üçlüsü oluşturduğunu ispatlayalım. Böyle tanımlı $a$ sayısının çift olduğu aşikar olduğundan, geriye $a^2 + b^2 = c^2$ eşitliğinin sağlandığını ve $\text{ebob}(a, b, c) = 1$ olduğunu göstermek kalıyor. Bu sayılar için $a^2 + b^2$ toplamını hesaplayarak

$$\begin{aligned} a^2 + b^2 &= (2uv)^2 + (u^2 - v^2) \\ &= 4u^2v^2 + u^4 + 2u^2v^2 + v^4 \\ &= (u^2)^2 + 2u^2v^2 + (v^2)^2 \\ &= (u^2 + v^2)^2 \\ &= c^2 \end{aligned}$$

eşitliğinin sağlandığını, yani $(a, b, c)$'nin bir Pisagor üçlüsü olduğunu görüyoruz.

Şimdi de $\text{ebob}(a, b, c) = 1$ olduğunu göstermek için, olmayana ergi yöntemini kullanmak üzere $\text{ebob}(a, b, c) \neq 1$ olduğunu varsayalım. Bu durumda bir $p$ asalı $a, b$ ve $c$ sayılarının ortak böleni olmalıdır. Bu durumda, bu $p$ asalı $c$'yi böldüğünden $c^2$ sayısını da böler ve dolayısıyla

$$p \mid c^2 = u^2 + v^2 = (u + v)^2 - 2uv$$

sağlanır. Verilen özelliklerden $u \not\equiv v \pmod 2$ olduğunu, yani $u+v$ sayısının tek olduğunu biliyoruz. Dolayısıyla yukarıdaki ifadeden

$$c^2 = (u+v)^2 - 2uv$$

sayısının da tek olduğunu görüyoruz. Böylece, $p$ asalı bir tek sayıyı böldüğünden $p \neq 2$ sonucuna ulaşıyoruz.

Elimizdeki $p$ asalı $b$ ve $c$ sayılarını böldüğünden bu sayıların toplamını ve farkını da böler, dolayısıyla

$$\begin{aligned} &p \mid c+b && p \mid c-b \\ &p \mid u^2+v^2+u^2-v^2 && p \mid u^2+v^2-(u^2-v^2) \\ &p \mid 2u^2 && p \mid 2v^2 \end{aligned}$$

bölünürlük ilişkilerini elde ederiz. Buradan da; $p$ asal ve $p \neq 2$ olduğundan $p \mid u^2$ olduğunu görüyoruz ve $p \mid u$ sonucuna varıyoruz. Aynı şekilde $p \mid v$ olduğu da elde edilebilir. Böylece $p$ asalının $u$ ve $v$'nin bir ortak böleni olduğunu buluyoruz, ki bu $u$ ve $v$ sayılarının aralarında asal olduğuyla çelişir. □