Sayılar Teorisi

Açık Matematik

Açık Matematik — açık kaynaklı, reklamsız Türkçe matematik notları
acik-matematik.com

Bu sürüm: 20 Eylül 2026

İçindekiler

Giriş

Sayılar teorisi, tam sayıların yapısını ve aralarındaki gizli ilişkileri inceleyen; matematiğin en eski, en zarif ve —modern kriptografi sayesinde— en beklenmedik biçimde uygulamalı dallarından biridir.
Bu notlar iki ana bölümden oluşur. **Sayılar Teorisi 1**, bölünebilme kurallarından asal sayıların doğasına ve klasik modüler aritmetiğe kadar tam sayıların temel yapı taşlarını kurar. **Sayılar Teorisi 2** ise modern kriptografinin altyapısını oluşturan ileri kongrüanslar, kuadratik kalanlar ve primitif kökler gibi daha derin analitik araçları ele alır.

1. Tümevarım ve İyi Sıralama Prensibi

Sayılar teorisi, tam sayıların yapısını inceler. Bu yapının üzerine kurulduğu temel, doğal sayıların **sıralanışıdır**: her doğal sayıdan sonra bir sonraki gelir ve geriye doğru sonsuza kadar inilemez. Bu bölümde bu basit gözlemin iki farklı yüzü olan *tümevarım* ile *iyi sıralama prensibini* tanıtacak, dersin geri kalanında sürekli kullanacağımız ispat tekniklerini kuracağız.

1.1 Notasyon

Ders boyunca aşağıdaki gösterimleri kullanacağız.

Sembol	Küme	Elemanları
$\mathbb{N}$	Doğal sayılar	$1, 2, 3, \ldots$
$\mathbb{Z}$	Tam sayılar	$\ldots, -2, -1, 0, 1, 2, \ldots$
$\mathbb{Q}$	Rasyonel sayılar	$\frac{a}{b}$ biçimindeki sayılar $(a \in \mathbb{Z}, b \in \mathbb{N})$

i Notasyon anlaşması

Bu notlarda $\mathbb{N}$ kümesi 1'den başlar; 0 doğal sayı sayılmaz. Sıfırı da katmak istediğimizde $\mathbb{N} \cup \{0\}$ yazacağız.

1.2 Tümevarım Yöntemi

Sonsuz sayıda önermeyi tek tek doğrulamak mümkün değildir. Tümevarım, bu sonsuz doğrulamayı iki adımlık sonlu bir işe indirger: ilk önermeyi doğrularız, sonra da her önermenin bir sonrakini doğurduğunu gösteririz.

Teorem 1.1 (Tümevarım İlkesi). *Her $n \in \mathbb{N}$ için $p(n)$ bir önerme olsun. Eğer*

1. *$p(1)$ doğruysa (yani önerme $n = 1$ için doğruysa),*
2. *her $k \in \mathbb{N}$ için, $p(k)$ doğru olduğunda $p(k+1)$ de doğru oluyorsa,*

o hâlde her $n \in \mathbb{N}$ için $p(n)$ önermesi doğrudur.

Birinci koşula **başlangıç adımı**, ikincisine **tümevarım adımı** denir. Tümevarım adımında $p(k)$'nin doğruluğunu kabul ederiz; bu kabule **tümevarım hipotezi** adı verilir.

i Neden işe yarıyor?

Domino taşlarını düşünün. Başlangıç adımı ilk taşı devirir; tümevarım adımı ise "devrilen her taş bir sonrakini devirir" güvencesini verir. İkisi birlikte bütün taşların devrildiğini söyler.
İki koşuldan biri olmadan sonuç çökebilir: "n sayısı $n+1$'e eşittir" önermesi tümevarım adımını sağlar ($n = n+1$ ise $n+1 = n+2$'dir) ama başlangıç adımı sağlanmadığından hiçbir n için doğru değildir.

Örnek 1.1 (İlk n Doğal Sayının Toplamı). Her $n \in \mathbb{N}$ için

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

eşitliğini tümevarımla ispatlayınız.

Çözüm.
Her n pozitif tam sayısı için A_n ve B_n sayılarını

$$A_n := 1 + 2 + \cdots + n, \qquad B_n := \frac{n(n+1)}{2}$$

biçiminde tanımlayalım. Her $n \in \mathbb{N}$ için $A_n = B_n$ olduğunu göstermeliyiz.
Başlangıç adımı ($n = 1$).

$$A_1 = 1, \qquad B_1 = \frac{1 \cdot 2}{2} = 1$$

olduğundan $A_1 = B_1$'dir; önerme $n = 1$ için doğrudur.
Tümevarım adımı. $k \in \mathbb{N}$ olsun ve önermenin $n = k$ için doğru olduğunu, yani

$$A_k = B_k = \frac{k(k+1)}{2}$$

eşitliğini varsayalım. $n = k + 1$ için de doğru olduğunu gösterelim. Tanım gereği $A_{k+1} = A_k + (k + 1)$'dir. Tümevarım hipotezini kullanalım:

$$\begin{aligned} A_{k+1} &= A_k + (k+1) \\ &= \frac{k(k+1)}{2} + (k+1) \\ &= (k+1)\left(\frac{k}{2} + 1\right) \\ &= (k+1) \cdot \frac{k+2}{2} \\ &= \frac{(k+1)\,\big(\,(k+1)+1\,\big)}{2} = B_{k+1} \end{aligned}$$

Böylece $A_{k+1} = B_{k+1}$ elde edildi. Tümevarım ilkesi gereği her $n \in \mathbb{N}$ için eşitlik doğrudur.
■

i Gauss'un yöntemi

Aynı sonuç tümevarım kullanmadan da görülebilir. Toplamı bir kez düz, bir kez ters yazıp alt alta toplayalım:

$$\begin{aligned} S &= 1 + 2 + \cdots + (n-1) + n \\ S &= n + (n-1) + \cdots + 2 + 1 \\ 2S &= \underbrace{(n+1) + (n+1) + \cdots + (n+1)}_{n \text{ tane}} = n(n+1) \end{aligned}$$

Buradan $S = n(n+1)/2$ bulunur. Tümevarım bir formülü **doğrulamak** için birebir yöntemdir; ancak formülü **keşfetmek** için çoğu zaman böyle bir fikre ihtiyaç duyarız.

1.3 Tümevarımla Tanım Verme

Tümevarım yalnızca ispat aracı değildir; bir kavramı adım adım **tanımlamak** için de kullanılır. Bir nesneyi $n = 1$ için tanımlar, sonra n'inci adımdan $(n + 1)$'inci adımı üretecek bir kural veririz.

Tanım 1.1 (Faktöriyel). Her $n \in \mathbb{N}$ için $n!$ sembolü tümevarımla şu şekilde tanımlanır:

1. $1! = 1$,
2. her $n \in \mathbb{N}$ için $(n+1)! = n! \cdot (n+1)$.

Bu kural $n!$ sayısını $1 \cdot 2 \cdots n$ çarpımı olarak üretir: $2! = 2$, $3! = 6$, $4! = 24$ ve benzeri.

i 0! neden 1'dir?

Faktöriyelin ileride binom katsayılarıyla birlikte kullanılabilmesi için tanım $n = 0$ noktasına da genişletilir ve

$$0! = 1$$

kabul edilir. Bu keyfî bir seçim değildir: $(n+1)! = n! \cdot (n+1)$ kuralının $n = 0$ için de geçerli olması, yani $1! = 0! \cdot 1$ eşitliğinin bozulmaması isteniyorsa $0!$ mecburen 1 olmalıdır.

1.4 Güçlü Tümevarım

Bazen $p(k+1)$'i ispatlamak için yalnızca $p(k)$ yetmez; daha küçük indislerin hepsine ihtiyaç duyarız. Örneğin bir sayıyı çarpanlarına ayırırken $n = a \cdot b$ yazarız ve a ile b hakkındaki bilgiye başvururuz — bunlar $n-1$ olmak zorunda değildir. Tümevarımın aşağıdaki güçlendirilmiş biçimi tam olarak bu ihtiyacı karşılar.

Teorem 1.2 (Güçlü Tümevarım). *Her $n \in \mathbb{N}$ için $p(n)$ bir önerme olsun. Eğer*

1. *$p(1)$ doğruysa,*
2. *her $k \in \mathbb{N}$ için, $p(1), p(2), \ldots, p(k)$ önermelerinin **hepsi** doğru olduğunda $p(k+1)$ de doğru oluyorsa,*

o hâlde her $n \in \mathbb{N}$ için $p(n)$ önermesi doğrudur.

İki ilke arasındaki tek fark tümevarım hipotezinin genişliğidir: sıradan tümevarımda yalnızca bir önceki adımı, güçlü tümevarımda ise o ana kadarki bütün adımları kullanma hakkımız vardır. Bu, ispat gücünü artırır ama hiçbir şey kaybettirmez; çünkü daha geniş bir hipotezi kullanmak zorunda değilizdir.

Örnek 1.2 (Bir Dizi Eşitsizliği). Aşağıdaki gibi tanımlanan diziyi göz önüne alalım:

$$a_1 = 1, \qquad a_2 = 3, \qquad a_n = a_{n-1} + a_{n-2} \quad (n \geq 3)$$

Her n pozitif tam sayısı için

$$a_n < \left(\frac{7}{4}\right)^n$$

olduğunu gösteriniz. *(Bu diziye Lucas dizisi denir.)*

Çözüm.
Dizinin n'inci terimi kendisinden önceki **iki** terime bağlı olduğundan güçlü tümevarım kullanacağız. Bu nedenle başlangıç adımında iki terimi birden doğrulamamız gerekir.
Başlangıç adımları.

$$a_1 = 1 < \frac{7}{4}, \qquad a_2 = 3 < \left(\frac{7}{4}\right)^2 = \frac{49}{16} = 3{,}0625$$

Her iki eşitsizlik de sağlanıyor. *(İkincisinin ne kadar dar bir farkla sağlandığına dikkat ediniz; $7/4$ yerine daha küçük bir taban seçilseydi iddia bozulurdu.)*
Tümevarım adımı. $k \geq 2$ olsun ve iddianın $n = 1, 2, \ldots, k$ değerlerinin hepsi için doğru olduğunu varsayalım. $n = k+1$ için gösterelim. Dizinin tanımı gereği

$$a_{k+1} = a_k + a_{k-1}$$

yazılır. Tümevarım hipotezi hem k hem de $k-1$ indisi için kullanılabilir:

$$a_{k+1} < \left(\frac{7}{4}\right)^k + \left(\frac{7}{4}\right)^{k-1}$$

Sağ taraftaki ortak çarpanı ayıralım:

$$\left(\frac{7}{4}\right)^{k} + \left(\frac{7}{4}\right)^{k-1} = \left(\frac{7}{4}\right)^{k-1}\left(\frac{7}{4}+1\right) = \left(\frac{7}{4}\right)^{k-1} \cdot \frac{11}{4}$$

Şimdi kilit gözlem şudur:

$$\frac{11}{4} = 2,75 < \frac{49}{16} = 3,0625 = \left(\frac{7}{4}\right)^{2}$$

Bu eşitsizliği yukarıda yerine koyarsak

$$a_{k+1} < \left(\frac{7}{4}\right)^{k-1} \cdot \left(\frac{7}{4}\right)^{2} = \left(\frac{7}{4}\right)^{k+1}$$

elde edilir. Güçlü tümevarım ilkesi gereği eşitsizlik her $n \in \mathbb{N}$ için doğrudur.
■

1.5 İyi Sıralama Prensibi

Tümevarımın bir başka yüzü, doğal sayıların hiç boş olmayan her parçasının bir "en küçüğü" bulunduğu gözlemidir. Sayılar teorisinde en sık kullanacağımız araçlardan biri budur: bir şeyin var olduğunu göstermek için, uygun bir kümenin en küçük elemanını seçeriz.

Teorem 1.3 (İyi Sıralama Prensibi). *Doğal sayıların boş kümeden farklı her alt kümesinin bir en küçük elemanı vardır.*

İspat.
*$\emptyset \neq A \subseteq \mathbb{N}$ olsun. A kümesinin en küçük elemanının **olmadığını** varsayıp bir çelişki arayalım.*
A kümesinin $\mathbb{N}$ içindeki tümleyeni B olsun:

$$B = \{n \in \mathbb{N} : n \notin A\}$$

Her $n \in \mathbb{N}$ için $p(n)$ önermesini "$n \in B$" biçiminde tanımlayalım ve $p(n)$'in her n için doğru olduğunu güçlü tümevarımla gösterelim.
Başlangıç adımı. *$1 \in B$ midir? Eğer $1 \notin B$ olsaydı $1 \in A$ olurdu. Ama 1, $\mathbb{N}$ kümesinin en küçük elemanıdır; dolayısıyla A'nın da en küçük elemanı olurdu. Bu, A'nın en küçük elemanının olmadığı varsayımıyla çelişir. O hâlde $1 \in B$'dir.*
Tümevarım adımı. *$k \in \mathbb{N}$ olsun ve $1, 2, \ldots, k$ sayılarının hepsinin B içinde olduğunu varsayalım; yani bu sayıların hiçbiri A'da değildir. $k+1 \in B$ olduğunu gösterelim.*
Aksini varsayalım: $k+1 \in A$ olsun. A kümesinde $k+1$'den küçük hiçbir eleman yoktur, çünkü $1, \ldots, k$ sayılarının hepsi B'dedir. O hâlde $k+1$, A kümesinin en küçük elemanı olur — yine çelişki. Demek ki $k+1 \in B$'dir.
Güçlü tümevarım ilkesi gereği her $n \in \mathbb{N}$ için $n \in B$'dir; yani $B = \mathbb{N}$ ve dolayısıyla $A = \emptyset$'dir. Bu ise $A \neq \emptyset$ kabulümüzle çelişir.
Çelişki, "A'nın en küçük elemanı yoktur" varsayımından doğmuştur. O hâlde A kümesinin bir en küçük elemanı vardır.
■

i İki ilke aslında aynı şeydir

Yukarıda iyi sıralama prensibini tümevarımdan çıkardık. Ters yönde de gidilebilir: iyi sıralama prensibi kabul edilirse tümevarım ilkesi ispatlanabilir. Bunun için tümevarımın iki koşulunu sağlayan bir $p(n)$ önermesi verildiğinde, $p(n)$'in **yanlış** olduğu n'lerin kümesine bakılır; bu küme boş değilse en küçük elemanı m olsun. $p(1)$ doğru olduğundan $m \neq 1$, dolayısıyla $m-1 \in \mathbb{N}$'dir ve m'nin seçimi gereği $p(m-1)$ doğrudur. Ama tümevarım adımı $p(m)$'in de doğru olmasını gerektirir — çelişki. Yani iki ilke birbirine denktir; hangisinin kullanılacağı yalnızca kolaylık meselesidir.

Sonuç 1.1 (Sıfırın Katılması). *$\mathbb{N} \cup \{0\}$ kümesinin boştan farklı her alt kümesinin bir en küçük elemanı vardır.*

Bu sonuç doğrudan iyi sıralama prensibinden gelir: eğer küme 0 içeriyorsa en küçük eleman zaten 0'dır; içermiyorsa küme $\mathbb{N}$'nin bir alt kümesidir ve önceki teorem uygulanır. Bu küçük genişletmeye ihtiyaç duyacağız, çünkü bölme algoritmasında karşılaşacağımız kalanlar 0 olabilir.

1.6 Arşimed Prensibi

İyi sıralama prensibinin ilk uygulaması, "yeterince çok kez toplarsak her sayıyı geçeriz" biçimindeki sezgiyi kesinleştirir.

Teorem 1.4 (Arşimed Prensibi). *Her a ve b pozitif tam sayısı için*

$$na \geq b$$

olacak biçimde en az bir n doğal sayısı vardır.

> ***İspat.***
> *Teoremin doğru olmadığını varsayalım. Bu durumda **her** $n \in \mathbb{N}$ için*
>
> $$na < b$$
>
> *olur. O hâlde her $n \in \mathbb{N}$ için $b - na$ sayısı pozitiftir ve*
>
> $$S = \{b - na : n \in \mathbb{N}\}$$
>
> *kümesi doğal sayıların bir alt kümesidir. Ayrıca $n = 1$ alındığında $b - a \in S$ olduğundan S boş değildir. İyi sıralama prensibine göre S kümesinin bir en küçük elemanı vardır; buna m diyelim. $m \in S$ olduğundan*
>
> $$m = b - ka$$
>
> *olacak biçimde bir $k \in \mathbb{N}$ vardır. Şimdi $k+1$ de bir doğal sayı olduğundan $b - (k+1)a$ sayısı da S kümesine aittir. Oysa $a > 0$ olduğundan*
>
> $$b - (k+1)a = (b - ka) - a = m - a < m$$
>
> *olur; yani S kümesinde m'den küçük bir eleman bulduk. Bu, m'nin S'nin en küçük elemanı olmasıyla çelişir.*
> *O hâlde varsayımımız yanlıştır ve $na \geq b$ olacak biçimde bir n doğal sayısı vardır.*
> ■

1.7 Tümevarımla Çözülmüş Örnekler

Aşağıdaki örnekler, tümevarımın toplam formüllerinde nasıl kullanıldığını gösterir. Hepsinde izlenen şablon aynıdır: başlangıç adımını doğrula, tümevarım hipotezini yaz, $(k+1)$'inci terimi ekleyip ortak çarpan düzenlemesiyle hedef formüle ulaş.

Örnek 1.3 (İlk n Karenin Toplamı). Her $n \in \mathbb{N}$ için

$$\sum_{m=1}^{n} m^2 = 1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

eşitliğini tümevarımla ispatlayınız.

Çözüm.
Başlangıç adımı ($n = 1$). Sol taraf $1^2 = 1$'dir. Sağ taraf

$$\frac{1 \cdot 2 \cdot 3}{6} = 1$$

olduğundan eşitlik $n = 1$ için doğrudur.
Tümevarım adımı. Eşitliğin $n = k$ için doğru olduğunu varsayalım:

$$1^2 + 2^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}$$

Her iki tarafa $(k+1)^2$ ekleyelim:

$$\begin{aligned} 1^2 + \cdots + k^2 + (k+1)^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\ &= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6} \\ &= \frac{(k+1)\,\big[\,k(2k+1) + 6(k+1)\,\big]}{6} \\ &= \frac{(k+1)\,\big(\,2k^2 + 7k + 6\,\big)}{6} \end{aligned}$$

Köşeli parantez içindeki ifadeyi çarpanlarına ayıralım. $2k^2 + 7k + 6$ ifadesinin kökleri $k = -2$ ve $k = -3/2$ olduğundan

$$2k^2 + 7k + 6 = (k+2)(2k+3)$$

yazılır. Böylece

$$1^2 + \cdots + (k+1)^2 = \frac{(k+1)(k+2)(2k+3)}{6} = \frac{(k+1)\,\big(\,(k+1)+1\,\big)\,\big(\,2(k+1)+1\,\big)}{6}$$

bulunur; bu tam olarak formülün $n = k+1$ hâlidir.
■

Örnek 1.4 (İlk n Tek Sayının Toplamı). Her $n \in \mathbb{N}$ için

$$\sum_{m=1}^{n} (2m-1) = 1 + 3 + \cdots + (2n-1) = n^2$$

eşitliğini tümevarımla ispatlayınız.

Çözüm.
Başlangıç adımı ($n = 1$). Sol taraf $2 \cdot 1 - 1 = 1$, sağ taraf $1^2 = 1$'dir.
Tümevarım adımı. Eşitliğin $n = k$ için doğru olduğunu, yani

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

olduğunu varsayalım. Sıradaki tek sayı $2(k+1) - 1 = 2k + 1$'dir; her iki tarafa ekleyelim:

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

Bu, formülün $n = k+1$ hâlidir.
■

i Şekille bakış

Son eşitlik resimle de görülebilir: $n \times n$ boyutunda bir kareyi, sol üst köşeden başlayarak "L" biçimindeki şeritlere ayırın. Şeritlerdeki birim kare sayıları sırasıyla $1, 3, 5, \ldots, 2n-1$ olur ve hepsinin toplamı karenin alanı olan n^2'ye eşittir.

Örnek 1.5 (Ardışık Çarpımların Toplamı). Her $n \in \mathbb{N}$ için

$$\sum_{m=1}^{n} m(m+1) = 1\cdot 2 + 2\cdot 3 + \cdots + n(n+1) = \frac{n(n+1)(n+2)}{3}$$

eşitliğini tümevarımla ispatlayınız.

Çözüm.
Başlangıç adımı ($n=1$). Sol taraf $1\cdot 2 = 2$; sağ taraf

$$\frac{1\cdot 2\cdot 3}{3} = 2$$

olduğundan eşitlik sağlanır.
Tümevarım adımı. Eşitlik $n=k$ için doğru olsun:

$$1\cdot 2 + \cdots + k(k+1) = \frac{k(k+1)(k+2)}{3}$$

Her iki tarafa $(k+1)(k+2)$ ekleyelim:

$$\begin{aligned} 1\cdot 2 + \cdots + (k+1)(k+2) &= \frac{k(k+1)(k+2)}{3} + (k+1)(k+2) \\ &= (k+1)(k+2)\left(\frac{k}{3}+1\right) \\ &= (k+1)(k+2)\cdot\frac{k+3}{3} \\ &= \frac{(k+1)\,\big(\,(k+1)+1\,\big)\,\big(\,(k+1)+2\,\big)}{3} \end{aligned}$$

Böylece formül $n=k+1$ için de doğrudur.
■

Örnek 1.6 (İlk n Küpün Toplamı). Her n pozitif tam sayısı için

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

olduğunu gösteriniz.

Çözüm.
Başlangıç adımı ($n=1$). Sol taraf $1^3 = 1$; sağ taraf $\left(\frac{1\cdot 2}{2}\right)^2 = 1$'dir.
Tümevarım adımı. Eşitlik $n=k$ için doğru olsun:

$$1^3 + 2^3 + \cdots + k^3 = \left(\frac{k(k+1)}{2}\right)^2 = \frac{k^2(k+1)^2}{4}$$

Her iki tarafa $(k+1)^3$ ekleyelim:

$$\begin{aligned}1^3 + \cdots + k^3 + (k+1)^3 &= \frac{k^2(k+1)^2}{4} + (k+1)^3 \\ &= (k+1)^2\left(\frac{k^2}{4} + (k+1)\right) \\ &= (k+1)^2 \cdot \frac{k^2+4k+4}{4} \\ &= \frac{(k+1)^2(k+2)^2}{4} \\ &= \left(\frac{(k+1)\,(\,(k+1)+1\,)}{2}\right)^2\end{aligned}$$

Böylece eşitlik $n = k+1$ için de sağlanır.
■

i Şaşırtıcı bir eşitlik

Örnek 1.1 ile Örnek 1.6 birlikte okunduğunda şu güzel sonuç çıkar:

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

Yani ilk n sayının küpleri toplamı, aynı sayıların toplamının karesine eşittir.

Örnek 1.7 (Kesirli Bir Toplam). Her n pozitif tam sayısı için

$$\sum_{i=1}^{n} \frac{i}{2^i} = 2 - \frac{n+2}{2^n}$$

olduğunu gösteriniz.

Çözüm.
Başlangıç adımı ($n = 1$). Sol taraf $\frac{1}{2}$; sağ taraf

$$2 - \frac{1+2}{2^1} = 2 - \frac{3}{2} = \frac{1}{2}$$

olduğundan eşitlik doğrudur.
Tümevarım adımı. Eşitlik $n = k$ için doğru olsun:

$$\sum_{i=1}^{k} \frac{i}{2^i} = 2 - \frac{k+2}{2^k}$$

Her iki tarafa sıradaki terim olan $\frac{k+1}{2^{k+1}}$'i ekleyelim:

$$\begin{aligned}\sum_{i=1}^{k+1} \frac{i}{2^i} &= 2 - \frac{k+2}{2^k} + \frac{k+1}{2^{k+1}} \\ &= 2 - \frac{2(k+2)}{2^{k+1}} + \frac{k+1}{2^{k+1}} \\ &= 2 - \frac{2k+4-k-1}{2^{k+1}} \\ &= 2 - \frac{k+3}{2^{k+1}} \\ &= 2 - \frac{(k+1)+2}{2^{k+1}}\end{aligned}$$

Bu, formülün $n = k + 1$ hâlidir.
■

i Toplam nereye yaklaşıyor?

n büyüdükçe $\frac{n+2}{2^n}$ ifadesi sıfıra yaklaşır; çünkü payda üstel hızla, pay ise doğrusal hızla büyür. Dolayısıyla toplam 2 sayısına yaklaşır ama onu hiçbir zaman geçmez. Tümevarımla ispatladığımız kapalı formül, bu davranışı tek bakışta okumamızı sağlar.

1.8 Çalışma Problemleri

Alıştırma 1.1 (Tümevarımla Toplam Formülleri). Aşağıdaki eşitlikleri tümevarımla ispatlayınız.
a) $\sum_{m=1}^{n} \frac{1}{m(m+1)} = \frac{n}{n+1}$
b) $\sum_{m=1}^{n} (2m-1)^2 = \frac{n(2n-1)(2n+1)}{3}$
c) $\sum_{m=1}^{n} m \cdot m! = (n+1)! - 1$
d) $\sum_{m=1}^{n} \frac{1}{2^m} = 1 - \frac{1}{2^n}$

Alıştırma 1.2 (Bir Çarpanlara Ayırma Özdeşliği). Her x reel sayısı ve her n pozitif tam sayısı için

$$x^{n+1} - 1 = (x-1)(x^n + x^{n-1} + \cdots + x + 1)$$

eşitliğini tümevarımla ispatlayınız.
İpucu: Tümevarım adımında $x^{n+2} - 1 = x \cdot (x^{n+1} - 1) + (x - 1)$ yazımından yararlanınız.

Alıştırma 1.3 (Üstel Büyüme). Her $2 < n$ tam sayısı için

$$n + 1 < 2^n$$

olduğunu tümevarımla gösteriniz. *(Bu eşitsizliği ileride, sözde-asal sayıların sonsuzluğunu ispatlarken kullanacağız.)*

Alıştırma 1.4 (İyi Sıralama Prensibiyle Bir İspat). Boş kümeden farklı bir $A \subseteq \mathbb{Z}$ kümesi alttan sınırlı olsun; yani her $a \in A$ için $c \leq a$ olacak biçimde bir c tam sayısı bulunsun. Bu durumda A kümesinin bir en küçük elemanı olduğunu gösteriniz.
İpucu: $B = \{a - c + 1 : a \in A\}$ kümesinin $\mathbb{N}$ içinde kaldığını gözlemleyip iyi sıralama prensibini B'ye uygulayınız.

2. Bölme Algoritması

İlkokuldan beri bildiğimiz "bölme işlemi" aslında bir teoremdir: verilen iki tam sayı için bölüm ve kalanın **var olduğu** ve **tek türlü belirli olduğu** ispatlanması gereken bir olgudur. Bu bölümde bu teoremi iyi sıralama prensibinden çıkaracak ve sayılar teorisinin en çok kullanılan ispat tekniklerinden birini — kalanlara göre durum ayırmayı — kuracağız.

2.1 Kalanlı Bölme

Teorem 2.1 (Bölme Algoritması). *$a, b \in \mathbb{Z}$ ve $a > 0$ olsun. Bu durumda*

$$b = aq + r, \qquad 0 \leq r < a$$

*olacak biçimde **tek türlü belirli** q ve r tam sayıları vardır.*

İspat.
İspatı iki parçaya ayıralım.
1. Varlık. *Aşağıdaki kümeyi tanımlayalım:*

$$S = \{b - ak : k \in \mathbb{Z}, b - ak \geq 0\}$$

Önce S kümesinin boş olmadığını gösterelim. $1 \leq a$ olduğundan $\mid b \mid \leq a \mid b \mid$'dir. $k = - \mid b \mid$ seçelim:

$$b - a(- \mid b \mid) = b + a \mid b \mid \geq b + \mid b \mid \geq 0$$

Demek ki $b + a \mid b \mid \in S$'dir; yani S boş kümeden farklıdır. Ayrıca tanımı gereği $S \subseteq \mathbb{N} \cup \{0\}$'dır. Sonuç 1.1 gereği S kümesinin bir en küçük elemanı vardır; buna r diyelim. $r \in S$ olduğundan

$$r = b - aq \qquad \text{yani} \qquad b = aq + r$$

olacak biçimde bir $q \in \mathbb{Z}$ vardır. Geriye $0 \leq r < a$ olduğunu göstermek kalıyor.
$r \in S$ olduğundan $0 \leq r$'dir. Şimdi $a \leq r$ olduğunu varsayalım ve çelişki arayalım:

$$0 \leq r - a = b - aq - a = b - a(q + 1)$$

Bu, $r - a$ sayısının da S kümesine ait olduğunu söyler. Oysa $a > 0$ olduğundan $r - a < r$'dir; bu da r'nin S'nin en küçük elemanı olmasıyla çelişir. O hâlde $r < a$'dır.
2. Teklik. *Aynı koşulları sağlayan iki yazılış olduğunu varsayalım:*

$$b = aq + r = aq' + r', \qquad 0 \leq r, r' < a$$

Her iki eşitsizlikten

$$0 \leq r' < a \quad \text{ve} \quad -a < -r \leq 0$$

yazılır; taraf tarafa toplarsak

$$-a < r' - r < a \qquad \text{yani} \qquad \mid r' - r \mid < a$$

elde edilir. Öte yandan $aq + r = aq' + r'$ eşitliğinden

$$a(q - q') = r' - r$$

bulunur. Mutlak değer alalım:

$$a \cdot \mid q - q' \mid = \mid r' - r \mid < a$$

Her iki tarafı $a > 0$'a bölersek $|\, q - q' \,| < 1$ olur. Ama $q - q'$ bir tam sayıdır ve mutlak değeri 1'den küçük olan tek tam sayı 0'dır. O hâlde

$$q = q' \qquad \text{ve buradan} \qquad r = b - aq = b - aq' = r'$$

bulunur; yazılış tek türlü belirlidir.
■

Tanım 2.1 (Bölüm ve Kalan). Bölme algoritmasındaki q ve r sayılarına sırasıyla, b'nin a ile bölünmesinden elde edilen **bölüm** ve **kalan** denir.

> **i** Kalan asla negatif değildir
>
> Tanımın en sık gözden kaçan yanı, kalanın $0 \leq r < a$ aralığında olmak **zorunda** olmasıdır. Negatif sayılarda bu, alışkanlıklarımızı zorlayabilir: -48 sayısını 21'e bölerken "$-48 = 21 \cdot (-2) - 6$" yazmak matematiksel olarak doğru bir eşitliktir ama bölme algoritmasının verdiği yazılış değildir; çünkü $-6 < 0$'dır. Doğru yazılış, bölümü bir azaltıp kalanı 21 artırarak elde edilir.

Örnek 2.1 (Pozitif Bölenle Bölme). Aşağıdaki a, b tam sayı çiftleri için $b = aq + r$, $0 \leq r < a$ koşulunu sağlayan q ve r sayılarını bulunuz.
a) $b = 56, a = 13$ **b)** $b = -48, a = 21$

Çözüm.
a) 13'ün katları $13, 26, 39, 52, 65, \ldots$ biçiminde ilerler. 56'yı geçmeyen en büyüğü $52 = 13 \cdot 4$'tür:

$$56 = 13 \cdot 4 + 4, \qquad 0 \leq 4 < 13$$

Yani $q = 4, r = 4$'tür.
b) Kalanın negatif olmaması gerektiğine dikkat edelim. 21'in katları arasında -48'i **geçmeyen** en büyüğünü ararız:

$$21 \cdot (-2) = -42 > -48, \qquad 21 \cdot (-3) = -63 \leq -48$$

O hâlde $q = -3$ alınmalıdır:

$$-48 = 21 \cdot (-3) + 15, \qquad 0 \leq 15 < 21$$

Yani $q = -3, r = 15$'tir.
■

Bölme algoritmasında bölenin pozitif olması istenmişti. Bölen negatif olduğunda da benzer bir sonuç geçerlidir; tek değişiklik, kalanın $|\, a \,|$ ile sınırlanmasıdır.

Sonuç 2.1 (Negatif Bölenle Bölme). *$a, b \in \mathbb{Z}$ ve $a \neq 0$ olsun. Bu durumda*

$$b = aq + r, \qquad 0 \leq r < |\, a \,|$$

olacak biçimde tek türlü belirli q ve r tam sayıları vardır.

İspat.
$a > 0$ ise $|\, a \,| = a$ olduğundan iddia Teorem 2.1 ile aynıdır; ispatlanacak bir şey yoktur.
$a < 0$ olsun. Bu durumda $|\, a \,| = -a > 0$'dır. Bölme algoritmasını b ile pozitif $|\, a \,|$ sayısına uygulayalım:

$$b = |\, a \,| \cdot q' + r, \qquad 0 \leq r < |\, a \,|$$

olacak biçimde tek türlü belirli q', r tam sayıları vardır. Burada $|\, a \,| = -a$ yazarsak

$$b = (-a)q' + r = a(-q') + r$$

elde edilir. O hâlde $q = -q'$ ve r aranan sayılardır.
Teklik. *$b = aq + r = aq'' + r''$ ve $0 \le r, r'' < |\,a\,|$ olsun. Yukarıdaki gibi $a(q - q'') = r'' - r$ ve $|\,r'' - r\,| < |\,a\,|$ yazılır. Mutlak değer alındığında*

$$|\,a\,| \cdot |\,q - q''\,| = |\,r'' - r\,| < |\,a\,|$$

olur; buradan $|\,q - q''\,| < 1$, yani $q = q''$ ve dolayısıyla $r = r''$ bulunur.
■

Örnek 2.2 (Negatif Bölenle Bölme). Aşağıdaki a, b tam sayı çiftleri için $b = aq + r$, $0 \le r < |\,a\,|$ koşulunu sağlayan q ve r sayılarını bulunuz.
a) $b = 62, a = -13$ **b)** $b = -48, a = -14$

Çözüm.
a) Önce $|\,a\,| = 13$ ile bölelim: $62 = 13 \cdot 4 + 10$. Şimdi $13 = -(-13)$ yazımıyla bölümün işaretini çevirelim:

$$62 = (-13) \cdot (-4) + 10, \qquad 0 \le 10 < 13$$

Yani $q = -4$, $r = 10$'dur.
b) Önce $|\,a\,| = 14$ ile bölelim. 14'ün katları arasında -48'i geçmeyen en büyüğü $14 \cdot (-4) = -56$'dır:

$$-48 = 14 \cdot (-4) + 8$$

İşareti çevirelim:

$$-48 = (-14) \cdot 4 + 8, \qquad 0 \le 8 < 14$$

Yani $q = 4$, $r = 8$'dir.
■

2.2 Çift ve Tek Sayılar

Bölme algoritmasının en basit özel hâli $a = 2$ durumudur: her tam sayı 2'ye bölündüğünde ya 0 ya da 1 kalanını verir. Bu, tam sayıları iki sınıfa ayırır.

Tanım 2.2 (Çift ve Tek Tam Sayı). a bir tam sayı olsun. a'nın 2 ile bölümünden elde edilen kalan 0 ise a'ya **çift**, 1 ise **tek** tam sayı denir.
Bir başka deyişle a çift ise $a = 2k$, tek ise $a = 2k + 1$ olacak biçimde bir $k \in \mathbb{Z}$ vardır.

Bölme algoritmasındaki kalanın tek türlü belirli olması, doğrudan şu sonucu verir: **her tam sayı ya tektir ya da çifttir; hiçbir tam sayı hem tek hem çift olamaz.**

Önerme 2.1 (Toplamın Pariteleri). *İki çift tam sayının toplamı çifttir. İki tek tam sayının toplamı da çifttir. Bir tek sayı ile bir çift sayının toplamı ise tektir.*

İspat.
Üç durumu ayrı ayrı ele alalım.
1. Çift + çift. *$a = 2k$ ve $b = 2m$ olsun ($k, m \in \mathbb{Z}$). O hâlde*

$$a + b = 2k + 2m = 2(k + m)$$

olur. $k + m$ bir tam sayı olduğundan $a + b$ çifttir.
2. Tek + tek. *$a = 2k + 1$ ve $b = 2m + 1$ olsun. Bu durumda*

$$a + b = (2k + 1) + (2m + 1) = 2k + 2m + 2 = 2(k + m + 1)$$

bulunur; $k + m + 1$ tam sayı olduğundan $a + b$ çifttir.
3. Tek + çift. *$a = 2k + 1$ ve $b = 2m$ olsun. O hâlde*

$$a+b = 2k+1+2m = 2(k+m)+1$$

olur. $k+m$ *tam sayı olduğundan* $a+b$*,* 2 *ile bölündüğünde* 1 *kalanını verir; yani tektir.*
■

2.3 Kalanlara Göre Durum Ayırma

Sayılar teorisinin en verimli tekniklerinden biri şudur: bir iddiayı **bütün** tam sayılar için ispatlamak yerine, sayıyı uygun bir a ile bölüp kalanına göre sonlu sayıda duruma ayırırız. Kalan yalnızca $0, 1, \ldots, a-1$ değerlerini alabileceğinden, sonsuz bir iddia sonlu sayıda hesaba indirgenir.

Örnek 2.3 (Tek Sayıların Kareleri). Her n tek tam sayısı için n^2 sayısının 8 ile bölümünden kalanın 1 olduğunu ispatlayınız.

Çözüm.
Bölme algoritmasına göre $n = 4k+r$, $0 \le r < 4$ olacak biçimde k, r tam sayıları vardır; yani $r \in \{0,1,2,3\}$'tür.
n tek olduğundan r da tek olmalıdır: $r=0$ ya da $r=2$ olsaydı $n=4k$ veya $n = 4k+2 = 2(2k+1)$ çift olurdu. Demek ki

$$n = 4k+1 \qquad \text{veya} \qquad n = 4k+3$$

biçimindedir. İki durumu da hesaplayalım.
Durum 1: $n = 4k+1$.

$$n^2 = 16k^2+8k+1 = 8\underbrace{(2k^2+k)}_{\in\mathbb{Z}}+1$$

Durum 2: $n = 4k+3$.

$$n^2 = 16k^2+24k+9 = 16k^2+24k+8+1 = 8\underbrace{(2k^2+3k+1)}_{\in\mathbb{Z}}+1$$

Her iki durumda da n^2 sayısı $8m+1$ biçimindedir ve $0 \le 1 < 8$ olduğundan bölme algoritmasının tekliği gereği kalan tam olarak 1'dir.
■

Örnek 2.4 (Karelerin Üçe Bölümünden Kalan). Her a tam sayısı için a^2 sayısının, k bir tam sayı olmak üzere $3k$ veya $3k+1$ biçiminde olduğunu gösteriniz.

Çözüm.
$a \in \mathbb{Z}$ olsun. Bölme algoritmasına göre

$$a = 3q+r, \qquad 0 \le r < 3$$

olacak biçimde q, r tam sayıları vardır; yani $r \in \{0,1,2\}$'dir. Üç durumu tek tek inceleyelim.
$r = 0$, yani $a = 3q$ ise:

$$a^2 = 9q^2 = 3(3q^2)$$

Bu $3k$ biçimindedir.
$r = 1$, yani $a = 3q+1$ ise:

$$a^2 = 9q^2+6q+1 = 3(3q^2+2q)+1$$

Bu $3k+1$ biçimindedir.
$r = 2$, yani $a = 3q+2$ ise:

$$a^2 = 9q^2+12q+4 = 9q^2+12q+3+1 = 3(3q^2+4q+1)+1$$

Bu da $3k+1$ biçimindedir.
Üç durumda da a^2 ya $3k$ ya da $3k+1$ biçiminde çıktı; başka bir seçenek yoktur.
■

i Olumsuzluk ispatlarının anahtarı

Son örnek şunu söylüyor: **hiçbir tam kare $3k+2$ biçiminde değildir.** Bu tür "hangi biçimler imkânsız" bilgileri, bir denklemin çözümü olmadığını göstermenin en pratik yoludur. Aşağıdaki iki örnek bu fikrin doğrudan uygulamasıdır.

i Hatırlatma: tam kare

Bir a tam sayısı için $a = b^2$ olacak biçimde bir $b \in \mathbb{Z}$ varsa a'ya **tam kare** denir.

Örnek 2.5 ($3 a^2 - 1$ Neden Tam Kare Olamaz?). a bir tam sayı olmak üzere $3a^2 - 1$ sayısının asla bir tam kare olamayacağını gösteriniz.

Çözüm.
$3a^2$ sayısı 3'ün bir katıdır. Buradan

$$3a^2 - 1 = 3a^2 - 3 + 2 = 3(a^2 - 1) + 2$$

yazılır; yani $3a^2 - 1$ daima $3k+2$ biçimindedir.
Oysa Örnek 2.4 gereği her tam kare $3k$ veya $3k+1$ biçimindedir; hiçbir tam kare $3k+2$ biçiminde olamaz. O hâlde $3a^2 - 1$ bir tam kare değildir.
■

Örnek 2.6 ($4 k + 2$ ve $4 k + 3$ Biçimindeki Sayılar). k bir tam sayı olmak üzere $4k+2$ veya $4k+3$ biçimindeki hiçbir tam sayının tam kare olamayacağını gösteriniz.

Çözüm.
Bir tam karenin 4 ile bölümünden kalanın yalnızca 0 veya 1 olabileceğini gösterelim. $a \in \mathbb{Z}$ bir tam kare olsun; yani $a = b^2$ olacak biçimde bir $b \in \mathbb{Z}$ vardır.
Bölme algoritmasına göre $b = 4q + r$, $0 \le r < 4$ olacak biçimde q, r tam sayıları vardır. Kareyi açalım:

$$a = b^2 = (4q + r)^2 = 16q^2 + 8qr + r^2$$

Şimdi $r \in \{0, 1, 2, 3\}$ değerlerini tek tek deneyelim.
$r = 0$: $a = 16q^2 + 8qr = 4(4q^2 + 2qr)$, yani $4k$ biçiminde.
$r = 1$: $a = 16q^2 + 8qr + 1 = 4(4q^2 + 2qr) + 1$, yani $4k+1$ biçiminde.
$r = 2$: $a = 16q^2 + 8qr + 4 = 4(4q^2 + 2qr + 1)$, yani $4k$ biçiminde.
$r = 3$: $a = 16q^2 + 8qr + 9 = 4(4q^2 + 2qr + 2) + 1$, yani $4k+1$ biçiminde.
Görüldüğü gibi her tam kare $4k$ veya $4k+1$ biçimindedir. Bölme algoritmasındaki kalanın tek türlü belirli olması nedeniyle bir sayı aynı anda hem $4k+1$ hem $4k+2$ biçiminde olamaz. O hâlde $4k+2$ ve $4k+3$ biçimindeki sayılar tam kare değildir.
■

2.4 Kalan Aralığını Kaydırmak

Bölme algoritmasında kalan $[0, a)$ aralığında istenmişti. Bu aralık keyfîdir: uzunluğu a olan **herhangi** bir aralık aynı işi görür. Aşağıdaki örnek bu esnekliği gösterir; ispat tekniği de öğreticidir, çünkü yeni bir teorem kurmak yerine elimizdeki teoremi kaydırarak kullanır.

Örnek 2.7 (Kaydırılmış Kalan Aralığı). $a, b \in \mathbb{Z}$ ve $a > 0$ olsun.

$$b = aq + r, \qquad 2a \leq r < 3a$$

olacak biçimde tek türlü belirli q ve r tam sayılarının var olduğunu gösteriniz.

Çözüm.
Varlık. Bölme algoritmasına göre

$$b = ak + s, \qquad 0 \leq s < a$$

olacak biçimde tek türlü belirli k ve s tam sayıları vardır. Şimdi eşitliğe $2a$ ekleyip çıkaralım:

$$b = ak - 2a + s + 2a = a(k-2) + (s+2a)$$

$0 \leq s < a$ eşitsizliğinin her tarafına $2a$ eklersek

$$2a \leq s + 2a < 3a$$

elde edilir. O hâlde

$$q = k - 2, \qquad r = s + 2a$$

alınırsa istenen yazılış elde edilmiş olur.
Teklik. Aynı koşulu sağlayan iki yazılış olsun:

$$b = aq + r = aq' + r', \qquad 2a \leq r, r' < 3a$$

Her iki kalan da uzunluğu a olan aynı aralıkta olduğundan aralarındaki fark a'yı geçemez:

$$| \, r' - r \, | < a$$

Öte yandan $a(q - q') = r' - r$ eşitliğinden mutlak değer alarak

$$a \cdot | \, q - q' \, | = | \, r' - r \, | < a$$

bulunur. Buradan $| \, q - q' \, | < 1$, yani $q = q'$ ve dolayısıyla $r = r'$ çıkar.
■

> **i** Genel ilke
>
> Yukarıdaki ispatta $2a$ sayısının özel bir rolü yoktur. Aynı akıl yürütmeyle, herhangi bir c tam sayısı için
>
> $$b = aq + r, \qquad ca \leq r < (c+1)a$$
>
> yazılışının var ve tek olduğu gösterilebilir. Teklik ispatının tek dayanağı, kalanların uzunluğu a olan **aynı** aralıkta bulunmasıdır.

2.5 Çalışma Problemleri

Alıştırma 2.1 (Bölüm ve Kalan Bulma). Aşağıdaki a, b çiftleri için $b = aq + r, 0 \leq r < | \, a \, |$ koşulunu sağlayan q ve r sayılarını bulunuz.
a) $b = 100, a = 7$ **b)** $b = -100, a = 7$ **c)** $b = 100, a = -7$ **d)** $b = -100, a = -7$

Alıştırma 2.2 (Çarpımın Paritesi). İki tek tam sayının çarpımının tek, çarpanlardan en az biri çift olan bir çarpımın ise çift olduğunu gösteriniz.

Alıştırma 2.3 (Kalanlara Göre Durum Ayırma). **a)** Her n tam sayısı için $n^2 + n$ sayısının çift olduğunu gösteriniz.
b) Her n tam sayısı için n^3 sayısının $9k$, $9k+1$ veya $9k+8$ biçiminde olduğunu gösteriniz.

c) $a^2 + b^2 = c^2$ eşitliğini sağlayan a, b, c tam sayılarında a ile b'den en az birinin çift olmak zorunda olduğunu gösteriniz.
İpucu (c): İkisi de tek olsaydı Örnek 2.3 gereği $a^2 + b^2$ sayısı $8k + 2$ biçiminde olurdu; oysa c^2 bu biçimde olamaz.

Alıştırma 2.4 (Ardışık Tam Kareler). Hiçbir tam karenin, kendisinden sonraki tam kareyle arasındaki farkın çift olmadığı durumları belirleyiniz; yani $(n+1)^2 - n^2$ ifadesinin her zaman tek olduğunu gösteriniz.

3. Tam Sayılarda Bölünebilme

Bölme algoritması her bölme işlemine bir kalan iliştirir. Sayılar teorisinin asıl ilgilendiği durum ise kalanın **sıfır** olduğu özel hâldir: bu durumda bölünen sayı, bölene "tam bölünür". Bu bölümde bu bağıntıyı kesin biçimde tanımlayacak ve dersin geri kalanında refleks hâline gelecek temel özelliklerini ispatlayacağız.

3.1 Bölünebilme Bağıntısı

Tanım 3.1 (Bölünebilme). a ve b birer tam sayı olsun. Eğer

$$b = a \cdot x$$

olacak biçimde bir $x \in \mathbb{Z}$ varsa "a sayısı b'yi tam böler" denir ve

$$a \mid b$$

yazılır. Bu durumda b'ye a'nın bir **katı**, a'ya da b'nin bir **böleni** denir.
Aksi hâlde, yani her $x \in \mathbb{Z}$ için $b \neq a \cdot x$ ise "a sayısı b'yi bölmez" denir ve $a \nmid b$ yazılır.

Örnek 3.1 (İlk Örnekler).

$$3 \mid 18, \qquad -4 \mid 28, \qquad -5 \mid -20$$

çünkü $18 = 3 \cdot 6$, $28 = (-4) \cdot (-7)$ ve $-20 = (-5) \cdot 4$'tür. Buna karşılık

$$2 \nmid 3$$

çünkü $3 = 2x$ eşitliğini sağlayan bir tam sayı yoktur.

> ⚠ Bölünebilme bir bağıntıdır, bir işlem değil
>
> $a \mid b$ gösterimi bir **önermedir**; doğru ya da yanlış olabilir. a/b ise bir **sayıdır**. İkisini karıştırmamak gerekir: $3 \mid 18$ ifadesi "doğru" değerini taşır, $18/3$ ifadesi ise 6 sayısını gösterir.
> Bu ayrım, tanımda bölme işlemine hiç başvurulmamış olmasının da nedenidir: tanım yalnızca bir çarpmanın varlığını ister.

3.2 Temel Özellikler

Aşağıdaki liste, ders boyunca sürekli kullanacağımız bölünebilme kurallarını toplar. Hepsinin ispatı tanımın doğrudan uygulanmasıdır: bölünebilmeyi çarpım olarak yazar, düzenler ve yeniden çarpım olarak okuruz.

Teorem 3.1 (Bölünebilmenin Temel Özellikleri). *Her $a, b, c, d, e, f \in \mathbb{Z}$ için aşağıdakiler geçerlidir.*

1. $1 \mid a$ *ve* $-1 \mid a$.
2. $a \mid 0$.
3. $0 \mid a$ *ise* $a = 0$.
4. $a \mid a$ (yansıma).
5. $a \mid b$ *ve* $b \mid c$ *ise* $a \mid c$ (geçişme).
6. $d \mid a$ *ve* $d \mid b$ *ise* $d \mid ae + bf$.
7. $d \mid a$ *ve* $d \mid b$ *ise* $d \mid a + b$ *ve* $d \mid a - b$.
8. $b \neq 0$ *ve* $a \mid b$ *ise* $\mid a \mid \leq \mid b \mid$.

9. $a \mid b$ ve $b \mid a$ ise $a = b$ veya $a = -b$.
10. $0 < a, b$ ve $a \mid b, b \mid a$ ise $a = b$.
11. $a \mid b$ ve $c \mid d$ ise $ac \mid bd$.
12. $ac \mid bc$ ve $c \neq 0$ ise $a \mid b$.
13. $a \mid b$ ise $a \mid -b, -a \mid b$ ve $-a \mid -b$.

İspat.
(1) $a = 1 \cdot a$ *olduğundan* $1 \mid a$*'dır. Benzer biçimde* $a = (-1) \cdot (-a)$ *olduğundan* $-1 \mid a$*'dır.*
(2) $0 = a \cdot 0$ *olduğundan* $a \mid 0$*'dır.* (Burada $a = 0$ olması da sakınca doğurmaz.)
(3) $0 \mid a$ *olsun. Tanım gereği* $a = 0 \cdot x$ *olacak biçimde bir* x *vardır; ama* $0 \cdot x = 0$ *olduğundan* $a = 0$*'dır.*
(4) $a = a \cdot 1$ *olduğundan* $a \mid a$*'dır.*
(5) $a \mid b$ *ve* $b \mid c$ *olsun. O hâlde* $b = ax$ *ve* $c = by$ *olacak biçimde* x, y *tam sayıları vardır. Birinciyi ikincide yerine yazalım:*

$$c = by = (ax)y = a(xy)$$

xy *bir tam sayı olduğundan* $a \mid c$*'dir.*
(6) $d \mid a$ *ve* $d \mid b$ *olsun; yani* $a = dx$ *ve* $b = dy$ *olacak biçimde* $x, y \in \mathbb{Z}$ *vardır. Bu durumda*

$$ae + bf = dxe + dyf = d(xe + yf)$$

olur. $xe + yf$ *bir tam sayı olduğundan* $d \mid ae + bf$*'dir.*
(7) *Altıncı özellikte* $e = f = 1$ *alınırsa* $d \mid a + b$*,* $e = 1$ *ve* $f = -1$ *alınırsa* $d \mid a - b$ *elde edilir.*
(8) $b \neq 0$ *ve* $a \mid b$ *olsun;* $b = ax$ *olacak biçimde bir* x *vardır.* $b \neq 0$ *olduğundan* $x \neq 0$*'dır, dolayısıyla* $\mid x \mid \geq 1$*'dir. Mutlak değer alalım:*

$$\mid b \mid = \mid a \mid \cdot \mid x \mid \geq \mid a \mid \cdot 1 = \mid a \mid$$

(9) $a \mid b$ *ve* $b \mid a$ *olsun. Önce* $a = 0$ *durumunu ayıralım:* $a = 0$ *ise (3) gereği* $b = 0$*'dır ve iddia sağlanır. Benzer biçimde* $b = 0$ *ise* $a = 0$*'dır.*
Şimdi $a \neq 0$ *ve* $b \neq 0$ *olsun. (8) özelliğini iki yönde de uygulayalım:*

$$\mid a \mid \leq \mid b \mid \qquad \text{ve} \qquad \mid b \mid \leq \mid a \mid$$

Buradan $\mid a \mid = \mid b \mid$*, yani* $a = b$ *veya* $a = -b$ *bulunur.*
(10) *(9) gereği* $a = b$ *veya* $a = -b$*'dir. İkinci seçenek* $a, b > 0$ *ile bağdaşmaz; çünkü* $a = -b < 0$ *olurdu. O hâlde* $a = b$*'dir.*
(11) $b = ax$ *ve* $d = cy$ *olsun. Taraf tarafa çarpalım:*

$$bd = (ax)(cy) = (ac)(xy)$$

xy *tam sayı olduğundan* $ac \mid bd$*'dir.*
(12) $ac \mid bc$ *ve* $c \neq 0$ *olsun.* $bc = (ac)x$ *olacak biçimde bir* x *vardır.* $c \neq 0$ *olduğundan her iki tarafı* c*'ye sadeleştirebiliriz:*

$$b = ax$$

Bu ise $a \mid b$ *demektir.*
(13) $b = ax$ *olsun. O hâlde*

$$-b = a(-x), \qquad b = (-a)(-x), \qquad -b = (-a)(x)$$

yazılır; üç eşitlik sırasıyla $a \mid -b, -a \mid b$ *ve* $-a \mid -b$ *olduğunu gösterir.*
■

i Altıncı özellik neden bu kadar önemli?

Listedeki en çok kullanacağımız madde altıncısıdır: bir d sayısı iki sayıyı birden bölüyorsa, onların **her doğrusal birleşimini** de böler. Bézout teoreminden Öklid algoritmasına kadar bu bölümden sonra gelen hemen her ispatta bu kural devreye girecektir.

i Sıfır sıfırı böler mi?

"$0 \mid 0$" önermesi doğrudur. Tanıma göre bunun anlamı, $0 = 0 \cdot x$ olacak biçimde bir x tam sayısının var olmasıdır — ki her x bunu sağlar.
Buradaki tuhaflık hissinin kaynağı, $0/0$ ifadesinin tanımsız olmasıdır. Ama bölünebilme bağıntısı bir bölme işlemi değildir; yalnızca uygun bir çarpanın varlığını sorar. Nitekim (3) özelliği tam da bu yüzden "0 yalnızca 0'ı böler" der.

3.3 Ardışık Sayıların Çarpımları

Bölünebilme sorularının büyük bölümü, bir ifadeyi ardışık tam sayıların çarpımı olarak görmeyi öğrenince kendiliğinden çözülür. Aşağıdaki temel gözlem bu tekniğin çekirdeğidir.

Örnek 3.2 (Ardışık Sayıların Çarpımı). Her n tam sayısı için
a) $2 \mid n(n+1)$ **b)** $3 \mid n(n+1)(n+2)$
olduğunu gösteriniz.

Çözüm.
a) Bölme algoritmasına göre n ya çift ya da tektir.

- $n = 2k$ ise $n(n+1) = 2k(n+1) = 2\,\big(\,k(n+1)\,\big)$ olur; yani $2 \mid n(n+1)$.
- $n = 2k+1$ ise $n+1 = 2k+2 = 2(k+1)$ olur ve

$$n(n+1) = n \cdot 2(k+1) = 2\,\big(\,n(k+1)\,\big)$$

yazılır; yine $2 \mid n(n+1)$.

Her iki durumda da çarpım çifttir. Sezgisel olarak: ardışık iki sayıdan biri mutlaka çifttir.
b) Bu kez n'yi 3 ile bölelim: $n = 3q + r$, $r \in \{0, 1, 2\}$.

- $r = 0$ ise $n = 3q$ olduğundan çarpımın ilk çarpanı 3'ün katıdır.
- $r = 1$ ise $n + 2 = 3q + 3 = 3(q+1)$ olduğundan üçüncü çarpan 3'ün katıdır.
- $r = 2$ ise $n + 1 = 3q + 3 = 3(q+1)$ olduğundan ikinci çarpan 3'ün katıdır.

Üç durumda da çarpanlardan biri 3'ün katıdır; dolayısıyla çarpımın tamamı 3 ile bölünür.
■

i Genel kural

Aynı akıl yürütme şunu verir: **ardışık k tam sayının çarpımı daima k ile bölünür.** Çünkü bu sayılar k ile bölündüklerinde $0, 1, \ldots, k-1$ kalanlarının hepsini birer kez verir; özel olarak biri k'nin katıdır.
(İleride, aritmetiğin esas teoremini kurduktan sonra bu çarpımın aslında $k!$ ile bölündüğünü de göreceğiz.)

Örnek 3.3 ($n^3 - n$ Üçe Bölünür). Her n tam sayısı için $3 \mid n^3 - n$ olduğunu gösteriniz.

Çözüm.
İfadeyi çarpanlarına ayıralım:

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

Bu, ardışık üç tam sayının çarpımıdır. Örnek 3.2 gereği ardışık üç sayının çarpımı 3 ile bölünür; o hâlde $3 \mid n^3 - n$'dir.
■

Örnek 3.4 (\$3 divides a \(a^2 + 2 \)\$). Her a tam sayısı için $\frac{a(a^2+2)}{3}$ ifadesinin bir tam sayı olduğunu gösteriniz.

> **Çözüm.**
> İfadenin tam sayı olması, $3 \mid a(a^2+2)$ demektir. Çarpımı, bildiğimiz bir yapıya benzetelim:
>
> $$a(a^2+2) = a^3 + 2a = (a^3 - a) + 3a$$
>
> Sağ taraftaki iki terimi ayrı ayrı inceleyelim:
>
> - Örnek 3.3 gereği $3 \mid a^3 - a$'dır.
> - Açıkça $3 \mid 3a$'dır.
>
> Teorem 3.1 (7) gereği 3 sayısı bu iki sayının toplamını da böler:
>
> $$3 \mid (a^3 - a) + 3a = a(a^2+2)$$
>
> O hâlde $\frac{a(a^2+2)}{3}$ bir tam sayıdır.
> ■

3.4 Tümevarımla Bölünebilme

Üstel ifadeler içeren bölünebilme iddiaları çoğunlukla tümevarımla ispatlanır. İzlenen yol hep aynıdır: $(k+1)$'inci ifadeyi, k'ıncı ifadenin bir katı artı bölünebilirliği bilinen bir terim biçiminde yazmak.

Örnek 3.5 (\$8 divides 5^(2 n) + 7\$). Her n pozitif tam sayısı için $8 \mid 5^{2n} + 7$ olduğunu gösteriniz.

> **Çözüm.**
> $5^{2n} = (5^2)^n = 25^n$ olduğunu gözlemleyelim; iddia $8 \mid 25^n + 7$ biçimine dönüşür.
> **Başlangıç adımı ($n = 1$).**
>
> $$25^1 + 7 = 32 = 8 \cdot 4$$
>
> olduğundan iddia doğrudur.
> **Tümevarım adımı.** İddianın $n = k$ için doğru olduğunu, yani $8 \mid 25^k + 7$ olduğunu varsayalım. $n = k+1$ için gösterelim:
>
> $$\begin{aligned} 25^{k+1} + 7 &= 25 \cdot 25^k + 7 \\ &= 25 \cdot 25^k + 25 \cdot 7 - 25 \cdot 7 + 7 \\ &= 25\left(25^k + 7\right) - 168 \end{aligned}$$
>
> Sağ taraftaki iki terime bakalım:
>
> - Tümevarım hipotezi gereği $8 \mid 25^k + 7$'dir; o hâlde $8 \mid 25(25^k+7)$'dir.
> - $168 = 8 \cdot 21$ olduğundan $8 \mid 168$'dir.
>
> Teorem 3.1 (7) gereği 8 sayısı bu ikisinin farkını da böler:
>
> $$8 \mid 25\left(25^k + 7\right) - 168 = 25^{k+1} + 7$$
>
> Tümevarım ilkesi gereği iddia her n için doğrudur.
> ■

Örnek 3.6 (\$24 divides 2 dot.op 7^n + 3 dot.op 5^n - 5\$). Her n pozitif tam sayısı için $2 \cdot 7^n + 3 \cdot 5^n - 5$ sayısının 24 ile tam bölündüğünü gösteriniz.

> **Çözüm.**
> Kısaca $f(n) = 2 \cdot 7^n + 3 \cdot 5^n - 5$ yazalım.
> **Başlangıç adımı ($n = 1$).**

$$f(1) = 2\cdot 7 + 3\cdot 5 - 5 = 14 + 15 - 5 = 24$$

olduğundan $24 \mid f(1)$'dir.
Tümevarım adımı. $24 \mid f(k)$ olduğunu varsayalım ve $f(k+1)$'i $f(k)$ cinsinden yazalım:

$$\begin{aligned} f(k+1) &= 2\cdot 7^{k+1} + 3\cdot 5^{k+1} - 5 \\ &= 7\cdot\left(2\cdot 7^{k}\right) + 5\cdot\left(3\cdot 5^{k}\right) - 5 \end{aligned}$$

Amacımız $7f(k)$ ifadesini ortaya çıkarmak. $7f(k) = 7\cdot 2\cdot 7^k + 7\cdot 3\cdot 5^k - 35$ olduğuna dikkat ederek çıkaralım:

$$\begin{aligned} f(k+1) - 7f(k) &= \left(5\cdot 3\cdot 5^k - 7\cdot 3\cdot 5^k\right) + (-5 + 35) \\ &= -2\cdot 3\cdot 5^k + 30 \\ &= -6\cdot 5^k + 30 \\ &= -6\left(5^k - 5\right) \end{aligned}$$

O hâlde

$$f(k+1) = 7f(k) - 6\left(5^k - 5\right)$$

yazılır. İki terimi ayrı ayrı inceleyelim.

- Tümevarım hipotezi gereği $24 \mid f(k)$, dolayısıyla $24 \mid 7f(k)$'dir.
- İkinci terim için $5^k - 5 = 5\left(5^{k-1} - 1\right)$ yazalım. Çarpanlara ayırma özdeşliği gereği

  $$5^{k-1} - 1 = (5-1)\left(5^{k-2} + \cdots + 5 + 1\right) = 4\cdot t$$

  olacak biçimde bir t tam sayısı vardır *(bu, $k = 1$ için de doğrudur; o zaman her iki taraf 0'dır).* Buradan

  $$6\left(5^k - 5\right) = 6\cdot 5\cdot 4t = 120\,t = 24\cdot 5t$$

  bulunur; yani $24 \mid 6(5^k - 5)$'tir.

Teorem 3.1 (7) gereği 24 sayısı farkı da böler:

$$24 \mid 7f(k) - 6\left(5^k - 5\right) = f(k+1)$$

Tümevarım ilkesi gereği iddia her n için doğrudur.
■

Örnek 3.7 (\$2\^n - 1 divides 2\^m - 1\$ Ne Zaman Olur?). Her n, m pozitif tam sayısı için

$$n \mid m \Leftrightarrow 2^n - 1 \mid 2^m - 1$$

olduğunu gösteriniz.

Çözüm.
Her iki yönü ayrı ayrı ele alacağız. Aşağıdaki çarpanlara ayırma özdeşliğini kullanacağız: her x ve her $s \in \mathbb{N}$ için

$$x^s - 1 = (x-1)\left(x^{s-1} + x^{s-2} + \cdots + x + 1\right) \qquad (*)$$

($\Rightarrow$) $n \mid m$ ise $2^n - 1 \mid 2^m - 1$.
$m = nq$ olacak biçimde bir $q \in \mathbb{N}$ vardır. $(*)$ özdeşliğinde $x = 2^n$ ve $s = q$ alalım:

$$2^m - 1 = 2^{nq} - 1 = (2^n)^q - 1 = (2^n - 1)\left((2^n)^{q-1} + \cdots + 2^n + 1\right)$$

Sağ taraftaki ikinci çarpan bir tam sayıdır; o hâlde $2^n - 1 \mid 2^m - 1$'dir.
($\Leftarrow$) $2^n - 1 \mid 2^m - 1$ ise $n \mid m$.

Bölme algoritmasına göre

$$m = nq + r, \qquad 0 \leq r < n$$

yazalım. $2^m - 1$ ifadesini bu yazılıma göre parçalayalım:

$$\begin{aligned} 2^m - 1 &= 2^{nq+r} - 1 \\ &= 2^r \cdot 2^{nq} - 1 \\ &= 2^r(2^{nq} - 1) + 2^r - 1 \end{aligned}$$

İlk yönde gösterdiğimiz gibi $2^n - 1 \mid 2^{nq} - 1$'dir, dolayısıyla $2^n - 1$ sayısı $2^r(2^{nq} - 1)$ terimini de böler. Hipotez gereği $2^n - 1$ sayısı $2^m - 1$'i de bölüyor. O hâlde farkı da böler:

$$2^n - 1 \mid (2^m - 1) - 2^r(2^{nq} - 1) = 2^r - 1$$

Şimdi r'nin büyüklüğüne bakalım. $0 \leq r < n$ olduğundan

$$0 \leq 2^r - 1 < 2^n - 1$$

olur. Ama $2^n - 1$ sayısı $2^r - 1$'i bölüyor ve Teorem 3.1 (8) gereği, bölünen sıfırdan farklı olsaydı $2^n - 1 \leq 2^r - 1$ olması gerekirdi — bu ise yukarıdaki eşitsizlikle çelişir. Geriye tek olasılık kalır:

$$2^r - 1 = 0 \Longrightarrow 2^r = 1 \Longrightarrow r = 0$$

$r = 0$ olduğundan $m = nq$, yani $n \mid m$'dir.
■

3.5 Doğru mu, Yanlış mı?

Bölünebilmeyle ilgili sezgiler çoğu zaman yanıltıcıdır. Aşağıdaki örnek, benzer görünen önermelerden hangilerinin doğru hangilerinin yanlış olduğunu ayırt etmeyi gösterir; yanlış bir önermeyi çürütmek için tek bir karşı örnek yeterlidir.

Örnek 3.8 (Önermeleri Sınama). Aşağıdaki önermelerin doğru olup olmadığını araştırınız. Doğru olanları ispatlayınız, yanlış olanlara karşı örnek veriniz.
a) Her a, b, c için, $a \mid b$ veya $a \mid c$ ise $a \mid bc$'dir.
b) Her a, b, c için, $a \mid bc$ ise $a \mid b$ veya $a \mid c$'dir.
c) Her a, b için, $a \mid b$ ise $a \leq b$'dir.
d) Her a için $3 \mid a(a+2)$'dir.
e) Her a için $3 \mid a(a+7)(a-2)$'dir.
f) Her a için $3 \mid a(a+1)(2a+1)$'dir.

Çözüm.
a) Doğru. Simetri gereği $a \mid b$ durumunu incelemek yeterlidir. $b = ax$ olsun. O hâlde

$$bc = (ax)c = a(xc)$$

olur ve xc tam sayı olduğundan $a \mid bc$'dir.
b) Yanlış. $a = 6, b = 2, c = 3$ alalım. $bc = 6$ olduğundan $6 \mid bc$'dir; ama $6 \nmid 2$ ve $6 \nmid 3$'tür.
(Bu önerme yalnızca a asal olduğunda doğrudur; ileride bunu Öklid lemması olarak göreceğiz.)
c) Yanlış. $a = -3, b = 3$ alalım. $3 = (-3) \cdot (-1)$ olduğundan $a \mid b$'dir, ama $-3 \leq 3$ eşitsizliği doğru olsa da önerme genel olarak bozulur: $a = 3, b = -3$ alalım. $-3 = 3 \cdot (-1)$ olduğundan $3 \mid -3$'tür, oysa $3 \leq -3$ yanlıştır.
(Doğru olan biçim Teorem 3.1 (8)'dir: $b \neq 0$ ise $\mid a \mid \leq \mid b \mid$.)
d) Yanlış. $a = 2$ alalım:

$$a(a+2) = 2 \cdot 4 = 8$$

ve $3 \nmid 8$'dir.
e) Yanlış. $a = 1$ alalım:

$$a(a+7)(a-2) = 1 \cdot 8 \cdot (-1) = -8$$

ve $3 \nmid -8$'dir.
f) Doğru. a'yı 3 ile bölelim: $a = 3q + r$, $r \in \{0, 1, 2\}$.

- $r = 0$ ise ilk çarpan $a = 3q$, yani 3'ün katıdır.
- $r = 1$ ise $2a + 1 = 6q + 3 = 3(2q + 1)$, yani üçüncü çarpan 3'ün katıdır.
- $r = 2$ ise $a + 1 = 3q + 3 = 3(q + 1)$, yani ikinci çarpan 3'ün katıdır.

Üç durumda da çarpanlardan biri 3'ün katı olduğundan çarpım 3 ile bölünür.
■

i (d) ve (e) neden bozuluyor?

Bir çarpımın 3 ile bölünmesi için çarpanların 3 ile bölümünden kalanlarının $0, 1, 2$ değerlerinin **hepsini** taraması gerekmez; yalnızca birinin 0 olması yeterlidir. (f) şıkkında a, $a + 1$ ve $2a + 1$ kalanları birlikte her durumda bir 0 üretir. (d) ve (e) şıklarında ise iki çarpan aynı kalanı verdiğinden bir boşluk kalır ve o boşluğa düşen a değerleri karşı örnek olur.

3.6 Çalışma Problemleri

Alıştırma 3.1 (Temel Bölünebilme İddiaları). Aşağıdakileri ispatlayınız.
a) Her n pozitif tam sayısı için $9 \mid 10^n - 1$.
b) Her n pozitif tam sayısı için $6 \mid n^3 + 5n$.
c) Her n pozitif tam sayısı için $7 \mid 2^{3n} - 1$.
d) Her n tam sayısı için $5 \mid n^5 - n$.

Alıştırma 3.2 (Bölenlerin Taşınması). **a)** $a \mid b$ ise her $n \in \mathbb{N}$ için $a^n \mid b^n$ olduğunu gösteriniz.
b) $d \mid n$ ve $d \mid n + 2$ ise $d \mid 2$ olduğunu gösteriniz. Buradan, ardışık iki tek sayının ortak bölenlerinin yalnızca ± 1 olduğu sonucunu çıkarınız.
c) $a \mid b + c$ ve $a \mid b - c$ ise $a \mid 2b$ ve $a \mid 2c$ olduğunu gösteriniz.

Alıştırma 3.3 (Doğru mu, Yanlış mı?). Aşağıdaki önermelerin doğruluğunu araştırınız; yanlış olanlara karşı örnek veriniz.
a) $a \mid b + c$ ise $a \mid b$ veya $a \mid c$'dir.
b) $a^2 \mid b^2$ ise $a \mid b$'dir.
c) $a \mid b$ ve $a \mid c$ ise $a^2 \mid bc$'dir.

4. En Büyük Ortak Bölen ve Bézout Teoremi

İki tam sayının ortak bölenleri, aralarındaki çarpımsal akrabalığın ölçüsüdür. Bu bölümde bu akrabalığı tek bir sayıyla — en büyük ortak bölenle — özetleyecek ve bu sayının şaşırtıcı bir başka yüzü olduğunu göreceğiz: en büyük ortak bölen, aynı zamanda iki sayının **doğrusal birleşimi olarak yazılabilen en küçük pozitif tam sayıdır**. Bu ikinci yüz, Bézout teoreminin içeriğidir ve dersin geri kalanının motorudur.

4.1 Ortak Bölenler

Tanım 4.1 (Ortak Bölen). a, b ve d birer tam sayı olsun. Eğer $d \mid a$ ve $d \mid b$ ise d tam sayısına a ile b'nin bir **ortak böleni** denir.

Örnek 4.1 (Ortak Bölen Örneği). 4 tam sayısı 12 ile 20'nin bir ortak bölenidir; çünkü $4 \mid 12$ ve $4 \mid 20$'dir.
Buna karşılık 5 sayısı 20 ile 12'nin bir ortak böleni **değildir**: $5 \mid 20$ olsa da $5 \nmid 12$'dir.

Her a, b çifti için 1 sayısı bir ortak bölendir; dolayısıyla ortak bölenler kümesi hiçbir zaman boş değildir. Asıl soru bu kümenin en büyük elemanıdır.

Tanım 4.2 (En Büyük Ortak Bölen). a ve b ikisi birden sıfır olmayan tam sayılar olmak üzere, hem a'yı hem de b'yi bölen tam sayıların en büyüğüne a ile b'nin **en büyük ortak böleni** denir ve

$$\gcd(a, b)$$

ile gösterilir.

> **i** Tanımın iki incelikli noktası
>
> **1. Neden a ile b'nin ikisi birden sıfır olamıyor?**
> Her tam sayı 0'ı böldüğünden ($\thinspace$Teorem 3.1 (2)$\thinspace$), $a = b = 0$ alınırsa **her** tam sayı bir ortak bölen olur. Bu küme üstten sınırlı değildir; en büyük elemanı yoktur. Bu yüzden $\gcd(0, 0)$ tanımsız bırakılır.
> **2. En büyük ortak bölen gerçekten var mıdır?**
> Vardır. a ile b'nin ortak bölenlerinin kümesine D diyelim.
>
> - $1 \in D$ olduğundan $D \neq \emptyset$'dır.
> - a ile b'den en az biri, diyelim a, sıfırdan farklıdır. Her $d \in D$ için $d \mid a$ ve $a \neq 0$ olduğundan Teorem 3.1 (8) gereği $\mid d \mid \leq \mid a \mid$'dır; yani D kümesi $\mid a \mid$ ile üstten sınırlıdır.
>
> Boş olmayan ve üstten sınırlı bir tam sayı kümesinin en büyük elemanı vardır. O hâlde $\gcd(a, b)$ iyi tanımlıdır. Ayrıca $1 \in D$ olduğundan daima $\gcd(a, b) \geq 1 > 0$'dır.

Tanımı doğrudan kullanan bir ölçüt, ilerideki ispatlarda işimizi kolaylaştıracaktır.

Önerme 4.1 (EBOB'un Sıralamayla Karakterizasyonu). *a ile b ikisi birden sıfır olmayan tam sayılar ve $d \in \mathbb{Z}$ olsun. $d = \gcd(a, b)$ olabilmesi için gerek ve yeter koşullar şunlardır:*

1. *$d \mid a$ ve $d \mid b$;*
2. *her $c \in \mathbb{Z}$ için, $c \mid a$ ve $c \mid b$ ise $c \leq d$'dir.*

Bu ölçüt tanımın yeniden ifade edilmiş hâlidir: birinci madde d'nin bir ortak bölen olduğunu, ikincisi de ortak bölenlerin en büyüğü olduğunu söyler.

4.2 Bézout Teoremi

Şimdi bu bölümün — hatta dersin — en önemli teoremine geliyoruz. Teorem, en büyük ortak böleni yepyeni bir biçimde tanımlar: a ile b'nin katlarının toplamı olarak yazılabilen en küçük pozitif sayı.

Teorem 4.1 (Bézout Teoremi). *a ve b ikisi birden sıfır olmayan tam sayılar olsun. Bu durumda*

$$\gcd(a,b) = ax_0 + by_0$$

olacak biçimde x_0, y_0 tam sayıları vardır.

İspat.
Aşağıdaki kümeyi tanımlayalım:

$$S = \{ax + by : x, y \in \mathbb{Z}, ax + by > 0\}$$

1. S boş değildir. *$x = a$, $y = b$ seçelim:*

$$a \cdot a + b \cdot b = a^2 + b^2 > 0$$

(Toplam sıfır olamaz, çünkü a ile b'nin ikisi birden sıfır değildir.) *O hâlde $a^2 + b^2 \in S$'dir ve S boş kümeden farklı bir doğal sayı kümesidir.*
2. S'nin en küçük elemanı bir ortak bölendir. *İyi sıralama prensibine göre S kümesinin bir en küçük elemanı vardır; buna d diyelim. $d \in S$ olduğundan*

$$d = ax_1 + by_1$$

olacak biçimde x_1, y_1 tam sayıları vardır.
İddia. *$d \mid a$'dır.*
İddianın ispatı. *Bölme algoritmasına göre*

$$a = dq + r, \qquad 0 \leq r < d$$

olacak biçimde q, r tam sayıları vardır. $d \nmid a$ olduğunu varsayalım; bu durumda $r \neq 0$, yani $0 < r < d$'dir. Şimdi r'yi a ile b cinsinden yazalım:

$$\begin{aligned} r &= a - dq \\ &= a - (ax_1 + by_1)q \\ &= a(1 - x_1 q) + b(-y_1 q) \end{aligned}$$

Görüldüğü gibi r sayısı a ile b'nin bir doğrusal birleşimidir ve $r > 0$'dır; yani $r \in S$'dir. Ama $r < d$ olması, d'nin S'nin en küçük elemanı olmasıyla çelişir. O hâlde $r = 0$, yani $d \mid a$ olmalıdır.
Tamamen benzer biçimde $d \mid b$ olduğu da gösterilir. Demek ki d sayısı a ile b'nin bir ortak bölenidir. En büyük ortak bölen, ortak bölenlerin en büyüğü olduğundan

$$d \leq \gcd(a,b) \tag{1}$$

yazılır.
3. Ters eşitsizlik. $\gcd(a,b) \mid a$ *ve* $\gcd(a,b) \mid b$ *olduğundan, Teorem 3.1 (6) gereği* $\gcd(a,b)$ *sayısı a ile b'nin her doğrusal birleşimini böler; özel olarak*

$$\gcd(a,b) \mid ax_1 + by_1 = d$$

olur. $d > 0$ olduğundan Teorem 3.1 (8) gereği

$$\gcd(a,b) \leq d \tag{2}$$

bulunur.
(1) ve (2) birlikte $d = \gcd(a,b)$ verir; yani $\gcd(a,b) = ax_1 + by_1$'dir.
■

İspatın kendisi, teoremden daha fazlasını söyler; bu ek bilgiyi ayrıca kaydedelim.

Sonuç 4.1 (EBOB, En Küçük Pozitif Doğrusal Birleşimdir). *a ve b ikisi birden sıfır olmayan tam sayılar olsun. Bu durumda a ile b'nin en büyük ortak böleni,*

$$S = \{ax + by : x, y \in \mathbb{Z},\ ax + by > 0\}$$

kümesinin en küçük elemanıdır:

$$\gcd(a, b) = \min S = \min\{ax + by : x, y \in \mathbb{Z},\ ax + by > 0\}$$

⚠ Bézout katsayıları tek türlü belirli değildir

Teorem x_0 ile y_0'ın **var olduğunu** söyler, tek olduğunu değil. Nitekim

$$\gcd(a, b) = ax_0 + by_0 = a(x_0 + b) + b(y_0 - a)$$

eşitliği gösteriyor ki katsayılar sonsuz çok biçimde seçilebilir. Örneğin

$$\gcd(4, 6) = 2 = 4 \cdot (-1) + 6 \cdot 1 = 4 \cdot 2 + 6 \cdot (-1)$$

Bu esneklik bir kusur değil, avantajdır: ileride Diofant denklemlerinin sonsuz çözümünü tam olarak bu serbestlik üretecektir.

4.3 Doğrusal Birleşimlerin Kümesi

Bézout teoremi en küçük pozitif doğrusal birleşimi tanır. Bir sonraki sonuç, **bütün** doğrusal birleşimlerin ne olduğunu söyler.

Sonuç 4.2 (Doğrusal Birleşimler Kümesi). *a ve b ikisi birden sıfır olmayan tam sayılar olsun ve $d = \gcd(a, b)$ biçiminde tanımlansın. Bu durumda*

$$T = \{ax + by : x, y \in \mathbb{Z}\}$$

kümesi, d'nin tüm katlarının kümesidir:

$$T = \{dk : k \in \mathbb{Z}\}$$

İspat.
İki kapsamayı ayrı ayrı gösterelim.
$T \subseteq \{dk\}$. *$ax + by \in T$ olsun. $d \mid a$ ve $d \mid b$ olduğundan Teorem 3.1 (6) gereği $d \mid ax + by$'dir; yani $ax + by$ sayısı d'nin bir katıdır.*
$\{dk\} \subseteq T$. *Bézout teoremi gereği $d = ax_0 + by_0$ olacak biçimde x_0, y_0 tam sayıları vardır. Herhangi bir $k \in \mathbb{Z}$ için her iki tarafı k ile çarpalım:*

$$dk = a(x_0 k) + b(y_0 k)$$

$x_0 k$ ve $y_0 k$ tam sayı olduğundan $dk \in T$'dir.
İki kapsama birlikte $T = \{dk : k \in \mathbb{Z}\}$ verir.
■

ℹ Pratikte ne işe yarar?

Bu sonuç, "$ax + by = c$ denkleminin tam sayı çözümü var mıdır?" sorusuna tek satırda cevap verir: **çözüm vardır ancak ve ancak $\gcd(a, b) \mid c$ ise.** Diofant denklemleri bölümünde bu ölçütü doğrudan kullanacağız.

Aşağıdaki karakterizasyon, en büyük ortak böleni "en büyük" sıfatından kurtarır: ortak bölenlerin yalnızca daha küçük değil, aynı zamanda d'yi **bölen** sayılar olduğunu söyler. Bu, ileride sıralamanın anlamsız olduğu ortamlarda da kullanılabilecek olan asıl tanımdır.

Teorem 4.2 (EBOB'un Bölünebilmeyle Karakterizasyonu). *$a, b, d \in \mathbb{Z}$, a ile b ikisi birden sıfır değil ve $d > 0$ olsun. $d = \gcd(a, b)$ olabilmesi için gerek ve yeter koşullar şunlardır:*

1. *$d \mid a$ ve $d \mid b$;*
2. *her $c \in \mathbb{Z}$ için, $c \mid a$ ve $c \mid b$ ise $c \mid d$'dir.*

İspat.
(⇒) $d = \gcd(a, b)$ olsun. Birinci koşul en büyük ortak bölenin tanımı gereği sağlanır.
İkinci koşul için $c \mid a$ ve $c \mid b$ olsun. Bézout teoremi gereği $d = ax_0 + by_0$ yazılabilir. Teorem 3.1 (6) gereği c sayısı bu doğrusal birleşimi böler:

$$c \mid ax_0 + by_0 = d$$

(⇐) $d > 0$ olsun ve iki koşulu sağlasın. Birinci koşul gereği d bir ortak bölendir. Şimdi c herhangi bir ortak bölen olsun. İkinci koşul gereği $c \mid d$'dir ve $d > 0$ olduğundan Teorem 3.1 (8) gereği

$$c \leq \mid c \mid \leq \mid d \mid = d$$

bulunur. Yani d, ortak bölenlerin en büyüğüdür: $d = \gcd(a, b)$.
■

4.4 EBOB'un Temel Özellikleri

Önerme 4.2 (EBOB'un Temel Özellikleri). *Aşağıdakiler geçerlidir.*

1. *Her $a \neq 0$ için $\gcd(a, 0) = \mid a \mid$.*
2. *$a \neq 0$ ve $a \mid b$ ise $\gcd(a, b) = \mid a \mid$.*
3. *İkisi birden sıfır olmayan her a, b için*

$$\gcd(a, b) = \gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b)$$

4. *İkisi birden sıfır olmayan her a, b ve her $0 < m \in \mathbb{Z}$ için*

$$\gcd(ma, mb) = m \cdot \gcd(a, b)$$

İspat.
(1) *Her tam sayı 0'ı böldüğünden, a ile 0'ın ortak bölenleri tam olarak a'nın bölenleridir. $a \neq 0$ olduğundan bunların en büyüğü $\mid a \mid$'dır: $\mid a \mid \mid a$ olduğu açıktır ve Teorem 3.1 (8) gereği a'nın her böleni mutlak değerce $\mid a \mid$'yı geçemez.*
(2) *$a \mid b$ olsun. a ile b'nin ortak bölenlerini belirleyelim. $\mid a \mid$ sayısı hem a'yı hem de (geçişme gereği) b'yi böler; yani bir ortak bölendir. Öte yandan her ortak bölen a'yı böldüğünden mutlak değerce $\mid a \mid$'yı geçemez. O hâlde $\gcd(a, b) = \mid a \mid$'dır.*
(3) *Teorem 3.1 (13) gereği $c \mid a$ ile $c \mid -a$ önermeleri denktir. Dolayısıyla $\{a, b\}$ çiftinin ortak bölenleri ile $\{-a, b\}$, $\{a, -b\}$, $\{-a, -b\}$ çiftlerinin ortak bölenleri **aynı** kümedir. Aynı kümenin en büyük elemanı da aynı olacağından dört en büyük ortak bölen eşittir.*
(4) *Sonuç 4.1 gereği en büyük ortak bölen, pozitif doğrusal birleşimlerin en küçüğüdür. $m > 0$ olduğundan*

$$\begin{aligned}\gcd(ma, mb) &= \min\{(ma)x + (mb)y : x, y \in \mathbb{Z}, (ma)x + (mb)y > 0\} \\ &= \min\{m(ax + by) : x, y \in \mathbb{Z}, ax + by > 0\} \\ &= m \cdot \min\{ax + by : x, y \in \mathbb{Z}, ax + by > 0\} \\ &= m \cdot \gcd(a, b)\end{aligned}$$

Üçüncü satırda $m > 0$ olmasını kullandık: pozitif bir sayıyla çarpmak sıralamayı bozmaz, dolayısıyla minimumu dışarı alabiliriz.
■

4.5 Aralarında Asal Sayılar

En büyük ortak bölenin alabileceği en küçük değer 1'dir. Bu durum o kadar sık karşımıza çıkar ki kendi adını hak eder.

Tanım 4.3 (Aralarında Asal Sayılar). a ve b ikisi birden sıfır olmayan tam sayılar olsun. Ancak ve yalnız

$$\gcd(a,b)=1$$

olması durumunda "a ile b **aralarında asaldır**" denir.

Bézout teoreminin en çok kullanılan biçimi, aralarında asallık için verdiği pratik ölçüttür.

Sonuç 4.3 (Aralarında Asallık Ölçütü). *a ve b ikisi birden sıfır olmayan tam sayılar olsun. a ile b'nin aralarında asal olması için gerek ve yeter koşul*

$$1=ax+by$$

olacak biçimde x, y tam sayılarının var olmasıdır.

> ***İspat.***
> ***(⇒)*** $\gcd(a,b)=1$ *olsun. Bézout teoremi gereği* $\gcd(a,b)=ax_0+by_0$ *olacak biçimde* x_0, y_0 *tam sayıları vardır; yani* $1=ax_0+by_0$*'dır.*
> ***(⇐)*** $1=ax+by$ *olacak biçimde x, y tam sayıları bulunsun. $d=\gcd(a,b)$ diyelim. $d \mid a$ ve $d \mid b$ olduğundan Teorem 3.1 (6) gereği*
>
> $$d \mid ax+by=1$$
>
> *olur. d pozitif bir tam sayı ve $d \mid 1$ olduğundan $d=1$'dir.*
> ■

> **i** Ölçütü nasıl kullanacağız?
>
> İki sayının aralarında asal olduğunu göstermek için artık bütün ortak bölenleri incelemek gerekmez: **değeri 1 olan tek bir doğrusal birleşim bulmak yeterlidir.** Aşağıdaki örneklerin çoğu bu tek satırlık numaraya dayanır.
> Dikkat: ölçüt yalnızca 1 değeri için bu kadar keskindir. $ax+by=6$ biçiminde bir birleşim bulmak $\gcd(a,b)=6$ olduğunu **göstermez**; yalnızca $\gcd(a,b) \mid 6$ olduğunu söyler.

4.6 Çözümlü Örnekler

Örnek 4.2 (Ardışık Sayılar Aralarında Asaldır). Her n tam sayısı için $\gcd(n,n+1)=1$ olduğunu gösteriniz.

> **Çözüm.**
> **1. Yol (Bézout ölçütü).** Aşağıdaki doğrusal birleşimi yazalım:
>
> $$(n+1)\cdot 1+n\cdot(-1)=1$$
>
> Sonuç 4.3 gereği $\gcd(n,n+1)=1$'dir.
> **2. Yol (doğrudan).** $d=\gcd(n,n+1)$ olsun. O hâlde $d \mid n$ ve $d \mid n+1$'dir. Teorem 3.1 (7) gereği d sayısı farkı da böler:
>
> $$d \mid (n+1)-n=1$$
>
> d pozitif olduğundan $d=1$'dir.
> ■

Örnek 4.3 ($gcd \(a \, a + n \)$ Sayısı n'yi Böler). İkisi birden sıfır olmayan her n, a tam sayısı için $\gcd(a, a+n)$ sayısının n'yi böldüğünü gösteriniz.

Çözüm.
$d = \gcd(a, a+n)$ biçiminde tanımlansın. En büyük ortak bölenin tanımı gereği

$$d \mid a \qquad \text{ve} \qquad d \mid a+n$$

olur. Teorem 3.1 (7) gereği d sayısı bu ikisinin farkını da böler:

$$d \mid (a+n) - a = n$$

O hâlde $\gcd(a, a+n) \mid n$'dir.
■

Örnek 4.4 (Hangi Değerler Ortaya Çıkar?). n sıfırdan farklı bir tam sayı olmak üzere

$$\{\gcd(a, a+n) : a \in \mathbb{Z}\} = \{k \in \mathbb{Z} : 0 < k, k \mid n\}$$

olduğunu gösteriniz.

Çözüm.
Kümeleri kısaca adlandıralım:

$$A \coloneqq \{\gcd(a, a+n) : a \in \mathbb{Z}\}, \qquad B \coloneqq \{k \in \mathbb{Z} : 0 < k, k \mid n\}$$

$A \subseteq B$. $d \in A$ olsun; yani $d = \gcd(a, a+n)$ olacak biçimde bir $a \in \mathbb{Z}$ vardır. Örnek 4.3 gereği $d \mid n$'dir. Ayrıca en büyük ortak bölen daima pozitiftir. O hâlde $d \in B$'dir.
$B \subseteq A$. $k \in B$ olsun; yani $0 < k$ ve $k \mid n$'dir. Şimdi $a = k$ seçelim ve $\gcd(k, k+n) = k$ olduğunu gösterelim:

- $k \mid k$ olduğu açıktır.
- $k \mid n$ olduğundan Teorem 3.1 (7) gereği $k \mid k+n$'dir.

Demek ki k, $\{k, k+n\}$ çiftinin bir ortak bölenidir. Öte yandan her ortak bölen k'yı böldüğünden mutlak değerce k'yı geçemez. O hâlde

$$\gcd(k, k+n) = k$$

olur ve $k \in A$'dır.
İki kapsama birlikte $A = B$ verir.
■

Örnek 4.5 (Doğrusal İfadelerin Aralarında Asallığı). Her a tam sayısı için $\gcd(2a+1, 9a+4) = 1$ olduğunu gösteriniz.

Çözüm.
Sonuç 4.3 gereği, değeri 1 olan bir doğrusal birleşim bulmamız yeterlidir. Katsayıları a terimini yok edecek biçimde seçelim: $2a+1$ ifadesini 9 ile, $9a+4$ ifadesini 2 ile çarparsak her ikisinde de $18a$ elde ederiz.

$$\begin{aligned}(2a+1) \cdot 9 + (9a+4) \cdot (-2) &= 18a + 9 - 18a - 8 \\ &= 1\end{aligned}$$

Değeri 1 olan bir doğrusal birleşim bulduğumuz için $\gcd(2a+1, 9a+4) = 1$'dir.
■

Örnek 4.6 (Tek Sayılarda Bir EBOB Hesabı). Her a tek tam sayısı için $\gcd(7a, 7a+2) = 1$ olduğunu gösteriniz.

Çözüm.
$d := \gcd(7a, 7a+2)$ biçiminde tanımlansın. O hâlde $d \mid 7a$ ve $d \mid 7a+2$'dir; farkı da böler:

$$d \mid (7a+2) - 7a = 2$$

d pozitif olduğundan $d \in \{1, 2\}$'dir. Şimdi $d = 2$ olasılığını eleyelim.
a tek bir tam sayı olduğundan $7a$ da tektir *(tek sayıların çarpımı tektir)*. Dolayısıyla $2 \nmid 7a$'dır. Oysa $d = 2$ olsaydı $d \mid 7a$, yani $2 \mid 7a$ olurdu — çelişki.
O hâlde $d \neq 2$ ve sonuç olarak

$$\gcd(7a, 7a+2) = d = 1$$

bulunur.
■

Örnek 4.7 (Bézout Katsayıları Aralarında Asaldır). a ve b ikisi birden sıfır olmayan tam sayılar, $x, y \in \mathbb{Z}$ ve

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

olsun. Bu durumda $\gcd(x, y) = 1$ olduğunu gösteriniz.

Çözüm.
$d := \gcd(a, b)$ biçiminde tanımlansın. Buradaki kilit fikir, a ile b'yi d'nin katları olarak yazıp eşitliği sadeleştirmektir.
$d \mid a$ ve $d \mid b$ olduğundan

$$a = da', \qquad b = db'$$

olacak biçimde a', b' tam sayıları vardır. Bunları hipotezde yerine koyalım:

$$d = ax + by = (da')x + (db')y = d\left(\, a'x + b'y \,\right)$$

a ile b'nin ikisi birden sıfır olmadığından $d \neq 0$'dır; her iki tarafı d'ye sadeleştirebiliriz:

$$1 = a'x + b'y$$

Şimdi $k := \gcd(x, y)$ diyelim. $k \mid x$ ve $k \mid y$ olduğundan Teorem 3.1 (6) gereği k sayısı x ile y'nin her doğrusal birleşimini böler; özel olarak

$$k \mid a'x + b'y = 1$$

k pozitif bir tam sayı ve $k \mid 1$ olduğundan $k = 1$, yani $\gcd(x, y) = 1$'dir.
■

4.7 Çalışma Problemleri

Alıştırma 4.1 (EBOB Hesapları). Aşağıdaki en büyük ortak bölenleri bulunuz ve her biri için değeri EBOB'a eşit olan bir doğrusal birleşim yazınız.
a) $\gcd(12, 18)$ **b)** $\gcd(-15, 25)$ **c)** $\gcd(17, 0)$ **d)** $\gcd(24, 36)$

Alıştırma 4.2 (Toplam ve Farkın EBOB'u). İkisi birden sıfır olmayan a, b tam sayıları için $\gcd(a, b) = 1$ olsun. Bu durumda

$$\gcd(a+b, a-b) \in \{1, 2\}$$

olduğunu gösteriniz.
İpucu: $d = \gcd(a+b, a-b)$ diyerek $d \mid 2a$ ve $d \mid 2b$ olduğunu gösteriniz, ardından Önerme 4.2 (4)'ü kullanınız.

Alıştırma 4.3 (Bir Doğrusal Birleşim Kurma). Her a tam sayısı için

$$1 = a(5x + 7y) + 2x + 3y$$

olacak biçimde x, y tam sayılarının var olduğunu gösteriniz.
İpucu: Önce $\gcd(5a + 2, 7a + 3) = 1$ olduğunu gösterip Sonuç 4.3'ü uygulayınız, sonra elde ettiğiniz birleşimi düzenleyiniz.

Alıştırma 4.4 (Çapraz Çarpımların Farkı). $a, b, c, d \in \mathbb{Z} \setminus \{0\}$ olsun. Eğer

$$ac - bd \in \{1, -1\}$$

ise $\gcd(a + b, c + d) = 1$ olduğunu gösteriniz.
İpucu: $k = \gcd(a + b, c + d)$ diyerek $k \mid c(a + b) - b(c + d)$ hesabını yapınız.

Alıştırma 4.5 (Üç Sayının EBOB'u). Hepsi birden sıfır olmayan a, b, c tam sayılarının en büyük ortak böleni $\gcd(a, b, c)$, bu üç sayının ortak bölenlerinin en büyüğü olarak tanımlanır.
a) $\gcd(a, b, c) = \gcd\big(\gcd(a, b), c\big)$ olduğunu gösteriniz.
b) $\gcd(a, b, c)$ sayısının $ax + by + cz$ biçiminde yazılabileceğini gösteriniz.

5. Öklid Lemması ve Aralarında Asallık

Bézout teoremi elimize güçlü bir alet verdi: aralarında asal iki sayının doğrusal birleşimiyle 1 elde edilebiliyor. Bu bölümde bu aletin ne kadar iş gördüğünü göreceğiz. Elde edeceğimiz teoremler — özellikle Öklid lemması — aritmetiğin esas teoreminin ispatında ve kongrüans hesaplarında sürekli karşımıza çıkacak.

5.1 Sadeleştirme

En büyük ortak bölene bölmek, iki sayıyı aralarında asal hâle getirir. Bu basit gözlem, kesirlerin "en sade biçimi" fikrinin arkasındaki matematiktir.

Sonuç 5.1 (EBOB'a Bölmek Aralarında Asal Yapar). *a ve b ikisi birden sıfır olmayan tam sayılar olsun ve $d = \gcd(a, b)$ biçiminde tanımlansın. Bu durumda*

$$\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

İspat.
$d \mid a$ ve $d \mid b$ olduğundan a/d ile b/d birer tam sayıdır; ifadenin anlamlı olduğunu böylece belirlemiş olduk.
Bézout teoremi gereği

$$d = ax + by$$

olacak biçimde x, y tam sayıları vardır. $d \neq 0$ olduğundan her iki tarafı d'ye bölelim:

$$1 = \frac{a}{d}\,x + \frac{b}{d}\,y$$

Sağ tarafta a/d ile b/d tam sayılarının bir doğrusal birleşimi vardır ve değeri 1'dir. Sonuç 4.3 gereği bu iki sayı aralarında asaldır.
■

Sonuç 5.2 (Kesirlerin En Sade Biçimi). *Her α rasyonel sayısı için*

$$\alpha = \frac{a}{b}, \qquad b > 0, \qquad \gcd(a, b) = 1$$

olacak biçimde a, b tam sayıları vardır.

İspat.
α rasyonel olduğundan $\alpha = m/n$ olacak biçimde $m, n \in \mathbb{Z}$, $n \neq 0$ vardır. Gerekirse pay ve paydayı -1 ile çarparak $n > 0$ olduğunu varsayabiliriz.
$d = \gcd(m, n)$ diyelim ve

$$a := \frac{m}{d}, \qquad b := \frac{n}{d}$$

tanımlayalım. Bunlar birer tam sayıdır; ayrıca $d > 0$ ve $n > 0$ olduğundan $b > 0$'dır. Kesri sadeleştirirsek

$$\frac{a}{b} = \frac{m/d}{n/d} = \frac{m}{n} = \alpha$$

bulunur. Son olarak Sonuç 5.1 gereği $\gcd(a, b) = 1$'dir.
■

Örnek 5.1 ($sqrt(2)$ İrrasyoneldir). $\sqrt{2}$ sayısının rasyonel olmadığını gösteriniz.

Çözüm.
Aksini varsayalım: $\sqrt{2}$ rasyonel olsun. Sonuç 5.2 gereği

$$\sqrt{2} = \frac{a}{b}, \qquad b > 0, \qquad \gcd(a,b) = 1$$

olacak biçimde a, b tam sayıları vardır. Her iki tarafın karesini alıp paydadan kurtulalım:

$$2 = \frac{a^2}{b^2} \Longrightarrow a^2 = 2b^2 \tag{$*$}$$

1. a çifttir. $(*)$ eşitliği a^2 sayısının çift olduğunu söyler. Eğer a tek olsaydı, tek sayıların çarpımı tek olacağından a^2 de tek olurdu. O hâlde a çifttir; yani $a = 2k$ olacak biçimde bir $k \in \mathbb{Z}$ vardır.
2. b de çifttir. $a = 2k$ değerini $(*)$'da yerine koyalım:

$$(2k)^2 = 2b^2 \Longrightarrow 4k^2 = 2b^2 \Longrightarrow b^2 = 2k^2$$

Aynı akıl yürütmeyle b^2 çift, dolayısıyla b de çifttir.
3. Çelişki. a ile b'nin ikisi de çift olduğundan 2 sayısı ikisinin de bir ortak bölenidir; yani

$$2 \mid \gcd(a,b) = 1$$

olur. Bu imkânsızdır.
Çelişki, $\sqrt{2}$'nin rasyonel olduğu varsayımından doğmuştur. O hâlde $\sqrt{2}$ irrasyoneldir.
■

> **i** İspatın can damarı
>
> Yukarıdaki ispatın işlemesinin tek nedeni, kesri **en sade biçimde** yazmış olmamızdır. $\gcd(a,b) = 1$ kabulü olmasaydı "a ile b çifttir" sonucu bir çelişki üretmez, yalnızca kesri sadeleştirmemiz gerektiğini söylerdi. Bu teknik ileride $\sqrt{p}$ sayılarının irrasyonelliğini gösterirken de aynen tekrarlanacaktır.

5.2 Öklid Lemması

Şimdi bölümün merkezindeki teoreme geliyoruz. "a bir çarpımı bölüyorsa çarpanlardan birini böler" önermesinin genel olarak **yanlış** olduğunu görmüştük ($6 \mid 2 \cdot 3$ ama $6 \nmid 2$ ve $6 \nmid 3$). Öklid lemması, doğru olması için gereken ek koşulu tam olarak söyler.

Teorem 5.1 (Öklid Lemması). *$a, b, c \in \mathbb{Z}$ olsun. Eğer*

$$a \mid bc \qquad \text{ve} \qquad \gcd(a,b) = 1$$

ise $a \mid c$'dir.

İspat.
$\gcd(a,b) = 1$ olduğundan Sonuç 4.3 gereği

$$1 = ax + by$$

olacak biçimde x, y tam sayıları vardır. Her iki tarafı c ile çarpalım:

$$c = acx + bcy$$

Sağ taraftaki iki terimi ayrı ayrı inceleyelim:

- *$acx = a(cx)$ olduğundan $a \mid acx$'tir.*
- *Hipotez gereği $a \mid bc$'dir; Teorem 3.1 (11) gereği $a \mid bcy$'dir.*

Teorem 3.1 (7) gereği a sayısı bu ikisinin toplamını da böler:

$$a \mid acx + bcy = c$$

■

⚠ Aralarında asallık koşulu vazgeçilmezdir

$a = 6,\ b = 2,\ c = 3$ alalım. $6 \mid 2 \cdot 3$ doğrudur, ama $6 \nmid 3$'tür. Lemma bozulmuş değildir: burada $\gcd(6, 2) = 2 \neq 1$'dir.
Öklid lemmasının en çok kullanılan hâli, a'nın **asal** olduğu durumdur; bir asal sayı, bölmediği her sayıyla aralarında asal olduğundan koşul kendiliğinden sağlanır. Bu özel hâli asal sayılar bölümünde ayrıca ele alacağız.

Teorem 5.2 (İki Bölenin Çarpımı). *$a, b, c \in \mathbb{Z}$ olsun. Eğer*

$$a \mid c, \qquad b \mid c, \qquad \gcd(a, b) = 1$$

ise $ab \mid c$'dir.

İspat.
$a \mid c$ olduğundan

$$c = as$$

olacak biçimde bir $s \in \mathbb{Z}$ vardır. Hipotez gereği $b \mid c = as$'tir.
Şimdi Öklid lemmasını b, a ve s sayılarına uygulayalım: $b \mid as$ ve $\gcd(b, a) = 1$ olduğundan

$$b \mid s$$

bulunur. O hâlde $s = bt$ olacak biçimde bir $t \in \mathbb{Z}$ vardır. Bunu ilk eşitlikte yerine koyalım:

$$c = as = a(bt) = (ab)\, t$$

t bir tam sayı olduğundan $ab \mid c$'dir.
■

ℹ Bölünebilme iddialarını birleştirmenin yolu

Bu teorem, sayılar teorisi problemlerinde en sık kullanılan "birleştirme kuralıdır". Bir sayının 24 ile bölündüğünü göstermek istiyorsak, doğrudan 24 ile uğraşmak yerine

$$24 = 3 \cdot 8, \qquad \gcd(3, 8) = 1$$

yazıp 3 ile ve 8 ile bölünmeyi ayrı ayrı gösteririz. Aşağıdaki örnekler bu stratejinin uygulamalarıdır. Kuralın aralarında asallık koşulu olmadan **çalışmadığına** dikkat ediniz: $4 \mid 12$ ve $6 \mid 12$ olmasına rağmen $24 \nmid 12$'dir; çünkü $\gcd(4, 6) = 2 \neq 1$'dir.

Teorem 5.3 (Çarpımla Aralarında Asallık). *$a, b, c \in \mathbb{Z}$ olsun. Eğer*

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

ise $\gcd(a, bc) = 1$'dir.

İspat.
Sonuç 4.3 gereği

$$1 = ax + by, \qquad 1 = au + cv$$

olacak biçimde x, y, u, v tam sayıları vardır. İki eşitliği taraf tarafa çarpalım:

$$1 = (ax + by)(au + cv) = a^2xu + acxv + abyu + bcyv$$

İlk üç terimde a ortak çarpandır; onları gruplayalım:

$$1 = a\ (\ axu + cxv + byu\ ) + (bc)\ (\ yv\ )$$

Böylece 1 sayısını a ile bc'nin bir doğrusal birleşimi olarak yazdık. Sonuç 4.3 gereği $\gcd(a, bc) = 1$'dir.
■

Sonuç 5.3 (Kuvvetlerle Aralarında Asallık). *$a, b \in \mathbb{Z}$ ve $\gcd(a, b) = 1$ olsun. Bu durumda her m, n pozitif tam sayısı için*

$$\gcd(a^m, b^n) = 1$$

İspat.
Önce sabit bir a için $\gcd(a, b^n) = 1$ olduğunu n üzerinden tümevarımla gösterelim.
Başlangıç adımı ($n = 1$). $\gcd(a, b) = 1$ *hipotezdir.*
Tümevarım adımı. $\gcd(a, b^k) = 1$ *olduğunu varsayalım. Elimizde*

$$\gcd(a, b) = 1 \qquad \text{ve} \qquad \gcd(a, b^k) = 1$$

vardır. Teorem 5.3 gereği

$$\gcd\big(a, b \cdot b^k\big) = \gcd\big(a, b^{k+1}\big) = 1$$

bulunur. Tümevarım gereği her n için $\gcd(a, b^n) = 1$'dir.
Şimdi b^n sayısını sabit tutup aynı akıl yürütmeyi a için tekrarlayalım: $\gcd(b^n, a) = 1$ olduğundan, yukarıdaki sonucu a ile b^n'nin rollerini değiştirerek uygularsak

$$\gcd(b^n, a^m) = 1$$

elde edilir. En büyük ortak bölen sıralamadan bağımsız olduğundan $\gcd(a^m, b^n) = 1$'dir.
■

5.3 Bölünebilme İddialarını Birleştirme

Örnek 5.2 (\$6 divides n \(n + 1 \) \(n + 2 \)\$). Her n tam sayısı için $6 \mid n(n+1)(n+2)$ olduğunu gösteriniz.

Çözüm.
$6 = 2 \cdot 3$ ve $\gcd(2, 3) = 1$ olduğundan, Teorem 5.2 gereği çarpımın hem 2 hem de 3 ile bölündüğünü göstermek yeterlidir.
2 ile bölünme. Örnek 3.2 (a) gereği $2 \mid n(n+1)$'dir; dolayısıyla 2 sayısı $n(n+1)(n+2)$ çarpımını da böler.
3 ile bölünme. Örnek 3.2 (b) gereği $3 \mid n(n+1)(n+2)$'dir.
$2 \mid n(n+1)(n+2)$, $3 \mid n(n+1)(n+2)$ ve $\gcd(2, 3) = 1$ olduğundan

$$2 \cdot 3 = 6 \mid n(n+1)(n+2)$$

bulunur.
■

Örnek 5.3 (Tek Sayılarda \$24 divides a \(a^2 - 1 \)\$). Her a tek tam sayısı için $24 \mid a(a^2 - 1)$ olduğunu gösteriniz.

Çözüm.
$24 = 3 \cdot 8$ ve $\gcd(3, 8) = 1$ olduğundan, Teorem 5.2 gereği $3 \mid a(a^2 - 1)$ ve $8 \mid a(a^2 - 1)$ olduğunu ayrı ayrı göstermek yeterlidir.

3 ile bölünme. İfadeyi çarpanlarına ayıralım:

$$a(a^2-1) = a(a-1)(a+1) = (a-1)\,a\,(a+1)$$

Bu, ardışık üç tam sayının çarpımıdır; Örnek 3.2 (b) gereği 3 ile bölünür.
8 ile bölünme. a tek olduğundan Örnek 2.3 gereği $a^2 = 8k+1$ olacak biçimde bir k tam sayısı vardır. Buradan

$$a^2 - 1 = 8k$$

bulunur; yani $8 \mid a^2-1$'dir. O hâlde 8 sayısı $a(a^2-1)$ çarpımını da böler.
Birleştirme. $3 \mid a(a^2-1)$, $8 \mid a(a^2-1)$ ve $\gcd(3,8) = 1$ olduğundan

$$3 \cdot 8 = 24 \mid a(a^2-1)$$

bulunur.
■

Örnek 5.4 ($6 divides a \(a^2 + 11 \)$). Her a tam sayısı için $6 \mid a(a^2+11)$ olduğunu gösteriniz.

Çözüm.
İfadeyi, bölünebilirliğini bildiğimiz bir yapıya indirgeyelim:

$$a(a^2+11) = a^3 + 11a = (a^3-a) + 12a = (a-1)\,a\,(a+1) + 12a$$

Sağ taraftaki iki terimi ayrı ayrı ele alalım.

- Örnek 5.2 gereği ardışık üç tam sayının çarpımı 6 ile bölünür: $6 \mid (a-1)a(a+1)$.
- $12a = 6 \cdot (2a)$ olduğundan $6 \mid 12a$'dır.

Teorem 3.1 (7) gereği 6 sayısı toplamı da böler:

$$6 \mid (a-1)a(a+1) + 12a = a(a^2+11)$$

■

Örnek 5.5 ($6 divides n \(7\,n^2 + 5 \)$). Her n tam sayısı için $6 \mid n(7n^2+5)$ olduğunu gösteriniz.

Çözüm.
İfadeyi açalım ve 6'nın katlarını ayıklayalım:

$$\begin{aligned} n(7n^2+5) &= 7n^3 + 5n \\ &= 6n^3 + n^3 + 6n - n \\ &= 6(n^3+n) + (n^3-n) \\ &= 6(n^3+n) + (n-1)\,n\,(n+1) \end{aligned}$$

Sağ taraftaki iki terime bakalım:

- İlk terim 6'nın açık bir katıdır.
- Örnek 5.2 gereği ardışık üç tam sayının çarpımı 6 ile bölünür.

O hâlde 6 sayısı toplamı da böler:

$$6 \mid n(7n^2+5)$$

■

5.4 Kuvvetler ve Bölünebilme

Örnek 5.6 ($a divides b arrow.l.r.double a^n divides b^n$). n sabit bir pozitif tam sayı olmak üzere, her a, b tam sayısı için

$$a \mid b \Leftrightarrow a^n \mid b^n$$

olduğunu gösteriniz.

Çözüm.
(⇒) $a \mid b$ olsun; $b = ax$ olacak biçimde bir $x \in \mathbb{Z}$ vardır. Her iki tarafın n'inci kuvvetini alalım:

$$b^n = (ax)^n = a^n x^n$$

x^n bir tam sayı olduğundan $a^n \mid b^n$'dir.
(⇐) $a^n \mid b^n$ olsun. $a = 0$ ise $a^n = 0$ olur ve Teorem 3.1 (3) gereği $b^n = 0$, yani $b = 0$ olur; bu durumda $a \mid b$ sağlanır. O hâlde $a \neq 0$ varsayabiliriz. Benzer biçimde $b = 0$ ise $a \mid 0$ zaten doğrudur; $b \neq 0$ da varsayalım.
$d := \gcd(a, b)$ diyelim ve

$$a = da', \qquad b = db'$$

yazalım. Sonuç 5.1 gereği $\gcd(a', b') = 1$'dir. Hipotezi bu yazılımla ifade edelim:

$$d^n (a')^n \mid d^n (b')^n$$

$d \neq 0$ olduğundan Teorem 3.1 (12) gereği d^n çarpanını sadeleştirebiliriz:

$$(a')^n \mid (b')^n$$

Öte yandan $\gcd(a', b') = 1$ olduğundan Sonuç 5.3 gereği

$$\gcd((a')^n, (b')^n) = 1$$

olur. Bir sayı hem $(b')^n$'i bölüyor hem de onunla aralarında asal ise, kendisiyle 1'in ortak bölenidir:

$$(a')^n \mid \gcd((a')^n, (b')^n) = 1$$

Buradan $(a')^n = \pm 1$, dolayısıyla $a' = \pm 1$ bulunur. O hâlde

$$a = da' = \pm d$$

olur. $d = \gcd(a, b) \mid b$ olduğundan Teorem 3.1 (13) gereği $a = \pm d$ sayısı da b'yi böler:

$$a \mid b$$

■

5.5 Çalışma Problemleri

Alıştırma 5.1 (Aralarında Asallığın Taşınması). a, b, c tam sayıları için aşağıdakileri gösteriniz.
a) $\gcd(a, b) = 1$ ise $\gcd(c, b) = \gcd(ac, b)$'dir.
b) $\gcd(a, b) = 1$ ve $c \mid a - b$ ise $\gcd(a, c) = 1$'dir.
c) $c \mid a$ ve $\gcd(a, b) = 1$ ise $\gcd(c, b) = 1$'dir.
İpucu (b): $d = \gcd(a, c)$ diyerek $d \mid a - (a - b)$ hesabını yapınız.

Alıştırma 5.2 (Bölünebilme İddialarını Birleştirme). Aşağıdakileri ispatlayınız.
a) Her n tam sayısı için $30 \mid n^5 - n$.
b) Her n tam sayısı için $12 \mid n^4 - n^2$.
c) Her n tek tam sayısı için $48 \mid n^3 - n$ olduğu doğru mudur? Değilse doğru olan en büyük sabiti bulunuz.

Alıştırma 5.3 (EBOB ve EKOK Arasında). a, b sıfırdan farklı tam sayılar ve c herhangi bir tam sayı olsun. Eğer $a \mid c$ ve $b \mid c$ ise, $\gcd(a,b) = d$ olmak üzere

$$\frac{ab}{d} \Big| c$$

olduğunu gösteriniz.
İpucu: $a = da'$, $b = db'$ yazıp Sonuç 5.1 ile Teorem 5.2'ı birlikte kullanınız. *(Bir sonraki bölümde ab/d sayısının a ile b'nin en küçük ortak katı olduğunu göreceğiz.)*

Alıştırma 5.4 (Bir İrrasyonellik İspatı). $\sqrt{3}$ sayısının irrasyonel olduğunu gösteriniz.
İpucu: Örnek 5.1'deki yolu izleyiniz; "çift/tek" ayrımının yerini "3 ile bölünen / bölünmeyen" ayrımı alacak ve Örnek 2.4'ten yararlanacaksınız.

6. Öklid Algoritması

Bézout teoremi $\gcd(a,b) = ax_0 + by_0$ eşitliğini sağlayan katsayıların **var olduğunu** söylüyor, ama onları nasıl bulacağımızı söylemiyor. Küçük sayılarda deneme yanılma işe yarar; $\gcd(1234, 4321)$ gibi bir hesapta ise yararsız kalır. Bu bölümde hem en büyük ortak böleni hem de Bézout katsayılarını sistemli biçimde üreten bir yöntem kuracağız.

6.1 Algoritmanın Dayandığı Gözlem

Bütün yöntem tek bir basit kurala dayanır: bir sayıdan diğerinin katını çıkarmak en büyük ortak böleni değiştirmez.

Önerme 6.1 (EBOB Kat Çıkarmayla Değişmez). *Her $a, b, k \in \mathbb{Z}$ için (a ile b ikisi birden sıfır olmamak üzere)*

$$\gcd(a,b) = \gcd(a, b - ak)$$

> ***İspat.***
> *İki çiftin **ortak bölenler kümelerinin aynı** olduğunu göstermek yeterlidir; aynı kümenin en büyük elemanı da aynı olacaktır.*
> *($\subseteq$) c sayısı a ile b'nin bir ortak böleni olsun; yani $c \mid a$ ve $c \mid b$. Teorem 3.1 (6) gereği c sayısı a ile b'nin her doğrusal birleşimini böler; özel olarak*
>
> $$c \mid b - ak$$
>
> *O hâlde c, a ile $b - ak$'nın da bir ortak bölenidir.*
> *($\supseteq$) c sayısı a ile $b - ak$'nın bir ortak böleni olsun. Yine aynı özellik gereği*
>
> $$c \mid (b - ak) + ak = b$$
>
> *olur; yani c, a ile b'nin de bir ortak bölenidir.*
> *İki kapsama birlikte, ortak bölenler kümelerinin çakıştığını gösterir. Dolayısıyla en büyük ortak bölenler de eşittir.*
> ■

> **i** Bölme algoritmasıyla birleştirince
>
> $b = ak + r$ yazılışında $r = b - ak$ olduğundan, yukarıdaki önerme şunu söyler:
>
> $$b = ak + r \Longrightarrow \gcd(a,b) = \gcd(a,r)$$
>
> Yani **bölen ile kalanın en büyük ortak böleni, bölünen ile bölenin en büyük ortak bölenine eşittir.** Kalan bölenden küçük olduğuna göre, bu kuralı tekrar tekrar uygulamak sayıları hızla küçültür. Öklid algoritması tam olarak budur.

6.2 Algoritma

Teorem 6.1 (Öklid Algoritması). *$a, b \in \mathbb{Z}$ ve $a > 0$ olsun. Bölme algoritmasını ardışık olarak uygulayalım:*

$$\begin{aligned} b &= aq_1 + r_1, & 0 < r_1 < a \\ a &= r_1q_2 + r_2, & 0 < r_2 < r_1 \\ r_1 &= r_2q_3 + r_3, & 0 < r_3 < r_2 \\ &\vdots \\ r_{n-2} &= r_{n-1}q_n + r_n, & 0 < r_n < r_{n-1} \\ r_{n-1} &= r_nq_{n+1} & (\text{kalan } 0) \end{aligned}$$

Bu durumda

$$\gcd(a, b) = r_n$$

yani ***en büyük ortak bölen, sıfırdan farklı son kalandır****.*

İspat.
1. Algoritma durur. *Kalanlar*

$$a > r_1 > r_2 > r_3 > \cdots \geq 0$$

biçiminde azalan, negatif olmayan tam sayılardır. Sonsuza kadar azalan bir doğal sayı dizisi olamaz: aksi hâlde bu kalanların kümesi, boş olmayan ama en küçük elemanı bulunmayan bir doğal sayı kümesi olurdu ve iyi sıralama prensibiyle çelişirdi. O hâlde bir adımdan sonra kalan 0 *olur; sıfırdan farklı son kalana* r_n *diyoruz.*
2. Son kalan, aranan EBOB'tur. *Önerme 6.1'i her satıra sırayla uygulayalım. İlk satırda* $b = aq_1 + r_1$*, yani* $r_1 = b - aq_1$ *olduğundan*

$$\gcd(a, b) = \gcd(a, r_1)$$

İkinci satırda $a = r_1q_2 + r_2$ *olduğundan aynı kuralla*

$$\gcd(a, r_1) = \gcd(r_1, r_2)$$

Bu şekilde devam edersek

$$\gcd(a, b) = \gcd(a, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-1}, r_n)$$

zinciri elde edilir. Son satırda $r_{n-1} = r_nq_{n+1}$*, yani* $r_n \mid r_{n-1}$*'dir. Önerme 4.2 (2) gereği*

$$\gcd(r_{n-1}, r_n) = \mid r_n \mid = r_n$$

(son eşitlikte $r_n > 0$ olmasını kullandık). *Zinciri birleştirirsek* $\gcd(a, b) = r_n$ *bulunur.*
■

> **i** Ne kadar hızlı?
>
> Algoritmanın çekiciliği hızındadır. Her adımda kalan en az yarıya iner; çünkü $r_{k+1} < r_k$ olmasının yanı sıra, ardışık iki adımda kalan mutlaka yarıdan küçük hâle gelir. Bu yüzden $\gcd(a, b)$ hesabı, sayıların basamak sayısıyla orantılı sayıda bölme işleminde biter — çarpanlara ayırmaya hiç gerek kalmadan.
> Bu, algoritmanın ders açısından da önemli bir yanıdır: en büyük ortak böleni bulmak için sayıların asal çarpanlarını bilmemiz **gerekmez**.

6.3 Bézout Katsayılarını Bulma

Algoritma bittiğinde elimizde bölmelerin listesi kalır. Bu listeyi **sondan başa** okuyup her kalanı bir önceki satırdan gelen ifadeyle değiştirirsek, en büyük ortak böleni adım adım a ile b cinsinden yazarız. Bu işleme **geriye doğru yerine koyma** denir.

Örnek 6.1 (\$gcd \(182 \, 70 \)\$ ve Bézout Katsayıları). **a)** $\gcd(182, 70)$ değerini bulunuz.
b) $\gcd(182, 70) = 182x + 70y$ koşulunu sağlayan x, y tam sayılarını bulunuz.

Çözüm.
a) Öklid algoritması.

$$\begin{aligned} 182 &= 2 \cdot 70 + 42 \\ 70 &= 1 \cdot 42 + 28 \\ 42 &= 1 \cdot 28 + 14 \\ 28 &= 2 \cdot 14 + 0 \end{aligned}$$

Sıfırdan farklı son kalan 14 olduğundan

$$\gcd(182, 70) = 14$$

b) Geriye doğru yerine koyma. Önce her satırdaki kalanı yalnız bırakalım:

$$\begin{aligned} 42 &= 182 - 2 \cdot 70 \\ 28 &= 70 - 1 \cdot 42 \\ 14 &= 42 - 1 \cdot 28 \end{aligned}$$

Şimdi en alttan başlayıp yukarı doğru yerine koyalım:

$$\begin{aligned} 14 &= 42 - 28 \\ &= 42 - (70 - 42) && (\ 28 \ \text{yerine kondu}) \\ &= 2 \cdot 42 - 70 \\ &= 2(182 - 2 \cdot 70) - 70 && (\ 42 \ \text{yerine kondu}) \\ &= 2 \cdot 182 - 4 \cdot 70 - 70 \\ &= 182 \cdot 2 + 70 \cdot (-5) \end{aligned}$$

(Sağlama: $364 - 350 = 14$ ✓*)*
O hâlde $x = 2$, $y = -5$ alınabilir.
■

> **i** Yerine koyarken sadeleştirmeyin
>
> Geriye doğru yerine koyarken en sık yapılan hata, ara adımlarda sayıları çarpıp toplamaktır. Örneğin yukarıdaki üçüncü satırda $2 \cdot 42 - 70$ ifadesini $84 - 70 = 14$ diye hesaplarsak elimizde yalnızca 14 kalır ve 182 ile 70'e nasıl ulaşacağımızı kaybederiz.
> Kural şudur: **182 ile 70 sembollerini asla sayıya dönüştürmeyin**, yalnızca katsayılarını düzenleyin.

Örnek 6.2 (\$gcd \(70 \, 48 \)\$ ve Bézout Katsayıları). Öklid algoritmasını kullanarak $\gcd(70, 48)$ değerini ve

$$\gcd(70, 48) = 70x_0 + 48y_0$$

koşuluna uyan bir (x_0, y_0) tam sayı ikilisi bulunuz.

Çözüm.
Algoritma.

$$\begin{aligned} 70 &= 1 \cdot 48 + 22 \\ 48 &= 2 \cdot 22 + 4 \\ 22 &= 5 \cdot 4 + 2 \\ 4 &= 2 \cdot 2 + 0 \end{aligned}$$

Sıfırdan farklı son kalan 2 olduğundan $\gcd(70, 48) = 2$'dir.
Geriye doğru yerine koyma. Kalanları yalnız bırakalım:

$$\begin{aligned} 22 &= 70 - 48 \\ 4 &= 48 - 2 \cdot 22 \\ 2 &= 22 - 5 \cdot 4 \end{aligned}$$

Aşağıdan yukarı doğru ilerleyelim:

$$\begin{aligned} 2 &= 22 - 5 \cdot 4 \\ &= 22 - 5(48 - 2 \cdot 22) \\ &= 22 - 5 \cdot 48 + 10 \cdot 22 \\ &= 11 \cdot 22 - 5 \cdot 48 \\ &= 11(70 - 48) - 5 \cdot 48 \\ &= 11 \cdot 70 - 11 \cdot 48 - 5 \cdot 48 \\ &= 70 \cdot 11 + 48 \cdot (-16) \end{aligned}$$

(Sağlama: $770 - 768 = 2$ ✓*)*
O hâlde $(x_0, y_0) = (11, -16)$'dır.
■

6.4 Üç ve Daha Fazla Sayının EBOB'u

Hepsi birden sıfır olmayan a, b, c tam sayılarının en büyük ortak böleni, üçünün ortak bölenlerinin en büyüğüdür ve $\gcd(a, b, c)$ ile gösterilir. Bu değeri hesaplamak için yeni bir yönteme ihtiyaç yoktur: ikişer ikişer ilerlemek yeterlidir.

Önerme 6.2 (Üç Sayının EBOB'u). *Hepsi birden sıfır olmayan her a, b, c tam sayısı için*

$$\gcd(a, b, c) = \gcd\big(\,\gcd(a, b),\, c\,\big)$$

Bunun nedeni şudur: Teorem 4.2 gereği bir sayı a ile b'nin ortak böleni olmakla $\gcd(a, b)$'nin böleni olmak aynı şeydir. Dolayısıyla $\{a, b, c\}$ üçlüsünün ortak bölenleri ile $\{\gcd(a, b), c\}$ ikilisinin ortak bölenleri aynı kümedir; en büyük elemanları da aynıdır.

Örnek 6.3 ($gcd \(56 \, 21 \, 231 \)$ Bir Doğrusal Birleşim Olarak).

$$\gcd(56, 21, 231) = 56x + 21y + 231z$$

koşulunu sağlayan bir (x, y, z) tam sayı üçlüsü bulunuz.

Çözüm.
1. Adım: $\gcd(56, 21)$.

$$\begin{aligned} 56 &= 2 \cdot 21 + 14 \\ 21 &= 1 \cdot 14 + 7 \\ 14 &= 2 \cdot 7 + 0 \end{aligned}$$

O hâlde $\gcd(56, 21) = 7$'dir. Geriye doğru yerine koyalım:

$$\begin{aligned} 7 &= 21 - 14 \\ &= 21 - (56 - 2 \cdot 21) \\ &= 56 \cdot (-1) + 21 \cdot 3 \end{aligned}$$

(Sağlama: $-56 + 63 = 7$ ✓*)*
2. Adım: $\gcd(7, 231)$. $231 = 33 \cdot 7$ olduğundan $7 \mid 231$'dir; Önerme 4.2 (2) gereği

$$\gcd(7, 231) = 7$$

3. Adım: Sonucu birleştirme. Önerme 6.2 gereği

$$\gcd(56, 21, 231) = \gcd\big(\,\gcd(56, 21),\, 231\,\big) = \gcd(7, 231) = 7$$

Birinci adımda bulduğumuz birleşimde 231 katsayısını 0 alalım:

$$7 = 56 \cdot (-1) + 21 \cdot 3 + 231 \cdot 0$$

O hâlde $(x, y, z) = (-1, 3, 0)$ bir çözümdür.
■

Örnek 6.4 ($gcd \(100 \, 70 \, 55 \)$ Bir Doğrusal Birleşim Olarak).

$$\gcd(100, 70, 55) = 100x + 70y + 55z$$

koşulunu sağlayan bir (x, y, z) tam sayı üçlüsü bulunuz.

Çözüm.
1. Adım: $\gcd(100, 70)$.

$$\begin{aligned} 100 &= 1 \cdot 70 + 30 \\ 70 &= 2 \cdot 30 + 10 \\ 30 &= 3 \cdot 10 + 0 \end{aligned}$$

O hâlde $\gcd(100, 70) = 10$'dur. Geriye doğru yerine koyalım:

$$\begin{aligned} 10 &= 70 - 2 \cdot 30 \\ &= 70 - 2(100 - 70) \\ &= 100 \cdot (-2) + 70 \cdot 3 \end{aligned}$$

(Sağlama: $-200 + 210 = 10$ ✓*)*
2. Adım: $\gcd(10, 55)$.

$$\begin{aligned} 55 &= 5 \cdot 10 + 5 \\ 10 &= 2 \cdot 5 + 0 \end{aligned}$$

O hâlde $\gcd(10, 55) = 5$'tir ve

$$5 = 55 - 5 \cdot 10$$

3. Adım: Birleştirme. Önerme 6.2 gereği

$$\gcd(100, 70, 55) = \gcd(10, 55) = 5$$

Şimdi son eşitlikte 10 yerine birinci adımda bulduğumuz ifadeyi koyalım:

$$\begin{aligned} 5 &= 55 - 5 \cdot 10 \\ &= 55 - 5(100 \cdot (-2) + 70 \cdot 3) \\ &= 55 + 10 \cdot 100 - 15 \cdot 70 \\ &= 100 \cdot 10 + 70 \cdot (-15) + 55 \cdot 1 \end{aligned}$$

(Sağlama: $1000 - 1050 + 55 = 5$ ✓*)*
O hâlde $(x, y, z) = (10, -15, 1)$ bir çözümdür.
■

i Genel yöntem

Üç sayıda işleyen bu strateji istenildiği kadar uzatılabilir. $\gcd(a_1, a_2, \ldots, a_k)$ hesabı için soldan başlayıp ikişer ikişer ilerlenir:

$$\gcd(a_1, a_2, \ldots, a_k) = \gcd\Big(\gcd\big(\cdots \gcd(a_1, a_2), \ldots\big), a_k\Big)$$

Doğrusal birleşim de aynı sırayla, her adımda bir önceki adımın ifadesi yerine konularak elde edilir.

6.5 Çalışma Problemleri

Alıştırma 6.1 (Öklid Algoritması Uygulamaları). Aşağıdaki en büyük ortak bölenleri Öklid algoritmasıyla hesaplayınız ve her biri için Bézout katsayılarını bulunuz.
a) $\gcd(1001, 357)$ **b)** $\gcd(272, 1479)$ **c)** $\gcd(-84, 132)$ **d)** $\gcd(2024, 748)$

Alıştırma 6.2 (Üç Sayının EBOB'u). Aşağıdaki değerleri hesaplayıp birer doğrusal birleşim olarak yazınız.
a) $\gcd(6, 10, 15)$ **b)** $\gcd(42, 70, 105)$ **c)** $\gcd(105, 140, 350)$

Alıştırma 6.3 (Ardışık Fibonacci Sayıları). $F_1 = F_2 = 1$ ve $F_n = F_{n-1} + F_{n-2}$ ile tanımlanan Fibonacci dizisini göz önüne alınız.
a) $\gcd(F_{n+1}, F_n) = 1$ olduğunu tümevarımla gösteriniz.
b) $\gcd(F_{n+1}, F_n)$ hesabında Öklid algoritmasının kaç adım sürdüğünü gözlemleyiniz. *(Fibonacci sayıları, algoritmayı en çok yavaşlatan girdilerdir.)*

7. En Küçük Ortak Kat

En büyük ortak bölen, iki sayının **ortak bölenlerine** bakıyordu. Şimdi aynayı çevirip **ortak katlarına** bakacağız. Ortaya çıkan kavram, en büyük ortak bölenin ikizidir; nitekim ikisi arasında çok kullanışlı bir çarpım bağıntısı vardır.

7.1 Tanım ve Varlık

Tanım 7.1 (En Küçük Ortak Kat). a, b sıfırdan farklı tam sayılar, m ise bir pozitif tam sayı olsun. Eğer

1. $a \mid m$ ve $b \mid m$;
2. her $c \in \mathbb{N}$ için, $a \mid c$ ve $b \mid c$ ise $m \leq c$

koşulları sağlanırsa m sayısına a ile b'nin **en küçük ortak katı** denir ve

$$\operatorname{lcm}(a, b)$$

ile gösterilir.

> **i** Tanımın iki incelikli noktası
>
> **1. En küçük ortak kat gerçekten var mıdır?**
> Vardır. a ile b'nin pozitif ortak katlarının kümesine M diyelim. $\mid ab \mid$ sayısı hem a'nın hem de b'nin katıdır ve pozitiftir; yani $M \neq \emptyset$'dır. M boş olmayan bir doğal sayı kümesi olduğundan, iyi sıralama prensibi gereği bir en küçük elemanı vardır. Bu eleman tanımdaki iki koşulu da sağlar.
> **2. Neden a ile b'nin sıfırdan farklı olması isteniyor?**
> $a = 0$ olsaydı, 0'ın tek katı yine 0 olduğundan hiçbir **pozitif** ortak kat bulunamazdı; M boş kalır ve en küçük eleman tanımlanamazdı.
> Ayrıca en küçük eleman tek türlü belirli olduğundan $\operatorname{lcm}(a, b)$ tek türlü belirlidir.

Örnek 7.1 (İlk Örnekler).

$$\operatorname{lcm}(4, 6) = 12, \qquad \operatorname{lcm}(-6, 10) = 30$$

Birincisi için: 4'ün pozitif katları $4, 8, 12, 16, \ldots$ ve 6'nın pozitif katları $6, 12, 18, \ldots$'dir. Ortak olanların en küçüğü 12'dir.
İkincisinde işaretin bir rolü yoktur; -6'nın katları ile 6'nın katları aynı kümedir.

Az önceki gözlemi ayrıca kaydedelim: bölünebilme işaretten etkilenmediğinden en küçük ortak kat da etkilenmez.

Önerme 7.1 (EKOK ve İşaret). *Sıfırdan farklı her a, b tam sayısı için*

$$\operatorname{lcm}(a, b) = \operatorname{lcm}(-a, b) = \operatorname{lcm}(a, -b) = \operatorname{lcm}(-a, -b)$$

Gerçekten de Teorem 3.1 (13) gereği $a \mid m$ ile $-a \mid m$ önermeleri denktir; dolayısıyla dört çiftin pozitif ortak katları aynı kümedir ve en küçük elemanları da aynıdır.

7.2 EBOB ile EKOK Arasındaki Bağıntı

Şimdi iki kavramı birbirine bağlayan teoreme geliyoruz. Teorem pratikte çok işe yarar: en küçük ortak katı hesaplamak için ayrı bir algoritmaya ihtiyaç duymayız, Öklid algoritmasıyla bulduğumuz en büyük ortak bölen yeterlidir.

Teorem 7.1 (EBOB $times$ EKOK $=$ Çarpım). *Her a, b pozitif tam sayısı için*

$$a \cdot b = \gcd(a,b) \cdot \operatorname{lcm}(a,b)$$

İspat.
$d := \gcd(a,b)$ olsun. $d \mid a$ ve $d \mid b$ olduğundan

$$a = dr, \qquad b = ds$$

olacak biçimde r, s pozitif tam sayıları vardır. Ayrıca Bézout teoremi gereği

$$d = ax + by$$

olacak biçimde x, y tam sayıları vardır.
Şimdi aday sayımızı tanımlayalım:

$$m := \frac{a \cdot b}{d}$$

Bu sayının bir tam sayı olduğunu görmek kolaydır:

$$m = \frac{ab}{d} = \frac{(dr)b}{d} = r \cdot b = a \cdot s$$

m sayısının a ile b'nin en küçük ortak katı olduğunu, tanımdaki iki koşulu doğrulayarak gösterelim.
Koşul 1: m bir ortak kattır. *Yukarıdaki yazılışlardan $m = a \cdot s$ ve $m = r \cdot b$ olduğundan*

$$a \mid m \qquad \text{ve} \qquad b \mid m$$

Ayrıca $a, b, d > 0$ olduğundan $m > 0$'dır.
Koşul 2: m ortak katların en küçüğüdür. *$c \in \mathbb{N}$ olsun ve $a \mid c$, $b \mid c$ olsun. Bu durumda*

$$c = au, \qquad c = bv$$

olacak biçimde u, v tam sayıları vardır. Şimdi c/m oranını hesaplayalım ve payda görünen d yerine Bézout ifadesini koyalım:

$$\begin{aligned} \frac{c}{m} &= \frac{c\,d}{ab} \\ &= \frac{c\,(ax+by)}{ab} \\ &= \frac{c\,ax}{ab} + \frac{c\,by}{ab} \\ &= \frac{c}{b}\,x + \frac{c}{a}\,y \\ &= vx + uy \end{aligned}$$

Son satırda $c/b = v$ ve $c/a = u$ olduğunu kullandık. $vx + uy$ bir tam sayı olduğundan

$$c = m\,(vx + uy)$$

yazılır; yani $m \mid c$'dir. c pozitif olduğundan Teorem 3.1 (8) gereği

$$m \leq c$$

bulunur.
İki koşul da sağlandığından $m = \operatorname{lcm}(a,b)$'dir. Buradan

$$\text{lcm}\ (a,b) = \frac{ab}{d} = \frac{ab}{\gcd(a,b)}$$

ve düzenlemeyle istenen

$$a \cdot b = \gcd(a,b) \cdot \text{lcm}\ (a,b)$$

eşitliği elde edilir.
■

İspatın ikinci adımı, teoremin ifadesinden daha fazlasını söylüyordu: her ortak katın m tarafından **bölündüğünü** gösterdik, yalnızca m'den büyük olduğunu değil. Bu kuvvetli biçimi ayrıca kaydedelim.

Sonuç 7.1 (Ortak Katlar EKOK'un Katlarıdır). *a, b sıfırdan farklı tam sayılar ve c herhangi bir tam sayı olsun. Eğer $a \mid c$ ve $b \mid c$ ise*

$$\text{lcm}\ (a,b) \mid c$$

i EBOB ile EKOK'un simetrisi

Bu sonuç, iki kavram arasındaki güzel simetriyi tamamlar:

- **EBOB:** her ortak bölen, en büyük ortak böleni **böler** ($\thinspace$Teorem 4.2$\thinspace$).
- **EKOK:** en küçük ortak kat, her ortak katı **böler**.

Yani "en büyük" ve "en küçük" sıfatları aslında sıralamayla değil, bölünebilmeyle ilgilidir.

Sonuç 7.2 (Aralarında Asal Sayılarda EKOK). *Her a, b pozitif tam sayısı için*

$$\text{lcm}\ (a,b) = a \cdot b$$

olabilmesi için gerek ve yeter koşul a ile b'nin aralarında asal olmasıdır.

Bu, Teorem 7.1'un doğrudan sonucudur: $ab = \gcd(a,b) \cdot \text{lcm}\ (a,b)$ eşitliğinde $\text{lcm}\ (a,b) = ab$ olması, ancak ve ancak $\gcd(a,b) = 1$ olduğunda mümkündür.
Teoremi pozitif sayılar için ifade etmiştik. İşaretlerden bağımsız genel biçimi de kaydedelim.

Sonuç 7.3 (Genel Çarpım Bağıntısı). *Sıfırdan farklı her a, b tam sayısı için*

$$\mid a \cdot b \mid = \gcd(a,b) \cdot \text{lcm}\ (a,b)$$

Gerçekten de Önerme 4.2 (3) ile Önerme 7.1 gereği her iki taraf da a ile b'nin işaretlerinden etkilenmez; dolayısıyla $\mid a \mid$ ve $\mid b \mid$ pozitif sayılarına Teorem 7.1'u uygulamak yeterlidir.

7.3 Çözümlü Örnekler

Örnek 7.2 (EKOK Hesabı). $\text{lcm}\ (182, 70)$ değerini bulunuz.

Çözüm.
Örnek 6.1'de Öklid algoritmasıyla $\gcd(182, 70) = 14$ bulmuştuk. Teorem 7.1 gereği

$$\text{lcm}\ (182,70) = \frac{182 \cdot 70}{\gcd(182,70)} = \frac{12740}{14} = 910$$

(Sağlama: $910 = 182 \cdot 5 = 70 \cdot 13$ ✓*)*
■

i Neden önce EBOB?

En küçük ortak katı doğrudan aramak — yani katları tek tek listeleyip ilk ortak olanı bulmak — büyük sayılarda umutsuzdur. Oysa Öklid algoritması birkaç bölmede biter. Bu yüzden pratikte daima önce gcd hesaplanır, sonra bölme yapılır.
Bölmeyi çarpmadan **önce** yapmak da iyi bir alışkanlıktır: $\frac{182}{14} \cdot 70 = 13 \cdot 70 = 910$ hesabı, 12740 gibi büyük bir sayı üretmeden aynı sonucu verir.

Örnek 7.3 (EBOB ile EKOK Ne Zaman Eşittir?). $a, b \in \mathbb{Z} \setminus \{0\}$ olsun. $\gcd(a,b) = \operatorname{lcm}(a,b)$ olabilmesi için gerek ve yeter koşulun $a = \pm b$ olduğunu gösteriniz.

Çözüm.
(⇒) $\gcd(a,b) = \operatorname{lcm}(a,b) = m$ olsun.
En büyük ortak bölenin tanımı gereği $m \mid a$'dır. En küçük ortak katın tanımı gereği ise $a \mid m$'dir. Teorem 3.1 (9) gereği bu ikisi birlikte

$$a = \pm m$$

verir. Tamamen aynı akıl yürütmeyle $b = \pm m$ bulunur. O hâlde a ile b mutlak değerce eşittir:

$$|a| = |b| = m \Longrightarrow a = \pm b$$

(⇐) $a = \pm b$ olsun. Önerme 4.2 (3) ve Önerme 7.1 gereği işaretler sonucu değiştirmediğinden $a = b > 0$ durumunu incelemek yeterlidir. Bu durumda

$$\gcd(a,a) = a \qquad \text{ve} \qquad \operatorname{lcm}(a,a) = a$$

olur; yani ikisi eşittir. *(İlki için Önerme 4.2 (2)'yi, ikincisi için a'nın kendisinin en küçük pozitif ortak kat olduğunu kullandık.)*
■

Örnek 7.4 (Ortak Katın Bölünmesi). a, b sıfırdan farklı iki tam sayı, c ise herhangi bir tam sayı olsun. Eğer $a \mid c$ ve $b \mid c$ ise $\operatorname{lcm}(a,b)$ sayısının da c'yi böldüğünü gösteriniz.

Çözüm.
$m := \operatorname{lcm}(a,b)$ diyelim. Bölme algoritmasına göre

$$c = mq + r, \qquad 0 \le r < m$$

olacak biçimde q, r tam sayıları vardır. Amacımız $r = 0$ olduğunu göstermek.
r'yi yalnız bırakalım:

$$r = c - mq$$

Şimdi a sayısının sağ tarafı böldüğünü gösterelim:

- Hipotez gereği $a \mid c$'dir.
- m bir ortak kat olduğundan $a \mid m$, dolayısıyla $a \mid mq$'dur.

Teorem 3.1 (7) gereği $a \mid c - mq = r$'dir. Tamamen benzer biçimde $b \mid r$'dir.
Demek ki r sayısı a ile b'nin ortak bir katıdır. Eğer $r > 0$ olsaydı, en küçük ortak katın tanımındaki ikinci koşul gereği $m \le r$ olması gerekirdi; oysa $r < m$'dir. Bu çelişki, $r > 0$ olamayacağını gösterir. O hâlde $r = 0$ ve

$$c = mq \Longrightarrow \operatorname{lcm}(a,b) \mid c$$

■

i İki ispat, tek sonuç

Bu sonucu Teorem 7.1'un ispatı içinde zaten elde etmiştik ($\thinspace$Sonuç 7.1$\thinspace$). Yukarıdaki ikinci ispat ise Bézout teoremine hiç başvurmaz; yalnızca bölme algoritmasını ve en küçük ortak katın tanımını kullanır.
Bu tür "kalanı yazıp en küçüklüğe ters düşme" argümanı sayılar teorisinde çok yaygındır; Bézout teoreminin ispatında da aynı fikri kullanmıştık.

7.4 Çalışma Problemleri

Alıştırma 7.1 (EKOK Hesapları). Aşağıdaki değerleri hesaplayınız.
a) $\operatorname{lcm}(12, 18)$ **b)** $\operatorname{lcm}(35, 42)$ **c)** $\operatorname{lcm}(-24, 36)$ **d)** $\operatorname{lcm}(1001, 357)$

Alıştırma 7.2 (EKOK'un Özellikleri). Pozitif a, b, m tam sayıları için aşağıdakileri gösteriniz.
a) $\operatorname{lcm}(ma, mb) = m \cdot \operatorname{lcm}(a, b)$.
b) $a \mid b$ ise $\operatorname{lcm}(a, b) = b$.
c) $\operatorname{lcm}(a, b) = b$ ise $a \mid b$.

Alıştırma 7.3 (Üç Sayının EKOK'u). Sıfırdan farklı a, b, c tam sayılarının en küçük ortak katı, üçünün pozitif ortak katlarının en küçüğü olarak tanımlanır.
a) $\operatorname{lcm}(a, b, c) = \operatorname{lcm}\big(\operatorname{lcm}(a, b), c\big)$ olduğunu gösteriniz.
b) $abc = \gcd(a, b, c) \cdot \operatorname{lcm}(a, b, c)$ eşitliğinin **genel olarak yanlış** olduğunu bir karşı örnekle gösteriniz.
İpucu (b): $a = b = c = 2$ deneyiniz.

8. Diofant Denklemleri

Bir denklemin çözümlerini reel sayılar arasında değil, yalnızca **tam sayılar** arasında aramak bambaşka bir problemdir. $172x + 20y = 1000$ denkleminin sonsuz çok reel çözümü olduğu açıktır — bir doğru denklemidir. Asıl soru şudur: bu doğru üzerinde her iki koordinatı da tam sayı olan noktalar var mıdır, varsa hangileridir?
Şaşırtıcı biçimde bu sorunun cevabı, önceki bölümlerde kurduğumuz araçlarda çoktan gizlidir.

8.1 Tanım

Tanım 8.1 (Birinci Dereceden İki Bilinmeyenli Diofant Denklemi). a ile b ikisi birden sıfır olmayan tam sayılar, c herhangi bir tam sayı ve x, y birer bilinmeyen olmak üzere

$$ax + by = c$$

denklemine bir **(doğrusal) Diofant denklemi** denir.
x_0, y_0 birer tam sayı olmak üzere $ax_0 + by_0 = c$ ise, (x_0, y_0) ikilisine bu denklemin bir **çözümü** denir. En az bir çözümü olan denkleme **çözülebilir**, hiç çözümü olmayana **çözülemez** denir.

> **i** Anahtar gözlem
>
> $ax + by$ ifadesi, a ile b'nin bir **doğrusal birleşimidir**. Sonuç 4.2'de bütün doğrusal birleşimlerin kümesini belirlemiştik:
>
> $$\{ax + by : x, y \in \mathbb{Z}\} = \{dk : k \in \mathbb{Z}\}, \qquad d = \gcd(a, b)$$
>
> Yani $ax + by$ ifadesi tam olarak $\gcd(a, b)$'nin katlarını üretebilir, başka hiçbir değeri üretemez. Diofant denkleminin çözülebilirlik ölçütü bu gözlemin doğrudan okunuşudur.

8.2 Çözülebilirlik ve Genel Çözüm

Teorem 8.1 (Diofant Denkleminin Çözümü). *a ile b ikisi birden sıfır olmayan tam sayılar, $c \in \mathbb{Z}$ ve $d = \gcd(a, b)$ olsun.*
1. *$ax + by = c$ denkleminin çözülebilir olması için gerek ve yeter koşul $d \mid c$ olmasıdır.*
2. *(x_0, y_0) bu denklemin bir çözümü ise, denklemin **bütün** çözümleri t tam sayılarını dolaşmak üzere*

$$x = x_0 + \frac{b}{d}\,t, \qquad y = y_0 - \frac{a}{d}\,t$$

biçimindedir.

> ***İspat.***
> *Genelliği bozmadan $b \neq 0$ olduğunu varsayabiliriz* (aksi hâlde $a \neq 0$ olur ve x ile y'nin rolleri değiştirilir).
> *$d = \gcd(a, b)$ olduğundan $d \mid a$ ve $d \mid b$'dir; yazalım:*
>
> $$a = dk, \qquad b = ds$$
>
> *Sonuç 5.1 gereği $\gcd(k, s) = 1$'dir. Ayrıca $b \neq 0$ olduğundan $s \neq 0$'dır. Son olarak Bézout teoremi gereği*
>
> $$d = au + bv$$
>
> *olacak biçimde u, v tam sayıları vardır.*

1. Çözülebilirlik ölçütü.
($\Rightarrow$) *Denklem çözülebilir olsun;* $ax_0 + by_0 = c$ *olacak biçimde* x_0, y_0 *tam sayıları vardır.* $d \mid a$ *ve* $d \mid b$ *olduğundan Teorem 3.1 (6) gereği*

$$d \mid ax_0 + by_0 = c$$

($\Leftarrow$) $d \mid c$ *olsun;* $c = dz$ *olacak biçimde bir* z *tam sayısı vardır. Bézout ifadesini kullanalım:*

$$c = dz = (au + bv)z = a(uz) + b(vz)$$

Demek ki (uz, vz) *ikilisi denklemin bir çözümüdür.*
2. Bütün çözümler. (x_0, y_0) *bir çözüm olsun. Denklemin çözüm kümesine* S*, teoremde tarif edilen kümeye* T *diyelim:*

$$T = \left\{ \left(x_0 + \frac{b}{d}t,\ y_0 - \frac{a}{d}t \right) : t \in \mathbb{Z} \right\}$$

$\boldsymbol{T \subseteq S.}$ $t \in \mathbb{Z}$ *olsun ve tarif edilen ikiliyi denklemde yerine koyalım:*

$$\begin{aligned} a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right) &= ax_0 + \frac{ab}{d}t + by_0 - \frac{ab}{d}t \\ &= ax_0 + by_0 \\ &= c \end{aligned}$$

Görüldüğü gibi t *içeren terimler birbirini götürür; her* t *için bir çözüm elde edilir.*
$\boldsymbol{S \subseteq T.}$ (x_1, y_1) *herhangi bir çözüm olsun. O hâlde*

$$ax_1 + by_1 = c = ax_0 + by_0$$

Terimleri düzenleyelim:

$$a(x_1 - x_0) = b(y_0 - y_1)$$

$a = dk$ *ve* $b = ds$ *yazıp* $d \neq 0$ *olduğundan sadeleştirelim:*

$$dk(x_1 - x_0) = ds(y_0 - y_1) \Longrightarrow k(x_1 - x_0) = s(y_0 - y_1)$$

Bu eşitlik $s \mid k(x_1 - x_0)$ *olduğunu söyler.* $\gcd(s, k) = 1$ *olduğundan Teorem 5.1 gereği*

$$s \mid x_1 - x_0$$

bulunur; yani $x_1 - x_0 = st$ *olacak biçimde bir* $t \in \mathbb{Z}$ *vardır. Buradan*

$$x_1 = x_0 + st = x_0 + \frac{b}{d}\,t$$

elde edilir. Şimdi bunu yukarıdaki eşitlikte yerine koyalım:

$$k \cdot st = s(y_0 - y_1)$$

$s \neq 0$ *olduğundan sadeleştirebiliriz:*

$$kt = y_0 - y_1 \Longrightarrow y_1 = y_0 - kt = y_0 - \frac{a}{d}\,t$$

Demek ki $(x_1, y_1) \in T$*'dir.*
İki kapsama birlikte $S = T$ *verir.*
■

i Bir çözüm bulan hepsini bulur

Teoremin ikinci kısmı, problemin bütün zorluğunu **tek bir** çözüm bulmaya indirger. O tek çözümü bulduktan sonra sonsuz çoklukta olan diğerleri hiçbir ek çaba gerektirmez; yalnızca b/d ve a/d katsayılarını yazmak yeterlidir.
Adımların sırası şudur:

1. $d = \gcd(a, b)$ hesaplanır ve $d \mid c$ olup olmadığına bakılır.
2. Öklid algoritmasıyla $d = au + bv$ yazılır.
3. Her iki taraf c/d ile çarpılarak özel çözüm elde edilir.
4. Genel çözüm formülü yazılır.

8.3 Çözümlü Örnekler

Örnek 8.1 (Çözümü Olmayan Bir Denklem). $24x + 30y = 5$ Diofant denkleminin çözümü var mıdır?

Çözüm.
Çözülebilirlik ölçütünü uygulayalım:

$$\gcd(24, 30) = 6$$

Oysa $6 \nmid 5$'tir. Teorem 8.1 (1) gereği denklemin **hiçbir tam sayı çözümü yoktur**.
Sezgisel açıklama: sol taraftaki her iki terim de 6'nın katı olduğundan toplam daima 6'nın katı olmak zorundadır; 5 ise değildir.
■

Örnek 8.2 ($132 x + 84 y = 24$). $132x + 84y = 24$ Diofant denkleminin tüm tam sayı çözümlerini bulunuz.

Çözüm.
1. Çözülebilirlik. Öklid algoritmasıyla en büyük ortak böleni bulalım:

$$\begin{aligned} 132 &= 1 \cdot 84 + 48 \\ 84 &= 1 \cdot 48 + 36 \\ 48 &= 1 \cdot 36 + 12 \\ 36 &= 3 \cdot 12 + 0 \end{aligned}$$

O hâlde $d = \gcd(132, 84) = 12$'dir. $24 = 2 \cdot 12$ olduğundan $12 \mid 24$'tür; denklem çözülebilirdir.
2. Bézout katsayıları. Geriye doğru yerine koyalım:

$$\begin{aligned} 12 &= 48 - 36 \\ &= 48 - (84 - 48) \\ &= 2 \cdot 48 - 84 \\ &= 2(132 - 84) - 84 \\ &= 132 \cdot 2 + 84 \cdot (-3) \end{aligned}$$

(Sağlama: $264 - 252 = 12$ ✓*)*
3. Özel çözüm. Sağ taraf 12 değil 24 olduğundan eşitliğin iki tarafını 2 ile çarpalım:

$$24 = 132 \cdot 4 + 84 \cdot (-6)$$

(Sağlama: $528 - 504 = 24$ ✓*)* Yani $x_0 = 4$, $y_0 = -6$'dır.
4. Genel çözüm. Teorem 8.1 (2) gereği

$$x = 4 + \frac{84}{12}\,t = 4 + 7t, \qquad y = -6 - \frac{132}{12}\,t = -6 - 11t \qquad (t \in \mathbb{Z})$$

Sağlama. Bu çift, her t için denklemi gerçekten sağlar ✓:

$$132(4+7t)+84(-6-11t)=528+924t-504-924t=24$$

■

Örnek 8.3 (\$182 x + 70 y = 210\$). $182x+70y=210$ Diofant denklemini çözünüz.

Çözüm.
1. Çözülebilirlik. Örnek 6.1'de $\gcd(182,70)=14$ bulmuştuk. $210=15\cdot 14$ olduğundan $14\mid 210$'dur; denklem çözülebilirdir.
2. Bézout katsayıları. Yine aynı örnekte

$$14=182\cdot 2+70\cdot(-5)$$

elde etmiştik.
3. Özel çözüm. Her iki tarafı 15 ile çarpalım:

$$210=182\cdot 30+70\cdot(-75)$$

(Sağlama: $5460-5250=210$ ✓*)* Yani $x_0=30$, $y_0=-75$'tir.
4. Genel çözüm.

$$x=30+\frac{70}{14}t=30+5t,\qquad y=-75-\frac{182}{14}t=-75-13t\qquad (t\in\mathbb{Z})$$

Çözüm kümesi:

$$\{\,(30+5t,-75-13t):t\in\mathbb{Z}\,\}$$

■

8.4 Çözümleri Bir Aralıkla Sınırlamak

Uygulamalarda genellikle bütün çözümler değil, belli bir aralığa düşenler istenir. Genel çözüm parametreli biçimde yazıldığından bu, t üzerinde basit bir eşitsizliğe dönüşür.

Örnek 8.4 (Belli Bir Aralıktaki Çözümler). $172x+20y=1000$ Diofant denkleminin $495<x<510$ koşuluna uyan tüm çözümlerini bulunuz.

Çözüm.
1. Çözülebilirlik. Öklid algoritması:

$$\begin{aligned}172&=8\cdot 20+12\\20&=1\cdot 12+8\\12&=1\cdot 8+4\\8&=2\cdot 4+0\end{aligned}$$

O hâlde $d=\gcd(172,20)=4$'tür. $1000=250\cdot 4$ olduğundan $4\mid 1000$'dir; denklem çözülebilirdir.
2. Bézout katsayıları.

$$\begin{aligned}4&=12-8\\&=12-(20-12)\\&=2\cdot 12-20\\&=2(172-8\cdot 20)-20\\&=172\cdot 2+20\cdot(-17)\end{aligned}$$

(Sağlama: $344-340=4$ ✓*)*
3. Özel çözüm. Her iki tarafı 250 ile çarpalım:

$$1000=172\cdot 500+20\cdot(-4250)$$

Yani $x_0 = 500$, $y_0 = -4250$'dir.
4. Genel çözüm.

$$x = 500 + \frac{20}{4}\,t = 500 + 5t, \qquad y = -4250 - \frac{172}{4}\,t = -4250 - 43t$$

5. Aralık koşulu. Şimdi $495 < x < 510$ eşitsizliğini t cinsinden çözelim:

$$\begin{aligned} 495 &< 500 + 5t < 510 \\ -5 &< 5t < 10 \\ -1 &< t < 2 \end{aligned}$$

Bu aralıktaki tam sayılar $t = 0$ ve $t = 1$'dir.

- $t = 0$ için: $(x, y) = (500, -4250)$
- $t = 1$ için: $(x, y) = (505, -4293)$

(Sağlama: $172 \cdot 505 + 20 \cdot (-4293) = 86860 - 85860 = 1000$ ✓*)*
■

> **i** Bu konu ileride tekrar karşımıza çıkacak
>
> Diofant denklemleri, lineer kongrüanslarla birebir aynı problemdir; nitekim
>
> $$ax + by = c \Leftrightarrow ax \equiv c \pmod{b}$$
>
> denkliği vardır. Kongrüanslar bölümünde bu köprüyü kuracak ve aynı denklemleri bu kez kongrüans diliyle çözeceğiz.
> Daha fazla çözümlü örnek için Sayılar Teorisi II'deki Doğrusal Diofant Denklemleri bölümüne de bakabilirsiniz.

8.5 Çalışma Problemleri

Alıştırma 8.1 (Diofant Denklemleri). Aşağıdaki denklemlerin bütün tam sayı çözümlerini bulunuz; çözümü olmayanları belirtiniz.
a) $56x + 72y = 40$ **b)** $24x + 138y = 18$ **c)** $221x + 35y = 11$ **d)** $84x + 990y = 186$
e) $18x + 14y = 48$ **f)** $60x + 18y = 97$

Alıştırma 8.2 (Pozitif Çözümler). $5x + 3y = 52$ denkleminin **pozitif** tam sayı çözümlerini bulunuz.
İpucu: Önce genel çözümü yazınız, ardından $x > 0$ ve $y > 0$ eşitsizliklerini t cinsinden çözüp iki koşulu birlikte sağlayan t değerlerini belirleyiniz.

Alıştırma 8.3 (Bir Uygulama). Bir kırtasiye, tanesi 7 liradan defter ve tanesi 11 liradan kalem satmaktadır. Toplam 100 lira harcayan bir müşteri kaç defter ve kaç kalem almış olabilir?
İpucu: $7x + 11y = 100$ denkleminin negatif olmayan çözümlerini arayınız.

9. Asal Sayılar

Bölünebilme kuramının merkezinde, başka sayılara ayrılamayan sayılar durur. Bu bölümde bu "bölünemez" sayıları tanımlayacak, aralarında asallık kuramımızın onlara nasıl özellikle iyi uyduğunu göreceğiz. Elde edeceğimiz sonuçlar bir sonraki bölümde aritmetiğin esas teoremini kuracak.

9.1 Tanım

Tanım 9.1 (Asal Sayı). $1 < p \in \mathbb{Z}$ olsun. Eğer p'nin 1 ve kendisinden başka hiç pozitif böleni yoksa p'ye bir **asal sayı** denir.
Asal olmayan $1 < n$ tam sayılarına **bileşik sayı** denir.

Örnek 9.1 (İlk Asal Sayılar). $2, 3, 5, 7, 11, 13$ birer asal sayıdır. Buna karşılık $6 = 2 \cdot 3$ olduğundan 6 asal değildir; bileşiktir.
Tanım gereği 1 asal **değildir**; çünkü tanım $1 < p$ koşulunu içerir.

> **i** 1 neden asal sayılmıyor?
>
> Bu, keyfî bir dışlama değildir. Bir sonraki bölümde her sayının asalların çarpımı olarak **tek türlü** yazıldığını göreceğiz. 1 asal sayılsaydı bu teklik anında bozulurdu:
>
> $$6 = 2 \cdot 3 = 1 \cdot 2 \cdot 3 = 1 \cdot 1 \cdot 2 \cdot 3 = \cdots$$
>
> Yani 1'i dışarıda bırakmak, aritmetiğin esas teoremini kurtarmak içindir.

Bileşik sayıların tanımını biraz açalım. $1 < n$ asal değilse, n'nin 1'den ve n'den farklı bir k pozitif böleni vardır. O hâlde

$$n = k \cdot m$$

olacak biçimde bir m tam sayısı vardır ve $1 < m < n$'dir. Kısaca: **asal olmayan bir $1 < n$ tam sayısı, kendisinden küçük iki tam sayının çarpımı biçiminde yazılabilir.** Bu gözlemi ileride tümevarım adımlarında kullanacağız.

9.2 Asal Sayılar ve Aralarında Asallık

Asal sayıların bölünebilme kuramındaki gücü, aşağıdaki basit gözlemden gelir: bir asal sayı, her sayıyla ya "tamamen ilgilidir" ya da "hiç ilgili değildir".

Önerme 9.1 (Bir Asalla EBOB). *Her $a \in \mathbb{Z}$ ve her p asal sayısı için*

$$\gcd(p, a) = \begin{cases} 1, & p \nmid a \quad \text{ise} \\ p, & p \mid a \quad \text{ise} \end{cases}$$

İspat.
$d := \gcd(p, a)$ diyelim. d pozitif bir tam sayıdır ve $d \mid p$'dir. p asal olduğundan pozitif bölenleri yalnızca 1 ve p'dir; o hâlde

$$d = 1 \qquad \text{veya} \qquad d = p$$

Şimdi iki durumu ayıralım.
$p \mid a$ ise. *Bu durumda p sayısı hem p'yi hem a'yı böler; yani bir ortak bölendir. Ortak bölenlerin en büyüğü p'yi geçemeyeceğinden ve p bir ortak bölen olduğundan $d = p$'dir.*

> ***p ∤ a ise.*** *$d = p$ olsaydı $d \mid a$, yani $p \mid a$ olurdu — hipoteze aykırı. O hâlde $d = 1$'dir.*
> ■

Sonuç 9.1 (Farklı Asallar Aralarında Asaldır). *p ile q farklı iki asal sayı olsun. Bu durumda $p \nmid q$ ve dolayısıyla*

$$\gcd(p, q) = 1$$

Gerçekten de q'nun pozitif bölenleri yalnızca 1 ve q'dur. $p \mid q$ olsaydı $p = 1$ veya $p = q$ olurdu; ikisi de hipoteze aykırıdır. Önerme 9.1 gereği $\gcd(p, q) = 1$'dir.

9.3 Öklid Lemmasının Asal Hâli

Öklid lemması "$a \mid bc$ ve $\gcd(a, b) = 1$ ise $a \mid c$" diyordu. Modül asal olduğunda aralarında asallık koşulu kendiliğinden sağlanır ve lemma çok daha kullanışlı bir biçim alır.

Teorem 9.1 (Asal Sayılar İçin Öklid Lemması). *Her $a, b \in \mathbb{Z}$ ve her p asal sayısı için*

$$p \mid ab \Longrightarrow p \mid a \quad \text{veya} \quad p \mid b$$

Bir başka deyişle: bir asal sayı iki tam sayının çarpımını bölerse, bu tam sayılardan en az birini böler.

> ***İspat.***
> *$p \mid ab$ olsun. İki durum vardır.*
> ***Durum 1: $p \mid a$.*** *İddia zaten sağlanmıştır; gösterilecek bir şey yoktur.*
> ***Durum 2: $p \nmid a$.*** *Önerme 9.1 gereği $\gcd(p, a) = 1$'dir. Elimizde*
>
> $$p \mid ab \qquad \text{ve} \qquad \gcd(p, a) = 1$$
>
> *vardır. Teorem 5.1 gereği $p \mid b$'dir.*
> *Her iki durumda da $p \mid a$ veya $p \mid b$ sonucuna ulaşılır.*
> ■

> ⚠ Asallık şartı vazgeçilmezdir
>
> $6 \mid 2 \cdot 3$ olmasına rağmen $6 \nmid 2$ ve $6 \nmid 3$'tür. Teorem bozulmuş değildir: 6 asal değildir.
> Nitekim bu özellik asallığı **karakterize eder**: $1 < n$ tam sayısı bu özelliği taşıyorsa asal olmak zorundadır (bkz. Alıştırma 9.1).

Sonuç 9.2 (Çok Çarpanlı Hâl). *p bir asal sayı ve $a_1, \ldots, a_n \in \mathbb{Z}$ olsun. Eğer*

$$p \mid a_1 a_2 \cdots a_n$$

ise, $p \mid a_s$ olacak biçimde bir $s \in \{1, \ldots, n\}$ vardır.

> ***İspat.***
> *n üzerinden tümevarım yapalım.*
> ***Başlangıç adımı ($n = 1$).*** *$p \mid a_1$ olduğundan $s = 1$ alınır.*
> ***Tümevarım adımı.*** *İddianın $n = k$ için doğru olduğunu varsayalım ve*
>
> $$p \mid a_1 a_2 \cdots a_k a_{k+1}$$
>
> *olsun. Çarpımı iki parçaya ayıralım:*
>
> $$p \mid \underbrace{(a_1 \cdots a_k)}_{A} \cdot a_{k+1}$$

Teorem 9.1 gereği $p \mid A$ veya $p \mid a_{k+1}$'dir.

- *$p \mid a_{k+1}$ ise $s = k+1$ alınır.*
- *$p \mid A = a_1 \cdots a_k$ ise tümevarım hipotezi gereği $p \mid a_s$ olacak biçimde bir $s \in \{1, \ldots, k\}$ vardır.*

Her iki durumda da istenen s bulunur.
■

Sonuç 9.3 (Asalların Çarpımını Bölen Asal). *$p, q_1, \ldots, q_n$ asal sayılar olmak üzere, eğer*

$$p \mid q_1 q_2 \cdots q_n$$

ise $p = q_k$ olacak biçimde bir $k \in \{1, \ldots, n\}$ vardır.

Bunun nedeni açıktır: Sonuç 9.2 gereği $p \mid q_k$ olacak biçimde bir k vardır. q_k asal olduğundan pozitif bölenleri yalnızca 1 ve q_k'dır; $p > 1$ olduğundan $p = q_k$ olmak zorundadır.

Sonuç 9.4 (Kuvvetleri Bölmek). *Her a tam sayısı, her k pozitif tam sayısı ve her p asal sayısı için*

$$p \mid a^k \Leftrightarrow p \mid a$$

Gerçekten de ($\Leftarrow$) yönü açıktır. ($\Rightarrow$) yönü ise Sonuç 9.2'in $a_1 = \cdots = a_k = a$ alınmış hâlidir.

9.4 Her Sayının Bir Asal Böleni Vardır

Lemma 9.1 (Asal Bölenin Varlığı). *1'den büyük her tam sayının en az bir asal böleni vardır.*

İspat.
$1 < n$ bir tam sayı olsun. n'nin 1'den büyük pozitif bölenlerinin kümesini alalım:

$$D = \{d \in \mathbb{N} : d > 1, d \mid n\}$$

$n \mid n$ ve $n > 1$ olduğundan $n \in D$'dir; yani D boş değildir. İyi sıralama prensibi gereği D kümesinin bir en küçük elemanı vardır; buna p diyelim.
İddia: p asaldır. *Aksini varsayalım. $p > 1$ ve p asal olmadığından*

$$p = ab, \qquad 1 < a < p$$

olacak biçimde tam sayılar vardır. Şimdi $a \mid p$ ve $p \mid n$ olduğundan geçişme gereği $a \mid n$'dir. Ayrıca $a > 1$'dir. Demek ki $a \in D$'dir ve $a < p$'dir — bu, p'nin D'nin en küçük elemanı olmasıyla çelişir.
O hâlde p asaldır ve n'nin bir bölenidir.
■

9.5 Asal Sayılar Sonsuzdur

Teorem 9.2 (Öklid Teoremi). *Sonsuz tane asal sayı vardır.*

İspat.
Aksini varsayalım: yalnızca sonlu sayıda asal sayı bulunsun ve bunların hepsi

$$p_1, p_2, \ldots, p_n$$

olsun. Şimdi şu sayıyı tanımlayalım:

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

Bütün p_i'ler 2'den büyük veya eşit olduğundan $N > 1$'dir. Lemma 9.1 gereği N sayısının bir p asal böleni vardır.

Varsayımımıza göre bütün asallar listemizde olduğundan $p = p_j$ olacak biçimde bir j vardır. Buradan iki bilgi çıkar:

- *$p = p_j$ çarpımın bir çarpanı olduğundan $p \mid p_1 p_2 \cdots p_n$'dir.*
- *$p \mid N$'dir.*

Teorem 3.1 (7) gereği p sayısı farkı da böler:

$$p \mid N - p_1 p_2 \cdots p_n = 1$$

Ama p asal olduğundan $p > 1$'dir ve 1'i bölemez. Çelişki.
O hâlde asal sayıların kümesi sonlu olamaz; sonsuz tane asal sayı vardır.
■

i İspatın sık yapılan bir yanlış okunuşu

İspat, "$p_1 p_2 \cdots p_n + 1$ sayısı asaldır" demez — bu genel olarak **yanlıştır**. Örneğin

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$$

bileşiktir. İspatın söylediği yalnızca şudur: bu sayının asal böleni, listedeki asalların hiçbiri olamaz. Listeyi sonlu kabul etmek işte bu yüzden çelişki üretir.

9.6 Eratosthenes Kalburu

Bir sayının asal olup olmadığını anlamak için bütün küçük sayıları denemek gerekmez. Aşağıdaki teorem, denenecek bölen sayısını çarpıcı biçimde azaltır.

Teorem 9.3 (Eratosthenes Kalburu). *Asal olmayan her $n > 1$ tam sayısının*

$$p \leq \sqrt{n}$$

koşuluna uyan bir p asal böleni vardır.

İspat.
$1 < n$ asal olmayan bir tam sayı olsun. Bu durumda

$$n = k \cdot l, \qquad 1 < k \leq l < n$$

olacak biçimde k, l tam sayıları vardır. (Çarpanlardan küçük olanına k dedik; eşit olabilirler.)
$1 < k$ olduğundan Lemma 9.1 gereği k'nın bir p asal böleni vardır. Teorem 3.1 (8) gereği

$$p \leq k$$

Ayrıca $p \mid k$ ve $k \mid n$ olduğundan geçişme gereği $p \mid n$'dir.
Son olarak $p \leq k \leq l$ olduğundan

$$p^2 \leq k \cdot l = n$$

yazılır. Her iki tarafın karekökünü alırsak $p \leq \sqrt{n}$ bulunur.
■

Teoremin karşıt tersini almak, doğrudan bir asallık testi verir.

i Asallık testi

$1 < n \in \mathbb{Z}$ olsun. Eğer n tam sayısının

$$p \leq \sqrt{n}$$

koşuluna uyan hiç p asal çarpanı yoksa, n **asaldır**.

Örnek 9.2 (\$101\$ Asal mıdır?). 101 sayısının asal olduğunu gösteriniz.

Çözüm.
$\sqrt{101} \approx 10,05$ olduğundan, yalnızca 10'u geçmeyen asalları denememiz yeterlidir:

$$2, \quad 3, \quad 5, \quad 7$$

Sırayla bakalım:

- 101 tektir, yani $2 \nmid 101$.
- Rakamlar toplamı $1 + 0 + 1 = 2$ olduğundan $3 \nmid 101$.
- Son rakamı 0 veya 5 olmadığından $5 \nmid 101$.
- $101 = 7 \cdot 14 + 3$ olduğundan $7 \nmid 101$.

$\sqrt{101}$'i geçmeyen hiçbir asal 101'i bölmediğinden, Teorem 9.3 gereği 101 asaldır.
■

Örnek 9.3 (\$10\$ ile \$100\$ Arasındaki Asallar). Eratosthenes kalburunu kullanarak 10 ile 100 arasındaki tüm asal sayıları belirleyiniz.

Çözüm.
100'ü geçmeyen bir sayı bileşikse, $\sqrt{100} = 10$'u geçmeyen bir asal böleni vardır. O hâlde yalnızca

$$2, \quad 3, \quad 5, \quad 7$$

asallarının katlarını elemek yeterlidir.
1. Adım. 10 ile 100 arasındaki bütün sayıları yazıp 2'nin katlarını (çift sayıları) eleyelim. Geriye yalnızca tek sayılar kalır.
2. Adım. Kalanlardan 3'ün katlarını eleyelim: $15, 21, 27, 33, 39, 45, 51, 57, 63, 69, 75, 81, 87, 93, 99$.
3. Adım. 5'in katlarını eleyelim: $25, 35, 55, 65, 85, 95$. *(Diğerleri zaten elenmişti.)*
4. Adım. 7'nin katlarını eleyelim: $49, 77, 91$. *(Geri kalanları önceki adımlarda elenmişti.)*
Elemeden sonra geriye kalan sayılar aranan asallardır:

$$11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$$

Toplam 21 asal sayı vardır.
■

9.7 Asalların Biçimi Üzerine

Örnek 9.4 (\$2\$ ve \$3\$ Dışındaki Asallar). 2 ve 3 dışındaki her asal sayının, k bir tam sayı olmak üzere $6k + 1$ veya $6k - 1$ biçiminde olduğunu gösteriniz.

Çözüm.
p sayısı 2 ve 3'ten farklı bir asal olsun. Bölme algoritmasına göre

$$p = 6q + r, \qquad r \in \{0, 1, 2, 3, 4, 5\}$$

yazılır. Kalanları tek tek eleyelim.

- $\boldsymbol{r = 0}$**:** $p = 6q$ olur; $2 \mid p$'dir. p asal ve $p \neq 2$ olduğundan bu imkânsızdır.

- **$r = 2$:** $p = 6q + 2 = 2(3q + 1)$ olur; yine $2 \mid p$'dir, imkânsız.
- **$r = 4$:** $p = 6q + 4 = 2(3q + 2)$ olur; yine $2 \mid p$'dir, imkânsız.
- **$r = 3$:** $p = 6q + 3 = 3(2q + 1)$ olur; $3 \mid p$'dir. p asal ve $p \neq 3$ olduğundan imkânsız.

Geriye yalnızca $r = 1$ ve $r = 5$ kalır:

- $r = 1$ ise $p = 6q + 1$'dir.
- $r = 5$ ise $p = 6q + 5 = 6(q + 1) - 1$'dir; yani $p = 6k - 1$ biçimindedir.

■

⚠ Tersi doğru değildir

Her asal $6k \pm 1$ biçimindedir, ama $6k \pm 1$ biçimindeki her sayı asal değildir: $25 = 6 \cdot 4 + 1$ ve $35 = 6 \cdot 6 - 1$ bileşiktir.
Yine de bu gözlem asallık aramalarını altı kat hızlandırır: $6k$, $6k + 2$, $6k + 3$, $6k + 4$ biçimindeki sayılara hiç bakmaya gerek yoktur.

Örnek 9.5 ($2^n - 1$ Asalsa n Asaldır). Her n pozitif tam sayısı için, $2^n - 1$ sayısı asalsa n'nin de asal olduğunu gösteriniz.

Çözüm.
Karşıt tersini ispatlayacağız: ***n* asal değilse $2^n - 1$ de asal değildir.**
$n = 1$ ise $2^1 - 1 = 1$ olur ve 1 asal değildir; iddia sağlanır. O hâlde $n > 1$ ve n bileşik olsun. Bu durumda

$$n = a \cdot b, \qquad 1 < a < n$$

olacak biçimde tam sayılar vardır.
$a \mid n$ olduğundan Örnek 3.7 gereği

$$2^a - 1 \mid 2^n - 1$$

Şimdi bu bölenin **öz** bir bölen olduğunu, yani 1'den ve $2^n - 1$'in kendisinden farklı olduğunu görelim:

- $a > 1$ olduğundan $2^a - 1 \geq 2^2 - 1 = 3 > 1$'dir.
- $a < n$ olduğundan $2^a - 1 < 2^n - 1$'dir.

Demek ki $2^n - 1$ sayısının 1 ile kendisinden farklı bir pozitif böleni vardır; yani asal değildir.
Karşıt ters ispatlandığından, $2^n - 1$ asalsa n asaldır.
■

⚠ Bu önermenin tersi yanlıştır

n asal olduğunda $2^n - 1$ asal olmak zorunda değildir. En küçük karşı örnek $n = 11$'dir:

$$2^{11} - 1 = 2048 - 1 = 2047 = 23 \cdot 89$$

$2^p - 1$ biçimindeki asallara **Mersenne asalları** denir; bugün bilinen en büyük asal sayılar bu ailedendir.

Örnek 9.6 (p ile $p^2 + 2$ Asalsa). p ve $p^2 + 2$ birer asal sayı ise $p^2 + 4$ sayısının da asal olduğunu gösteriniz.

Çözüm.
Önce p'nin ne olabileceğini belirleyelim. $p \neq 3$ olduğunu varsayalım ve çelişki arayalım.
$p \neq 3$ asal olduğundan $3 \nmid p$'dir. Bölme algoritmasına göre $p = 3q + r$, $r \in \{1, 2\}$ yazılır *(kalan 0 olamaz, çünkü $3 \nmid p$)*. Her iki durumda karesini hesaplayalım:

- $p = 3q + 1$ ise $p^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1$.
- $p = 3q + 2$ ise $p^2 = 9q^2 + 12q + 4 = 3(3q^2 + 4q + 1) + 1$.

Her iki durumda da p^2 sayısı $3k + 1$ biçimindedir. O hâlde

$$p^2 + 2 = 3k + 3 = 3(k + 1)$$

olur; yani $3 \mid p^2 + 2$'dir. Ayrıca $p \geq 2$ olduğundan $p^2 + 2 \geq 6 > 3$'tür. Demek ki $p^2 + 2$ sayısı, 1 ile kendisinden farklı olan 3 böleni tarafından bölünmektedir; asal olamaz. Bu, hipotezle çelişir.
O hâlde $p = 3$ olmak zorundadır. Şimdi doğrulayalım:

$$p^2 + 2 = 11 \quad \text{(asal)}, \qquad p^2 + 4 = 13 \quad \text{(asal)}$$

Böylece $p^2 + 4$ asaldır.
■

9.8 Çalışma Problemleri

Alıştırma 9.1 (Asallığın Bir Karakterizasyonu). $1 < n \in \mathbb{Z}$ olsun ve

$$\text{"her } \ a, b \in \mathbb{Z} \ \text{ için } \ n \mid ab \ \text{ ise } \ n \mid a \ \text{ veya } \ n \mid b \text{ "}$$

koşulunun sağlandığı varsayılsın. Bu durumda n'nin bir asal sayı olduğunu ispatlayınız.
İpucu: n bileşik olsaydı $n = ab$, $1 < a, b < n$ yazılabilirdi; koşulu bu a ile b'ye uygulayınız.

Alıştırma 9.2 (Asal Sayı ve Binom Katsayıları). p bir asal sayı olmak üzere, her $k \in \{1, \ldots, p-1\}$ için

$$p \,\Big|\, \binom{p}{k}$$

olduğunu gösteriniz.
İpucu: $k! \, (p-k)! \, \dbinom{p}{k} = p!$ eşitliğinden yola çıkınız. p asal olduğundan ve $k!$ ile $(p-k)!$ çarpanlarının hepsi p'den küçük olduğundan Sonuç 9.2 gereği $p \nmid k!\,(p-k)!$'dir; ardından Teorem 5.1′nı uygulayınız.

Alıştırma 9.3 (Faktöriyelin Komşularındaki Asallar). **a)** Her $2 < n$ tam sayısı için $n < p < n!$ koşuluna uyan bir p asal sayısının var olduğunu gösteriniz.
b) Her $1 < n$ tam sayısı için, $n! + 1$ sayısının her asal çarpanının n'den büyük bir tek sayı olduğunu gösteriniz.
İpucu (a): $n! - 1$ sayısının bir asal bölenini alıp, bu bölenin n'yi geçmesi gerektiğini gösteriniz.

Alıştırma 9.4 ($2^n + 1$ Ne Zaman Asal Olabilir?). **a)** Her n pozitif tam sayısı ve her k negatif olmayan tam sayısı için

$$n + 1 \mid n^{2k+1} + 1$$

olduğunu tümevarımla gösteriniz.
b) $2^n + 1$ sayısı asal ise $n = 2^k$ olacak biçimde negatif olmayan bir k tam sayısının var olduğunu gösteriniz.
c) (b) şıkkının tersinin yanlış olduğunu $n = 32$ için gösteriniz. *(İpucu:* $2^{32} + 1 = 641 \cdot 6700417$.*)*

Alıştırma 9.5 ($4 k + 3$ Biçimindeki Asallar). **a)** $4k + 1$ biçimindeki sonlu sayıda tam sayının çarpımının yine $4k + 1$ biçiminde olduğunu gösteriniz.
b) $4k + 3$ biçiminde sonsuz sayıda asal sayı olduğunu ispatlayınız.
İpucu (b): Sonlu sayıda olduklarını varsayıp $q_1, \ldots, q_n$ diyelim ve $N = 4q_1q_2 \cdots q_n - 1$ sayısını inceleyiniz; (a) şıkkı bu sayının $4k + 3$ biçiminde bir asal böleni olması gerektiğini söyler.

10. Aritmetiğin Esas Teoremi

Asal sayıları "bölünemez" sayılar olarak tanımladık. Şimdi bu sayıların gerçekten de aritmetiğin yapı taşları olduğunu göreceğiz: 1'den büyük her tam sayı asalların çarpımıdır ve bu çarpım — sıralama dışında — **tek türlü belirlidir**. Bu teklik, bölünebilme kuramının tamamına düzen getirir.

10.1 Teorem ve İspatı

Teorem 10.1 (Aritmetiğin Esas Teoremi). *1'den büyük her n tam sayısı, bir takım asal sayıların çarpımı biçiminde yazılabilir.*
Ayrıca bu yazılış tek türlü belirlidir: eğer $p_1, \ldots, p_m$ ve $q_1, \ldots, q_s$ asal sayılar olmak üzere

$$p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_s$$

ise $m = s$'dir ve — gerekirse $q_1, \ldots, q_s$ asalları yeniden sıralanarak —

$$p_1 = q_1, \quad p_2 = q_2, \quad \ldots, \quad p_m = q_m$$

olur.

İspat.
İspatı iki parçaya ayıralım.
1. Varlık. *Şu iddiayı güçlü tümevarımla ispatlayalım:*

> *Her $1 < n$ tam sayısı için $n = r_1 r_2 \cdots r_m$ olacak biçimde $r_1, \ldots, r_m$ asal sayıları vardır.*

Başlangıç adımı ($n = 2$). *2 asal olduğundan tek çarpanlı bir çarpım olarak yazılır.*
Tümevarım adımı. *$2 < k$ olsun ve iddianın $n = 2, 3, \ldots, k-1$ değerlerinin hepsi için doğru olduğunu varsayalım. $n = k$ için gösterelim.*
k asalsa iddia zaten sağlanır; tek çarpanlı çarpım olarak yazılır. O hâlde k'nın asal olmadığını varsayabiliriz. Bu durumda

$$k = a \cdot b, \qquad 1 < a, b < k$$

olacak biçimde a, b tam sayıları vardır. $a, b \in \{2, \ldots, k-1\}$ olduğundan güçlü tümevarım hipotezi hem a hem b için kullanılabilir:

$$a = r_1 \cdots r_d, \qquad b = t_1 \cdots t_f$$

olacak biçimde $r_1, \ldots, r_d, t_1, \ldots, t_f$ asalları vardır. O hâlde

$$k = a \cdot b = r_1 \cdots r_d \, t_1 \cdots t_f$$

yazılır; yani k da asalların çarpımıdır. Güçlü tümevarım ilkesi gereği iddia her $1 < n$ için doğrudur.
2. Teklik. *Bu kez m üzerinden tümevarım yapalım.*
Başlangıç adımı ($m = 1$). *$p_1 = q_1 q_2 \cdots q_s$ olsun. $s = 1$ olduğunu gösterelim.*
$s \geq 2$ olduğunu varsayalım. Bu durumda

$$p_1 = q_1 \cdot \underbrace{(q_2 \cdots q_s)}_{\geq 2}$$

yazılır. Demek ki $q_1 \mid p_1$ ve

$$1 < q_1 \leq \frac{p_1}{2} < p_1$$

olur; yani p_1 sayısının 1 ile kendisinden farklı bir pozitif böleni vardır. Bu, p_1'in asal olmasıyla çelişir. O hâlde $s = 1$ ve $p_1 = q_1$'dir.
Tümevarım adımı. *k bir pozitif tam sayı olsun ve teklik iddiasının $m = k$ için doğru olduğunu varsayalım. $m = k+1$ için gösterelim:*

$$p_1 \cdots p_k \, p_{k+1} = q_1 \cdots q_s$$

olsun. Sol taraf p_{k+1} ile bölündüğünden sağ taraf da bölünür:

$$p_{k+1} \mid q_1 q_2 \cdots q_s$$

Sonuç 9.3 gereği $p_{k+1} = q_i$ olacak biçimde bir $i \in \{1, \ldots, s\}$ vardır. Çarpanların sırasını değiştirmekte serbest olduğumuzdan $p_{k+1} = q_s$ olduğunu varsayabiliriz. Eşitliği yeniden yazalım:

$$p_1 \cdots p_k \, p_{k+1} = q_1 \cdots q_{s-1} \, q_s = q_1 \cdots q_{s-1} \, p_{k+1}$$

$p_{k+1} \neq 0$ olduğundan her iki tarafı p_{k+1}'e sadeleştirebiliriz:

$$p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_{s-1}$$

Şimdi sol tarafta k tane asal vardır; tümevarım hipotezi uygulanabilir. Buradan

$$k = s - 1 \qquad \text{yani} \qquad k + 1 = s$$

ve — uygun bir sıralamayla — $p_1 = q_1, \ldots, p_k = q_k$ bulunur. Zaten $p_{k+1} = q_s = q_{k+1}$ olduğunu görmüştük.
Tümevarım ilkesi gereği teklik her m için geçerlidir.
■

> **i** Tekliğin gerçek kaynağı
>
> Varlık kısmı kolaydır; sayıyı parçalamaya devam edersiniz, sonunda asallara ulaşırsınız. Asıl derin olan tekliktir ve ispata bakıldığında bütün ağırlığın **tek bir adıma** bindiği görülür:
>
> $$p \mid q_1 q_2 \cdots q_s \Longrightarrow p = q_i \ (\text{bir} \quad i \quad \text{için})$$
>
> Bu ise Teorem 9.1'in, yani Öklid lemmasının asal hâlinin sonucudur. Öklid lemması da Bézout teoreminden gelir. Yani **teklik, ta en başta iyi sıralama prensibinden çıkardığımız Bézout teoremine dayanır.**

10.2 Kanonik Gösterim

Tanım 10.1 (Asal Çarpanlara Ayrılış). $1 < n \in \mathbb{Z}$ olsun. Teorem 10.1'taki

$$n = p_1 p_2 \cdots p_m$$

yazılışına n sayısının **asal çarpanlara ayrılışı** denir.

Örnek 10.1 (Asal Çarpanlara Ayrılış Örnekleri).

$$60 = 2 \cdot 2 \cdot 3 \cdot 5, \qquad 37 = 37$$

İkinci örnekte 37 asal olduğundan çarpanlara ayrılış tek çarpandan oluşur.

Aynı asal birden çok kez görünebildiğinden, tekrarları kuvvet olarak toplamak ve asalları küçükten büyüğe sıralamak daha kullanışlıdır.

Sonuç 10.1 (Kanonik Gösterim). *Her $n > 1$ tam sayısı için*

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}, \qquad p_1 < p_2 < \cdots < p_r$$

olacak biçimde ***tek türlü belirli*** $p_1, \ldots, p_r$ *asal sayıları ve* $k_1, \ldots, k_r$ *pozitif tam sayıları vardır.*

Bu, Teorem 10.1'ın yeniden düzenlenmiş hâlidir: çarpanlara ayrılıştaki eşit asallar bir araya toplanır ve sonuç küçükten büyüğe sıralanır. Teklik, teoremin teklik kısmından gelir.

Örnek 10.2 (Kanonik Gösterim Örneği).

$$120 = 2^3 \cdot 3^1 \cdot 5^1$$

Gerçekten de $120 = 8 \cdot 15 = 2^3 \cdot 3 \cdot 5$'tir ve asallar küçükten büyüğe sıralanmıştır.

10.3 Köklerin İrrasyonelliği

Aritmetiğin esas teoreminin ilk büyük kazancı, irrasyonel sayılar üretmenin sistemli bir yolunu vermesidir. Örnek 5.1'de $\sqrt{2}$'nin irrasyonelliğini çift/tek ayrımıyla göstermiştik; şimdi aynı fikri tek hamlede genelleştireceğiz.

Teorem 10.2 (Rasyonel Kök Tam Sayıdır). *n ve a birer pozitif tam sayı olsun. Eğer $\sqrt[n]{a}$ sayısı rasyonel ise, bir tam sayıdır.*

> ***İspat.***
> *$\sqrt[n]{a}$ rasyonel olsun. Sonuç 5.2 gereği*
>
> $$\sqrt[n]{a} = \frac{r}{s}, \qquad s > 0, \qquad \gcd(r, s) = 1$$
>
> *olacak biçimde r, s tam sayıları vardır. Her iki tarafın n'inci kuvvetini alalım:*
>
> $$a = \frac{r^n}{s^n} \Longrightarrow a\, s^n = r^n \tag{$*$}$$
>
> ***İddia: $s = 1$'dir.*** *Aksini varsayalım; $s > 1$ olsun. Lemma 9.1 gereği s sayısının bir p asal böleni vardır. $p \mid s$ olduğundan $p \mid s^n$, dolayısıyla $p \mid a s^n$'dir. $(*)$ gereği*
>
> $$p \mid r^n$$
>
> *olur. Sonuç 9.4 gereği bu, $p \mid r$ demektir.*
> *Demek ki p sayısı hem r'yi hem de s'yi böler; yani*
>
> $$p \mid \gcd(r, s) = 1$$
>
> *Bu imkânsızdır, çünkü $p > 1$'dir. O hâlde $s = 1$ ve*
>
> $$\sqrt[n]{a} = \frac{r}{1} = r \in \mathbb{Z}$$
>
> ■

Sonuç 10.2 (Tam Kuvvet Değilse Kök İrrasyoneldir). *n ve a pozitif tam sayılar olsun. Eğer $a = m^n$ olacak biçimde bir m tam sayısı* ***yoksa****, $\sqrt[n]{a}$ irrasyoneldir.*

Gerçekten de $\sqrt[n]{a}$ rasyonel olsaydı, Teorem 10.2 gereği bir m tam sayısına eşit olurdu ve her iki tarafın n'inci kuvveti alındığında $a = m^n$ bulunurdu — hipoteze aykırı.

Örnek 10.3 ($sqrt(7)$ İrrasyoneldir). $\sqrt{7}$ sayısının irrasyonel olduğunu gösteriniz.

> **Çözüm.**
> $7 = m^2$ olacak biçimde bir m tam sayısı olsaydı $m^2 = 7$ olurdu. Oysa

$$2^2 = 4 < 7 < 9 = 3^2$$

olduğundan böyle bir tam sayı yoktur; 7 bir tam kare değildir. Sonuç 10.2 gereği $\sqrt{7}$ irrasyoneldir.
■

> **i** Aynı akıl yürütme her asal için işler
>
> p bir asal sayı olsun. $p = m^2$ olsaydı $m \mid p$ ve $1 < m < p$ olurdu; bu, p'nin asallığıyla çelişir. O hâlde hiçbir asal sayı tam kare değildir ve **her p asalı için $\sqrt{p}$ irrasyoneldir.**

Örnek 10.4 ($sqrt(3) + sqrt(7)$ İrrasyoneldir). $\sqrt{3} + \sqrt{7}$ sayısının irrasyonel olduğunu gösteriniz.

Çözüm.
Aksini varsayalım: $\alpha := \sqrt{3} + \sqrt{7}$ rasyonel olsun. Karesini alalım:

$$\alpha^2 = 3 + 2\sqrt{3}\sqrt{7} + 7 = 10 + 2\sqrt{21}$$

Buradan $\sqrt{21}$'i yalnız bırakalım:

$$\sqrt{21} = \frac{\alpha^2 - 10}{2}$$

α rasyonel ise α^2 de, dolayısıyla sağ taraf da rasyoneldir. O hâlde $\sqrt{21}$ rasyonel olurdu.
Oysa 21 bir tam kare değildir:

$$4^2 = 16 < 21 < 25 = 5^2$$

Sonuç 10.2 gereği $\sqrt{21}$ irrasyoneldir. Çelişki.
O hâlde $\sqrt{3} + \sqrt{7}$ irrasyoneldir.
■

Örnek 10.5 ($root(n, n)$ İrrasyoneldir). Her $2 \leq n$ tam sayısı için $\sqrt[n]{n}$ sayısının irrasyonel olduğunu gösteriniz.

Çözüm.
Aksini varsayalım: $\sqrt[n]{n}$ rasyonel olsun. Teorem 10.2 gereği bir m tam sayısına eşittir ve

$$m^n = n$$

olur. $n \geq 2$ olduğundan $m \geq 2$ olmalıdır; çünkü $m = 1$ olsaydı $n = 1$ bulunurdu ve $m = 0$ olsaydı $n = 0$ olurdu.
O hâlde $m \geq 2$ ve

$$n = m^n \geq 2^n$$

Şimdi her $n \geq 1$ için $2^n > n$ olduğunu hatırlayalım *(bkz. Alıştırma 1.3)*. Bu durumda

$$n \geq 2^n > n$$

çelişkisi ortaya çıkar.
O hâlde $\sqrt[n]{n}$ irrasyoneldir.
■

10.4 Çalışma Problemleri

Alıştırma 10.1 (Asal Çarpanlara Ayırma). Aşağıdaki sayıları kanonik biçimde yazınız.
a) 360 **b)** 1001 **c)** 5040 **d)** $2^{10} - 1$

Alıştırma 10.2 (İrrasyonellik İspatları). Aşağıdaki sayıların irrasyonel olduğunu gösteriniz.
a) $\sqrt{15}$ **b)** $\sqrt[3]{2}$ **c)** $\sqrt{2}+\sqrt{3}$ **d)** $\log_{10} 2$
İpucu (d): $\log_{10} 2 = a/b$ olsaydı $10^a = 2^b$ olurdu; her iki tarafı asal çarpanlarına ayırıp tekliği kullanınız.

Alıştırma 10.3 (Tam Kareler ve Çarpanlar). $1 < n$ bir tam sayı ve

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

kanonik gösterimi olsun. n sayısının bir tam kare olması için gerek ve yeter koşulun, bütün k_i üslerinin çift olması olduğunu gösteriniz.

Alıştırma 10.4 (Aralarında Asal Çarpanların Kareliği). a, b pozitif tam sayılar, $\gcd(a,b) = 1$ ve ab bir tam kare olsun. Bu durumda hem a'nın hem de b'nin birer tam kare olduğunu gösteriniz.
İpucu: a ile b'nin kanonik gösterimlerinde ortak asal bulunmadığını gözlemleyip Alıştırma 10.3'yi kullanınız.

11. Asal Çarpanlardan Bölenlere

Aritmetiğin esas teoremi her sayıya bir "kimlik kartı" verdi: asal çarpanları ve üsleri. Bu bölümde kartı okumayı öğreneceğiz. Bir sayının bütün bölenleri, kaç böleni olduğu, hatta iki sayının en büyük ortak böleni ve en küçük ortak katı — hepsi doğrudan üslerden okunabilir.

11.1 Asal Bölenler Kümesi

Tanım 11.1 (Asal Bölenler Kümesi). n bir tam sayı olmak üzere, n'nin bütün asal bölenlerinin kümesi $\pi(n)$ ile gösterilir:

$$\pi(n) = \{p : p \text{ asal ve } p \mid n\}$$

> ⚠ Notasyon uyarısı
>
> Bu notlarda $\pi(n)$ sembolü bir **kümedir**. Literatürde aynı sembol çoğunlukla "x'i geçmeyen asalların sayısı" anlamındaki asal sayma fonksiyonu için kullanılır. Karıştırmamak gerekir; burada $\pi(n)$ daima bir asal sayılar kümesidir.

Örnek 11.1 (Asal Bölenler Kümesi Örnekleri).

$$60 = 2^2 \cdot 3 \cdot 5 \Longrightarrow \pi(60) = \{2, 3, 5\}$$

$$16 = 2^4 \Longrightarrow \pi(16) = \{2\}$$

Ayrıca $\pi(1) = \pi(-1) = \emptyset$'dır; 1'in ve -1'in asal böleni yoktur.

Önerme 11.1 (Bölünebilme ve Asal Bölenler). *Her a, b tam sayısı için, eğer $a \mid b$ ise $\pi(a) \subseteq \pi(b)$'dir.*

Bunun nedeni geçişmedir: $p \in \pi(a)$ ise $p \mid a$ ve $a \mid b$ olduğundan $p \mid b$, yani $p \in \pi(b)$'dir.

> ℹ Tersi doğru değildir
>
> $\pi(a) \subseteq \pi(b)$ olması $a \mid b$ olmasını gerektirmez. Örneğin $a = 8$ ve $b = 2$ için
>
> $$\pi(8) = \{2\} \subseteq \{2\} = \pi(2)$$
>
> olmasına rağmen $8 \nmid 2$'dir. Asal bölenler kümesi hangi asalların göründüğünü söyler, **kaç kez** göründüğünü değil.

11.2 Aynı Asalın Kuvvetleri

Bölenleri okuyabilmek için önce tek bir asalın kuvvetleri arasındaki bölünebilmeyi belirlememiz gerekir.

Önerme 11.2 (Kuvvetler Arasında Bölünebilme). *$1 < a$ bir tam sayı ve k, s negatif olmayan tam sayılar olsun. Bu durumda*

$$a^k \mid a^s \Leftrightarrow k \leq s$$

> ***İspat.***

(⇐) $k \leq s$ *olsun. Bu durumda* $s - k \geq 0$*'dır ve*

$$a^s = a^k \cdot a^{s-k}$$

yazılır. a^{s-k} *bir tam sayı olduğundan* $a^k \mid a^s$*'dir.*
(⇒) $a^k \mid a^s$ *olsun ve aksini, yani* $k > s$ *olduğunu varsayalım.*
$a > 1$ *olduğundan* $a^s \neq 0$*'dır. Teorem 3.1 (8) gereği*

$$a^k \leq a^s$$

Öte yandan $a > 1$ *ve* $k > s$ *olduğundan üstel fonksiyon artandır:*

$$a^k = a^s \cdot a^{k-s} > a^s \cdot 1 = a^s$$

(Burada $k - s \geq 1$ olduğundan $a^{k-s} \geq a > 1$ olduğunu kullandık.) *İki eşitsizlik çelişir.*
O hâlde $k \leq s$*'dir.*
■

11.3 Bütün Bölenleri Okumak

Teorem 11.1 (Bölenler Kümesi). $0 < n \in \mathbb{Z}, p_1, p_2, \ldots, p_r$ *ikişer ikişer farklı asal sayılar ve* $0 \leq k_i \in \mathbb{Z}$ *olmak üzere*

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

olsun. Bu durumda n*'nin tüm pozitif bölenlerinin kümesi*

$$\left\{p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r} : m_i \in \mathbb{Z}, 0 \leq m_i \leq k_i \ (i = 1, \ldots, r)\right\}$$

kümesidir.

İspat.
Kümeleri adlandıralım:

$$A := \{d \in \mathbb{Z} : 0 < d, d \mid n\}, \qquad B := \left\{p_1^{m_1} \cdots p_r^{m_r} : 0 \leq m_i \leq k_i\right\}$$

1. $\boldsymbol{B \subseteq A}$**.** $b = p_1^{m_1} \cdots p_r^{m_r} \in B$ *olsun. Her* i *için* $m_i \leq k_i$ *olduğundan Önerme 11.2 gereği* $p_i^{m_i} \mid p_i^{k_i}$*'dir. Teorem 3.1 (11) gereği bölünebilmeler çarpılabilir:*

$$p_1^{m_1} \cdots p_r^{m_r} \,\Big|\, p_1^{k_1} \cdots p_r^{k_r} = n$$

Ayrıca $b > 0$ *olduğundan* $b \in A$*'dır.*
2. $\boldsymbol{A \subseteq B}$**.** $d \in A$ *olsun; yani* $0 < d$ *ve* $d \mid n$*'dir.*
$d = 1$ *ise bütün* m_i*'leri* 0 *alarak* $d = p_1^0 \cdots p_r^0 \in B$ *elde ederiz.*
Şimdi $d > 1$ *olsun. Önerme 11.1 gereği*

$$\pi(d) \subseteq \pi(n) \subseteq \{p_1, \ldots, p_r\}$$

O hâlde d*'nin kanonik gösteriminde yalnızca* $p_1, \ldots, p_r$ *asalları görünebilir:*

$$d = p_1^{s_1} p_2^{s_2} \cdots p_r^{s_r}, \qquad 0 \leq s_i$$

Geriye her i *için* $s_i \leq k_i$ *olduğunu göstermek kalıyor. Bir* i *sabitleyelim ve* n*'yi iki parçaya ayıralım:*

$$n = p_i^{k_i} \cdot \underbrace{\left(p_1^{k_1} \cdots p_{i-1}^{k_{i-1}} p_{i+1}^{k_{i+1}} \cdots p_r^{k_r}\right)}_{M}$$

p_i *ile diğer* p_j *asalları farklı olduğundan Sonuç 9.1 gereği* $\gcd(p_i, p_j) = 1$*'dir; Sonuç 5.3 gereği* $\gcd(p_i^{s_i}, p_j^{k_j}) = 1$ *ve Teorem 5.3'in tekrarlı uygulanmasıyla*

$$\gcd\left(p_i^{s_i}, M\right) = 1$$

bulunur.
Öte yandan $p_i^{s_i} \mid d$ ve $d \mid n$ olduğundan $p_i^{s_i} \mid n = p_i^{k_i} M$'dir. Teorem 5.1 gereği ($p_i^{s_i}$ ile M aralarında asal olduğundan)

$$p_i^{s_i} \Big| p_i^{k_i}$$

elde edilir. Önerme 11.2 gereği $s_i \leq k_i$'dir.
Bu her i için geçerli olduğundan $d \in B$'dir.
İki kapsama birlikte $A = B$ verir.
■

Örnek 11.2 (Bölenleri Listeleme). $12 = 2^2 \cdot 3$ olduğundan, bölenler $2^{m_1}3^{m_2}$ biçimindedir ve $0 \leq m_1 \leq 2, 0 \leq m_2 \leq 1$'dir:

	3^0	3^1
2^0	1	3
2^1	2	6
2^2	4	12

Yani 12'nin pozitif bölenleri $1, 2, 3, 4, 6, 12$'dir; toplam 6 tane.

11.4 Bölen Sayısı

Yukarıdaki tablo, bölen **sayısını** hesaplamanın da yolunu gösteriyor: her üs için bağımsız bir seçim yapılır.

Tanım 11.2 (Bölen Sayısı Fonksiyonu). $0 < n$ bir tam sayı olmak üzere, n'nin pozitif bölenlerinin sayısı $\tau(n)$ ile gösterilir.

Sonuç 11.1 (Bölen Sayısı Formülü). *$n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ kanonik gösterimi olsun. Bu durumda*

$$\tau(n) = \prod_{i=1}^{r}(k_i + 1) = (k_1 + 1)(k_2 + 1)\cdots(k_r + 1)$$

İspat.
Teorem 11.1 gereği n'nin her pozitif böleni

$$p_1^{m_1}p_2^{m_2}\cdots p_r^{m_r}, \qquad 0 \leq m_i \leq k_i$$

biçimindedir. Ayrıca farklı $(m_1, \ldots, m_r)$ üs dizileri farklı bölenler verir; çünkü aritmetiğin esas teoremi gereği kanonik gösterim tek türlü belirlidir.
O hâlde bölenler ile üs dizileri arasında birebir eşleme vardır. Her m_i için

$$m_i \in \{0, 1, 2, \ldots, k_i\}$$

yani $k_i + 1$ seçenek bulunur ve seçimler birbirinden bağımsızdır. Toplam seçenek sayısı çarpımlarıdır:

$$\tau(n) = (k_1 + 1)(k_2 + 1)\cdots(k_r + 1)$$

■

Örnek 11.3 (Bölen Sayısı Hesapları). $\tau(120)$, $\tau(1001)$ ve $\tau(p^k)$ değerlerini hesaplayınız *(p asal).*

Çözüm.
$\tau(120)$. Örnek 10.2'de $120 = 2^3 \cdot 3^1 \cdot 5^1$ bulmuştuk. O hâlde

$$\tau(120) = (3+1)(1+1)(1+1) = 4 \cdot 2 \cdot 2 = 16$$

$\tau(1001)$. $1001 = 7 \cdot 11 \cdot 13$'tür *(üç farklı asal, hepsinin üssü 1)*:

$$\tau(1001) = (1+1)(1+1)(1+1) = 8$$

$\tau(p^k)$. Tek bir asal ve tek bir üs vardır:

$$\tau(p^k) = k+1$$

Nitekim p^k sayısının bölenleri $1, p, p^2, \ldots, p^k$'dır; $k+1$ tane.
■

11.5 EBOB ve EKOK'u Üslerden Okumak

Bölenleri üsler cinsinden tanıdığımıza göre, ortak bölenleri ve ortak katları da aynı dille ifade edebiliriz.

Teorem 11.2 (Üslerle EBOB ve EKOK). *$p_1 < p_2 < \cdots < p_r$ asal sayılar, $k_1, \ldots, k_r$ ve $l_1, \ldots, l_r$ negatif olmayan tam sayılar olmak üzere*

$$n = p_1^{k_1} \cdots p_r^{k_r}, \qquad m = p_1^{l_1} \cdots p_r^{l_r}$$

olsun. Bu durumda aşağıdakiler geçerlidir:

$$\text{i)} \quad \gcd(n,m) = \prod_{i=1}^{r} p_i^{\min\{k_i, l_i\}}$$

$$\text{ii)} \quad \operatorname{lcm}(n,m) = \prod_{i=1}^{r} p_i^{\max\{k_i, l_i\}}$$

$$\text{iii)} \quad n \cdot m = \gcd(n,m) \cdot \operatorname{lcm}(n,m)$$

İspat.
i) *$d := \prod_i p_i^{\min\{k_i,l_i\}}$ diyelim. Teorem 4.2'nun iki koşulunu doğrulayacağız.*
d bir ortak bölendir. *Her i için $\min\{k_i,l_i\} \le k_i$ olduğundan Teorem 11.1 gereği $d \mid n$'dir. Aynı biçimde $\min\{k_i,l_i\} \le l_i$ olduğundan $d \mid m$'dir.*
Her ortak bölen *d*'yi böler. *c pozitif bir ortak bölen olsun. $c \mid n$ olduğundan Teorem 11.1 gereği*

$$c = p_1^{s_1} \cdots p_r^{s_r}, \qquad s_i \le k_i$$

yazılır. Aynı teorem $c \mid m$ için de uygulanınca $s_i \le l_i$ bulunur. İkisi birlikte

$$s_i \le \min\{k_i, l_i\}$$

verir; yine Teorem 11.1 gereği $c \mid d$'dir.
(Negatif ortak bölenler için Teorem 3.1 (13) gereği aynı sonuç geçerlidir.)
İki koşul da sağlandığından $d = \gcd(n,m)$'dir.
ii) *$M := \prod_i p_i^{\max\{k_i,l_i\}}$ diyelim.*
M bir ortak kattır. *Her i için $k_i \le \max\{k_i,l_i\}$ olduğundan Teorem 11.1 gereği $n \mid M$'dir; benzer biçimde $m \mid M$'dir.*
Her ortak kat *M* ile bölünür. *c pozitif bir ortak kat olsun. $n \mid c$ ve $m \mid c$'dir. Her i için $p_i^{k_i} \mid n \mid c$ ve $p_i^{l_i} \mid m \mid c$ olduğundan $p_i^{\max\{k_i,l_i\}} \mid c$'dir. Farklı asalların kuvvetleri ikişer ikişer aralarında asal olduğundan Teorem 5.2'ın tekrarlı uygulanmasıyla çarpımları da c'yi böler:*

$$M = \prod_i p_i^{\max\{k_i,l_i\}} \,\Big|\, c$$

Özel olarak $M \le c$'dir. O hâlde M, en küçük pozitif ortak kattır: $M = \operatorname{lcm}(n,m)$.
iii) *Her i için, iki sayıdan küçüğü ile büyüğünün toplamı, sayıların toplamına eşittir:*

$$\min\{k_i, l_i\} + \max\{k_i, l_i\} = k_i + l_i$$

Bu yüzden

$$\gcd(n,m) \cdot \operatorname{lcm}(n,m) = \prod_i p_i^{\min\{k_i,l_i\}+\max\{k_i,l_i\}} = \prod_i p_i^{k_i+l_i} = n \cdot m$$

■

i Ortak asal listesi kullanmak

Teoremde iki sayı için **aynı** $p_1, \ldots, p_r$ listesi kullanıldı. Bu bir kısıtlama değildir: bir asal sayılardan birinde görünmüyorsa üssü 0 alınır. Örneğin

$$12 = 2^2 \cdot 3^1 \cdot 5^0, \qquad 50 = 2^1 \cdot 3^0 \cdot 5^2$$

yazılabilir ve teorem doğrudan uygulanır.

Örnek 11.4 (Üslerle EBOB ve EKOK Hesabı). $\gcd(360, 84)$ ve $\operatorname{lcm}(360, 84)$ değerlerini asal çarpanlara ayırarak bulunuz.

Çözüm.
Önce kanonik gösterimleri yazalım:

$$360 = 2^3 \cdot 3^2 \cdot 5^1 \cdot 7^0, \qquad 84 = 2^2 \cdot 3^1 \cdot 5^0 \cdot 7^1$$

Her asal için üsleri karşılaştıralım:

Asal	360'ın üssü	84'ün üssü	Minimum	Maksimum
2	3	2	2	3
3	2	1	1	2
5	1	0	0	1
7	0	1	0	1

Teorem 11.2 gereği

$$\gcd(360, 84) = 2^2 \cdot 3^1 \cdot 5^0 \cdot 7^0 = 4 \cdot 3 = 12$$

$$\operatorname{lcm}(360, 84) = 2^3 \cdot 3^2 \cdot 5^1 \cdot 7^1 = 8 \cdot 9 \cdot 5 \cdot 7 = 2520$$

(Sağlama: $12 \cdot 2520 = 30240$ *ve* $360 \cdot 84 = 30240$ ✓*)*
■

⚠ Hangi yöntem ne zaman?

Üsler yöntemi kavramsal olarak aydınlatıcıdır ama **pratikte yavaştır**: sayıları asal çarpanlarına ayırmak, büyük sayılarda son derece zordur. Öklid algoritması ise çarpanlara hiç bakmadan birkaç bölmede sonuca ulaşır.
Kısacası: anlamak için üsler, hesaplamak için Öklid algoritması.

11.6 Asal Bölenler Kümesiyle Çalışmak

Örnek 11.5 (\$pi\$ Kümesinin Temel Özellikleri). Her a, b tam sayısı ve her k pozitif tam sayısı için

$$\pi(ab) = \pi(a) \cup \pi(b), \qquad \pi\left(a^k\right) = \pi(a)$$

olduğunu gösteriniz.

> **Çözüm.**
> **Birinci eşitlik.**
> *(⊇)* $p \in \pi(a)$ olsun; $p \mid a$'dır. $a \mid ab$ olduğundan geçişme gereği $p \mid ab$, yani $p \in \pi(ab)$'dir. Aynı akıl yürütme $\pi(b)$ için de geçerlidir.
> *(⊆)* $p \in \pi(ab)$ olsun; p asal ve $p \mid ab$'dir. Teorem 9.1 gereği $p \mid a$ veya $p \mid b$'dir; yani $p \in \pi(a) \cup \pi(b)$'dir.
> **İkinci eşitlik.** p asal olmak üzere Sonuç 9.4 gereği
>
> $$p \mid a^k \Leftrightarrow p \mid a$$
>
> olduğundan iki küme aynı elemanlara sahiptir.
> ■

Örnek 11.6 (Aralarında Asallığın pi ile İfadesi). İkisi birden sıfır olmayan her a, b tam sayısı için

$$\gcd(a, b) = 1 \Leftrightarrow \pi(a) \cap \pi(b) = \emptyset$$

olduğunu gösteriniz.

> **Çözüm.**
> **(⇒)** $\gcd(a, b) = 1$ olsun. $\pi(a) \cap \pi(b)$ kümesinde bir p elemanı bulunsaydı, p hem a'yı hem b'yi bölen bir asal olurdu. Bu durumda p bir ortak bölendir ve Teorem 4.2 gereği
>
> $$p \mid \gcd(a, b) = 1$$
>
> olurdu; oysa $p > 1$'dir. O hâlde kesişim boştur.
> **(⇐)** $\pi(a) \cap \pi(b) = \emptyset$ olsun ve $d := \gcd(a, b)$ diyelim. $d > 1$ olduğunu varsayalım. Lemma 9.1 gereği d'nin bir p asal böleni vardır. $p \mid d$, $d \mid a$ ve $d \mid b$ olduğundan geçişme gereği
>
> $$p \mid a \qquad \text{ve} \qquad p \mid b$$
>
> olur; yani $p \in \pi(a) \cap \pi(b)$'dir. Bu, kesişimin boş olmasıyla çelişir.
> O hâlde $d = 1$'dir.
> ■

11.7 Çalışma Problemleri

Alıştırma 11.1 (Bölenler ve Bölen Sayısı). **a)** $2^4 \cdot 3^2 \cdot 5$ sayısının kaç pozitif böleni vardır?
b) $\tau(n) = 3$ olacak biçimdeki bütün n sayılarını belirleyiniz.
c) $\tau(n)$ değerinin tek sayı olması için gerek ve yeter koşulun n'nin bir tam kare olması olduğunu gösteriniz.
İpucu (c): Alıştırma 10.3'yi ve bölen sayısı formülünü birlikte kullanınız.

Alıştırma 11.2 (Bölenlerin Çarpımı). $0 < n$ bir tam sayı olsun. n'nin bütün pozitif bölenlerinin çarpımının

$$n^{\tau(n)/2}$$

olduğunu gösteriniz.
İpucu: d bir bölense n/d de bir bölendir; bölenleri $(d, n/d)$ çiftleri hâlinde eşleştiriniz.

Alıştırma 11.3 (Üslerle Hesaplar). Aşağıdaki değerleri kanonik gösterimleri kullanarak hesaplayınız.
a) $\gcd(2^5 \cdot 3^3 \cdot 7, 2^2 \cdot 3^4 \cdot 11)$
b) $\operatorname{lcm}(2^5 \cdot 3^3 \cdot 7, 2^2 \cdot 3^4 \cdot 11)$

c) $\gcd(1001, 2431)$ *(İpucu:* $2431 = 11 \cdot 13 \cdot 17$*.)*

12. Kongrüans Kavramı

Bölme algoritması her tam sayıya bir kalan iliştiriyordu. Şimdi bu fikri bir adım öteye taşıyacağız: **aynı kalanı veren sayıları birbirinden ayırt etmeyeceğiz.** Ortaya çıkan dil — kongrüans dili — sayılar teorisinin en güçlü hesap aracıdır; büyük sayılarla yapılan bölünebilme hesaplarını çoğu zaman birkaç satıra indirir.

12.1 Tanım

Tanım 12.1 (Kongrüans). n sabit bir pozitif tam sayı ve $a, b \in \mathbb{Z}$ olsun. Eğer n sayısı $a - b$ farkını bölerse, yani

$$a - b = kn$$

olacak biçimde bir k tam sayısı varsa, "a ve b tam sayıları **modülo n kongrüdür**" denir ve

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

yazılır. Aksi hâlde $a \not\equiv b \pmod{n}$ yazılır. n sayısına **modül** denir.

Örnek 12.1 (İlk Örnekler). $n = 7$ olsun.

$$20 \equiv 6 \pmod{7}, \qquad -22 \equiv 13 \pmod{7}, \qquad -108 \equiv -101 \pmod{7}$$

çünkü sırasıyla $20 - 6 = 14$, $-22 - 13 = -35$ ve $-108 - (-101) = -7$ sayılarının hepsi 7 ile bölünür. Buna karşılık

$$18 \not\equiv 5 \pmod{7}$$

çünkü $18 - 5 = 13$ sayısı 7 ile bölünmez.

> **i** Modül neden 1'den büyük alınıyor?
>
> Herhangi iki tam sayı daima modülo 1 kongrüdür; çünkü 1 her farkı böler. Bu yüzden $n = 1$ hiçbir bilgi taşımaz ve bundan sonra $n > 1$ olduğunu varsayacağız.

12.2 Temel Özellikler

Kongrüans bağıntısı, eşitliğe çok benzer biçimde davranır: yansıma, simetri ve geçişme özelliklerini taşır; ayrıca iki tarafı toplayabilir, çıkarabilir, çarpabilir ve kuvvet alabiliriz. Aşağıdaki teorem bu benzerliğin sınırlarını çizer.

Teorem 12.1 (Kongrüansın Temel Özellikleri). *$1 < n$ sabit bir tam sayı olmak üzere, her a, b, c, d tam sayısı için aşağıdakiler geçerlidir.*
(a) $a \equiv a \pmod{n}$.
(b) $a \equiv b \pmod{n}$ *ise* $b \equiv a \pmod{n}$.
(c) $a \equiv b \pmod{n}$ *ve* $b \equiv c \pmod{n}$ *ise* $a \equiv c \pmod{n}$.
(d) $a \equiv b \pmod{n}$ *ve* $c \equiv d \pmod{n}$ *ise*

$$a + c \equiv b + d \pmod{n} \qquad \text{ve} \qquad ac \equiv bd \pmod{n}$$

(e) $a \equiv b \pmod{n}$ *ise* $a + c \equiv b + c \pmod{n}$ *ve* $ac \equiv bc \pmod{n}$.
(f) $a \equiv b \pmod{n}$ *ise her k pozitif tam sayısı için* $a^k \equiv b^k \pmod{n}$.

İspat.
(a) $a - a = 0 = n \cdot 0$ *olduğundan* $n \mid a - a$*'dır.*
(b) $n \mid a - b$ *olsun. Teorem 3.1 (13) gereği* $n \mid -(a-b) = b - a$*'dır.*
(c) $n \mid a - b$ *ve* $n \mid b - c$ *olsun. Teorem 3.1 (7) gereği* n *toplamı da böler:*

$$n \mid (a-b) + (b-c) = a - c$$

(d) $n \mid a - b$ *ve* $n \mid c - d$ *olsun.*
Toplam için:

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

Sağ taraftaki her iki terim n *ile bölündüğünden toplamları da bölünür.*
Çarpım için: *İfadeye* bc *terimini ekleyip çıkararak parçalayalım:*

$$\begin{aligned} ac - bd &= ac - bc + bc - bd \\ &= c(a-b) + b(c-d) \end{aligned}$$

$n \mid a - b$ *olduğundan* $n \mid c(a-b)$; $n \mid c - d$ *olduğundan* $n \mid b(c-d)$*'dir. Teorem 3.1 (7) gereği* n *toplamı, yani* $ac - bd$*'yi böler.*
(e) *(d) özelliğinde* $c \equiv c \pmod{n}$ *alınırsa* (bu (a) gereği doğrudur) *istenen elde edilir.*
(f) k *üzerinden tümevarım yapalım.* $k = 1$ *için iddia hipotezdir.* $a^k \equiv b^k \pmod{n}$ *olduğunu varsayalım. Elimizde*

$$a^k \equiv b^k \pmod{n} \qquad \text{ve} \qquad a \equiv b \pmod{n}$$

vardır; (d) özelliğinin çarpım kısmı gereği

$$a^k \cdot a \equiv b^k \cdot b \pmod{n} \qquad \text{yani} \qquad a^{k+1} \equiv b^{k+1} \pmod{n}$$

Tümevarım gereği iddia her k *için doğrudur.*
■

⚠ Bölme kuralı eksik!

Listede toplama, çıkarma, çarpma ve kuvvet alma var — ama **bölme yok**. Bu bir unutkanlık değildir: kongrüanslarda sadeleştirme her zaman serbest değildir. Örneğin

$$2 \cdot 3 \equiv 2 \cdot 6 \pmod{6}$$

doğrudur *(her iki taraf da* $\equiv 0$*)*, ama 2'yi sadeleştirip $3 \equiv 6 \pmod{6}$ yazamayız; bu yanlıştır. Sadeleştirmenin hangi koşulda serbest olduğunu birazdan göreceğiz.

12.3 Aynı Kalanı Verme Ölçütü

Kongrüansın sezgisel anlamı, tanımdaki fark koşulundan daha açıktır.

Teorem 12.2 (Kongrüans, Aynı Kalanı Vermektir). $1 < n$ *sabit bir tam sayı ve* $a, b \in \mathbb{Z}$ *olsun.* $a \equiv b \pmod{n}$ *olabilmesi için gerek ve yeter koşul,* a *ile* b*'nin* n *ile bölündüklerinde* ***aynı kalanı*** *vermesidir.*

İspat.
Bölme algoritmasına göre

$$a = nq_1 + r_1, \qquad b = nq_2 + r_2, \qquad 0 \le r_1, r_2 < n$$

yazalım.
(⇐) $r_1 = r_2$ *olsun. Farkı hesaplayalım:*

$$a - b = nq_1 + r_1 - nq_2 - r_2 = n(q_1 - q_2)$$

O hâlde $n \mid a-b$, yani $a \equiv b \pmod{n}$'dir.
(⇒) *$a \equiv b \pmod{n}$ olsun; $n \mid a-b$'dir. Farkı yukarıdaki gibi yazalım:*

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

n sayısı hem $a-b$'yi hem de $n(q_1-q_2)$'yi böldüğünden, farklarını da böler:

$$n \mid r_1 - r_2$$

Öte yandan $0 \leq r_1, r_2 < n$ olduğundan

$$-n < r_1 - r_2 < n \qquad \text{yani} \qquad |\, r_1 - r_2 \,| < n$$

n ile bölünen ve mutlak değeri n'den küçük olan tek tam sayı 0'dır. O hâlde $r_1 = r_2$'dir.
■

i Bu ölçüt neden bu kadar kullanışlı?

Ölçüt, kongrüans hesabını "kalan hesabına" çevirir. Bir sayının n ile bölümünden kalanı bulmak istiyorsak, o sayıyı modülo n mümkün olduğunca küçük bir sayıya indirgeriz; elde ettiğimiz $0 \leq r < n$ değeri doğrudan aranan kalandır.
Aşağıdaki örnekler bu stratejinin uygulamalarıdır.

12.4 Büyük Kuvvetlerle Hesap

Örnek 12.2 (3^10 Sayısının 41 ile Bölümünden Kalan). **a)** 41 sayısının $3^{10} - 9$ sayısını böldüğünü gösteriniz.
b) 3^{10} sayısının 41 ile bölümünden elde edilen kalanı bulunuz.

Çözüm.
a) Kuvveti doğrudan hesaplamak yerine küçük bir kuvvetten başlayalım:

$$3^4 = 81 = 2 \cdot 41 - 1$$

O hâlde

$$3^4 \equiv -1 \pmod{41}$$

Şimdi Teorem 12.1 (f) gereği her iki tarafın karesini alalım:

$$3^8 \equiv (-1)^2 = 1 \pmod{41}$$

Son olarak $3^{10} = 3^8 \cdot 3^2$ olduğundan, (d) özelliğiyle çarpalım:

$$3^{10} \equiv 1 \cdot 3^2 = 9 \pmod{41}$$

Bu, tanım gereği $41 \mid 3^{10} - 9$ demektir.
b) $3^{10} \equiv 9 \pmod{41}$ bulduk ve $0 \leq 9 < 41$'dir. Teorem 12.2 gereği aranan kalan **9**'dur.
■

i -1 avı

Yukarıdaki hesabın püf noktası, $3^4 \equiv -1$ eşitliğini fark etmekti. Kuvvet hesaplarında modülo n'de 1 veya -1 değerini veren bir kuvvet bulmak, geri kalan her şeyi çözer: o kuvvetten sonrası periyodik olarak tekrarlanır.
Bu yüzden strateji şudur: $a^1, a^2, a^3, \ldots$ değerlerini modülo n hesaplayın ve ilk kez ± 1 göründüğü yerde durun.

Örnek 12.3 (\$3^405\$ Sayısının \$17\$ ile Bölümünden Kalan). 3^{405} sayısının 17 ile bölümünden elde edilen kalanı bulunuz.

Çözüm.
Önce 3'ün küçük kuvvetlerini modülo 17 hesaplayalım:

$$3^1 \equiv 3, \qquad 3^2 \equiv 9, \qquad 3^3 \equiv 27 \equiv 10, \qquad 3^4 \equiv 30 \equiv 13 \pmod{17}$$

Devam edelim:

$$3^8 \equiv 13^2 = 169 = 9 \cdot 17 + 16 \equiv 16 \equiv -1 \pmod{17}$$

-1'i bulduk. Karesini alalım:

$$3^{16} \equiv (-1)^2 = 1 \pmod{17}$$

Şimdi üssü 16'ya bölelim:

$$405 = 16 \cdot 25 + 5$$

Buradan

$$3^{405} = (3^{16})^{25} \cdot 3^5 \equiv 1^{25} \cdot 3^5 = 3^5 \pmod{17}$$

Son olarak $3^5 = 243 = 14 \cdot 17 + 5$ olduğundan

$$3^{405} \equiv 5 \pmod{17}$$

$0 \leq 5 < 17$ olduğundan aranan kalan $\mathbf{5}$'tir.
■

Örnek 12.4 (Faktöriyellerin Toplamı).

$$1! + 2! + 3! + \cdots + 99! + 100!$$

sayısının 240 ile bölümünden elde edilen kalanı bulunuz.

Çözüm.
Anahtar gözlem, toplamdaki terimlerin büyük çoğunluğunun modülo 240'ta yok olmasıdır.

$$240 = 2^4 \cdot 3 \cdot 5$$

Şimdi 6! sayısına bakalım:

$$6! = 720 = 3 \cdot 240$$

Demek ki $240 \mid 6!$'dir. Her $n \geq 6$ için $6! \mid n!$ olduğundan *(çünkü $n! = 6! \cdot 7 \cdot 8 \cdots n$)*, geçişme gereği

$$240 \mid n! \qquad \text{yani} \qquad n! \equiv 0 \pmod{240} \qquad (n \geq 6)$$

O hâlde toplamdaki 6!'den 100!'e kadar olan bütün terimler modülo 240'ta sıfırdır. Geriye ilk beş terim kalır:

$$\begin{aligned} 1! + 2! + \cdots + 100! &\equiv 1! + 2! + 3! + 4! + 5! \pmod{240} \\ &= 1 + 2 + 6 + 24 + 120 \\ &= 153 \end{aligned}$$

$0 \leq 153 < 240$ olduğundan aranan kalan **153**'tür.
■

Örnek 12.5 (Tam Karelerin Son Rakamı). Her n tam sayısı için n^2 sayısının birler basamağındaki rakamın yalnızca

$$0, \quad 1, \quad 4, \quad 5, \quad 6, \quad 9$$

rakamlarından biri olabileceğini gösteriniz.

Çözüm.
Bir sayının birler basamağı, o sayının 10 ile bölümünden kalandır. O hâlde n^2 sayısını modülo 10 incelemeliyiz.
$n \equiv r \pmod{10}$, $r \in \{0, 1, \ldots, 9\}$ olsun. Teorem 12.1 (f) gereği

$$n^2 \equiv r^2 \pmod{10}$$

Şimdi r^2 değerlerini modülo 10 hesaplayalım:

r	0	1	2	3	4	5	6	7	8	9
r^2	0	1	4	9	16	25	36	49	64	81
$r^2 \bmod 10$	0	1	4	9	6	5	6	9	4	1

Son satırda görünen değerler kümesi

$$\{0, 1, 4, 5, 6, 9\}$$

olduğundan, başka hiçbir rakam bir tam karenin son basamağı olamaz.
■

i Hangi sayılar tam kare olamaz?

Bu tablo hızlı bir eleme aracıdır: son rakamı 2, 3, 7 veya 8 olan hiçbir sayı tam kare değildir. Örneğin 123456787 sayısının tam kare olup olmadığını anlamak için karekök almaya gerek yoktur; son rakamı 7 olduğundan tam kare olamaz.

12.5 Sadeleştirme Kuralı

Şimdi kongrüanslarda bölmenin ne zaman serbest olduğunu belirleyelim.

Teorem 12.3 (Sadeleştirme Kuralı). *$a, b, c, n \in \mathbb{Z}$, $1 < n$ ve $d = \gcd(c, n)$ olsun. Eğer*

$$ca \equiv cb \pmod{n}$$

ise

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

İspat.
$ca \equiv cb \pmod{n}$ olsun; yani $n \mid c(a-b)$'dir. O hâlde

$$c(a-b) = nk$$

olacak biçimde bir k tam sayısı vardır.
$d = \gcd(c, n)$ *olduğundan*

$$c = dc', \qquad n = dn'$$

yazalım; Sonuç 5.1 gereği $\gcd(c', n') = 1$*'dir. Bunları yerine koyalım:*

$$dc'(a-b) = dn'k$$

$d \neq 0$ *olduğundan sadeleştirebiliriz:*

$$c'(a-b) = n'k$$

Bu eşitlik $n' \mid c'(a-b)$ *olduğunu söyler.* $\gcd(n', c') = 1$ *olduğundan Teorem 5.1 gereği*

$$n' \mid a-b$$

bulunur; yani

$$a \equiv b \pmod{n'}, \qquad n' = \frac{n}{d}$$

■

Sonuç 12.1 (Aralarında Asal Çarpanla Sadeleştirme). *$a, b, c, n \in \mathbb{Z}$ ve $1 < n$ olsun.*
1. *Eğer $ca \equiv cb \pmod{n}$ ve $\gcd(c, n) = 1$ ise $a \equiv b \pmod{n}$'dir.*
2. *p bir asal sayı olmak üzere, eğer $ca \equiv cb \pmod{p}$ ve $p \nmid c$ ise $a \equiv b \pmod{p}$'dir.*

Birincisi Teorem 12.3'nin $d = 1$ hâlidir. İkincisi ise Önerme 9.1 gereği $p \nmid c$ olduğunda $\gcd(c, p) = 1$ olmasından çıkar.

⚠ Koşul kaldırılamaz

Bölümün başındaki karşı örneğe dönelim:

$$2 \cdot 3 \equiv 2 \cdot 6 \pmod{6}$$

Burada $\gcd(2, 6) = 2$'dir. Teorem 12.3 yalnızca

$$3 \equiv 6 \pmod{3}$$

sonucunu verir — ki bu doğrudur. Modülü küçültmeden sadeleştirmek yanlış olurdu.

12.6 Modülle EBOB Değişmez

Önerme 12.1 (Kongrü Sayıların Modülle EBOB'u). *$a, b, n \in \mathbb{Z}$ ve $1 < n$ olsun. Eğer $a \equiv b \pmod{n}$ ise*

$$\gcd(n, a) = \gcd(n, b)$$

Gerçekten de $a \equiv b \pmod{n}$ ise $a = b + nk$ olacak biçimde bir k tam sayısı vardır. Önerme 6.1 gereği

$$\gcd(n, a) = \gcd(n, b + nk) = \gcd(n, b)$$

i Ne işe yarar?

Bu küçük önerme ileride birkaç yerde işimizi görecek: bir kalan sınıfının modülle aralarında asal olup olmadığı, sınıftan hangi temsilciyi seçtiğimize bağlı değildir. Euler'in ϕ fonksiyonunu kalan sınıfları üzerinden tanımlarken bu bilgi vazgeçilmez olacak.

12.7 Polinomlarla Kongrüans

Teorem 12.4 (Polinomlar Kongrüansı Korur). *$0 < m \in \mathbb{Z}$ ve*

$$P(x) = c_m x^m + c_{m-1} x^{m-1} + \cdots + c_1 x + c_0$$

katsayıları tam sayı olan bir polinom olsun. Eğer $a \equiv b \pmod{n}$ ise

$$P(a) \equiv P(b) \pmod{n}$$

İspat.
$a \equiv b \pmod{n}$ olsun. Teorem 12.1 (f) gereği her $k \in \{0, 1, \ldots, m\}$ için

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

(burada $k = 0$ için her iki taraf 1'dir). *Şimdi (e) özelliğiyle her iki tarafı c_k ile çarpalım:*

$$c_k a^k \equiv c_k b^k \pmod{n}$$

Son olarak (d) özelliğinin toplam kısmını $m + 1$ terim için ardışık olarak uygularsak

$$\sum_{k=0}^{m} c_k a^k \equiv \sum_{k=0}^{m} c_k b^k \pmod{n}$$

yani $P(a) \equiv P(b) \pmod{n}$ bulunur.
■

Sonuç 12.2 (Çözümler Sınıf Hâlinde Gelir). *$P(x)$ tam katsayılı bir polinom olsun. Eğer a tam sayısı*

$$P(x) \equiv 0 \pmod{n}$$

kongrüansının bir çözümü ve $b \equiv a \pmod{n}$ ise, b de bu kongrüansın bir çözümüdür.

Gerçekten de Teorem 12.4 gereği $P(b) \equiv P(a) \equiv 0 \pmod{n}$'dir.

i Sonlu arama

Bu sonuç son derece pratiktir: bir kongrüansın çözümlerini ararken sonsuz sayıda tam sayıyı denemek gerekmez. $0, 1, \ldots, n-1$ değerlerini denemek yeterlidir; geri kalan her tam sayı bunlardan birine kongrüdür ve aynı sonucu verir.

Örnek 12.6 ($p divides a^2 - b^2$ İse). p bir asal sayı ve $a, b \in \mathbb{Z}$ olmak üzere

$$a^2 \equiv b^2 \pmod{p} \Longrightarrow a \equiv b \pmod{p} \quad \text{veya} \quad a \equiv -b \pmod{p}$$

olduğunu gösteriniz.

Çözüm.
$a^2 \equiv b^2 \pmod{p}$ olsun; tanım gereği

$$p \mid a^2 - b^2$$

Sol tarafı çarpanlarına ayıralım:

$$a^2 - b^2 = (a-b)(a+b)$$

O hâlde

$$p \mid (a-b)(a+b)$$

p asal olduğundan Teorem 9.1 gereği

$$p \mid a-b \qquad \text{veya} \qquad p \mid a+b$$

Bunlar sırasıyla

$$a \equiv b \pmod{p} \qquad \text{veya} \qquad a \equiv -b \pmod{p}$$

demektir.
■

⚠ Modül asal değilse bozulur

p'nin asal olması vazgeçilmezdir. $n = 8$ alalım:

$$3^2 = 9 \equiv 1 = 1^2 \pmod{8}$$

olmasına rağmen $3 \not\equiv 1$ ve $3 \not\equiv -1 \equiv 7 \pmod{8}$'dir. Nitekim modülo 8'de $x^2 \equiv 1$ kongrüansının dört çözümü vardır: $1, 3, 5, 7$.

12.8 Çalışma Problemleri

Alıştırma 12.1 (Kalan Hesapları). Aşağıdaki kalanları bulunuz.
a) 2^{100} sayısının 7 ile bölümünden kalan.
b) 7^{1000} sayısının 11 ile bölümünden kalan.
c) $1! + 2! + \cdots + 50!$ sayısının 15 ile bölümünden kalan.
d) $\sum_{k=1}^{100} k^5$ toplamının 4 ile bölümünden kalan.

Alıştırma 12.2 (Modülü Değiştirmek). $a, b, n, m \in \mathbb{Z}$ ve $1 < n, m$ olsun.
a) $a \equiv b \pmod{n}$ ve $m \mid n$ ise $a \equiv b \pmod{m}$ olduğunu gösteriniz.
b) $a \equiv b \pmod{n}$ ve $n \mid m$ ise $a \equiv b \pmod{m}$ önermesinin **yanlış** olduğunu bir karşı örnekle gösteriniz.
c) $\gcd(n, m) = 1$ olsun. $a \equiv b \pmod{n}$ ve $a \equiv b \pmod{m}$ olması için gerek ve yeter koşulun $a \equiv b \pmod{nm}$ olduğunu gösteriniz.
İpucu (c): Teorem 5.2'ı kullanınız.

Alıştırma 12.3 (Kongrüanslarla Bölünebilme). Aşağıdakileri kongrüans diliyle ispatlayınız.
a) Her n pozitif tam sayısı için $7 \mid 5^{2n} + 3 \cdot 2^{5n-2}$.
b) Her n tam sayısı için $15 \mid 3n^5 + 5n^3 + 7n$.
c) Her n tam sayısı için, $7 \nmid n$ ise $7 \mid n^3 + 1$ veya $7 \mid n^3 - 1$'dir.

Alıştırma 12.4 (Küçük Fermat'ya Hazırlık). p bir asal sayı olmak üzere, her a, b tam sayısı için

$$(a+b)^p \equiv a^p + b^p \pmod{p}$$

olduğunu gösteriniz.
İpucu: Binom açılımını yazıp Alıştırma 9.2'u kullanınız: aradaki bütün katsayılar p ile bölünür.

13. Tam Kalan Sistemleri

Kongrüans, tam sayıları n gruba ayırır: aynı kalanı verenler bir arada. Bu bölümde bu grupların her birinden birer temsilci seçmenin ne anlama geldiğini inceleyeceğiz. "Tam kalan sistemi" adını verdiğimiz bu temsilci listeleri, ileride Euler ve Fermat teoremlerinin ispatında merkezî rol oynayacak.

13.1 Her Sayı Tam Bir Kalana Kongrüdür

Lemma 13.1 (Kalanların Temsil Gücü). *$1 < n$ sabit bir tam sayı olsun. Bu durumda her tam sayı*

$$0, \quad 1, \quad 2, \quad \ldots, \quad n-1$$

*sayılarından **tam birisine** modülo n kongrüdür.*

> ***İspat.***
> *a herhangi bir tam sayı olsun.*
> ***Varlık.** Bölme algoritmasına göre*
>
> $$a = nq + r, \qquad 0 \leq r < n$$
>
> *olacak biçimde q, r tam sayıları vardır. Buradan $a - r = nq$, yani $n \mid a - r$ olur; demek ki*
>
> $$a \equiv r \pmod{n}$$
>
> *ve $r \in \{0, 1, \ldots, n-1\}$'dir.*
> ***Teklik.** $a \equiv r \pmod{n}$ ve $a \equiv r' \pmod{n}$ olsun; $r, r' \in \{0, 1, \ldots, n-1\}$ olduğunu varsayalım. Teorem 12.1 (b) ve (c) gereği*
>
> $$r \equiv r' \pmod{n}$$
>
> *olur; yani $n \mid r - r'$'dür. Öte yandan*
>
> $$0 \leq r, r' \leq n-1 \Longrightarrow \mid r - r' \mid \leq n - 1 < n$$
>
> *n ile bölünen ve mutlak değeri n'den küçük olan tek tam sayı 0'dır; o hâlde $r = r'$'dür.*
> ■

13.2 Tam Kalan Sistemi

Tanım 13.1 (Tam Kalan Sınıfları Kümesi). $1 < n$ sabit bir tam sayı ve $\{a_1, a_2, \ldots, a_n\}$ tam sayıların bir alt kümesi olsun. Eğer

her tam sayı, $a_1, a_2, \ldots, a_n$ sayılarından **tam birisine** modülo n kongrüdür

koşulu sağlanırsa, bu kümeye **modülo n tam kalan sınıfları kümesi** *(kısaca tam kalan sistemi)* denir.

Örnek 13.1 (En Tanıdık Örnek). $1 < n$ olmak üzere

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

kümesi bir modülo n tam kalan sistemidir; bu, Lemma 13.1'nin doğrudan ifadesidir.

Tanım 13.2 (Negatif Olmayan En Küçük Tam Kalan Sistemi). $1 < n$ olmak üzere $\{0, 1, 2, ..., n-1\}$ kümesine **negatif olmayan en küçük tam kalan sınıfları kümesi** denir.

Bir tam kalan sistemi olup olmadığını anlamak için tanımdaki "her tam sayı" koşulunu tek tek sınamak gerekmez; çok daha pratik bir ölçüt vardır.

Teorem 13.1 (Tam Kalan Sistemi Ölçütü). *$1 < n$ sabit bir tam sayı ve $A = \{a_1, a_2, ..., a_n\} \subset \mathbb{Z}$ **n elemanlı** bir küme olsun. A'nın bir modülo n tam kalan sistemi olması için gerek ve yeter koşul, elemanlarının ikişer ikişer birbirine kongrü olmamasıdır:*

$$i \neq j \Longrightarrow a_i \not\equiv a_j \pmod{n}$$

İspat.
(⇒) A bir tam kalan sistemi olsun. $i \neq j$ için $a_i \equiv a_j \pmod{n}$ olduğunu varsayalım.
Teorem 12.1 (a) gereği $a_i \equiv a_i \pmod{n}$'dir. O hâlde a_i tam sayısı, A kümesinin iki farklı elemanına — hem a_i'ye hem a_j'ye — modülo n kongrü olur. Bu, tanımdaki "tam birisine" koşuluyla çelişir.
(⇐) A'nın elemanları ikişer ikişer kongrü olmasın. Her a_i için, Lemma 13.1 gereği

$$a_i \equiv r_i \pmod{n}, \qquad r_i \in \{0, 1, ..., n-1\}$$

olacak biçimde tek türlü belirli bir r_i vardır.
r_i'ler birbirinden farklıdır. *$i \neq j$ için $r_i = r_j$ olsaydı, geçişme gereği*

$$a_i \equiv r_i = r_j \equiv a_j \pmod{n}$$

olurdu; bu, hipoteze aykırıdır.
O hâlde $r_1, ..., r_n$ sayıları, n elemanlı $\{0, 1, ..., n-1\}$ kümesinin birbirinden farklı n elemanıdır. Demek ki

$$\{r_1, r_2, ..., r_n\} = \{0, 1, ..., n-1\}$$

Şimdi herhangi bir m tam sayısı alalım. Lemma 13.1 gereği m, $\{0, ..., n-1\}$ kümesinin tam bir elemanına kongrüdür; bu eleman bir r_i'dir ve dolayısıyla

$$m \equiv r_i \equiv a_i \pmod{n}$$

olur. Başka bir a_j'ye de kongrü olsaydı $a_i \equiv a_j$ olurdu — hipoteze aykırı. O hâlde m, A'nın tam bir elemanına kongrüdür.
■

> **i** İki koşul birden gerekli
>
> Ölçütü kullanırken kümenin **tam n elemanlı** olduğunu doğrulamayı unutmayın. Örneğin $\{0, 1\}$ kümesinin elemanları modülo 5'te kongrü değildir, ama 5 elemanlı olmadığından tam kalan sistemi değildir.
> Kısacası: n eleman + ikişer ikişer kongrü olmama = tam kalan sistemi.

Örnek 13.2 (Bir Tam Kalan Sistemi).

$$\{-19, -11, 18, 22, 62, 82, 91\}$$

kümesinin modülo 7 bir tam kalan sistemi olduğunu gösteriniz.

Çözüm.
Küme 7 elemanlıdır; Teorem 13.1 gereği elemanların ikişer ikişer kongrü olmadığını göstermek yeterlidir. Bunun için her elemanın modülo 7 kalanını hesaplayalım:

$$-19 \equiv 2, -11 \equiv 3, 18 \equiv 4, \qquad 22 \equiv 1 \pmod 7$$
$$62 \equiv 6, \quad 82 \equiv 5, 91 \equiv 0 \pmod 7$$

(Örneğin $-19 + 21 = 2, 62 - 56 = 6$ *ve* $91 = 13 \cdot 7$*'dir.)*
Kalanlar

$$\{2, 3, 4, 1, 6, 5, 0\} = \{0, 1, 2, 3, 4, 5, 6\}$$

biçiminde birbirinden farklı çıktığından elemanlar ikişer ikişer kongrü değildir. O hâlde verilen küme modülo 7 bir tam kalan sistemidir.
■

13.3 Sistemi Bozmayan Dönüşümler

Bir tam kalan sisteminden yeni sistemler üretmenin sistematik bir yolu vardır: bütün elemanları uygun bir sayıyla çarpmak.

Teorem 13.2 (Aralarında Asal Bir Sayıyla Çarpmak). *$1 < n$ sabit bir tam sayı, $\{a_1, a_2, ..., a_n\}$ bir modülo n tam kalan sistemi, $a \in \mathbb{Z}$ ve $\gcd(a, n) = 1$ olsun. Bu durumda*

$$\{aa_1, aa_2, ..., aa_n\}$$

kümesi de bir modülo n tam kalan sistemidir.

İspat.
Teorem 13.1'ü kullanacağız; iki şeyi doğrulamalıyız.
1. Küme n elemanlıdır. *$i \neq j$ için $aa_i \neq aa_j$ olduğunu görelim. Eşit olsalardı, $\gcd(a, n) = 1$ olduğundan $a \neq 0$'dır ve sadeleştirmeyle $a_i = a_j$ bulunurdu — oysa küme n elemanlıdır.*
2. Elemanlar ikişer ikişer kongrü değildir. *$i \neq j$ için*

$$aa_i \equiv aa_j \pmod n$$

olduğunu varsayalım. $\gcd(a, n) = 1$ olduğundan Sonuç 12.1 (1) gereği a çarpanını sadeleştirebiliriz:

$$a_i \equiv a_j \pmod n$$

Ama $\{a_1, ..., a_n\}$ bir tam kalan sistemi olduğundan Teorem 13.1 gereği $i = j$ olmalıdır — çelişki.
İki koşul da sağlandığından $\{aa_1, ..., aa_n\}$ bir tam kalan sistemidir.
■

⚠ Aralarında asallık şart

$n = 6$ ve $a = 2$ alalım. $\{0, 1, 2, 3, 4, 5\}$ bir tam kalan sistemidir, ama ikiyle çarpılmış hâli

$$\{0, 2, 4, 6, 8, 10\}$$

modülo 6'da $\{0, 2, 4, 0, 2, 4\}$ kalanlarını verir; hiçbir tek kalan üretilemez. Burada $\gcd(2, 6) = 2 \neq 1$'dir.

Örnek 13.3 (Yalnızca Çift Sayılardan Oluşan Bir Sistem). Her $1 < n$ tek tam sayısı için, her bir elemanı çift olan bir modülo n tam kalan sistemi bulunduğunu gösteriniz.

Çözüm.
n tek olduğundan $2 \nmid n$'dir; Önerme 9.1 gereği

$$\gcd(2, n) = 1$$

Şimdi negatif olmayan en küçük tam kalan sistemi olan $\{0, 1, \ldots, n-1\}$ kümesini alıp bütün elemanlarını 2 ile çarpalım. Teorem 13.2 gereği

$$\{0, 2, 4, \ldots, 2(n-1)\}$$

kümesi de bir modülo n tam kalan sistemidir. Bu kümenin her elemanı çifttir.
■

Örnek 13.4 (Modülo 9 İçin Örnek). Her bir elemanı çift olan bir modülo 9 tam kalan sistemi örneği veriniz.

Çözüm.
9 tek olduğundan Örnek 13.3'daki kuruluş uygulanabilir. $\{0, 1, \ldots, 8\}$ kümesini 2 ile çarpalım:

$$\{0, 2, 4, 6, 8, 10, 12, 14, 16\}$$

Doğrulayalım; kalanları modülo 9 hesaplayalım:

Eleman	0	2	4	6	8	10	12	14	16
Kalan	0	2	4	6	8	1	3	5	7

Kalanlar 0'dan 8'e kadar bütün değerleri birer kez veriyor; küme 9 elemanlı ve elemanları ikişer ikişer kongrü değil. O hâlde bu bir modülo 9 tam kalan sistemidir ve bütün elemanları çifttir.
■

Örnek 13.5 (Çift Modülde Neden Olmaz?). n çift bir tam sayı olmak üzere, her bir elemanı çift olan bir kümenin **asla** modülo n tam kalan sistemi olamayacağını gösteriniz.

Çözüm.
n çift olsun ve $A = \{a_1, \ldots, a_n\}$ kümesinin bütün elemanlarının çift olduğunu varsayalım.
Herhangi bir a_i için bölme algoritmasını yazalım:

$$a_i = nq_i + r_i, \qquad 0 \leq r_i < n$$

Buradan

$$r_i = a_i - nq_i$$

olur. Sağ taraftaki iki terime bakalım: a_i çifttir ve n çift olduğundan nq_i de çifttir. İki çift sayının farkı çift olduğundan *(bkz. Önerme 2.1)* r_i çifttir.
Demek ki A kümesinin elemanlarının verdiği bütün kalanlar çifttir. Oysa bir tam kalan sisteminin kalanları $\{0, 1, \ldots, n-1\}$ kümesinin **tamamını** vermelidir ve $n > 1$ olduğundan bu kümede 1 gibi tek sayılar da vardır.
Tek bir kalan bile üretilemediğinden A bir tam kalan sistemi olamaz.
■

i İki örneğin birlikte söylediği

Örnek 13.3 ile Örnek 13.5 birlikte tam bir sınıflandırma verir:

> Yalnızca çift sayılardan oluşan bir modülo n tam kalan sistemi vardır **ancak ve ancak** n tek ise.

Bu, Teorem 13.2'deki aralarında asallık koşulunun ne kadar keskin olduğunu gösterir: koşul sağlandığında dönüşüm işler, sağlanmadığında hiçbir şey kurtaramaz.

13.4 Çalışma Problemleri

Alıştırma 13.1 (Tam Kalan Sistemi mi?). Aşağıdaki kümelerin belirtilen modüle göre tam kalan sistemi olup olmadığını belirleyiniz.
a) $\{1, 2, 3, 4, 5\}$, modülo 5
b) $\{-2, -1, 0, 1, 2\}$, modülo 5
c) $\{0, 3, 6, 9, 12, 15\}$, modülo 6
d) $\{1, 5, 9, 13, 17, 21\}$, modülo 6

Alıştırma 13.2 (Öteleme ve Çarpma). $\{a_1, ..., a_n\}$ bir modülo n tam kalan sistemi olsun.
a) Her $b \in \mathbb{Z}$ için $\{a_1 + b, ..., a_n + b\}$ kümesinin de bir tam kalan sistemi olduğunu gösteriniz.
b) $\gcd(a, n) = 1$ ve $b \in \mathbb{Z}$ olmak üzere $\{aa_1 + b, ..., aa_n + b\}$ kümesinin de bir tam kalan sistemi olduğunu gösteriniz.

Alıştırma 13.3 (Bir Tam Kalan Sisteminin Toplamı). $1 < n$ tek bir tam sayı ve $\{a_1, ..., a_n\}$ bir modülo n tam kalan sistemi olsun.

$$a_1 + a_2 + \cdots + a_n \equiv 0 \pmod{n}$$

olduğunu gösteriniz. n çift olduğunda bu sonucun neden bozulduğunu açıklayınız.
İpucu: Toplam, $0 + 1 + \cdots + (n-1) = \frac{n(n-1)}{2}$ sayısına kongrüdür.

14. Taban Gösterimi ve Bölünebilme Kuralları

"Bir sayı, rakamlarının toplamı 3 ile bölünüyorsa 3 ile bölünür" kuralını hepimiz biliriz. Bu kuralın neden doğru olduğu ise nadiren sorulur. Cevap kongrüans dilinde tek satırdır ve aynı fikir bütün bölünebilme kurallarını üretir. Önce sayıların basamaklarla yazılışını sağlam bir temele oturtalım.

14.1 Bir Tabana Göre Yazılış

Teorem 14.1 (Taban Gösterimi). *Her n pozitif tam sayısı ve her $2 \le b$ tam sayısı için*

$$n = d_m b^m + d_{m-1} b^{m-1} + \cdots + d_1 b + d_0, \qquad d_m \neq 0$$

olacak biçimde ***tek türlü belirli*** $d_0, d_1, \ldots, d_m \in \{0, 1, \ldots, b-1\}$ *sayıları vardır.*

İspat.
1. Varlık. *İddiayı n üzerinden güçlü tümevarımla ispatlayalım.*
Başlangıç durumu ($1 \le n < b$). *$m = 0$ ve $d_0 = n$ alalım. $n \ge 1$ olduğundan $d_0 \neq 0$'dır ve $0 \le d_0 < b$ koşulu sağlanır.*
Tümevarım adımı. *$n \ge b$ olsun ve iddianın n'den küçük bütün pozitif tam sayılar için doğru olduğunu varsayalım.*
Bölme algoritmasına göre

$$n = bq + r, \qquad 0 \le r < b$$

yazalım. Burada q pozitiftir (çünkü $n \ge b$) *ve $q < n$'dir* (çünkü $b \ge 2$ olduğundan $q \le n/b \le n/2 < n$). *Güçlü tümevarım hipotezini q'ya uygulayalım:*

$$q = c_k b^k + c_{k-1} b^{k-1} + \cdots + c_0, \qquad c_k \neq 0, \quad 0 \le c_i < b$$

Şimdi bunu $n = bq + r$ eşitliğinde yerine koyalım:

$$n = b\big(c_k b^k + \cdots + c_0\big) + r = c_k b^{k+1} + c_{k-1} b^k + \cdots + c_0 b + r$$

O hâlde $d_0 = r$ ve $i \ge 1$ için $d_i = c_{i-1}$ alınırsa istenen yazılış elde edilir; baş katsayı $d_{k+1} = c_k \neq 0$'dır.
2. Teklik. *Aynı n için iki yazılış olduğunu varsayalım. Her iki yazılışta da b ile bölünen bütün terimleri bir kenara koyup modülo b'ye geçelim:*

$$n \equiv d_0 \pmod b, \qquad n \equiv d_0' \pmod b$$

(çünkü $d_i b^i$ terimleri $i \ge 1$ için b ile bölünür). *Buradan $d_0 \equiv d_0' \pmod b$ olur ve $0 \le d_0, d_0' < b$ olduğundan Lemma 13.1 gereği*

$$d_0 = d_0'$$

bulunur. Şimdi her iki yazılıştan d_0'ı çıkarıp b'ye bölelim:

$$\frac{n - d_0}{b} = d_m b^{m-1} + \cdots + d_1 = d_{m'}' b^{m'-1} + \cdots + d_1'$$

Sol taraf n'den küçük bir pozitif tam sayıdır (ya da sıfırdır). *Aynı akıl yürütmeyi tekrarlayarak $d_1 = d_1'$, $d_2 = d_2'$, ... elde ederiz. Basamak sayıları da eşit olmak zorundadır; aksi hâlde baş katsayılardan biri 0 olurdu.*
■

Tanım 14.1 (b Tabanına Göre Yazılış). Teorem 14.1'ndeki

$$n = d_m b^m + \cdots + d_1 b + d_0$$

yazılışına "n sayısının b tabanına göre yazılışı" denir ve

$$n = (d_m \ldots d_1 d_0)_b$$

gösterimi kullanılır. d_i sayılarına **rakamlar** denir.

Örnek 14.1 (104 Sayısını Üç Tabanında Yazmak). 104 sayısını 3 tabanında yazınız.

Çözüm.
İspattaki yol doğrudan bir algoritma verir: sayıyı ardışık olarak 3'e böler, kalanları biriktiririz.

$$\begin{aligned} 104 &= 3 \cdot 34 + 2 \\ 34 &= 3 \cdot 11 + 1 \\ 11 &= 3 \cdot 3 + 2 \\ 3 &= 3 \cdot 1 + 0 \\ 1 &= 3 \cdot 0 + 1 \end{aligned}$$

Rakamlar, kalanların **ters sırada** okunmasıyla elde edilir:

$$104 = (1\,0\,2\,1\,2)_3$$

(Sağlama: $1 \cdot 81 + 0 \cdot 27 + 2 \cdot 9 + 1 \cdot 3 + 2 = 81 + 18 + 3 + 2 = 104$ ✓*)*
■

i Onluk taban

Günlük hayatta $b = 10$ kullanırız ve tabanı yazmayız. Bundan sonra bir sayının "rakamları" dendiğinde onluk tabandaki rakamları kastedilecektir:

$$N = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_1 \cdot 10 + a_0$$

14.2 Bölünebilme Kurallarının Kaynağı

Bütün bölünebilme kuralları tek bir gözlemden doğar: **10 sayısının modüldeki kalanı ne ise, 10'un kuvvetleri de o kalanın kuvvetlerini verir.** Modül küçük olduğunda bu kalanlar çok basitleşir.

Modül	10'un kalanı	10^k'nin kalanı
2	0	0 ($k \geq 1$ için)
5	0	0 ($k \geq 1$ için)
3	1	1
9	1	1
11	-1	$(-1)^k$

Şimdi bu satırların her birini birer teoreme dönüştürelim.

Teorem 14.2 (Dokuza ve Üçe Bölünebilme). *$1 \leq N$ tam sayısının onluk tabana göre yazılışı*

$$N = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_1 \cdot 10 + a_0$$

ve rakamlar toplamı

$$S = a_0 + a_1 + \cdots + a_m$$

olsun. Bu durumda

$$9 \mid N \Leftrightarrow 9 \mid S, \qquad 3 \mid N \Leftrightarrow 3 \mid S$$

İspat.
Önce 9 *için gösterelim.* $10 = 9 + 1$ *olduğundan*

$$10 \equiv 1 \pmod 9$$

Teorem 12.1 (f) gereği her $k \geq 0$ *için*

$$10^k \equiv 1^k = 1 \pmod 9$$

Şimdi N*'nin yazılışındaki her terime bu bilgiyi uygulayalım. (e) özelliği gereği*

$$a_k 10^k \equiv a_k \cdot 1 = a_k \pmod 9$$

ve (d) özelliğinin toplam kısmıyla bütün terimleri toplarsak

$$N = \sum_{k=0}^{m} a_k 10^k \equiv \sum_{k=0}^{m} a_k = S \pmod 9$$

O hâlde $N \equiv S \pmod 9$*'dur. İki sayı modülo* 9 *kongrü olduğundan biri* 9 *ile bölünüyorsa diğeri de bölünür:*

$$9 \mid N \Leftrightarrow N \equiv 0 \Leftrightarrow S \equiv 0 \Leftrightarrow 9 \mid S \pmod 9$$

3 *için ispat kelimesi kelimesine aynıdır; tek fark* $10 \equiv 1 \pmod 3$ *eşitliğinden başlanmasıdır.*
■

Teorem 14.3 (On Bire Bölünebilme). $1 \leq N$ *tam sayısının onluk tabana göre yazılışı*

$$N = a_m 10^m + \cdots + a_1 \cdot 10 + a_0$$

ve ***alterne basamak toplamı***

$$T = \sum_{k=0}^{m} (-1)^k a_k = a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^m a_m$$

olsun. Bu durumda

$$11 \mid N \Leftrightarrow 11 \mid T$$

İspat.
$10 = 11 - 1$ *olduğundan*

$$10 \equiv -1 \pmod{11}$$

Teorem 12.1 (f) gereği her $k \geq 0$ *için*

$$10^k \equiv (-1)^k \pmod{11}$$

Her terimi a_k *ile çarpıp toplayalım:*

$$N = \sum_{k=0}^{m} a_k 10^k \equiv \sum_{k=0}^{m} (-1)^k a_k = T \pmod{11}$$

$N \equiv T \pmod{11}$ *olduğundan biri* 11 *ile bölünüyorsa diğeri de bölünür.*
■

Önerme 14.1 (İkiye ve Beşe Bölünebilme). $1 \leq N$ *tam sayısının birler basamağı* a_0 *olsun. Bu durumda*

$$2 \mid N \Leftrightarrow 2 \mid a_0, \qquad 5 \mid N \Leftrightarrow 5 \mid a_0$$

Yani bir sayının 2 ile bölünmesi için son rakamının çift, 5 ile bölünmesi için son rakamının 0 veya 5 olması gerek ve yeterlidir.

Bunun nedeni $10 \equiv 0 \pmod 2$ ve $10 \equiv 0 \pmod 5$ olmasıdır: $k \geq 1$ için 10^k terimlerinin hepsi her iki modülde de sıfırdır, geriye yalnızca a_0 kalır.

14.3 Çözümlü Örnekler

Örnek 14.2 (\$5896167376\$ Sayısı \$11\$ ile Bölünür mü?). $N = 5896167376$ sayısının 11 ile bölünüp bölünmediğini belirleyiniz.

Çözüm.
Rakamları **sağdan sola** doğru numaralandıralım:

$$a_0 = 6, a_1 = 7, a_2 = 3, a_3 = 7, a_4 = 6, a_5 = 1, a_6 = 6, a_7 = 9, a_8 = 8, a_9 = 5$$

Alterne toplamı hesaplayalım:

$$\begin{aligned} T &= a_0 - a_1 + a_2 - a_3 + a_4 - a_5 + a_6 - a_7 + a_8 - a_9 \\ &= 6 - 7 + 3 - 7 + 6 - 1 + 6 - 9 + 8 - 5 \\ &= 0 \end{aligned}$$

$11 \mid 0$ olduğundan Teorem 14.3 gereği

$$11 \mid 5896167376$$

■

Örnek 14.3 (\$45634598712\$ Sayısı \$11\$ ile Bölünür mü?). $N = 45634598712$ sayısının 11 ile bölünüp bölünmediğini belirleyiniz; bölünmüyorsa kalanı bulunuz.

Çözüm.
Rakamları sağdan sola numaralandıralım:

$$a_0 = 2, a_1 = 1, a_2 = 7, a_3 = 8, a_4 = 9, a_5 = 5, a_6 = 4, a_7 = 3, a_8 = 6, a_9 = 5, a_{10} = 4$$

Alterne toplam:

$$\begin{aligned} T &= 2 - 1 + 7 - 8 + 9 - 5 + 4 - 3 + 6 - 5 + 4 \\ &= 10 \end{aligned}$$

$11 \nmid 10$ olduğundan sayı 11 ile bölünmez.
Dahası, ispatta $N \equiv T \pmod{11}$ elde etmiştik. $T = 10$ ve $0 \leq 10 < 11$ olduğundan Teorem 12.2 gereği N sayısının 11 ile bölümünden kalan **10**'dur.
■

> **i** Kural yalnızca 'evet/hayır' demiyor
>
> Yukarıdaki örneğin son adımına dikkat ediniz: alterne toplam yalnızca bölünüp bölünmediğini değil, **kalanı da** verir. Aynı şey rakamlar toplamı için de geçerlidir: bir sayının 9 ile bölümünden kalan, rakamları toplamının 9 ile bölümünden kalana eşittir.
> Örneğin $N = 5896167376$ için rakamlar toplamı $S = 58$ ve $58 = 6 \cdot 9 + 4$ olduğundan $N \equiv 4 \pmod 9$'dur.

Örnek 14.4 (Dokuza Bölünebilme Uygulaması). $N = 123456789$ sayısının 9 ve 3 ile bölünüp bölünmediğini belirleyiniz.

Çözüm.
Rakamlar toplamı:

$$S = 1+2+3+4+5+6+7+8+9 = 45$$

$45 = 9 \cdot 5$ olduğundan $9 \mid 45$'tir. Teorem 14.2 gereği

$$9 \mid 123456789$$

$9 \mid N$ ve $3 \mid 9$ olduğundan geçişme gereği $3 \mid N$'dir de.
■

14.4 Çalışma Problemleri

Alıştırma 14.1 (Taban Değiştirme). **a)** 250 sayısını 2, 5 ve 7 tabanlarında yazınız.
b) $(1101101)_2$ sayısını onluk tabanda yazınız.
c) $(2021)_3$ sayısını onluk tabanda yazınız.

Alıştırma 14.2 (Bölünebilme Testleri). Aşağıdaki sayıların 3, 9 ve 11 ile bölünüp bölünmediğini belirleyiniz; bölünmüyorsa kalanları bulunuz.
a) 8 675 309 **b)** 1 234 321 **c)** 999 999 999

Alıştırma 14.3 (Yeni Bir Kural Türetmek). **a)** $10^3 \equiv -1 \pmod 7$ olduğunu gösteriniz.
b) Bu bilgiyi kullanarak 7 ile bölünebilme için bir kural türetiniz: sayıyı sağdan başlayarak üçer basamaklı gruplara ayırıp bu grupları dönüşümlü olarak toplayıp çıkarmak.
c) Kuralınızı 1 000 003 sayısına uygulayınız.
Not: Aynı gözlem 11 ve 13 için de işler; çünkü $1001 = 7 \cdot 11 \cdot 13$'tür.

Alıştırma 14.4 (Herhangi Bir Tabanda Bölünebilme). n sayısı b tabanında $(d_m \ldots d_1 d_0)_b$ biçiminde yazılmış olsun.
a) $(b-1) \mid n$ olması için gerek ve yeter koşulun $(b-1) \mid (d_0 + d_1 + \cdots + d_m)$ olduğunu gösteriniz.
b) $(b+1) \mid n$ olması için gerek ve yeter koşulun $(b+1)$ sayısının alterne rakam toplamını bölmesi olduğunu gösteriniz.
Not: $b = 10$ alındığında (a) şıkkı dokuza, (b) şıkkı on bire bölünebilme kuralını verir.

15. Lineer Kongrüans Denklemleri

Diofant denklemlerinde "$ax + by = c$ denkleminin tam sayı çözümleri" sorusunu yanıtlamıştık. Kongrüans dilinde aynı soru çok daha derli toplu bir biçim alır. Bu bölümde bu biçimi kuracak, çözüm sayısını tam olarak belirleyecek ve modüler aritmetikte "bölme" işleminin karşılığı olan çarpımsal tersi tanımlayacağız.

15.1 Tanım

Tanım 15.1 (Lineer Kongrüans Denklemi). $a, b, n \in \mathbb{Z}$, $1 < n$ ve x bir bilinmeyen olmak üzere

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

ifadesine **bir bilinmeyenli lineer (doğrusal) kongrüans denklemi** denir.
$x_0 \in \mathbb{Z}$ olmak üzere $ax_0 \equiv b \pmod{n}$ ise, x_0 tam sayısına bu denklemin bir **çözümü** denir. En az bir çözümü olan denkleme **çözülebilir**, hiç çözümü olmayana **çözülebilir olmayan** denir.

Örnek 15.1 (İki Örnek).

$$4x \equiv 2 \pmod{6}$$

denklemi çözülebilirdir; $x_0 = 2$ bir çözümdür, çünkü $4 \cdot 2 = 8 \equiv 2 \pmod{6}$'dır.
Buna karşılık

$$2x \equiv 1 \pmod{4}$$

denkleminin hiç çözümü yoktur: $2x$ daima çifttir, dolayısıyla $2x - 1$ tektir ve 4 ile bölünemez.

> **i** Çözümleri nasıl sayacağız?
>
> Sonuç 12.2 gereği bir çözümün bütün kongrüleri de çözümdür. Bu yüzden çözümleri tek tek saymak anlamsızdır; sonsuz çok olurlar.
> Anlaşma şudur: **birbirine modülo n kongrü olmayan** çözümler ayrı sayılır, kongrü olanlar aynı sayılır. "Çözüm sayısı" dediğimizde bunu kastedeceğiz.

15.2 Diofant Denklemleriyle Köprü

Lemma 15.1 (Kongrüans ile Diofant Denklemi Denktir). *$a, b, n \in \mathbb{Z}$ ve $1 < n$ olsun.*

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

lineer kongrüans denklemini çözmek,

$$ax - ny = b$$

Diofant denklemini çözmeye eşdeğerdir.

> ***İspat.***
> *x_0 tam sayısı kongrüansın bir çözümü olsun. Tanım gereği $n \mid ax_0 - b$'dir; yani*
>
> $$ax_0 - b = ny_0$$
>
> *olacak biçimde bir y_0 tam sayısı vardır. Düzenlersek*

$$ax_0 - ny_0 = b$$

elde edilir; yani (x_0, y_0) *ikilisi Diofant denkleminin bir çözümüdür.*
Tersine, (x_0, y_0) *Diofant denkleminin bir çözümü olsun:* $ax_0 - ny_0 = b$*'dir. Buradan*

$$ax_0 - b = ny_0 \Longrightarrow n \mid ax_0 - b \Longrightarrow ax_0 \equiv b \pmod{n}$$

bulunur; yani x_0 *kongrüansın bir çözümüdür.*
■

15.3 Çözülebilirlik ve Çözüm Sayısı

Teorem 15.1 (Lineer Kongrüansın Çözümleri). $a, b, n \in \mathbb{Z}$, $1 < n$ *ve* $d = \gcd(a, n)$ *olsun.*
1. $ax \equiv b \pmod{n}$ *denkleminin çözülebilir olması için gerek ve yeter koşul* $d \mid b$ *olmasıdır.*
2. $d \mid b$ *ise, denklemin modülo* n *birbirine kongrü olmayan tam* ***d tane*** *çözümü vardır.*

İspat.
1. *Lemma 15.1 gereği kongrüansı çözmek* $ax - ny = b$ *Diofant denklemini çözmeye denktir. Önerme 4.2 (3) gereği* $\gcd(a, -n) = \gcd(a, n) = d$*'dir. Teorem 8.1 (1) gereği bu denklem çözülebilirdir ancak ve ancak* $d \mid b$ *ise.*
2. $d \mid b$ *olsun ve* x_0 *bir çözüm olsun. Teorem 8.1 (2) gereği Diofant denkleminin bütün çözümlerinde*

$$x = x_0 + \frac{n}{d}\,t, \qquad t \in \mathbb{Z}$$

olur. (Burada $-n$ katsayısının işareti t'nin işaretine yansır; t bütün tam sayıları dolaştığından bir fark yaratmaz.)
Şimdi bu çözümlerden hangilerinin modülo n ***aynı*** *sayıldığını belirleyelim.* t_1 *ile* t_2 *için elde edilen çözümler için*

$$\begin{aligned} x_0 + \frac{n}{d}t_1 \equiv x_0 + \frac{n}{d}t_2 \pmod{n} &\Leftrightarrow n \,\Big|\, \frac{n}{d}(t_1 - t_2) \\ &\Leftrightarrow \frac{n}{d}(t_1 - t_2) = ns \quad (s \in \mathbb{Z}) \\ &\Leftrightarrow t_1 - t_2 = ds \\ &\Leftrightarrow t_1 \equiv t_2 \pmod{d} \end{aligned}$$

Demek ki iki çözüm modülo n *kongrüdür ancak ve ancak karşılık gelen* t *değerleri modülo* d *kongrü ise.* t *parametresi modülo* d *tam* d *farklı sınıf ürettiğinden — örneğin* $t = 0, 1, \ldots, d-1$ *değerleri bir tam kalan sistemidir — birbirine kongrü olmayan çözüm sayısı tam olarak* d*'dir:*

$$x \equiv x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \ldots, x_0 + \frac{(d-1)n}{d} \pmod{n}$$

■

Sonuç 15.1 (Aralarında Asal Hâlde Tek Çözüm). $a, b, n \in \mathbb{Z}$, $1 < n$ *ve* $\gcd(a, n) = 1$ *olsun. Bu durumda*

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

denkleminin modülo n ***tek*** *çözümü vardır.* x_0 *bu çözümse, bütün tam sayı çözümlerinin kümesi*

$$\{x_0 + nk : k \in \mathbb{Z}\}$$

biçimindedir.

Bu, Teorem 15.1'ın $d = 1$ hâlidir: $1 \mid b$ daima doğrudur, dolayısıyla denklem her zaman çözülebilirdir ve tam 1 çözümü vardır.

15.4 Çözüm Teknikleri

Pratikte iki yol kullanılır. Birincisi Diofant denklemine geçip Öklid algoritmasıyla ilerlemek, ikincisi ise doğrudan kongrüans üzerinde çalışıp katsayıyı ± 1'e indirmektir. İkinci yol genellikle daha kısadır.

i Katsayıyı küçültme oyunu

$ax \equiv b \pmod{n}$ denklemini çözerken, her iki tarafı modülle aralarında asal bir sayıyla çarpmak serbesttir ($\thinspace$Teorem 12.1 (e)$\thinspace$) ve bu işlem tersine çevrilebilir olduğundan çözüm kümesini değiştirmez.
Amaç, a katsayısını 1 veya -1'e indirecek bir çarpan bulmaktır. a'nın modüle yakın bir katını üretecek çarpanlar aranır.

Örnek 15.2 ($35 x \equiv 21 \mod 42 \)$). $35x \equiv 21 \pmod{42}$ denklemini çözünüz.

Çözüm.
Çözülebilirlik. $\gcd(35, 42) = 7$ ve $7 \mid 21$ olduğundan denklem çözülebilirdir; Teorem 15.1 gereği modülo 42'de **7 tane** çözümü vardır.
Sadeleştirme. 7 sayısı 35'i, 21'i ve 42'yi böldüğünden denklemin tamamını 7'ye bölebiliriz — modülün de bölündüğüne dikkat ediniz:

$$5x \equiv 3 \pmod{6}$$

(Bu adımın geçerliliği Teorem 12.3'den gelir.)
Katsayıyı indirme. $\gcd(5, 6) = 1$'dir. Sağ tarafa 6'nın katlarını ekleyerek 5'in katını yakalayalım:

$$3 \equiv 3 + 12 = 15 \pmod{6}$$

Buradan

$$5x \equiv 15 \pmod{6}$$

$\gcd(5, 6) = 1$ olduğundan Sonuç 12.1 (1) gereği 5 sadeleştirilebilir:

$$x \equiv 3 \pmod{6}$$

Çözüm kümesi. Bütün tam sayı çözümleri:

$$\{3 + 6t : t \in \mathbb{Z}\}$$

Modülo 42'ye göre birbirine kongrü olmayan 7 çözüm ise şunlardır:

$$x \equiv 3, 9, 15, 21, 27, 33, 39 \pmod{42}$$

(Sağlama: $35 \cdot 9 = 315 = 7 \cdot 42 + 21$ ✓*)*
■

Örnek 15.3 ($140 x \equiv 133 \mod 301 \)$). $140x \equiv 133 \pmod{301}$ denklemini çözünüz.

Çözüm.
Çözülebilirlik. Öklid algoritmasıyla:

$$\begin{aligned} 301 &= 2 \cdot 140 + 21 \\ 140 &= 6 \cdot 21 + 14 \\ 21 &= 1 \cdot 14 + 7 \\ 14 &= 2 \cdot 7 + 0 \end{aligned}$$

O hâlde $d = \gcd(140, 301) = 7$'dir. $133 = 19 \cdot 7$ olduğundan $7 \mid 133$'tür; denklem çözülebilirdir ve modülo 301'de 7 çözümü vardır.
Sadeleştirme. Denklemi 7'ye bölelim *(modül dâhil)*:

$$20x \equiv 19 \pmod{43}$$

Katsayıyı indirme. $\gcd(20, 43) = 1$'dir. Her iki tarafı 2 ile çarpalım:

$$40x \equiv 38 \pmod{43}$$

$40 = 43 - 3$ olduğundan $40 \equiv -3$'tür:

$$-3x \equiv 38 \pmod{43}$$

Her iki tarafı -1 ile çarpalım ve $-38 \equiv 5 \pmod{43}$ olduğunu kullanalım:

$$3x \equiv 5 \pmod{43}$$

Şimdi 3'ü yok etmek için 14 ile çarpalım *($3 \cdot 14 = 42 \equiv -1$)*:

$$42x \equiv 70 \pmod{43} \Longrightarrow -x \equiv 27 \pmod{43}$$

(çünkü $70 = 43 + 27$). Her iki tarafı -1 ile çarparsak

$$x \equiv -27 \equiv 16 \pmod{43}$$

(Sağlama: $20 \cdot 16 = 320 = 7 \cdot 43 + 19$ ✓*)*
Çözüm kümesi. Bütün tam sayı çözümleri $\{16 + 43t : t \in \mathbb{Z}\}$'dir. Modülo 301'de birbirine kongrü olmayan 7 çözüm:

$$x \equiv 16, 59, 102, 145, 188, 231, 274 \pmod{301}$$

■

Örnek 15.4 (İki Kısa Örnek). Aşağıdaki denklemleri çözünüz.
a) $25x \equiv 15 \pmod{29}$ **b)** $36x \equiv 8 \pmod{102}$

Çözüm.
a) 29 asal ve $29 \nmid 25$ olduğundan $\gcd(25, 29) = 1$'dir; Sonuç 15.1 gereği tek çözüm vardır.
$25 = 29 - 4$ olduğundan $25 \equiv -4 \pmod{29}$'dur:

$$-4x \equiv 15 \pmod{29}$$

Her iki tarafı 7 ile çarpalım *($-4 \cdot 7 = -28 \equiv 1 \pmod{29}$)*:

$$-28x \equiv 105 \pmod{29} \Longrightarrow x \equiv 105 \pmod{29}$$

$105 = 3 \cdot 29 + 18$ olduğundan

$$x \equiv 18 \pmod{29}$$

(Sağlama: $25 \cdot 18 = 450 = 15 \cdot 29 + 15$ ✓*)*
b) $\gcd(36, 102)$ değerini bulalım:

$$102 = 2 \cdot 36 + 30, \qquad 36 = 1 \cdot 30 + 6, \qquad 30 = 5 \cdot 6 + 0$$

O hâlde $d = 6$'dır. Ancak $6 \nmid 8$'dir; Teorem 15.1 (1) gereği denklemin **hiç çözümü yoktur**.
■

15.5 Çarpımsal Ters

Reel sayılarda $ax = b$ denklemini $x = a^{-1}b$ diye çözeriz. Modüler aritmetikte de benzer bir "ters" kavramı vardır — ama her sayının tersi yoktur.

Tanım 15.2 (Çarpımsal Ters). $a, b, n \in \mathbb{Z}$ ve $1 < n$ olsun. Eğer

$$ab \equiv 1 \pmod{n}$$

ise b tam sayısına a'nın **modülo n çarpımsal tersi** denir.

Önerme 15.1 (Tersin Varlığı ve Tekliği). *$a, n \in \mathbb{Z}$ ve $1 < n$ olsun.*
1. *a sayısının modülo n çarpımsal tersinin var olması için gerek ve yeter koşul $\gcd(a, n) = 1$ olmasıdır.*
2. *Ters varsa modülo n'ye göre tek türlü belirlidir.*

Gerçekten de a'nın tersinin var olması, $ax \equiv 1 \pmod{n}$ denkleminin çözülebilir olması demektir. Teorem 15.1 (1) gereği bu, $\gcd(a, n) \mid 1$, yani $\gcd(a, n) = 1$ koşuluna denktir. Bu durumda Sonuç 15.1 gereği çözüm modülo n tektir.

i Tersi olan sayılarla bölme yapabiliriz

$\gcd(a, n) = 1$ olduğunda $ax \equiv b \pmod{n}$ denklemi tek adımda çözülür: her iki tarafı a'nın tersi olan a^{-1} ile çarpmak yeterlidir:

$$x \equiv a^{-1}b \pmod{n}$$

Yani modüler aritmetikte "bölme", tersle çarpmaktır ve yalnızca modülle aralarında asal sayılar için tanımlıdır.

Örnek 15.5 (\$49\$ Sayısının Modülo \$120\$ Tersi). 49 tam sayısının modülo 120 çarpımsal tersini bulunuz.

Çözüm.
Önce tersin var olduğunu doğrulayalım; Öklid algoritmasını uygulayalım:

$$\begin{aligned} 120 &= 2 \cdot 49 + 22 \\ 49 &= 2 \cdot 22 + 5 \\ 22 &= 4 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

$\gcd(49, 120) = 1$ olduğundan Önerme 15.1 gereği ters vardır ve tektir.
Şimdi geriye doğru yerine koyalım:

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 - 2(22 - 4 \cdot 5) \\ &= 9 \cdot 5 - 2 \cdot 22 \\ &= 9(49 - 2 \cdot 22) - 2 \cdot 22 \\ &= 9 \cdot 49 - 20 \cdot 22 \\ &= 9 \cdot 49 - 20(120 - 2 \cdot 49) \\ &= 49 \cdot 49 - 120 \cdot 20 \end{aligned}$$

(Sağlama: $2401 - 2400 = 1$ ✓*)*
Bu eşitliği modülo 120 okuyalım:

$$49 \cdot 49 \equiv 1 \pmod{120}$$

O hâlde 49 sayısının modülo 120 tersi yine **49**'dur.
■

i Kendi tersi olan sayılar

$49^2 = 2401 = 20 \cdot 120 + 1$ olması bir rastlantı değildir: $49^2 - 1 = 48 \cdot 50 = 2400$ ve $120 \mid 2400$'dür. Kendi tersi olan sayılar, $x^2 \equiv 1 \pmod{n}$ denkleminin çözümleridir; bu denklemin kaç çözümü olduğu Wilson teoremi bölümünde tekrar karşımıza çıkacak.

15.6 Diofant Denklemlerini Kongrüansla Çözmek

Lemma 15.1 iki yönlüdür: kongrüansları Diofant denklemine çevirebildiğimiz gibi, Diofant denklemlerini de kongrüansa çevirip çözebiliriz. Katsayılardan biri küçükse bu ikinci yol çok daha hızlıdır.

Örnek 15.6 ($5 x - 53 y = 17$). $5x - 53y = 17$ Diofant denklemini kongrüans kullanarak çözünüz.

Çözüm.
Denklemi modülo 53 okuyalım; $53y$ terimi kaybolur:

$$5x \equiv 17 \pmod{53}$$

$\gcd(5, 53) = 1$ olduğundan tek çözüm vardır. Katsayıyı indirmek için her iki tarafı 21 ile çarpalım ($5 \cdot 21 = 105 = 2 \cdot 53 - 1 \equiv -1$):

$$105x \equiv 357 \pmod{53} \Longrightarrow -x \equiv 357 \pmod{53}$$

$357 = 6 \cdot 53 + 39$ olduğundan $357 \equiv 39$'dur:

$$-x \equiv 39 \Longrightarrow x \equiv -39 \equiv 14 \pmod{53}$$

(Sağlama: $5 \cdot 14 = 70 = 53 + 17$ ✓*)*
$x_0 = 14$ için karşılık gelen y değerini bulalım:

$$5 \cdot 14 - 53y_0 = 17 \Longrightarrow 53y_0 = 70 - 17 = 53 \Longrightarrow y_0 = 1$$

Teorem 8.1 (2) gereği genel çözüm *(burada* $d = \gcd(5, -53) = 1$*)*:

$$x = 14 + 53t, \qquad y = 1 + 5t \qquad (t \in \mathbb{Z})$$

(Sağlama: $5(14 + 53t) - 53(1 + 5t) = 70 + 265t - 53 - 265t = 17$ ✓*)*
■

Örnek 15.7 ($12 x + 25 y = 331$). $12x + 25y = 331$ Diofant denklemini kongrüans kullanarak çözünüz.

Çözüm.
Denklemi modülo 25 okuyalım:

$$12x \equiv 331 \pmod{25}$$

$331 = 13 \cdot 25 + 6$ olduğundan sağ tarafı küçültelim:

$$12x \equiv 6 \pmod{25}$$

$\gcd(12, 25) = 1$'dir. Her iki tarafı 2 ile çarpalım ($12 \cdot 2 = 24 \equiv -1$):

$$24x \equiv 12 \pmod{25} \Longrightarrow -x \equiv 12 \pmod{25} \Longrightarrow x \equiv -12 \equiv 13 \pmod{25}$$

(Sağlama: $12 \cdot 13 = 156 = 6 \cdot 25 + 6$ ✓*)*
$x_0 = 13$ için y değerini bulalım:

$$12 \cdot 13 + 25y_0 = 331 \Longrightarrow 25y_0 = 331 - 156 = 175 \Longrightarrow y_0 = 7$$

Genel çözüm:

$$x = 13 + 25t, \qquad y = 7 - 12t \qquad (t \in \mathbb{Z})$$

Sağlama. Bu çift, her t için denklemi gerçekten sağlar ✓:

$$12(13 + 25t) + 25(7 - 12t) = 156 + 300t + 175 - 300t = 331$$

■

15.7 Çalışma Problemleri

Alıştırma 15.1 (Lineer Kongrüansları Çözme). Aşağıdaki denklemleri çözünüz; çözümü olmayanları belirtiniz ve çözüm sayısını yazınız.
a) $3x \equiv 5 \pmod 7$ **b)** $6x \equiv 15 \pmod{21}$ **c)** $9x \equiv 12 \pmod{21}$
d) $8x \equiv 6 \pmod{14}$ **e)** $4x \equiv 3 \pmod{10}$ **f)** $17x \equiv 3 \pmod{29}$

Alıştırma 15.2 (Çarpımsal Tersler). Aşağıdaki tersleri bulunuz; yoksa nedenini açıklayınız.
a) 7'nin modülo 26 tersi **b)** 10'un modülo 27 tersi
c) 6'nın modülo 9 tersi **d)** 2'nin modülo 31 tersi

Alıştırma 15.3 (Asal Modülde Tersi Bulmanın Bir Yolu). p bir asal sayı, $a, b \in \mathbb{Z}$ ve $\gcd(p, a) = 1$ olsun.
a) İleride ispatlayacağımız Fermat teoremini kullanarak — bu teorem $a^{p-1} \equiv 1 \pmod p$ der — $a^{p-2}b$ tam sayısının

$$ax \equiv b \pmod p$$

denkleminin bir çözümü olduğunu gösteriniz.
b) Bu yöntemle $2x \equiv 1 \pmod{31}$ ve $6x \equiv 5 \pmod{11}$ denklemlerini çözünüz.

Alıştırma 15.4 (Kongrüansla Diofant Denklemleri). Aşağıdaki Diofant denklemlerini kongrüansa çevirerek çözünüz.
a) $7x + 9y = 100$ **b)** $11x - 13y = 5$ **c)** $6x + 15y = 21$

16. Çin Kalan Teoremi

"Bir sayı 9 ile bölündüğünde 7, 10 ile bölündüğünde 4, 13 ile bölündüğünde 12 kalanını veriyor. Bu sayı kaçtır?" Bu tür sorular, birden çok kongrüansın **aynı anda** sağlanmasını ister. Çin kalan teoremi, modüller uygun koşulu sağladığında böyle bir sayının daima var olduğunu ve — büyük bir modüle göre — tek türlü belirli olduğunu söyler.

16.1 Teorem

Teorem 16.1 (Çin Kalan Teoremi). *$1 < n_1, n_2, \ldots, n_r \in \mathbb{Z}$ ikişer ikişer aralarında asal olsun; yani her $i \neq j$ için $\gcd(n_i, n_j) = 1$ olsun. Bu durumda*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

denklem sisteminin bir çözümü vardır ve bu çözüm

$$n = n_1 n_2 \cdots n_r$$

modülüne göre tek türlü belirlidir. x_0 bir çözümse, bütün çözümlerin kümesi

$$\{x_0 + nk : k \in \mathbb{Z}\}$$

biçimindedir.

İspat.
1. Varlık. *Her i için*

$$N_i := \frac{n}{n_i} = n_1 \cdots n_{i-1}\, n_{i+1} \cdots n_r$$

tanımlayalım; yani N_i, çarpımdan n_i çıkarılarak elde edilir.
$\gcd(N_i, n_i) = 1$'dir. *Gerçekten de N_i çarpımındaki her n_j $(j \neq i)$ hipotez gereği n_i ile aralarında asaldır; Teorem 5.3'in tekrarlı uygulanmasıyla çarpımları da n_i ile aralarında asaldır.*
Bu yüzden Sonuç 15.1 gereği her i için

$$N_i x \equiv 1 \pmod{n_i}$$

denkleminin bir x_i çözümü vardır. Şimdi aday çözümümüzü kuralım:

$$x_0 := a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_r N_r x_r$$

Bu sayı bütün denklemleri sağlar. *Bir i sabitleyelim ve x_0'ı modülo n_i inceleyelim. $j \neq i$ olduğunda n_i sayısı N_j çarpımının bir çarpanıdır; dolayısıyla*

$$N_j \equiv 0 \pmod{n_i} \qquad (j \neq i)$$

O hâlde toplamda i dışındaki bütün terimler kaybolur:

$$x_0 \equiv a_i N_i x_i \pmod{n_i}$$

x_i sayısı $N_i x \equiv 1 \pmod{n_i}$ denkleminin çözümü olduğundan $N_i x_i \equiv 1$'dir; buradan

$$x_0 \equiv a_i \cdot 1 = a_i \pmod{n_i}$$

bulunur. Bu her i için geçerli olduğundan x_0 sistemin bir çözümüdür.
2. Teklik. *x_0 ile x_1 sistemin iki çözümü olsun. Her i için*

$$x_0 \equiv a_i \equiv x_1 \pmod{n_i} \Longrightarrow n_i \mid x_0 - x_1$$

*Demek ki $x_0 - x_1$ sayısı $n_1, \ldots, n_r$ sayılarının **ortak katıdır**. Bu sayılar ikişer ikişer aralarında asal olduğundan Teorem 5.2'ın tekrarlı uygulanmasıyla çarpımları da böler:*

$$n = n_1 n_2 \cdots n_r \mid x_0 - x_1$$

Yani $x_0 \equiv x_1 \pmod{n}$'dir; çözüm modülo n tektir.
Son olarak x_0 bir çözümse, $x_0 + nk$ sayıları da her n_i modülünde x_0'a kongrüdür (çünkü $n_i \mid n$)*; dolayısıyla hepsi çözümdür.*
■

i İspat bir algoritma veriyor

İspat yalnızca varlığı göstermez, çözümü **kurar**. Adımlar şunlardır:

1. $n = n_1 n_2 \cdots n_r$ hesaplanır.
2. Her i için $N_i = n/n_i$ bulunur.
3. Her i için $N_i x \equiv 1 \pmod{n_i}$ denklemi çözülüp bir x_i bulunur.
4. $x_0 = \sum_i a_i N_i x_i$ hesaplanır ve modülo n indirgenir.

16.2 Çözümlü Örnekler

Örnek 16.1 (Üç Denklemli Bir Sistem).

$$x \equiv 1 \pmod{3}, \qquad x \equiv 17 \pmod{5}, \qquad x \equiv -15 \pmod{7}$$

sistemini çözünüz.

Çözüm.
Hazırlık. Önce sağ tarafları küçültelim:

$$17 \equiv 2 \pmod{5}, \qquad -15 \equiv -15 + 21 = 6 \pmod{7}$$

Sistem şu hâle gelir:

$$x \equiv 1 \pmod{3}, \qquad x \equiv 2 \pmod{5}, \qquad x \equiv 6 \pmod{7}$$

$3, 5, 7$ ikişer ikişer aralarında asaldır *(üçü de farklı asal)*; teorem uygulanabilir.
1. Adım. $n = 3 \cdot 5 \cdot 7 = 105$.
2. Adım.

$$N_1 = \frac{105}{3} = 35, \qquad N_2 = \frac{105}{5} = 21, \qquad N_3 = \frac{105}{7} = 15$$

3. Adım. Her biri için $N_i x \equiv 1$ denklemini çözelim:

- $35x \equiv 1 \pmod{3}$: $35 \equiv 2 \pmod{3}$ olduğundan $2x \equiv 1 \pmod{3}$; $x_1 = 2$'dir *($2 \cdot 2 = 4 \equiv 1$)*.
- $21x \equiv 1 \pmod{5}$: $21 \equiv 1 \pmod{5}$ olduğundan $x_2 = 1$'dir.
- $15x \equiv 1 \pmod{7}$: $15 \equiv 1 \pmod{7}$ olduğundan $x_3 = 1$'dir.

4. Adım.

$$\begin{aligned} x_0 &= a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 \\ &= 1 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 6 \cdot 15 \cdot 1 \\ &= 70 + 42 + 90 = 202 \end{aligned}$$

Modülo 105 indirgeyelim: $202 - 105 = 97$.

$$x \equiv 97 \pmod{105}$$

(Sağlama: $97 = 32 \cdot 3 + 1$, $97 = 19 \cdot 5 + 2$, $97 = 13 \cdot 7 + 6$ ✓*)*
■

Örnek 16.2 (Belli Bir Aralıktaki Çözümler). 9, 10 ve 13 sayıları ile bölündüğünde sırasıyla 7, 4 ve 12 kalanını veren ve $1 \leq x \leq 3000$ koşuluna uyan tüm x tam sayılarını bulunuz.

Çözüm.
Sistem şudur:

$$x \equiv 7 \pmod{9}, \qquad x \equiv 4 \pmod{10}, \qquad x \equiv 12 \pmod{13}$$

$\gcd(9, 10) = \gcd(9, 13) = \gcd(10, 13) = 1$ olduğundan teorem uygulanabilir.
1. Adım. $n = 9 \cdot 10 \cdot 13 = 1170$.
2. Adım.

$$N_1 = 130, \qquad N_2 = 117, \qquad N_3 = 90$$

3. Adım.

- $130x \equiv 1 \pmod{9}$: $130 = 14 \cdot 9 + 4$ olduğundan $4x \equiv 1 \pmod{9}$. $4 \cdot 7 = 28 \equiv 1 \pmod{9}$ olduğundan $x_1 = 7$'dir.
- $117x \equiv 1 \pmod{10}$: $117 \equiv 7 \pmod{10}$ olduğundan $7x \equiv 1 \pmod{10}$. $7 \cdot 3 = 21 \equiv 1$ olduğundan $x_2 = 3$'tür.
- $90x \equiv 1 \pmod{13}$: $90 = 6 \cdot 13 + 12$ olduğundan $12x \equiv 1 \pmod{13}$. $12 \equiv -1$ olduğundan $-x \equiv 1$, yani $x_3 = 12$'dir.

4. Adım.

$$\begin{aligned} x_0 &= 7 \cdot 130 \cdot 7 + 4 \cdot 117 \cdot 3 + 12 \cdot 90 \cdot 12 \\ &= 6370 + 1404 + 12960 \\ &= 20734 \end{aligned}$$

Modülo 1170 indirgeyelim: $1170 \cdot 17 = 19890$ ve $20734 - 19890 = 844$'tür.

$$x \equiv 844 \pmod{1170}$$

Aralık koşulu. Çözümler $844 + 1170t$ biçimindedir. $1 \leq x \leq 3000$ koşulunu sağlayanlar:

- $t = 0$: $x = 844$
- $t = 1$: $x = 2014$
- $t = 2$: $x = 3184 > 3000$ ✗

O hâlde aranan sayılar **844 ve 2014**'tür.
(Sağlama: $844 = 93 \cdot 9 + 7$, $844 = 84 \cdot 10 + 4$, $844 = 64 \cdot 13 + 12$ ✓*)*
■

Örnek 16.3 (Katsayılı Denklemlerden Oluşan Sistem).

$$5x \equiv 12 \pmod{7}, \qquad 10x \equiv 4 \pmod{11}, \qquad 7x \equiv 16 \pmod{10}$$

sistemini $1000 \leq x \leq 3000$ koşulu altında çözünüz.

Çözüm.
Hazırlık: her denklemi $x \equiv a \pmod{n}$ biçimine getirelim.
Birinci denklem. $12 \equiv 5 \pmod{7}$ olduğundan $5x \equiv 5 \pmod{7}$'dir. $\gcd(5, 7) = 1$ olduğundan Sonuç 12.1 (1) gereği sadeleştirebiliriz:

$$x \equiv 1 \pmod 7$$

İkinci denklem. $10 \equiv -1 \pmod{11}$ olduğundan $-x \equiv 4$, yani

$$x \equiv -4 \equiv 7 \pmod{11}$$

Üçüncü denklem. $16 \equiv 6 \pmod{10}$ olduğundan $7x \equiv 6 \pmod{10}$'dur. Her iki tarafı 3 ile çarpalım *($7 \cdot 3 = 21 \equiv 1$)*:

$$21x \equiv 18 \pmod{10} \Longrightarrow x \equiv 8 \pmod{10}$$

Sistem şu hâle geldi:

$$x \equiv 1 \pmod 7, \qquad x \equiv 7 \pmod{11}, \qquad x \equiv 8 \pmod{10}$$

Çin kalan teoremi. $\gcd(7,11) = \gcd(7,10) = \gcd(10,11) = 1$'dir.

$$n = 7 \cdot 11 \cdot 10 = 770, \qquad N_1 = 110, \quad N_2 = 70, \quad N_3 = 77$$

- $110x \equiv 1 \pmod 7$: $110 = 15 \cdot 7 + 5$ olduğundan $5x \equiv 1 \pmod 7$; $x_1 = 3$'tür *($15 \equiv 1$)*.
- $70x \equiv 1 \pmod{11}$: $70 = 6 \cdot 11 + 4$ olduğundan $4x \equiv 1 \pmod{11}$; $x_2 = 3$'tür *($12 \equiv 1$)*.
- $77x \equiv 1 \pmod{10}$: $77 \equiv 7 \pmod{10}$ olduğundan $7x \equiv 1 \pmod{10}$; $x_3 = 3$'tür *($21 \equiv 1$)*.

Şimdi toplayalım:

$$\begin{aligned} x_0 &= 1 \cdot 110 \cdot 3 + 7 \cdot 70 \cdot 3 + 8 \cdot 77 \cdot 3 \\ &= 330 + 1470 + 1848 \\ &= 3648 \end{aligned}$$

Modülo 770: $770 \cdot 4 = 3080$ ve $3648 - 3080 = 568$'dir.

$$x \equiv 568 \pmod{770}$$

Aralık koşulu. Çözümler $568 + 770t$ biçimindedir:

- $t = 1$: $x = 1338$
- $t = 2$: $x = 2108$
- $t = 3$: $x = 2878$
- $t = 4$: $x = 3648 > 3000$ ✗

Aranan sayılar **1338, 2108 ve 2878**'dir.
■

16.3 Modüller Aralarında Asal Değilse

Çin kalan teoremi modüllerin ikişer ikişer aralarında asal olmasını istiyordu. Bu koşul sağlanmadığında sistem çözülebilir de olabilir, olmayabilir de. Aşağıdaki teorem iki denklemli durumda ölçütü tam olarak verir.

Teorem 16.2 (Aralarında Asal Olmayan Modüller). *$a, b, n, m \in \mathbb{Z}$ ve $1 < n, m$ olsun.*

$$x \equiv a \pmod n, \qquad x \equiv b \pmod m$$

sisteminin bir ortak çözümünün olması için gerek ve yeter koşul

$$\gcd(n,m) \mid a - b$$

olmasıdır. Sistem çözülebilirse, çözüm $\operatorname{lcm}(n,m)$ *modülüne göre tek türlü belirlidir.*

İspat.
Çözülebilirlik. *x bir ortak çözüm olsun. Birinci denklem gereği $x = a + nu$, ikinci denklem gereği $x = b + mv$ olacak biçimde u, v tam sayıları vardır. İkisini eşitleyelim:*

$$a + nu = b + mv \Longrightarrow nu - mv = b - a$$

Demek ki sistemin çözülebilir olması, $nu - mv = b - a$ Diofant denkleminin çözülebilir olmasına denktir. Teorem 8.1 (1) ve Önerme 4.2 (3) gereği bu denklem çözülebilirdir ancak ve ancak

$$\gcd(n, -m) = \gcd(n, m) \mid b - a$$

ise. $\gcd(n, m) \mid b - a$ *ile* $\gcd(n, m) \mid a - b$ *aynı koşuldur.*
Teklik. x_0 *ile* x_1 *iki ortak çözüm olsun. Her iki denklemden*

$$n \mid x_0 - x_1 \qquad \text{ve} \qquad m \mid x_0 - x_1$$

çıkar; yani $x_0 - x_1$ *sayısı* n *ile* m*'nin ortak katıdır. Sonuç 7.1 gereği*

$$\operatorname{lcm}(n, m) \mid x_0 - x_1$$

olur; yani $x_0 \equiv x_1 \pmod{\operatorname{lcm}(n, m)}$*'dir.*
■

i Çin kalan teoremiyle tutarlılık

$\gcd(n, m) = 1$ olduğunda ölçüt kendiliğinden sağlanır *(çünkü* 1 *her sayıyı böler)* ve

$$\operatorname{lcm}(n, m) = \frac{nm}{\gcd(n, m)} = nm$$

olur. Yani Teorem 16.2, iki denklemli durumda Çin kalan teoremini kapsar.

Örnek 16.4 (Ortak Bölenli Modüller). Aşağıdaki sistemlerin çözülebilir olup olmadığını belirleyiniz; çözülebilenleri çözünüz.
a) $x \equiv 3 \pmod 8$ ve $x \equiv 7 \pmod{12}$
b) $x \equiv 3 \pmod 8$ ve $x \equiv 6 \pmod{12}$

Çözüm.
Her iki şıkta da $\gcd(8, 12) = 4$ ve $\operatorname{lcm}(8, 12) = 24$'tür.
a) $a - b = 3 - 7 = -4$ ve $4 \mid -4$ olduğundan sistem çözülebilirdir.
Birinci denklemden $x = 3 + 8u$ yazıp ikincide yerine koyalım:

$$3 + 8u \equiv 7 \pmod{12} \Longrightarrow 8u \equiv 4 \pmod{12}$$

$\gcd(8, 12) = 4$ ve $4 \mid 4$ olduğundan çözülebilir; denklemi 4'e bölelim:

$$2u \equiv 1 \pmod 3$$

$2 \equiv -1 \pmod 3$ olduğundan $-u \equiv 1$, yani $u \equiv -1 \equiv 2 \pmod 3$'tür. Buradan $u = 2 + 3s$ ve

$$x = 3 + 8(2 + 3s) = 19 + 24s$$

O hâlde

$$x \equiv 19 \pmod{24}$$

(Sağlama: $19 = 2 \cdot 8 + 3$ ✓ *ve* $19 = 12 + 7$ ✓*)*
b) $a - b = 3 - 6 = -3$ ve $4 \nmid -3$ olduğundan Teorem 16.2 gereği sistemin **hiç çözümü yoktur**.
Sezgisel açıklama: birinci denklem x'in tek olmasını gerektirir *(çünkü* $3 + 8u$ *daima tektir)*, ikincisi ise çift olmasını *(çünkü* $6 + 12v$ *daima çifttir).*
■

16.4 Çalışma Problemleri

Alıştırma 16.1 (Kongrüans Sistemleri). Aşağıdaki sistemleri çözünüz.
a) $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$
b) $x \equiv 5 \pmod{11}$, $x \equiv 14 \pmod{29}$, $x \equiv 15 \pmod{31}$
c) $3x \equiv 1 \pmod 4$, $4x \equiv 3 \pmod 5$, $5x \equiv 2 \pmod 7$

Alıştırma 16.2 (Bir Uygulama). Bir sepetteki yumurtalar 3'erli sayıldığında 2, 5'erli sayıldığında 3, 7'şerli sayıldığında 2 yumurta artmaktadır. Sepette en az kaç yumurta vardır?

Alıştırma 16.3 (Ortak Bölenli Modüller). Aşağıdaki sistemlerin çözülebilirliğini Teorem 16.2 ile inceleyiniz; çözülebilenleri çözünüz.
a) $x \equiv 4 \pmod 6$ ve $x \equiv 10 \pmod{15}$
b) $x \equiv 1 \pmod 4$ ve $x \equiv 2 \pmod 6$
c) $x \equiv 5 \pmod{12}$ ve $x \equiv 11 \pmod{18}$

Alıştırma 16.4 (Üç Denkleme Genelleme). n_1, n_2, n_3 modülleri ikişer ikişer aralarında asal olmasa bile,

$$x \equiv a_i \pmod{n_i} \qquad (i = 1, 2, 3)$$

sisteminin çözülebilir olması için gerek ve yeter koşulun

$$\gcd(n_i, n_j) \mid a_i - a_j \qquad (\text{her } \; i \neq j \; \text{ için})$$

olduğunu gösteriniz.
İpucu: İlk iki denklemi Teorem 16.2 ile birleştirip tek bir kongrüansa indirgeyiniz, sonra üçüncüyle aynı işlemi tekrarlayınız.

17. Kalan Sınıfları ve Birimler Grubu

Şimdiye kadar kongrüansı bir **bağıntı** olarak kullandık: iki sayının birbirine kongrü olup olmadığını sorduk. Bu bölümde bakış açısını değiştireceğiz. Birbirine kongrü sayıları tek bir nesnede toplayacak ve bu nesneler üzerinde toplama ile çarpma işlemleri tanımlayacağız. Ortaya çıkan yapı, Euler ve Fermat teoremlerini son derece doğal kılacak.

17.1 Kongrüans Bir Denklik Bağıntısıdır

Önerme 17.1 (Kongrüans Denklik Bağıntısıdır). *$1 < n \in \mathbb{Z}$ olmak üzere $\mathbb{Z}$ üzerinde tanımlanan*

$$R = \{(a, b) : a, b \in \mathbb{Z}, a \equiv b \pmod{n}\}$$

*bağıntısı bir **denklik bağıntısıdır**. Her $a \in \mathbb{Z}$ için a'nın denklik sınıfı*

$$\{a + nk : k \in \mathbb{Z}\} = a + n\mathbb{Z}$$

kümesidir.

> ***İspat.***
> *Denklik bağıntısı olmak için üç özellik gerekir; üçü de Teorem 12.1'nde ispatlanmıştı:*
>
> - ***Yansıma.*** *(a) gereği her a için $a \equiv a \pmod{n}$'dir.*
> - ***Simetri.*** *(b) gereği $a \equiv b$ ise $b \equiv a$'dır.*
> - ***Geçişme.*** *(c) gereği $a \equiv b$ ve $b \equiv c$ ise $a \equiv c$'dir.*
>
> *Şimdi a'nın denklik sınıfını belirleyelim. Tanım gereği bu sınıf, a'ya kongrü bütün tam sayılardan oluşur:*
>
> $$[a] = \{x \in \mathbb{Z} : x \equiv a \pmod{n}\}$$
>
> *$x \equiv a \pmod{n}$ olması, $n \mid x - a$, yani $x - a = nk$ olacak biçimde bir k tam sayısının var olması demektir. Buradan $x = a + nk$ bulunur. O hâlde*
>
> $$[a] = \{a + nk : k \in \mathbb{Z}\} = a + n\mathbb{Z}$$
>
> ■

Tanım 17.1 (Kalan Sınıfı). $a + n\mathbb{Z}$ kümesine a tam sayısının **modülo n kalan sınıfı** denir ve kısaca $\overline{a}$ ile de gösterilir.

Sonuç 17.1 (Sınıflar Ne Zaman Aynıdır?). *Her $k, l \in \mathbb{Z}$ için aşağıdakiler geçerlidir:*
i) $k + n\mathbb{Z} = l + n\mathbb{Z} \Leftrightarrow k \equiv l \pmod{n}$
ii) $(k + n\mathbb{Z}) \cap (l + n\mathbb{Z}) = \emptyset \Leftrightarrow k \not\equiv l \pmod{n}$

Bu, denklik bağıntılarının genel özelliğidir: iki denklik sınıfı ya tamamen çakışır ya da hiç kesişmez. Kongrüans dilinde bu, "aynı kalanı veren sayılar aynı sınıftadır" demektir.

⚠ Bir sınıfın birçok adı vardır

$n = 7$ için

$$\overline{3} = \overline{10} = \overline{-4} = \overline{17}$$

Hepsi aynı kümedir: $\{..., -11, -4, 3, 10, 17, ...\}$. Sınıfı adlandırmak için hangi temsilcinin seçildiği önemsizdir; bu yüzden bir işlem tanımlarken **sonucun temsilci seçiminden bağımsız olduğunu** doğrulamak zorundayız. Birazdan tam olarak bunu yapacağız.

Önerme 17.2 (Kalan Sınıfları Kümesi). *$1 < n \in \mathbb{Z}$ olsun. Modülo n kongrüans bağıntısının belirlediği tüm denklik sınıflarının kümesi*

$$\{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, ..., (n-1) + n\mathbb{Z}\}$$

kümesidir. Bu küme $\mathbb{Z}_n$ ile gösterilir.

> ***İspat.***
> *Lemma 13.1 gereği her a tam sayısı $0, 1, ..., n-1$ sayılarından tam birine kongrüdür. O hâlde Sonuç 17.1 (i) gereği*
>
> $$a + n\mathbb{Z} = r + n\mathbb{Z}$$
>
> *olacak biçimde tek türlü belirli bir $r \in \{0, ..., n-1\}$ vardır. Demek ki her sınıf listede bulunur.*
> *Ayrıca listedeki sınıflar birbirinden farklıdır: $0 \leq r < r' \leq n-1$ için $r \not\equiv r' \pmod{n}$ olduğundan Sonuç 17.1 (i) gereği $r + n\mathbb{Z} \neq r' + n\mathbb{Z}$'dir.*
> ■

Örnek 17.1 ($bb(Z)_10$ Kümesi).

$$\mathbb{Z}_{10} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}\}$$

Bu küme 10 elemanlıdır. Örneğin $\overline{3}$ sınıfı, son rakamı 3 olan pozitif tam sayıların hepsini *(ve $-7, -17, ...$ sayılarını)* içerir.

17.2 Sınıflarda Çarpma

Tanım 17.2 (Kalan Sınıflarının Çarpımı). $1 < n \in \mathbb{Z}$ olsun. Modülo n kalan sınıflarının çarpımı

$$(k + n\mathbb{Z})(l + n\mathbb{Z}) := (kl) + n\mathbb{Z}$$

biçiminde tanımlanır *(her $k, l \in \mathbb{Z}$ için)*.

Örnek 17.2 (Bir Çarpım Hesabı). $n = 20$ olsun:

$$(4 + 20\mathbb{Z})(7 + 20\mathbb{Z}) = 28 + 20\mathbb{Z} = 8 + 20\mathbb{Z}$$

Son eşitlikte $28 \equiv 8 \pmod{20}$ olmasını kullandık.

Tanımda bir tehlike vardır: çarpımı hesaplamak için sınıflardan **birer temsilci** seçtik. Başka temsilciler seçseydik farklı bir sonuç çıkabilir miydi? Aşağıdaki önerme çıkmayacağını söyler.

Önerme 17.3 (Çarpma İyi Tanımlıdır). *$1 < n \in \mathbb{Z}$ olsun. Her $a, b, c, d \in \mathbb{Z}$ için, eğer*

$$a + n\mathbb{Z} = c + n\mathbb{Z} \qquad \text{ve} \qquad b + n\mathbb{Z} = d + n\mathbb{Z}$$

ise

$$(ab) + n\mathbb{Z} = (cd) + n\mathbb{Z}$$

İspat.
Sonuç 17.1 (i) gereği hipotez şu demektir:

$$a \equiv c \pmod{n} \qquad \text{ve} \qquad b \equiv d \pmod{n}$$

Teorem 12.1 (d) gereği kongrüanslar çarpılabilir:

$$ab \equiv cd \pmod{n}$$

Yine Sonuç 17.1 (i) gereği bu, $(ab) + n\mathbb{Z} = (cd) + n\mathbb{Z}$ *demektir.*
■

i Neden bu kadar önemli?

İyi tanımlılık olmasaydı $\mathbb{Z}_n$ üzerinde çarpma diye bir işlem **olmazdı**: aynı iki sınıf, seçilen temsilcilere göre farklı sonuçlar verirdi ve hiçbir hesap güvenilir olmazdı.
Aynı gerekçeyle toplama da iyi tanımlıdır; ispatı Teorem 12.1 (d)'nin toplam kısmıyla birebir aynıdır.

17.3 Birim Sınıflar

Her sınıfın çarpımsal tersi yoktur. Örneğin $\mathbb{Z}_{10}$'da $\overline{2} \cdot \overline{x} = \overline{1}$ eşitliğini sağlayan bir $\overline{x}$ yoktur; çünkü $2x \equiv 1 \pmod{10}$ denklemi çözülemez. Tersi olan sınıfları ayırt etmek, bu bölümün geri kalanının konusudur.

Tanım 17.3 (Primitif (İlkel) Kalan Sınıfı). $a, n \in \mathbb{Z}$ ve $1 < n$ olsun. Eğer

$$\gcd(a, n) = 1$$

ise $a + n\mathbb{Z}$ kalan sınıfına bir **modülo n primitif (ilkel) kalan sınıfı** — kısaca **birim sınıf** — denir.

Önerme 17.4 (Birim Olmak İyi Tanımlıdır). *Primitif kalan sınıfı kavramı temsilci seçiminden bağımsızdır: eğer* $a + n\mathbb{Z} = b + n\mathbb{Z}$ *ise*

$$\gcd(a, n) = \gcd(b, n)$$

Gerçekten de $a + n\mathbb{Z} = b + n\mathbb{Z}$ olması $a \equiv b \pmod{n}$ demektir; Önerme 12.1 gereği bu iki en büyük ortak bölen eşittir.

Tanım 17.4 (Birimler Kümesi). $1 < n \in \mathbb{Z}$ olmak üzere, $\mathbb{Z}_n$ içindeki tüm primitif kalan sınıflarının kümesi

$$U(\mathbb{Z}_n)$$

ile gösterilir.

Örnek 17.3 (Birim Kümelerine Örnekler). **a)** $U(\mathbb{Z}_{10})$ kümesini bulunuz.
b) p bir asal sayı olmak üzere $U(\mathbb{Z}_p)$ kümesini belirleyiniz.
c) $U(\mathbb{Z}_{12})$ kümesini bulunuz.

Çözüm.
a) $0, 1, \ldots, 9$ temsilcilerinden hangilerinin 10 ile aralarında asal olduğuna bakalım:

$$\gcd(1, 10) = \gcd(3, 10) = \gcd(7, 10) = \gcd(9, 10) = 1$$

Geri kalanlar için gcd değeri 2, 5 veya 10 çıkar. O hâlde

$$U(\mathbb{Z}_{10}) = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$$

Bu küme 4 elemanlıdır.
b) p asal olduğundan Önerme 9.1 gereği $\gcd(a,p)$ değeri, $p \mid a$ ise p, aksi hâlde 1'dir. Temsilciler $0, 1, \ldots, p-1$ arasında p ile bölünen tek sayı 0'dır. O hâlde

$$U(\mathbb{Z}_p) = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}$$

Yani sıfır sınıfı dışındaki **bütün** sınıflar birimdir; bu küme $p-1$ elemanlıdır.
c) 12 ile aralarında asal olan $0 \leq a < 12$ sayıları $1, 5, 7, 11$'dir:

$$U(\mathbb{Z}_{12}) = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$$

■

17.4 Birimler Bir Grup Oluşturur

Teorem 17.1 (Birimler Grubu). *$1 < n \in \mathbb{Z}$ olsun. Bu durumda $U(\mathbb{Z}_n)$ kümesi, kalan sınıflarının çarpımı işlemine göre bir **grup** oluşturur.*

İspat.
Önerme 17.3'de çarpma işleminin iyi tanımlı olduğunu görmüştük. Şimdi grup aksiyomlarını doğrulayalım.
1. Kapalılık. *$\overline{a}, \overline{b} \in U(\mathbb{Z}_n)$ olsun; yani $\gcd(a,n) = 1$ ve $\gcd(b,n) = 1$'dir. Teorem 5.3 gereği*

$$\gcd(ab, n) = 1$$

olur; yani $\overline{a}\,\overline{b} = \overline{ab} \in U(\mathbb{Z}_n)$'dir.
2. Birleşme özelliği. *Tam sayılarda çarpma birleşmeli olduğundan*

$$\big(\overline{a}\,\overline{b}\big)\overline{c} = \overline{(ab)c} = \overline{a(bc)} = \overline{a}\big(\overline{b}\,\overline{c}\big)$$

3. Birim eleman. *$\gcd(1,n) = 1$ olduğundan $\overline{1} \in U(\mathbb{Z}_n)$'dir. Ayrıca her $\overline{a}$ için*

$$\overline{1} \cdot \overline{a} = \overline{a} = \overline{a} \cdot \overline{1}$$

Özel olarak $U(\mathbb{Z}_n) \neq \emptyset$'dır.
4. Ters eleman. *$\overline{a} \in U(\mathbb{Z}_n)$ olsun; $\gcd(a,n) = 1$'dir. Önerme 15.1 gereği*

$$ab \equiv 1 \pmod{n}$$

olacak biçimde bir b tam sayısı vardır; yani $\overline{a}\,\overline{b} = \overline{1}$'dir.
Geriye $\overline{b}$ sınıfının da bir birim olduğunu, yani $\gcd(b,n) = 1$ olduğunu göstermek kalıyor. $ab \equiv 1 \pmod{n}$ olduğundan

$$ab - 1 = nk \Longrightarrow ab - nk = 1$$

olacak biçimde bir k tam sayısı vardır. Sol tarafta b ile n'nin bir doğrusal birleşimi vardır ve değeri 1'dir; Sonuç 4.3 gereği $\gcd(b,n) = 1$'dir.
Dört aksiyom da sağlandığından $U(\mathbb{Z}_n)$ bir gruptur.
■

> **i** Grup olmak neyi garanti eder?
>
> Grup yapısının en somut faydası **sadeleştirmedir**: bir grupta $xy = xz$ ise x'in tersiyle çarparak $y = z$ elde edilir. $U(\mathbb{Z}_n)$ bağlamında bu, tam olarak Sonuç 12.1 (1)'in söylediği şeydir.
> İkinci fayda, sonlu gruplarla ilgili genel teoremlerin doğrudan uygulanabilmesidir. Nitekim Euler teoremi, bu grubun eleman sayısıyla ilgili bir sonuçtan başka bir şey değildir — bunu Euler teoremi bölümünde göreceğiz.

i İleriye bir not: grubun mertebesi

$U(\mathbb{Z}_n)$ kümesinin eleman sayısı, tanımı gereği

$$|U(\mathbb{Z}_n)| = \#\{a \in \{1, \ldots, n\} : \gcd(a, n) = 1\}$$

sayısıdır. Bu sayıya **Euler'in ϕ fonksiyonu** denir ve $\phi(n)$ ile gösterilir. Az önceki örneklerde

$$\phi(10) = 4, \qquad \phi(12) = 4, \qquad \phi(p) = p - 1$$

bulmuştuk. Bu fonksiyonu ve özelliklerini kendi bölümünde ayrıntılı inceleyeceğiz.

Örnek 17.4 ($U \(bb(Z)_8 \)$ İçin Çarpım Tablosu). $U(\mathbb{Z}_8)$ kümesini bulunuz ve çarpım tablosunu yazınız.

Çözüm.
8 ile aralarında asal olan $0 \leq a < 8$ sayıları $1, 3, 5, 7$'dir:

$$U(\mathbb{Z}_8) = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$$

Çarpımları modülo 8 hesaplayalım:

$\cdot$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{1}$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{7}$	$\overline{5}$
$\overline{5}$	$\overline{5}$	$\overline{7}$	$\overline{1}$	$\overline{3}$
$\overline{7}$	$\overline{7}$	$\overline{5}$	$\overline{3}$	$\overline{1}$

(Örneğin $3 \cdot 5 = 15 \equiv 7$ ve $5 \cdot 7 = 35 \equiv 3 \pmod 8$'dir.)
Tablonun köşegeninde yalnızca $\overline{1}$ görünüyor: bu grupta **her elemanın karesi birimdir**, yani her eleman kendi tersidir. Nitekim $1^2 = 1, 3^2 = 9 \equiv 1, 5^2 = 25 \equiv 1, 7^2 = 49 \equiv 1 \pmod 8$'dir.
■

17.5 Çalışma Problemleri

Alıştırma 17.1 (Kalan Sınıflarıyla Hesap). **a)** $\mathbb{Z}_6$ kümesinin elemanlarını yazınız ve çarpım tablosunu oluşturunuz.
b) $\mathbb{Z}_6$ içinde $\overline{2} \cdot \overline{3} = \overline{0}$ olduğunu gözlemleyiniz. İkisi de sıfırdan farklı olan iki sınıfın çarpımının sıfır olabilmesi, n hakkında ne söyler?
c) $\mathbb{Z}_n$ içinde sıfırdan farklı iki sınıfın çarpımının hiçbir zaman sıfır olmaması için gerek ve yeter koşulun n'nin asal olması olduğunu gösteriniz.

Alıştırma 17.2 (Birimler Kümeleri). Aşağıdaki kümeleri belirleyiniz ve eleman sayılarını yazınız.
a) $U(\mathbb{Z}_9)$ **b)** $U(\mathbb{Z}_{15})$ **c)** $U(\mathbb{Z}_{16})$ **d)** $U(\mathbb{Z}_7)$

Alıştırma 17.3 (Tersleri Bulma). $U(\mathbb{Z}_{15})$ kümesindeki her elemanın çarpımsal tersini bulunuz. Kendi tersi olan elemanları belirleyiniz.

Alıştırma 17.4 (Birimlerin Çarpımı). $1 < n$ ve $\{a_1, \ldots, a_k\}$ kümesi $U(\mathbb{Z}_n)$ elemanlarının temsilcileri olsun. $\gcd(a, n) = 1$ olmak üzere

$$\{aa_1, aa_2, \ldots, aa_k\}$$

kümesinin de aynı birim sınıfları — belki farklı sırayla — temsil ettiğini gösteriniz.
İpucu: Teorem 13.2'in ispatındaki fikri kullanınız; kapalılık ve sadeleştirme yeterlidir. *(Bu gözlem, Euler teoreminin ispatının çekirdeğidir.)*

18. Fermat Teoremi ve Sözde-Asal Sayılar

Elimizde artık büyük kuvvetlerin kalanlarını hesaplamak için bir yöntem var: modülde 1 veya -1 veren bir kuvvet aramak. Ama bu arama deneme yanılmaya dayanıyordu. Fermat'nın küçük teoremi, modül asal olduğunda böyle bir kuvvetin **nerede olduğunu** doğrudan söyler ve aramaya son verir.

18.1 Fermat Teoremi

Teorem 18.1 (Fermat'nın Küçük Teoremi). *p bir asal sayı ve $a \in \mathbb{Z}$ olsun. Eğer $p \nmid a$ ise*

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

İspat.
$p \nmid a$ olduğundan Önerme 9.1 gereği $\gcd(a, p) = 1$'dir.
Şimdi şu $p-1$ sayıyı göz önüne alalım:

$$a \cdot 1, \quad a \cdot 2, \quad \ldots, \quad a \cdot (p-1)$$

1. Hiçbiri p ile bölünmez. *$1 \le i \le p-1$ olsun. $p \nmid a$ ve $p \nmid i$'dir (çünkü $0 < i < p$). Teorem 9.1 gereği bir asal, bölmediği iki sayının çarpımını da bölemez; o hâlde $p \nmid ai$'dir.*
2. İkişer ikişer kongrü değildirler. *$1 \le i < j \le p-1$ için*

$$ai \equiv aj \pmod{p}$$

olduğunu varsayalım. $\gcd(a, p) = 1$ olduğundan Sonuç 12.1 (1) gereği a sadeleştirilebilir:

$$i \equiv j \pmod{p}$$

Ama $0 < j - i < p$ olduğundan $p \nmid j - i$'dir — çelişki.
3. Sonuç: kalanlar bir permütasyondur. *Her ai sayısının modülo p kalanı, 1 ile $p-1$ arasındadır* (1. adım gereği 0 olamaz). *Bu $p-1$ kalan ikişer ikişer farklı olduğundan* (2. adım), *$\{1, 2, \ldots, p-1\}$ kümesinin elemanlarını bir sırayla verirler.*
Şimdi bütün bu sayıları çarpalım. Sol taraf ile sağ taraf aynı kalanları — belki farklı sırada — içerdiğinden

$$(a \cdot 1)(a \cdot 2)\cdots\big(\,a(p-1)\,\big) \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}$$

Sol taraftaki a çarpanlarını toplayalım:

$$a^{p-1}\,(p-1)! \equiv (p-1)! \pmod{p}$$

4. Sadeleştirme. *$(p-1)!$ sayısı $1, 2, \ldots, p-1$ çarpanlarından oluşur ve hiçbiri p ile bölünmez; Sonuç 9.2 gereği $p \nmid (p-1)!$'dir. O hâlde Sonuç 12.1 (2) gereği $(p-1)!$ sadeleştirilebilir:*

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

■

Sonuç 18.1 (Fermat Teoreminin Kısıtsız Biçimi). *p bir asal sayı olmak üzere, **her** $a \in \mathbb{Z}$ için*

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

Gerçekten de iki durum vardır. $p \mid a$ ise her iki taraf da $\equiv 0 \pmod{p}$'dir. $p \nmid a$ ise Teorem 18.1 gereği $a^{p-1} \equiv 1$'dir; her iki tarafı a ile çarparsak $a^p \equiv a$ bulunur.

i Hangi biçimi kullanmalı?

İki biçim arasındaki fark önemlidir:

- $a^{p-1} \equiv 1 \pmod{p}$ — kullanışlı olan budur, ama $p \nmid a$ koşulunu gerektirir.
- $a^{p} \equiv a \pmod{p}$ — koşulsuzdur, ama sadeleştirilmiş bilgi taşımaz.

Kalan hesaplarında birincisi, teorik ispatlarda çoğunlukla ikincisi kullanılır.

18.2 Kuvvet Hesaplarına Uygulama

i Standart hesap şablonu

$a^N \bmod p$ hesabı artık üç adımdır:

1. $\gcd(a, p) = 1$ olduğunu doğrula.
2. Üssü $p-1$'e böl: $N = (p-1)q + r$.
3. $a^N = (a^{p-1})^q a^r \equiv a^r \pmod{p}$ yaz ve küçük olan a^r'yi hesapla.

Örnek 18.1 (8^138 Sayısının 13 ile Bölümünden Kalan). 8^{138} tam sayısının 13 ile bölünmesinden elde edilen kalanı bulunuz.

Çözüm.
13 asaldır ve $13 \nmid 8$'dir; Teorem 18.1 uygulanabilir:

$$8^{12} \equiv 1 \pmod{13}$$

Üssü 12'ye bölelim:

$$138 = 12 \cdot 11 + 6$$

Buradan

$$8^{138} = (8^{12})^{11} \cdot 8^6 \equiv 1^{11} \cdot 8^6 = 8^6 \pmod{13}$$

Geriye 8^6'yı hesaplamak kaldı. Küçük adımlarla ilerleyelim:

$$8^2 = 64 = 4 \cdot 13 + 12 \equiv 12 \equiv -1 \pmod{13}$$

O hâlde

$$8^6 = (8^2)^3 \equiv (-1)^3 = -1 \equiv 12 \pmod{13}$$

$0 \leq 12 < 13$ olduğundan aranan kalan **12**'dir.
■

Örnek 18.2 (Bir Bölünebilme İddiası). $\gcd(n, 35) = 1$ koşulunu sağlayan her n tam sayısı için

$$n^{12} \equiv 1 \pmod{35}$$

olduğunu gösteriniz.

Çözüm.
$35 = 5 \cdot 7$ ve $\gcd(5, 7) = 1$'dir. Teorem 5.2 gereği $5 \mid n^{12} - 1$ ve $7 \mid n^{12} - 1$ olduğunu ayrı ayrı göstermek yeterlidir.
Modülo 5. $\gcd(n, 35) = 1$ olduğundan $5 \nmid n$'dir. Teorem 18.1 gereği

$$n^4 \equiv 1 \pmod{5}$$

Her iki tarafın küpünü alalım:

$$n^{12} = \left(n^4\right)^3 \equiv 1 \pmod 5$$

Modülo 7. Benzer biçimde $7 \nmid n$'dir ve Teorem 18.1 gereği

$$n^6 \equiv 1 \pmod 7 \Longrightarrow n^{12} = \left(n^6\right)^2 \equiv 1 \pmod 7$$

Birleştirme. $5 \mid n^{12} - 1$, $7 \mid n^{12} - 1$ ve $\gcd(5, 7) = 1$ olduğundan

$$35 \mid n^{12} - 1 \qquad \text{yani} \qquad n^{12} \equiv 1 \pmod{35}$$

■

18.3 Asallık Testi Olarak Fermat

Sonuç 18.1'in karşıt tersi, bir sayının asal **olmadığını** göstermenin pratik bir yolunu verir: eğer $a^n \not\equiv a \pmod n$ olacak bir a bulunursa, n asal olamaz — ve bunun için n'yi çarpanlarına ayırmaya hiç gerek yoktur.

Örnek 18.3 (117 Asal mıdır?). $2^{117} \equiv 44 \pmod{117}$ olduğunu gösteriniz ve buradan 117 sayısının asal olmadığı sonucunu çıkarınız.

Çözüm.
$117 = 9 \cdot 13$ olduğunu kullanacağız *(bu bilgi yalnızca hesabı kolaylaştırmak içindir; testin kendisi çarpanlara ayırma gerektirmez).*
Modülo 9. 2'nin kuvvetlerini hesaplayalım:

$$2^1 \equiv 2, \quad 2^2 \equiv 4, \quad 2^3 \equiv 8, \quad 2^4 \equiv 7, \quad 2^5 \equiv 5, \quad 2^6 \equiv 1 \pmod 9$$

$117 = 6 \cdot 19 + 3$ olduğundan

$$2^{117} = \left(2^6\right)^{19} \cdot 2^3 \equiv 2^3 = 8 \pmod 9$$

Modülo 13. 13 asal ve $13 \nmid 2$ olduğundan Teorem 18.1 gereği $2^{12} \equiv 1 \pmod{13}$'tür. $117 = 12 \cdot 9 + 9$ olduğundan

$$2^{117} \equiv 2^9 \pmod{13}$$

$2^9 = 512 = 39 \cdot 13 + 5$ olduğundan

$$2^{117} \equiv 5 \pmod{13}$$

Birleştirme (Çin kalan teoremi). Sistem şudur:

$$x \equiv 8 \pmod 9, \qquad x \equiv 5 \pmod{13}$$

$x = 8 + 9k$ yazıp ikinci denklemde yerine koyalım:

$$8 + 9k \equiv 5 \pmod{13} \Longrightarrow 9k \equiv -3 \equiv 10 \pmod{13}$$

$9 \cdot 3 = 27 \equiv 1 \pmod{13}$ olduğundan 9'un tersi 3'tür; her iki tarafı 3 ile çarpalım:

$$k \equiv 30 \equiv 4 \pmod{13}$$

$k = 4$ için $x = 8 + 36 = 44$ bulunur:

$$2^{117} \equiv 44 \pmod{117}$$

Sonuç. 117 asal olsaydı Sonuç 18.1 gereği $2^{117} \equiv 2 \pmod{117}$ olması gerekirdi. Oysa

$$44 \not\equiv 2 \pmod{117}$$

O hâlde **117 asal değildir**.
(Nitekim $117 = 9 \cdot 13$*'tür.)*
■

18.4 Testin Tersi Neden Çalışmaz?

Fermat testinin bir sayının asal olmadığını gösterdiğini gördük. Peki test **geçilirse** sayı asal mıdır? Yani

$$n \mid 2^n - 2 \Longrightarrow n \quad \text{asaldır}$$

önermesi doğru mudur? Cevap hayırdır ve karşı örnek şaşırtıcı biçimde küçüktür.

Lemma 18.1 (İki Asalın Çarpımına Geçiş). *$a \in \mathbb{Z}$ ve $p \neq q$ iki farklı asal sayı olsun. Eğer*

$$a^p \equiv a \pmod{q} \qquad \text{ve} \qquad a^q \equiv a \pmod{p}$$

ise

$$a^{pq} \equiv a \pmod{pq}$$

İspat.
Modülo q. *Hipotez gereği $a^p \equiv a \pmod{q}$'dur. Her iki tarafın q'uncu kuvvetini alalım:*

$$a^{pq} = (a^p)^q \equiv a^q \pmod{q}$$

Öte yandan q asal olduğundan Sonuç 18.1 gereği $a^q \equiv a \pmod{q}$'dur. Geçişme ile

$$a^{pq} \equiv a \pmod{q}$$

Modülo p. *Simetrik biçimde, hipotezdeki $a^q \equiv a \pmod{p}$ eşitliğinin p'inci kuvvetini alalım:*

$$a^{pq} = (a^q)^p \equiv a^p \pmod{p}$$

ve Sonuç 18.1 gereği $a^p \equiv a \pmod{p}$ olduğundan

$$a^{pq} \equiv a \pmod{p}$$

Birleştirme. *$p \mid a^{pq} - a$ ve $q \mid a^{pq} - a$'dır. $p \neq q$ farklı asallar olduğundan Sonuç 9.1 gereği $\gcd(p, q) = 1$'dir; Teorem 5.2 gereği*

$$pq \mid a^{pq} - a \qquad \text{yani} \qquad a^{pq} \equiv a \pmod{pq}$$

■

Örnek 18.4 (\$341\$ Testi Geçer Ama Asal Değildir). $341 = 11 \cdot 31$ olduğunu ve buna rağmen

$$2^{341} \equiv 2 \pmod{341}$$

olduğunu gösteriniz.

Çözüm.
Lemma 18.1'ü $p = 11$, $q = 31$ ve $a = 2$ ile uygulayacağız. İki koşulu doğrulamalıyız.
Koşul 1: $2^{11} \equiv 2 \pmod{31}$.

$$2^5 = 32 \equiv 1 \pmod{31}$$

olduğundan

$$2^{11} = 2 \cdot (2^5)^2 \equiv 2 \cdot 1 = 2 \pmod{31}$$

Koşul 2: $2^{31} \equiv 2 \pmod{11}$.
11 asal ve $11 \nmid 2$ olduğundan Teorem 18.1 gereği $2^{10} \equiv 1 \pmod{11}$'dir. Buradan

$$2^{31} = 2 \cdot (2^{10})^3 \equiv 2 \cdot 1 = 2 \pmod{11}$$

Sonuç. Lemma 18.1 gereği

$$2^{341} = 2^{11 \cdot 31} \equiv 2 \pmod{11 \cdot 31} = \pmod{341}$$

Yani $341 \mid 2^{341} - 2$'dir. Buna rağmen $341 = 11 \cdot 31$ olduğundan 341 asal **değildir**.
■

Tanım 18.1 (Sözde-Asal Sayı). $1 < n$ asal olmayan bir tam sayı olsun. Eğer

$$n \mid 2^n - 2$$

ise n sayısına bir **sözde-asal sayı** denir.

Örnek 18.5 (İlk Sözde-Asal). Örnek 18.4 gereği 341 bir sözde-asal sayıdır. Bu, en küçük sözde-asal sayıdır.

18.5 Sözde-Asallar Sonsuzdur

Sözde-asallar birkaç istisna olsaydı Fermat testi pratikte yine de güvenilir olurdu. Ne yazık ki durum böyle değildir.

Teorem 18.2 (Sonsuz Çoklukta Sözde-Asal Vardır). *Sonsuz sayıda sözde-asal sayı vardır.*

İspat.
Aşağıdaki iddiayı ispatlarsak sonuç gelir.

> ***İddia.*** *n bir tek sözde-asal sayı ise, $M_n := 2^n - 1$ sayısı da n'den büyük bir tek sözde-asal sayıdır.*

1. M_n tektir. *2^n çift olduğundan $2^n - 1$ tektir.*
2. M_n asal değildir. *n sözde-asal olduğundan asal değildir; o hâlde*

$$n = r \cdot s, \qquad 1 < r \le s < n$$

olacak biçimde r, s tam sayıları vardır. $r \mid n$ olduğundan Örnek 3.7 gereği

$$2^r - 1 \mid 2^n - 1 = M_n$$

Ayrıca $1 < r < n$ olduğundan

$$1 < 2^r - 1 < 2^n - 1 = M_n$$

Demek ki M_n sayısının 1 ile kendisinden farklı bir pozitif böleni vardır; asal değildir.
3. $M_n \mid 2^{M_n} - 2$. *n sözde-asal olduğundan $n \mid 2^n - 2$'dir; yani*

$$2^n - 2 = nk$$

olacak biçimde bir k pozitif tam sayısı vardır. Şimdi $2^{M_n - 1}$ ifadesini hesaplayalım:

$$2^{M_n - 1} = 2^{(2^n - 1) - 1} = 2^{2^n - 2} = 2^{nk} = (2^n)^k$$

Buradan

$$2^{M_n - 1} - 1 = (2^n)^k - 1$$

olur. Çarpanlara ayırma özdeşliği gereği (bkz. Alıştırma 1.2)

$$(2^n)^k - 1 = (2^n - 1)\left((2^n)^{k-1} + \cdots + 2^n + 1\right)$$

Sağ taraftaki ilk çarpan tam olarak M_n'dir. O hâlde

$$M_n \mid 2^{M_n-1} - 1$$

Her iki tarafı 2 ile çarparsak

$$M_n \mid 2^{M_n} - 2$$

bulunur. (Burada M_n tek olduğundan 2 ile çarpmak bölünebilmeyi bozmaz; daha doğrusu $2^{M_n} - 2 = 2(2^{M_n-1} - 1)$ eşitliğini kullandık.)
4. $\boldsymbol{M_n > n}$. *Alıştırma 1.3 gereği her $2 < n$ için $n + 1 < 2^n$'dir; buradan*

$$n < 2^n - 1 = M_n$$

İddia ispatlandı.
Sonuç. 341 *bir tek sözde-asal sayıdır* (Örnek 18.4). *İddiayı tekrar tekrar uygularsak*

$$341 < M_{341} < M_{M_{341}} < \cdots$$

biçiminde, kesin artan sonsuz bir tek sözde-asal sayı dizisi elde ederiz. O hâlde sözde-asal sayılar sonsuzdur.
■

i Fermat testi yine de değerlidir

Sözde-asalların sonsuz olması testi işe yaramaz kılmaz. Bunun iki nedeni vardır:

1. Sözde-asallar **seyrektir**: 10^{10}'a kadar yaklaşık 455 milyon asal varken, yalnızca 14884 sözde-asal vardır.
2. Taban değiştirilebilir. 341 sayısı 2 tabanında testi geçer ama 3 tabanında geçmez: $3^{341} \not\equiv 3 \pmod{341}$'dir. Birden çok tabanla test etmek yanılma olasılığını hızla düşürür.

Modern asallık testlerinin çekirdeğinde hâlâ bu fikir vardır.

18.6 Çalışma Problemleri

Alıştırma 18.1 (Fermat ile Kalan Hesapları). Aşağıdaki kalanları bulunuz.
a) 5^{100} sayısının 17 ile bölümünden kalan.
b) 7^{222} sayısının 11 ile bölümünden kalan.
c) 2^{1000} sayısının 23 ile bölümünden kalan.

Alıştırma 18.2 (Fermat ile Bölünebilme). Aşağıdakileri ispatlayınız.
a) $\gcd(n, 42) = 1$ olan her n tam sayısı için $168 \mid n^6 - 1$.
b) $\gcd(n, 133) = \gcd(m, 133) = 1$ olan her n, m tam sayısı için $133 \mid n^{18} - m^{18}$.
c) Her n tam sayısı için $30 \mid n^5 - n$.
İpucu (a): $168 = 8 \cdot 3 \cdot 7$'dir; modülo 8 için n'nin tek olduğunu ve Örnek 2.3'i kullanınız.

Alıştırma 18.3 (Kuvvetlerin Kongrüansı). p bir asal sayı ve $a, b \in \mathbb{Z}$ olsun.
a) $a^p \equiv b^p \pmod p$ ise $a \equiv b \pmod p$ olduğunu gösteriniz.
b) $a^p \equiv b^p \pmod p$ ise $a^p \equiv b^p \pmod{p^2}$ olduğunu gösteriniz.
İpucu (b): (a) şıkkından $a = b + kp$ yazınız ve a^p ifadesini binom açılımıyla açıp p^2 ile bölünmeyen terimleri toplayınız.

Alıştırma 18.4 (Kuvvet Toplamları). p bir tek asal sayı olmak üzere aşağıdakileri ispatlayınız.
a) $1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \pmod p$
b) $1^p + 2^p + \cdots + (p-1)^p \equiv 0 \pmod p$

İpucu (a): Her terime Teorem 18.1'yı uygulayınız. *(b):* Her terime Sonuç 18.1'i uygulayıp Örnek 1.1'daki toplam formülünü kullanınız.

Alıştırma 18.5 (Farklı Bir İspat). Sonuç 18.1'i, yani her a tam sayısı ve her p asalı için $a^p \equiv a \pmod{p}$ olduğunu, a üzerinden tümevarımla ispatlayınız.
İpucu: Başlangıç adımı $a = 1$'dir. Tümevarım adımında $(a+1)^p$ ifadesini binom açılımıyla açıp Alıştırma 9.2'u kullanınız; negatif a değerleri için önce $a \equiv a + p$ olduğunu gözlemleyiniz.

19. Wilson Teoremi

Fermat teoremi bir sayının asal olmadığını göstermeye yarıyordu, ama asal **olduğunu** kanıtlamıyordu; sözde-asallar tam olarak bu boşluktan doğuyordu. Wilson teoremi ise bu boşluğu kapatır: asallığı, tek bir kongrüansla — istisnasız — karakterize eder.

19.1 Hazırlık: Kendi Tersi Olan Sınıflar

Wilson teoreminin ispatı, 1 ile $p-1$ arasındaki sayıları çarpımsal tersleriyle eşleştirmeye dayanır. Bu eşleştirmenin işe yaraması için önce kendi tersi olan sayıları belirlememiz gerekir.

Lemma 19.1 ($x^2 \equiv 1$ Denkleminin Çözümleri). *p bir asal sayı olsun.*

$$x^2 \equiv 1 \pmod{p}$$

denkleminin çözümleri tam olarak $x \equiv 1$ ve $x \equiv -1 \pmod{p}$'dir.

> ***İspat.***
> *$x^2 \equiv 1 \pmod{p}$ olsun. Bu, $p \mid x^2 - 1$, yani*
>
> $$p \mid (x-1)(x+1)$$
>
> *demektir. p asal olduğundan Teorem 9.1 gereği $p \mid x-1$ veya $p \mid x+1$'dir; yani*
>
> $$x \equiv 1 \pmod{p} \qquad \text{veya} \qquad x \equiv -1 \pmod{p}$$
>
> *Tersine, bu iki sınıfın her ikisi de denklemi sağlar: $1^2 = 1$ ve $(-1)^2 = 1$'dir.*
> ■

> ⚠ Modül asal değilse bu doğru değildir
>
> p asallığı vazgeçilmezdir. Örneğin $n = 8$ için Örnek 17.4'nda gördüğümüz gibi
>
> $$1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}$$
>
> olur; denklemin **dört** çözümü vardır. Örnek 15.5'teki $49^2 \equiv 1 \pmod{120}$ eşitliği de aynı olgunun bir örneğidir.

19.2 Wilson Teoremi

Teorem 19.1 (Wilson Teoremi). *p bir asal sayı olsun. Bu durumda*

$$(p-1)! \equiv -1 \pmod{p}$$

> ***İspat.***
> ***Küçük durumlar.*** *$p = 2$ için $(2-1)! = 1$ ve $1 \equiv -1 \pmod{2}$'dir ✓. $p = 3$ için $(3-1)! = 2$ ve $2 \equiv -1 \pmod{3}$'tür ✓.*
> *Bundan sonra $p \geq 5$ varsayalım.*
> ***1. Her sayının tek bir eşi vardır.*** *$a \in \{1, 2, \ldots, p-1\}$ olsun. p asal ve $p \nmid a$ olduğundan $\gcd(a, p) = 1$'dir; Önerme 15.1 gereği*
>
> $$aa' \equiv 1 \pmod{p}$$

*olacak biçimde tek türlü belirli bir $a' \in \{1, 2, \ldots, p-1\}$ vardır. Bu a' sayısına a'nın **eşi** diyelim. Eşlik karşılıklıdır: a'nın eşi a' ise a''nün eşi de a'dır.*
2. Yalnızca 1 ve $p-1$ kendi eşidir. *$a = a'$ olması $a^2 \equiv 1 \pmod{p}$ demektir. Lemma 19.1 gereği bu ancak*

$$a \equiv 1 \qquad \text{veya} \qquad a \equiv -1 \pmod{p}$$

hâlinde olur. $1 \leq a \leq p-1$ aralığında bu iki sınıfın temsilcileri sırasıyla $a = 1$ ve $a = p-1$'dir.
3. Ortadaki sayılar ikişerli gruplanır. *Geriye*

$$\{2, 3, \ldots, p-2\}$$

kümesi kalır; bu kümede $p-3$ eleman vardır ve hiçbiri kendi eşi değildir. Her elemanın eşi yine bu kümededir (çünkü 1 ile $p-1$ zaten kendi eşleridir ve eşlik tek türlü belirlidir). *O hâlde bu küme, çarpımı $\equiv 1$ olan*

$$\frac{p-3}{2}$$

tane ikiliye ayrılır. ($p \geq 5$ tek olduğundan $p-3$ çifttir.) *Bütün ikilileri çarparsak*

$$2 \cdot 3 \cdots (p-2) \equiv \underbrace{1 \cdot 1 \cdots 1}_{\frac{p-3}{2} \text{ tane}} = 1 \pmod{p}$$

4. Sonuç. *Şimdi eksik kalan iki çarpanı ekleyelim:*

$$(p-1)! = 1 \cdot \big(\, 2 \cdot 3 \cdots (p-2) \, \big) \cdot (p-1) \equiv 1 \cdot 1 \cdot (p-1) \pmod{p}$$

$p - 1 \equiv -1 \pmod{p}$ *olduğundan*

$$(p-1)! \equiv -1 \pmod{p}$$

■

Örnek 19.1 (Küçük Asallarda Doğrulama).

p	$(p-1)!$	$(p-1)! \bmod p$
2	1	$1 \equiv -1$
3	2	$2 \equiv -1$
5	24	$4 \equiv -1$
7	720	$6 \equiv -1$
11	3 628 800	$10 \equiv -1$

Örneğin $p = 7$ için ispattaki eşleştirme şöyledir: $\{2, 4\}$ *(*$2 \cdot 4 = 8 \equiv 1$*)* ve $\{3, 5\}$ *(*$3 \cdot 5 = 15 \equiv 1$*)*. Kendi eşi olanlar 1 ile 6'dır ve $6! \equiv 1 \cdot 1 \cdot 6 = 6 \equiv -1 \pmod{7}$'dir.

19.3 Teoremin Tersi

Fermat teoreminin tersi yanlıştı. Wilson teoreminin tersi ise doğrudur — üstelik ispatı çok kısadır.

Teorem 19.2 (Wilson Teoreminin Tersi). *$1 < n \in \mathbb{Z}$ olsun. Eğer*

$$(n-1)! \equiv -1 \pmod{n}$$

ise n asaldır.

İspat.

Karşıt tersini ispatlayalım: n asal değilse $(n-1)! \not\equiv -1 \pmod{n}$ olduğunu gösterelim.
n asal olmasın. O hâlde n'nin

$$1 < a < n$$

koşulunu sağlayan bir a böleni vardır.
a sayısı $1 \leq a \leq n-1$ aralığında olduğundan $(n-1)!$ çarpımının çarpanlarından biridir; dolayısıyla

$$a \mid (n-1)!$$

Şimdi $(n-1)! \equiv -1 \pmod{n}$ olduğunu varsayalım. Bu, $n \mid (n-1)!+1$ demektir. $a \mid n$ olduğundan Teorem 3.1 gereği

$$a \mid (n-1)!+1$$

a hem $(n-1)!$ sayısını hem de $(n-1)!+1$ sayısını böldüğünden farklarını da böler:

$$a \mid \big((n-1)!+1 \big) - (n-1)! = 1$$

Buradan $a = 1$ çıkar; oysa $a > 1$ idi. Çelişki.
O hâlde n asal değilse $(n-1)! \not\equiv -1 \pmod{n}$'dir.
■

i Asallığın tam karakterizasyonu

Teorem 19.1 ile Teorem 19.2 birlikte şunu verir: $1 < n$ için

$$n \text{ asaldır} \Leftrightarrow (n-1)! \equiv -1 \pmod{n}$$

Bu, asallığın **istisnasız** bir ölçütüdür — Fermat testindeki gibi bir "sözde-asal" boşluğu yoktur. Buna karşılık pratik bir test değildir: $(n-1)!$ sayısını hesaplamak, n'yi çarpanlarına ayırmaktan çok daha pahalıdır. Wilson teoreminin değeri hesapta değil, ispatlardadır.

19.4 Bileşik Sayılarda $(n-1)!$

Teorem 19.2'nin ispatı n bileşikken $(n-1)! \equiv -1$ olamayacağını gösterdi. Peki $(n-1)!$ o zaman neye kongrüdür? Cevap neredeyse her zaman 0'dır.

Teorem 19.3 (Bileşik Sayılarda Faktöriyel). *$4 \neq n$ bileşik bir tam sayı olsun* (yani $1 < n$ ve n asal değil). *Bu durumda*

$$(n-1)! \equiv 0 \pmod{n}$$

İspat.
n bileşik olduğundan $n = ab$ olacak biçimde $1 < a \leq b < n$ tam sayıları vardır. İki duruma ayıralım.
Durum 1: $a < b$. *Bu durumda a ile b farklı sayılardır ve her ikisi de $1 \leq a < b \leq n-1$ aralığındadır. O hâlde her ikisi de $(n-1)!$ çarpımında **ayrı** çarpanlar olarak görünür:*

$$(n-1)! = 1 \cdots a \cdots b \cdots (n-1)$$

Buradan $ab = n$ sayısı $(n-1)!$ değerini böler.
Durum 2: $a = b$, *yani $n = a^2$. Bu durumda $a > 1$'dir ve $n \neq 4$ olduğundan $a \geq 3$'tür.*
$a \geq 3$ olduğundan

$$2a < a \cdot a = n \Longrightarrow 2a \leq n-1$$

Demek ki a ile $2a$ sayılarının ikisi de 1 ile $n-1$ arasındadır ve birbirinden farklıdır. Her ikisi de $(n-1)!$ çarpımında ayrı çarpanlar olarak görünür; dolayısıyla

$$a \cdot 2a = 2a^2 = 2n \mid (n-1)!$$

Özel olarak $n \mid (n-1)!$*'dir.*
Her iki durumda da $n \mid (n-1)!$*, yani* $(n-1)! \equiv 0 \pmod{n}$*'dir.*
■

⚠ $n = 4$ neden istisna?

$n = 4$ için $(4-1)! = 6$ ve

$$6 \equiv 2 \pmod{4}$$

olur; ne -1'dir ne de 0. İspattaki Durum 2 tam olarak burada tıkanır: $a = 2$ için $2a = 4 = n$ olur ve $2a$ sayısı artık $n-1$ aralığına girmez.
4, $(n-1)!$ değerinin 0'a kongrü olmadığı **tek** bileşik sayıdır.

Sonuç 19.1 ($\(n - 2 \) !$ ile Asallık Ölçütü). *$1 < n \in \mathbb{Z}$ olsun. Bu durumda*

$$n \text{ asaldır} \Leftrightarrow (n-2)! \equiv 1 \pmod{n}$$

Gerçekten de $(n-1)! = (n-1)\cdot(n-2)!$ ve $n-1 \equiv -1 \pmod{n}$ olduğundan

$$(n-1)! \equiv -(n-2)! \pmod{n}$$

yazılabilir. O hâlde $(n-1)! \equiv -1$ olması ile $(n-2)! \equiv 1$ olması aynı koşuldur; Teorem 19.1 ve Teorem 19.2 bunu asallığa denk kılar.

19.5 Faktöriyel İçeren Kongrüanslar

Wilson teoreminin asıl kullanım biçimi, büyük faktöriyellerin kalanlarını hesaplamaktır. Yöntem daima aynıdır: hedefteki faktöriyeli $(p-1)!$ ile ilişkilendirmek ve aradaki çarpanları modül cinsinden **negatif** temsilcilerle yazmak.

Örnek 19.2 ($18 ! \equiv -1 \mod \(437 \)$). $18! \equiv -1 \pmod{437}$ olduğunu gösteriniz.

Çözüm.
$437 = 19 \cdot 23$'tür ve 19 ile 23 farklı asallardır. Teorem 5.2 gereği

$$19 \mid 18! + 1 \qquad \text{ve} \qquad 23 \mid 18! + 1$$

olduğunu ayrı ayrı göstermek yeterlidir.
Modülo 19. 19 asal olduğundan Teorem 19.1 doğrudan uygulanır:

$$18! = (19-1)! \equiv -1 \pmod{19}$$

Modülo 23. 23 asal olduğundan Teorem 19.1 gereği

$$22! \equiv -1 \pmod{23}$$

Şimdi 22! ile 18! arasındaki farkı yazalım:

$$22! = 22 \cdot 21 \cdot 20 \cdot 19 \cdot 18!$$

Baştaki dört çarpanı negatif temsilcilerle yazalım:

$$22 \equiv -1, \quad 21 \equiv -2, \quad 20 \equiv -3, \quad 19 \equiv -4 \pmod{23}$$

Çarpımları:

$$22 \cdot 21 \cdot 20 \cdot 19 \equiv (-1)(-2)(-3)(-4) = 24 \equiv 1 \pmod{23}$$

O hâlde

$$-1 \equiv 22! \equiv 1 \cdot 18! = 18! \pmod{23}$$

Birleştirme. $19 \mid 18! + 1$ ve $23 \mid 18! + 1$ olduğundan, $\gcd(19, 23) = 1$ olması nedeniyle

$$437 = 19 \cdot 23 \mid 18! + 1 \qquad \text{yani} \qquad 18! \equiv -1 \pmod{437}$$

■

Örnek 19.3 (\$97 !\$ Sayısının Modülo \$103\$ Tersi). $97!$ tam sayısının modülo 103 çarpımsal tersini bulunuz.

Çözüm.
103 asaldır; Teorem 19.1 gereği

$$102! \equiv -1 \pmod{103}$$

$102!$ ile $97!$ arasındaki çarpanları ayıralım:

$$102! = 102 \cdot 101 \cdot 100 \cdot 99 \cdot 98 \cdot 97!$$

Bu beş çarpanı negatif temsilcilerle yazalım:

$$102 \equiv -1, \quad 101 \equiv -2, \quad 100 \equiv -3, \quad 99 \equiv -4, \quad 98 \equiv -5 \pmod{103}$$

Çarpımları:

$$(-1)(-2)(-3)(-4)(-5) = -120$$

$-120 + 103 = -17$ olduğundan $-120 \equiv -17 \pmod{103}$'tür. O hâlde

$$-1 \equiv 102! \equiv (-17) \cdot 97! \pmod{103}$$

Her iki tarafı -1 ile çarpalım:

$$17 \cdot 97! \equiv 1 \pmod{103}$$

Tanım 15.2 gereği bu tam olarak aradığımız şeydir: $97!$ sayısının modülo 103 tersi $\mathbf{17}$'dir.
■

Örnek 19.4 (\$14 dot.op 35 !\$ Sayısının \$41\$ ile Bölümünden Kalan). $14 \cdot (35!)$ tam sayısının 41 ile bölünmesinden elde edilen kalanı bulunuz.

Çözüm.
41 asaldır; Teorem 19.1 gereği

$$40! \equiv -1 \pmod{41}$$

Aradaki çarpanları ayıralım:

$$40! = 40 \cdot 39 \cdot 38 \cdot 37 \cdot 36 \cdot 35!$$

Negatif temsilciler:

$$40 \equiv -1, \quad 39 \equiv -2, \quad 38 \equiv -3, \quad 37 \equiv -4, \quad 36 \equiv -5 \pmod{41}$$

Çarpımları -120'dir ve $-120 + 123 = 3$ olduğundan $-120 \equiv 3 \pmod{41}$'dir. O hâlde

$$-1 \equiv 40! \equiv 3 \cdot 35! \pmod{41}$$

Şimdi her iki tarafı 14 ile çarpalım — bu çarpanı seçmemizin nedeni $3 \cdot 14 = 42 \equiv 1 \pmod{41}$ olmasıdır:

$$14 \cdot (-1) \equiv 42 \cdot 35! \equiv 35! \pmod{41}$$

Yani

$$35! \equiv -14 \pmod{41}$$

Aradığımız değer ise $14 \cdot 35!$'dir:

$$14 \cdot 35! \equiv 14 \cdot (-14) = -196 \pmod{41}$$

$-196 + 5 \cdot 41 = -196 + 205 = 9$ olduğundan

$$14 \cdot 35! \equiv 9 \pmod{41}$$

Aranan kalan **9**'dur.
■

Örnek 19.5 (İkiz Asallar İçin Bir Kongrüans). p ile $p+2$ sayılarının ikisi de asal olsun *(böyle çiftlere **ikiz asallar** denir)*. Bu durumda

$$4\left(\,(p-1)!+1\,\right)+p \equiv 0 \pmod{p(p+2)}$$

olduğunu gösteriniz.

Çözüm.
$q := p+2$ yazalım. İfadeyi $N := 4\left(\,(p-1)!+1\,\right)+p$ ile gösterelim. $p \mid N$ ve $q \mid N$ olduğunu ayrı ayrı göstereceğiz.
Modülo p. p asal olduğundan Teorem 19.1 gereği $(p-1)! \equiv -1 \pmod{p}$'dir. Buradan

$$N = 4\left(\,(p-1)!+1\,\right)+p \equiv 4(-1+1)+0 = 0 \pmod{p}$$

Modülo $q = p+2$. q asal olduğundan Teorem 19.1 gereği

$$(q-1)! = (p+1)! \equiv -1 \pmod{q}$$

$(p+1)!$ ifadesini $(p-1)!$ cinsinden yazalım:

$$(p+1)! = (p+1) \cdot p \cdot (p-1)!$$

Baştaki iki çarpanı modülo $q = p+2$ negatif temsilcilerle yazalım:

$$p+1 \equiv -1 \pmod{q}, \qquad p \equiv -2 \pmod{q}$$

O hâlde

$$-1 \equiv (p+1)! \equiv (-1)(-2)(p-1)! = 2\,(p-1)! \pmod{q}$$

Her iki tarafı 2 ile çarparsak

$$4\,(p-1)! \equiv -2 \pmod{q}$$

Şimdi N ifadesini hesaplayalım:

$$N = 4\,(p-1)! + 4 + p \equiv -2 + 4 + p = p+2 = q \equiv 0 \pmod{q}$$

Birleştirme. $p \mid N$ ve $q \mid N$'dir. p ile $q = p+2$ farklı asallar olduğundan Sonuç 9.1 gereği $\gcd(p,q) = 1$'dir; Teorem 5.2 gereği

$$p(p+2) \mid N$$

(Sağlama: $p=3$, $q=5$ için $N = 4(2!+1)+3 = 4\cdot 3+3 = 15$ ve $p(p+2) = 15$ ✓)
■

19.6 Çalışma Problemleri

Alıştırma 19.1 (Faktöriyel Kalanları). Aşağıdaki kalanları bulunuz.
a) $15!$ sayısının 17 ile bölümünden kalan.
b) $(p-2)!$ sayısının p ile bölümünden kalan *(p asal).*
c) $2 \cdot (26!)$ sayısının 29 ile bölümünden kalan.

Alıştırma 19.2 (Wilson Teoreminin Uygulamaları). **a)** p tek bir asal sayı olmak üzere

$$\left(\frac{p-1}{2}\right)! \cdot \left(\frac{p-1}{2}\right)! \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$$

olduğunu gösteriniz.
İpucu: $(p-1)!$ çarpımındaki $\frac{p+1}{2}, \ldots, p-1$ çarpanlarını -1 ile $-\frac{p-1}{2}$ arasındaki temsilcilerle yazınız.
b) p asal ve $0 \leq k \leq p-1$ olmak üzere

$$k!\,(p-1-k)! \equiv (-1)^{k+1} \pmod{p}$$

olduğunu gösteriniz.

Alıştırma 19.3 (Bileşik Sayılarda Faktöriyel). **a)** $(n-1)! \equiv 0 \pmod{n}$ eşitliğinin sağlanmadığı bütün $1 < n$ tam sayılarını belirleyiniz.
b) $n \geq 6$ bileşik ise $n \mid (n-1)!$ olduğunu, üstelik $n^2 \mid (n-1)!$ olduğunu gösteriniz.
İpucu (b): Teorem 19.3'in ispatındaki iki durumu $n \geq 6$ koşulu altında yeniden inceleyiniz.

Alıştırma 19.4 (İki Teoremi Birlikte Kullanma). p bir asal sayı olsun. Aşağıdakileri ispatlayınız.
a) $p \equiv 1 \pmod{4}$ ise $x^2 \equiv -1 \pmod{p}$ denkleminin bir çözümü vardır.
İpucu: $x = \left(\frac{p-1}{2}\right)!$ alınız ve Alıştırma 19.2 (a)'yı kullanınız.
b) $p \equiv 3 \pmod{4}$ ise $x^2 \equiv -1 \pmod{p}$ denkleminin hiç çözümü yoktur.
İpucu: Böyle bir x olsaydı $x^{p-1} = \left(x^2\right)^{\frac{p-1}{2}}$ değerini hesaplayıp Teorem 18.1 ile çelişkiye varınız.

20. Euler'in Phi Fonksiyonu

Teorem 17.1'nda $U(\mathbb{Z}_n)$ kümesinin bir grup olduğunu görmüştük. Bu grubun eleman sayısı, sayılar teorisinin en önemli fonksiyonlarından birini tanımlar. Bu bölümde o sayıyı hesaplamayı öğreneceğiz; bir sonraki bölümde ise onu Fermat teoremini genelleştirmek için kullanacağız.

20.1 Tanım ve İlk Değerler

Tanım 20.1 (Euler'in $phi.alt$ Fonksiyonu). $1 \leq n \in \mathbb{Z}$ olsun. 1 ile n arasındaki *(uç değerler dâhil)* tam sayılardan n ile aralarında asal olanların sayısına n'nin **Euler ϕ değeri** denir ve $\phi(n)$ ile gösterilir:

$$\phi(n) = \#\{a \in \mathbb{Z} : 1 \leq a \leq n, \gcd(a, n) = 1\}$$

> **i** $\phi(n)$ birimler grubunun eleman sayısıdır
>
> Tanım 17.3 gereği $a + n\mathbb{Z}$ sınıfının birim olması $\gcd(a, n) = 1$ demekti ve Önerme 17.4 gereği bu özellik temsilci seçiminden bağımsızdı. $1, 2, \ldots, n$ sayıları modülo n bir tam kalan sistemi oluşturduğundan *(her sınıftan tam bir temsilci)*, $1 < n$ için
>
> $$\phi(n) = |U(\mathbb{Z}_n)|$$
>
> Yani $\phi(n)$, modülo n tersi olan sınıfların sayısıdır.

Örnek 20.1 (İlk Değerler). Küçük n değerleri için doğrudan sayarak:

n	n ile aralarında asal olanlar	$\phi(n)$
1	1	1
2	1	1
3	1, 2	2
4	1, 3	2
5	1, 2, 3, 4	4
6	1, 5	2
7	1, 2, 3, 4, 5, 6	6
8	1, 3, 5, 7	4
9	1, 2, 4, 5, 7, 8	6
10	1, 3, 7, 9	4
12	1, 5, 7, 11	4

$n = 1$ durumuna dikkat ediniz: $\gcd(1, 1) = 1$ olduğundan $\phi(1) = 1$'dir.

Elbette her n için tek tek saymak istemeyiz. Şimdi $\phi(n)$ değerini n'nin asal çarpanlarından okuyacak bir formül kuracağız.

20.2 Asal ve Asal Kuvvetlerde

Önerme 20.1 (Asal Sayılarda). *p bir asal sayı olmak üzere*

$$\phi(p) = p - 1$$

Gerçekten de Önerme 9.1 gereği $1 \leq a \leq p$ aralığındaki bir a için $\gcd(a, p) \neq 1$ olması ancak $p \mid a$ hâlinde olur; bu aralıkta p ile bölünen tek sayı $a = p$'dir. Geriye $p - 1$ sayı kalır.

Teorem 20.1 (Asal Kuvvetlerde). *p bir asal sayı ve $1 \leq k$ bir tam sayı olmak üzere*

$$\phi\left(p^k\right) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$$

> ***İspat.***
> *Aralarında asal olanları saymak yerine, **olmayanları** sayıp çıkaracağız.*
> *$1 \leq a \leq p^k$ olsun. Önerme 9.1 gereği $\gcd\left(a, p^k\right) \neq 1$ olması, a ile p^k sayılarının ortak bir asal böleninin olması demektir; p^k'nın tek asal böleni p olduğundan bu koşul*
>
> $$p \mid a$$
>
> *koşuluna denktir.*
> *Şimdi $1 \leq a \leq p^k$ aralığında p'nin katlarını sayalım. Bunlar*
>
> $$p, \quad 2p, \quad 3p, \quad \ldots, \quad p^{k-1} \cdot p = p^k$$
>
> *sayılarıdır; yani $a = mp$ biçiminde ve $1 \leq m \leq p^{k-1}$ koşuluyla yazılırlar. Demek ki tam p^{k-1} tane böyle sayı vardır.*
> *Geriye kalanlar p^k ile aralarında asaldır:*
>
> $$\phi\left(p^k\right) = p^k - p^{k-1}$$
>
> *Sağdaki ifadeyi p^k parantezine alırsak*
>
> $$p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$$
>
> ■

Örnek 20.2 (Asal Kuvvet Örnekleri).

$$\phi(8) = \phi(2^3) = 2^3 - 2^2 = 8 - 4 = 4$$

$$\phi(9) = \phi(3^2) = 9 - 3 = 6$$

$$\phi(125) = \phi(5^3) = 125 - 25 = 100$$

$$\phi(49) = \phi(7^2) = 49 - 7 = 42$$

$k = 1$ alındığında $\phi(p) = p - p^0 = p - 1$ bulunur; Önerme 20.1 bunun özel hâlidir.

20.3 Çarpımsallık

Genel bir n için formül kurmanın anahtarı, ϕ fonksiyonunun aralarında asal çarpanlar üzerinde "dağılmasıdır".

Teorem 20.2 ($phi.alt$ Çarpımsaldır). *m, n pozitif tam sayıları aralarında asal olsun; yani $\gcd(m, n) = 1$ olsun. Bu durumda*

$$\phi(mn) = \phi(m)\,\phi(n)$$

İspat.
$m = 1$ veya $n = 1$ ise $\phi(1) = 1$ olduğundan eşitlik açıktır; $1 < m, n$ varsayalım.
*Fikir şudur: modülo mn birim olan sınıflar ile, modülo m birim olan sınıf – modülo n birim olan sınıf **ikilileri** arasında birebir eşleme kuracağız. Böyle bir eşleme varsa iki kümenin eleman sayısı eşittir; yani $\phi(mn) = \phi(m)\phi(n)$ olur.*
Eşleme. *$\gcd(a, mn) = 1$ koşulunu sağlayan bir a tam sayısına, modülo m ve modülo n kalanlarından oluşan*

$$a \mapsto (a \bmod m,\ a \bmod n)$$

ikilisini karşılık getirelim.
1. Eşleme anlamlıdır. *$\gcd(a, mn) = 1$ olsun. $m \mid mn$ olduğundan a ile m'nin her ortak böleni a ile mn'nin de ortak bölenidir; dolayısıyla $\gcd(a, m) = 1$'dir. Aynı gerekçeyle $\gcd(a, n) = 1$'dir. Demek ki ikilinin her iki bileşeni de gerçekten birim sınıflardır.*
2. Eşleme birebirdir. *a ile b aynı ikiliye gitsin:*

$$a \equiv b \pmod m \qquad \text{ve} \qquad a \equiv b \pmod n$$

O hâlde $m \mid a - b$ ve $n \mid a - b$'dir. $\gcd(m, n) = 1$ olduğundan Teorem 5.2 gereği

$$mn \mid a - b \qquad \text{yani} \qquad a \equiv b \pmod{mn}$$

Demek ki a ile b modülo mn aynı sınıftadır.
3. Eşleme örtendir. *$\gcd(b, m) = 1$ ve $\gcd(c, n) = 1$ olan herhangi bir (b, c) ikilisi verilsin. $\gcd(m, n) = 1$ olduğundan Teorem 16.1 uygulanabilir:*

$$x \equiv b \pmod m, \qquad x \equiv c \pmod n$$

sisteminin bir a çözümü vardır. Önerme 12.1 gereği

$$\gcd(a, m) = \gcd(b, m) = 1 \qquad \text{ve} \qquad \gcd(a, n) = \gcd(c, n) = 1$$

Teorem 5.3 gereği $\gcd(a, mn) = 1$'dir; yani a modülo mn bir birim sınıftır ve tam olarak (b, c) ikilisine gitmektedir.
Sonuç. *Eşleme birebir ve örten olduğundan iki kümenin eleman sayıları eşittir. Sol taraftaki kümenin eleman sayısı $\phi(mn)$, sağ taraftaki ikililerin sayısı ise $\phi(m) \cdot \phi(n)$'dir:*

$$\phi(mn) = \phi(m)\,\phi(n)$$

■

⚠ Aralarında asal olma koşulu şart

$\gcd(m, n) = 1$ koşulu atılamaz. Örneğin $m = n = 2$ için

$$\phi(4) = 2 \qquad \text{ama} \qquad \phi(2)\,\phi(2) = 1 \cdot 1 = 1$$

Benzer biçimde $\phi(6) = 2 = \phi(2)\phi(3)$ doğrudur ($\gcd(2, 3) = 1$), ama $\phi(12) \neq \phi(2)\phi(6)$'dır: $\phi(12) = 4$ iken $\phi(2)\phi(6) = 1 \cdot 2 = 2$'dir.

20.4 Genel Formül

Teorem 20.3 (Euler $phi.alt$ Fonksiyonunun Çarpım Formülü). *$1 < n$ tam sayısının kanonik gösterimi*

$$n = p_1^{k_1}\, p_2^{k_2} \cdots p_r^{k_r}$$

olsun (bkz. Sonuç 10.1). *Bu durumda*

$$\phi(n) = \prod_{i=1}^{r}\left(p_i^{k_i} - p_i^{k_i-1}\right) = n\prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right)$$

İspat.
$p_1, \ldots, p_r$ farklı asallar olduğundan $p_i^{k_i}$ kuvvetleri ikişer ikişer aralarında asaldır (Sonuç 9.4). *Teorem 20.2'ı tekrar tekrar uygulayalım:*

$$\phi(n) = \phi\left(p_1^{k_1}\right)\phi\left(p_2^{k_2}\right)\cdots\phi\left(p_r^{k_r}\right)$$

Her çarpana Teorem 20.1'i uygulayalım:

$$\phi(n) = \prod_{i=1}^{r}\left(p_i^{k_i} - p_i^{k_i-1}\right) = \prod_{i=1}^{r} p_i^{k_i}\left(1 - \frac{1}{p_i}\right)$$

Çarpımdaki $p_i^{k_i}$ terimlerini bir araya toplarsak çarpımları n olur:

$$\phi(n) = n\prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right)$$

■

> **i** Formülü okuma biçimi
>
> İkinci biçim çok pratiktir: **n'yi yaz, sonra n'yi bölen her farklı asal için bir $\left(1 - \frac{1}{p}\right)$ çarpanı ekle.** Üsler formülde hiç görünmez; yalnızca hangi asalların böldüğü önemlidir.

Örnek 20.3 (Çarpım Formülüyle Hesaplar). Aşağıdaki değerleri hesaplayınız: $\phi(360)$, $\phi(100)$, $\phi(1001)$.

Çözüm.
$\phi(360)$. Kanonik gösterim $360 = 2^3 \cdot 3^2 \cdot 5$'tir. Farklı asallar $2, 3, 5$'tir:

$$\phi(360) = 360\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 360 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 96$$

(Çarpanlara ayırma biçimiyle: $\phi(8)\phi(9)\phi(5) = 4 \cdot 6 \cdot 4 = 96$ ✓)
$\phi(100)$. $100 = 2^2 \cdot 5^2$:

$$\phi(100) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40$$

$\phi(1001)$. $1001 = 7 \cdot 11 \cdot 13$'tür *(üç farklı asal, hepsinin üssü 1)*:

$$\phi(1001) = 1001 \cdot \frac{6}{7} \cdot \frac{10}{11} \cdot \frac{12}{13} = 6 \cdot 10 \cdot 12 = 720$$

(Son adımda $1001 = 7 \cdot 11 \cdot 13$ olduğundan paydalar sadeleşti.)
■

20.5 Temel Özellikler

Teorem 20.4 ($phi.alt \(n \)$ Ne Zaman Çifttir?). *$2 < n$ olan her tam sayı için $\phi(n)$ çifttir.*

İspat.
İki durum vardır.

Durum 1: n'nin tek bir asal böleni var. *Yani $n = 2^k$ olsun. $n > 2$ olduğundan $k \geq 2$'dir ve Teorem 20.1 gereği*

$$\phi(n) = 2^k - 2^{k-1} = 2^{k-1}$$

$k - 1 \geq 1$ olduğundan bu sayı çifttir.
Durum 2: n'nin bir tek asal böleni var. *p tek bir asal ve $p^k \parallel n$ olsun* (yani $p^k \mid n$ ve $p^{k+1} \nmid n$). *$n = p^k m$ ve $\gcd(p^k, m) = 1$ yazalım. Teorem 20.2 gereği*

$$\phi(n) = \phi(p^k)\phi(m) = p^{k-1}(p-1)\,\phi(m)$$

p tek asal olduğundan $p - 1$ çifttir; dolayısıyla çarpım da çifttir.
Bu iki durum bütün olasılıkları kapsar: $n > 2$ ise n ya yalnızca 2'nin kuvvetidir ya da tek bir asal böleni vardır.
■

> **i** Hemen bir sonuç
>
> Teorem 20.4, $\phi(n) = c$ denklemlerini çözerken hemen kullanılır: **c tek ve $c > 1$ ise denklemin hiç çözümü yoktur.** Örneğin $\phi(n) = 3$, $\phi(n) = 5$, $\phi(n) = 7$ denklemleri çözümsüzdür.
> $\phi(n) = 1$ denkleminin çözümleri ise yalnızca $n = 1$ ve $n = 2$'dir.

Önerme 20.2 ($phi.alt \(2 n \) = phi.alt \(n \)$ Ne Zaman Olur?). *$1 \leq n$ bir tam sayı olmak üzere*

$$\phi(2n) = \phi(n) \Leftrightarrow n \ \text{ tektir}$$

Ayrıca n çift ise $\phi(2n) = 2\,\phi(n)$'dir.

İspat.
($\Leftarrow$) n tek olsun. *Bu durumda $\gcd(2, n) = 1$'dir; Teorem 20.2 gereği*

$$\phi(2n) = \phi(2)\,\phi(n) = 1 \cdot \phi(n) = \phi(n)$$

($\Rightarrow$) n çift olsun. *$n = 2^k m$ yazalım; burada $k \geq 1$ ve m tektir. O hâlde $2n = 2^{k+1}m$'dir. İki kez Teorem 20.2 ve Teorem 20.1 uygulayalım:*

$$\phi(n) = \phi(2^k)\phi(m) = 2^{k-1}\phi(m)$$

$$\phi(2n) = \phi(2^{k+1})\phi(m) = 2^k\phi(m)$$

Buradan

$$\phi(2n) = 2\,\phi(n) \neq \phi(n)$$

(Son adımda $\phi(n) \neq 0$ olduğunu kullandık.) *Demek ki n çiftse eşitlik bozulur; karşıt tersi alırsak eşitlik ancak n tekken sağlanır.*
■

Teorem 20.5 ($phi.alt$ Bölenlerde). *d, n pozitif tam sayıları ve $d \mid n$ olsun. Bu durumda*

$$\phi(d) \mid \phi(n)$$

İspat.
$d = 1$ ise $\phi(1) = 1$ her sayıyı böler; $1 < d$ varsayalım.
$d \mid n$ olduğundan Önerme 11.1 gereği d'nin her asal böleni n'yi de böler ve Önerme 11.2 gereği üsler korunur. Yani

$$d = p_1^{b_1} \cdots p_s^{b_s}, \qquad n = p_1^{a_1} \cdots p_s^{a_s} \cdot q_1^{c_1} \cdots q_t^{c_t}$$

biçiminde yazılabilir; burada $1 \le b_i \le a_i$*'dir ve* q_j *asalları* d*'yi bölmeyen* (varsa) *asallardır. Teorem 20.3 gereği*

$$\phi(d) = \prod_{i=1}^{s} p_i^{b_i-1}(p_i-1), \qquad \phi(n) = \prod_{i=1}^{s} p_i^{a_i-1}(p_i-1) \cdot \prod_{j=1}^{t} q_j^{c_j-1}(q_j-1)$$

Şimdi $\phi(d)$ *çarpımındaki her terimi* $\phi(n)$ *çarpımındaki karşılığıyla kıyaslayalım.* $b_i - 1 \le a_i - 1$ *olduğundan*

$$p_i^{b_i-1}(p_i-1) \,\Big|\, p_i^{a_i-1}(p_i-1)$$

Bölen ilişkisi çarpım altında korunduğundan (Teorem 3.1) bu terimlerin çarpımı da bölünür:

$$\phi(d) = \prod_{i=1}^{s} p_i^{b_i-1}(p_i-1) \,\Big|\, \prod_{i=1}^{s} p_i^{a_i-1}(p_i-1)$$

Sağdaki çarpım da $\phi(n)$*'yi böldüğünden geçişme ile* $\phi(d) \mid \phi(n)$ *bulunur.*
■

Önerme 20.3 ($phi.alt (n^2) = n \, phi.alt \(n \)$). *Her* $1 \le n$ *tam sayısı için*

$$\phi(n^2) = n\,\phi(n)$$

İspat.
$n = 1$ *için her iki taraf da* 1*'dir.* $1 < n$ *olsun ve kanonik gösterimi*

$$n = p_1^{k_1} \cdots p_r^{k_r}$$

olsun. n^2 *ile* n ***aynı*** *asalları içerir; yalnızca üsler ikiye katlanır. Teorem 20.3'ün ikinci biçimini kullanalım:*

$$\phi(n^2) = n^2 \prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right)$$

$$\phi(n) = n \prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right)$$

Birinci eşitliği $n^2 = n \cdot n$ *biçiminde ayırıp ikinciyi yerine koyalım:*

$$\phi(n^2) = n \cdot \left(n \prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right)\right) = n\,\phi(n)$$

■

20.6 $\phi(n) = c$ Denklemleri

Örnek 20.4 ($phi.alt \(n \) = 6$ Denklemi). $\phi(n) = 6$ eşitliğini sağlayan bütün n pozitif tam sayılarını bulunuz.

Çözüm.
n bir çözüm olsun ve p^k, n'yi bölen bir asal kuvvet olsun *(yani* $p^k \mid n$ *ve* $p^{k+1} \nmid n$*).* Teorem 20.5 gereği

$$\phi(p^k) = p^{k-1}(p-1) \,\Big|\, \phi(n) = 6$$

1. Hangi asallar n'yi bölebilir? p tek asal ise $p-1$ sayısı 6'yı bölmelidir:

$$p - 1 \in \{1, 2, 3, 6\} \Longrightarrow p \in \{2, 3, 4, 7\}$$

Bunlardan asal olanlar 3 ve 7'dir. $p = 2$ de mümkündür. O hâlde n'nin asal bölenleri yalnızca 2, 3 ve 7 olabilir.
2. Hangi üsler mümkün?

- $p = 2$: $\phi\left(2^k\right) = 2^{k-1} \mid 6$ olmalı; $2^{k-1} \in \{1, 2\}$, yani $k \leq 2$. Ama $k = 2$ için $\phi(4) = 2$'dir ve geri kalan çarpanın 3 olması gerekir — Teorem 20.4 gereği 1'den büyük tek bir ϕ değeri olamaz. O hâlde $k \leq 1$'dir.
- $p = 3$: $\phi\left(3^k\right) = 2 \cdot 3^{k-1} \mid 6$ olmalı; $3^{k-1} \mid 3$, yani $k \leq 2$'dir.
- $p = 7$: $\phi\left(7^k\right) = 6 \cdot 7^{k-1} \mid 6$ olmalı; $7^{k-1} = 1$, yani $k = 1$'dir.

3. Olasılıkları tarayalım. $n = 2^a 3^b 7^c$ ile $a \leq 1$, $b \leq 2$, $c \leq 1$'dir ve

$$\phi(n) = \phi(2^a)\phi\left(3^b\right)\phi(7^c) = 6$$

$\phi(2^a) = 1$ *(hem $a = 0$ hem $a = 1$ için)* olduğundan koşul

$$\phi\left(3^b\right)\phi(7^c) = 6$$

hâline gelir. Değerler $\phi(3^0) = 1$, $\phi(3) = 2$, $\phi(9) = 6$ ve $\phi(7^0) = 1$, $\phi(7) = 6$'dır. Çarpımı 6 yapan ikililer:

- $\phi(9) \cdot \phi(7^0) = 6 \cdot 1$: $b = 2, c = 0$
- $\phi(3^0) \cdot \phi(7) = 1 \cdot 6$: $b = 0, c = 1$

($\phi(3)\phi(7) = 2 \cdot 6 = 12 \neq 6$'dır.)
Her ikisinde $a \in \{0, 1\}$ serbesttir. Dört çözüm bulunur:

$$n \in \{9, 18, 7, 14\}$$

(Sağlama: $\phi(9) = 6$, $\phi(18) = \phi(2)\phi(9) = 6$, $\phi(7) = 6$, $\phi(14) = \phi(2)\phi(7) = 6$ ✓)
■

Örnek 20.5 ($phi.alt \(n \) = 14$ Denklemi). $\phi(n) = 14$ eşitliğini sağlayan bir n tam sayısının bulunmadığını gösteriniz.

Çözüm.
$\phi(n) = 14$ olduğunu varsayalım. $14 = 2 \cdot 7$ olduğundan $7 \mid \phi(n)$'dir.
Teorem 20.3 gereği $\phi(n)$, n'yi bölen asal kuvvetlerin ϕ değerlerinin çarpımıdır. 7 asal olduğundan Sonuç 9.2 gereği bu çarpanlardan **en az birini** bölmelidir: bir $p^k \mid n$ asal kuvveti için

$$7 \,\Big|\, \phi(p^k) = p^{k-1}(p-1)$$

7 asal olduğundan Teorem 9.1 gereği iki durum vardır.
Durum 1: $7 \mid p^{k-1}$. Bu ancak $p = 7$ ve $k \geq 2$ ise olur. O hâlde $49 \mid n$'dir ve Teorem 20.5 gereği

$$\phi(49) = 42 \,\Big|\, \phi(n) = 14$$

Ama $42 > 14 > 0$ olduğundan 42 sayısı 14'ü bölemez — çelişki.
Durum 2: $7 \mid p - 1$. Bu durumda $p \equiv 1 \pmod 7$'dir. Bu koşulu sağlayan asalların en küçüğü 29'dur *($8, 15, 22$ asal değildir)*; yani $p \geq 29$'dur. Teorem 20.5 gereği

$$\phi(p) = p - 1 \,\Big|\, \phi(n) = 14$$

Ama $p - 1 \geq 28 > 14 > 0$ olduğundan bu imkânsızdır — çelişki.
Her iki durum da çelişkiye vardığından $\phi(n) = 14$ eşitliğini sağlayan bir n **yoktur**.
■

20.7 Çalışma Problemleri

Alıştırma 20.1 ($phi.alt$ Değerlerini Hesaplama). Aşağıdaki değerleri hesaplayınız.

a) $\phi(720)$ **b)** $\phi(1024)$ **c)** $\phi(2431)$ **d)** $\phi(5^4 \cdot 11)$
İpucu (c): $2431 = 11 \cdot 13 \cdot 17$'dir.

Alıştırma 20.2 ($phi.alt \(n \) = c$ Denklemleri). Aşağıdaki denklemlerin bütün çözümlerini bulunuz; çözümü olmayanların nedenini açıklayınız.
a) $\phi(n) = 4$ **b)** $\phi(n) = 8$ **c)** $\phi(n) = 10$ **d)** $\phi(n) = 12$

Alıştırma 20.3 ($phi.alt$ Fonksiyonunun Özellikleri). Aşağıdakileri ispatlayınız.
a) n tek ise $\phi(4n) = 2\,\phi(n)$'dir.
b) $\phi(n) = \frac{n}{2}$ olması için gerek ve yeter koşul, n'nin bir 2 kuvveti olmasıdır.
c) p asal ve $p \mid n$ ise $\phi(pn) = p\,\phi(n)$'dir.
d) p asal ve $p \nmid n$ ise $\phi(pn) = (p-1)\,\phi(n)$'dir.

Alıştırma 20.4 (Bölenler Üzerinden Toplam). n pozitif bir tam sayı olmak üzere

$$\sum_{d \mid n} \phi(d) = n$$

olduğunu gösteriniz. *(Toplam, n'nin bütün pozitif bölenleri üzerinden alınmaktadır.)*
a) Önce $n = 12$ için doğrudan hesaplayarak doğrulayınız.
b) $n = p^k$ için ispatlayınız.
c) Teorem 20.2'ı kullanarak genel durumu elde ediniz.
İpucu (b): p^k'nın bölenleri $1, p, \ldots, p^k$'dır ve toplam teleskopiktir.

21. Euler Teoremi

Fermat teoremi yalnızca asal modüllerde işe yarıyordu: p asalken $a^{p-1} \equiv 1 \pmod{p}$ idi. Modül asal olmadığında $p-1$ üssünün yerini ne alacak? Cevap, geçen bölümde tanıdığımız $\phi(n)$ sayısıdır. Bu bölümde Fermat teoremini bütün modüllere genişleteceğiz.

21.1 İndirgenmiş Kalan Sistemleri

Fermat teoremini ispatlarken $1, 2, ..., p-1$ sayılarını kullanmıştık; bunlar modülo p tersi olan bütün sınıfların temsilcileriydi. Genel modülde bu rolü aşağıdaki kavram üstlenir.

Tanım 21.1 (İndirgenmiş Kalan Sistemi). $1 < n \in \mathbb{Z}$ olsun. $\{r_1, r_2, ..., r_{\phi(n)}\}$ tam sayı kümesi

- her i için $\gcd(r_i, n) = 1$ ve
- $i \neq j$ için $r_i \not\equiv r_j \pmod{n}$

koşullarını sağlıyorsa bu kümeye **modülo n indirgenmiş kalan sistemi** denir.

> **i** Tam kalan sistemiyle farkı
>
> Tanım 13.1'ndeki tam kalan sistemi $\mathbb{Z}_n$'nin **bütün** sınıflarından birer temsilci içeriyordu ve n elemanlıydı.
> İndirgenmiş kalan sistemi ise yalnızca **birim** sınıflardan birer temsilci içerir; yani $U(\mathbb{Z}_n)$ grubunun bir temsilci listesidir ve $\phi(n)$ elemanlıdır.
> En doğal örnek, bir tam kalan sisteminden n ile aralarında asal olmayanları atmakla elde edilir. Örneğin $n = 10$ için $\{0, 1, ..., 9\}$ kümesinden geriye $\{1, 3, 7, 9\}$ kalır ve $\phi(10) = 4$'tür.

Teorem 21.1 (İndirgenmiş Sistemi Bir Birimle Çarpmak). *$1 < n$ ve $\gcd(a, n) = 1$ olsun. $\{r_1, ..., r_{\phi(n)}\}$ modülo n bir indirgenmiş kalan sistemi ise*

$$\{ar_1, ar_2, ..., ar_{\phi(n)}\}$$

kümesi de modülo n bir indirgenmiş kalan sistemidir.

İspat.
İki koşulu doğrulayalım.
1. Her eleman n ile aralarında asaldır. $\gcd(a, n) = 1$ *ve* $\gcd(r_i, n) = 1$ *olduğundan Teorem 5.3 gereği*

$$\gcd(ar_i, n) = 1$$

2. Elemanlar ikişer ikişer kongrü değildir. *$i \neq j$ için*

$$ar_i \equiv ar_j \pmod{n}$$

olduğunu varsayalım. $\gcd(a, n) = 1$ *olduğundan Teorem 12.3 gereği a sadeleştirilebilir:*

$$r_i \equiv r_j \pmod{n}$$

Bu, $\{r_i\}$ kümesinin indirgenmiş kalan sistemi olmasıyla çelişir.
Küme $\phi(n)$ elemanlıdır ve iki koşulu da sağladığından bir indirgenmiş kalan sistemidir.
■

> **i** Aynı sınıflar, farklı sıra
>
> Teorem 21.1'in söylediği şey şudur: a ile çarpmak, birim sınıfları **kendi aralarında karıştırır**. Hiçbiri kaybolmaz, hiçbiri iki kez ortaya çıkmaz; yalnızca sıraları değişir.
> Bu, Teorem 17.1'nun bir yansımasıdır: bir grupta sabit bir elemanla çarpmak daima birebir ve örtendir.

21.2 Euler Teoremi

Teorem 21.2 (Euler Teoremi). *$1 < n \in \mathbb{Z}$, $a \in \mathbb{Z}$ ve $\gcd(a,n) = 1$ olsun. Bu durumda*

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

İspat.
$\{r_1, r_2, \ldots, r_{\phi(n)}\}$ modülo n bir indirgenmiş kalan sistemi olsun.
Teorem 21.1 gereği

$$\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$$

kümesi de bir indirgenmiş kalan sistemidir. İki sistem de $U(\mathbb{Z}_n)$ grubunun bütün sınıflarından birer temsilci içerdiğinden, ikinci listenin elemanları birinci listenin elemanlarına — belki farklı bir sırayla — kongrüdür.
*O hâlde iki listenin **çarpımları** birbirine kongrüdür:*

$$(ar_1)(ar_2)\cdots\left(ar_{\phi(n)}\right) \equiv r_1 r_2 \cdots r_{\phi(n)} \pmod{n}$$

Sol taraftaki a çarpanlarını toplayalım; toplam $\phi(n)$ tanedir:

$$a^{\phi(n)}\, r_1 r_2 \cdots r_{\phi(n)} \equiv r_1 r_2 \cdots r_{\phi(n)} \pmod{n}$$

Şimdi $R := r_1 r_2 \cdots r_{\phi(n)}$ yazalım. Her r_i için $\gcd(r_i, n) = 1$ olduğundan Teorem 5.3'in tekrarlı uygulanmasıyla

$$\gcd(R, n) = 1$$

O hâlde Teorem 12.3 gereği R sadeleştirilebilir:

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

■

Sonuç 21.1 (Fermat Teoremi Euler Teoreminin Özel Hâlidir). *p bir asal sayı ve $p \nmid a$ olsun. Önerme 20.1 gereği $\phi(p) = p - 1$'dir; Teorem 21.2 bu durumda*

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

verir. Bu tam olarak Teorem 18.1'dır.

> **i** İki teoremin ispatları da aynıdır
>
> Teorem 18.1'nın ispatında $1, 2, \ldots, p-1$ sayılarını a ile çarpıp kalanların bir permütasyon olduğunu göstermiştik. Teorem 21.2'in ispatı da birebir aynı fikri kullanır; tek fark, listenin $\{1, \ldots, p-1\}$ yerine bir indirgenmiş kalan sistemi olmasıdır.
> Fermat teoremini önce görmemizin nedeni, bu fikrin en sade hâlini oradaki somut listede tanımaktı.

21.3 Kuvvet Hesaplarına Uygulama

i Genel hesap şablonu

$a^N \bmod n$ hesabı için:

1. $\gcd(a,n)=1$ olduğunu doğrula. *(Değilse aşağıdaki Örnek 21.2'e bakınız.)*
2. $\phi(n)$ değerini Teorem 20.3 ile hesapla.
3. Üssü $\phi(n)$'ye böl: $N=\phi(n)\,q+r$.
4. $a^N=\left(a^{\phi(n)}\right)^q a^r\equiv a^r \pmod n$ yaz ve a^r'yi hesapla.

Örnek 21.1 (3^100 Sayısının Son İki Rakamı). 3^{100} sayısının son iki rakamını bulunuz.

Çözüm.
Son iki rakamı bulmak, sayının 100 ile bölümünden kalanını bulmaktır.
1. Aralarında asallık. $\gcd(3,100)=1$'dir; Teorem 21.2 uygulanabilir.
2. $\phi(100)$. $100=2^2\cdot 5^2$ olduğundan Teorem 20.3 gereği

$$\phi(100)=100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)=100\cdot\frac{1}{2}\cdot\frac{4}{5}=40$$

O hâlde $3^{40}\equiv 1 \pmod{100}$'dür.
3. Üssü indirgeme. $100=40\cdot 2+20$ olduğundan

$$3^{100}=\left(3^{40}\right)^2\cdot 3^{20}\equiv 3^{20} \pmod{100}$$

4. 3^{20} hesabı. Kareler alarak ilerleyelim:

$$3^4=81,\qquad 3^5=243\equiv 43 \pmod{100}$$

$$3^{10}=\left(3^5\right)^2\equiv 43^2=1849\equiv 49 \pmod{100}$$

$$3^{20}=\left(3^{10}\right)^2\equiv 49^2=2401\equiv 1 \pmod{100}$$

O hâlde

$$3^{100}\equiv 1 \pmod{100}$$

Son iki rakam **01**'dir.
■

Örnek 21.2 (Aralarında Asal Olmadığında Ne Yapılır?). 2^{1000} sayısının son iki rakamını bulunuz.

Çözüm.
$\gcd(2,100)=2\neq 1$ olduğundan Teorem 21.2 doğrudan uygulanamaz. Bunun yerine $100=4\cdot 25$ ayrışmasını kullanıp iki parçada çalışacağız.
Modülo 4. $1000\geq 2$ olduğundan $4=2^2$ sayısı 2^{1000}'i böler:

$$2^{1000}\equiv 0 \pmod 4$$

Modülo 25. $\gcd(2,25)=1$'dir. Teorem 20.1 gereği

$$\phi(25)=25-5=20$$

$1000=20\cdot 50$ olduğundan Teorem 21.2 gereği

$$2^{1000}=\left(2^{20}\right)^{50}\equiv 1^{50}=1 \pmod{25}$$

Birleştirme. $\gcd(4,25)=1$ olduğundan Teorem 16.1 uygulanabilir:

$$x \equiv 0 \pmod 4, \qquad x \equiv 1 \pmod{25}$$

$x = 25k + 1$ yazıp birinci denklemde yerine koyalım:

$$25k + 1 \equiv 0 \pmod 4 \Longrightarrow k + 1 \equiv 0 \pmod 4 \Longrightarrow k \equiv 3 \pmod 4$$

(Burada $25 \equiv 1 \pmod 4$ *olmasını kullandık.)* $k = 3$ için

$$x = 75 + 1 = 76$$

O hâlde $2^{1000} \equiv 76 \pmod{100}$'dür; son iki rakam **76**'dır.
■

Örnek 21.3 ($855 divides n^72 - 1$ Bölünebilmesi). $\gcd(n, 855) = 1$ koşulunu sağlayan her n tam sayısı için

$$n^{72} \equiv 1 \pmod{855}$$

olduğunu gösteriniz.

Çözüm.
$855 = 3^2 \cdot 5 \cdot 19$'dur. Bu üç asal kuvvet ikişer ikişer aralarında asal olduğundan, Teorem 5.2 gereği

$$9 \mid n^{72} - 1, \qquad 5 \mid n^{72} - 1, \qquad 19 \mid n^{72} - 1$$

olduğunu ayrı ayrı göstermek yeterlidir. Her üçünde de $\gcd(n, 855) = 1$ olması ilgili modülle aralarında asallığı garanti eder.
Modülo 9. $\phi(9) = 6$'dır; Teorem 21.2 gereği $n^6 \equiv 1 \pmod 9$'dur. $72 = 6 \cdot 12$ olduğundan

$$n^{72} = \left(n^6\right)^{12} \equiv 1 \pmod 9$$

Modülo 5. $\phi(5) = 4$'tür; $n^4 \equiv 1 \pmod 5$'tir. $72 = 4 \cdot 18$ olduğundan

$$n^{72} = \left(n^4\right)^{18} \equiv 1 \pmod 5$$

Modülo 19. $\phi(19) = 18$'dir; $n^{18} \equiv 1 \pmod{19}$'dur. $72 = 18 \cdot 4$ olduğundan

$$n^{72} = \left(n^{18}\right)^4 \equiv 1 \pmod{19}$$

Birleştirme. Üç modül de $n^{72} - 1$ sayısını böler ve ikişer ikişer aralarında asaldır; o hâlde çarpımları da böler:

$$855 = 9 \cdot 5 \cdot 19 \mid n^{72} - 1$$

■

i Neden $\phi(855) = 432$ değil de 72?

Teorem 21.2 doğrudan $n^{432} \equiv 1 \pmod{855}$ verirdi *($\phi(855) = 6 \cdot 4 \cdot 18 = 432$).* Ama biz çok daha küçük bir üs bulduk.
Nedeni şudur: her modül için ayrı ayrı çalışırken üssün **her birinin** ϕ değerine bölünmesi yeterlidir; hepsinin çarpımına değil. Aranan en küçük üs

$$\operatorname{lcm}\left(\phi(9), \phi(5), \phi(19)\right) = \operatorname{lcm}\left(6, 4, 18\right) = 36$$

olur — nitekim $72 = 2 \cdot 36$ de işe yarar. Bu, Euler teoreminin verdiğinden daha iyi bir üstür ve pratikte sık kullanılır.

21.4 Mertebe Kavramına Bir Bakış

Yukarıdaki gözlem doğal bir soruya götürür: $a^k \equiv 1 \pmod{n}$ eşitliğini sağlayan **en küçük** k nedir? Teorem 21.2 bize $k = \phi(n)$ değerinin daima işe yaradığını söylüyor. Ama bu, en küçük değer olmak zorunda değildir: Örnek 21.1'de $3^{20} \equiv 1 \pmod{100}$ bulmuştuk, oysa $\phi(100) = 40$'tır. Benzer biçimde Örnek 21.3'te $\phi(855) = 432$ iken 72 üssünün yettiğini gördük.

> **i** İleriye bir not: mertebe
>
> $a^k \equiv 1 \pmod{n}$ eşitliğini sağlayan en küçük pozitif k değerine, a sayısının **modülo n mertebesi** denir. Mertebenin daima $\phi(n)$'yi böldüğü gösterilebilir; bu da mertebe ararken yalnızca $\phi(n)$'nin bölenlerini denemenin yeterli olduğu anlamına gelir.
> Mertebe, kuvvet kongrüanslarının ve primitif köklerin anahtar kavramıdır. Sayılar Teorisi 2 dersinde ayrı bir bölümde ayrıntılı olarak ele alınmaktadır.

21.5 Euler Teoremiyle Ters Bulma

Sonuç 21.2 (Çarpımsal Tersin Kapalı Formülü). *$1 < n$ ve $\gcd(a, n) = 1$ olsun. Bu durumda a'nın modülo n çarpımsal tersi*

$$a^{-1} \equiv a^{\phi(n)-1} \pmod{n}$$

ile verilir.

Gerçekten de Teorem 21.2 gereği

$$a \cdot a^{\phi(n)-1} = a^{\phi(n)} \equiv 1 \pmod{n}$$

olur; Tanım 15.2 gereği bu, $a^{\phi(n)-1}$ sayısının a'nın tersi olduğunu söyler.

Örnek 21.4 (\$7\$ Sayısının Modülo \$30\$ Tersi). 7 tam sayısının modülo 30 çarpımsal tersini Sonuç 21.2 ile bulunuz.

Çözüm.
$30 = 2 \cdot 3 \cdot 5$ olduğundan

$$\phi(30) = 30 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 8$$

$\gcd(7, 30) = 1$ olduğundan Sonuç 21.2 uygulanabilir:

$$7^{-1} \equiv 7^{8-1} = 7^7 \pmod{30}$$

Şimdi 7^7 değerini adım adım hesaplayalım:

$$7^2 = 49 \equiv 19 \pmod{30}$$

$$7^4 = (7^2)^2 \equiv 19^2 = 361 \equiv 1 \pmod{30}$$

(Burada $\phi(30) = 8$ üssüne hiç ulaşmadan 1'e vardık; bu, yukarıda mertebe üzerine söylediklerimizin bir örneğidir.)

$$7^7 = 7^4 \cdot 7^2 \cdot 7 \equiv 1 \cdot 19 \cdot 7 = 133 \equiv 13 \pmod{30}$$

O hâlde 7'nin modülo 30 tersi **13**'tür.
(Sağlama: $7 \cdot 13 = 91 = 3 \cdot 30 + 1$ ✓*)*
■

i Hangi yöntem daha iyi?

Ters bulmanın iki yolunu gördük:

- **Öklid algoritması** *(Örnek 15.5)*: $\phi(n)$ bilinmese de çalışır ve hızlıdır.
- **Euler teoremi** *(Sonuç 21.2)*: kapalı bir formül verir, ama $\phi(n)$'yi — dolayısıyla n'nin asal çarpanlarını — bilmeyi gerektirir.

Büyük sayılarda çarpanlara ayırmak çok zor olduğundan pratikte birinci yol kullanılır. İkinci yolun değeri teoriktir: tersin varlığını ve biçimini tek satırda açıklar.

21.6 Çalışma Problemleri

Alıştırma 21.1 (Euler Teoremiyle Kalan Hesapları). Aşağıdaki kalanları bulunuz.
a) 7^{1000} sayısının 24 ile bölümünden kalan.
b) 9^{794} sayısının 100 ile bölümünden kalan.
c) 5^{2000} sayısının 63 ile bölümünden kalan.
d) 3^{1000} sayısının son üç rakamı.

Alıştırma 21.2 (Euler Teoremiyle Bölünebilme). Aşağıdakileri ispatlayınız.
a) $\gcd(n, 100) = 1$ olan her n için $100 \mid n^{20} - 1$.
b) $\gcd(n, 65) = 1$ olan her n için $65 \mid n^{12} - 1$.
c) Her n tam sayısı için $\gcd(n, 1729) = 1$ ise $1729 \mid n^{36} - 1$.
İpucu (c): $1729 = 7 \cdot 13 \cdot 19$'dur.

Alıştırma 21.3 (İndirgenmiş Kalan Sistemleri). **a)** Modülo 18 bir indirgenmiş kalan sistemi yazınız ve eleman sayısının $\phi(18)$ ile uyuştuğunu doğrulayınız.
b) $\{1, 5, 7, 11\}$ kümesinin modülo 12 bir indirgenmiş kalan sistemi olduğunu gösteriniz. Her elemanı 5 ile çarpıp sonucu modülo 12 indirgeyiniz ve Teorem 21.1'in söylediğini doğrulayınız.
c) $2 < n$ ve $\left\{r_1, \ldots, r_{\phi(n)} ight\}$ modülo n bir indirgenmiş kalan sistemi olsun.

$$r_1 + r_2 + \cdots + r_{\phi(n)} \equiv 0 \pmod{n}$$

olduğunu gösteriniz.
İpucu (c): $\gcd(r, n) = 1$ ise $\gcd(n - r, n) = 1$'dir; elemanları r ile $n - r$ biçiminde ikişerli eşleştiriniz ve $2 < n$ iken $reqn - r$ olduğunu gözlemleyiniz.

Alıştırma 21.4 (Euler Teoreminin Bir Genellemesi). m, n pozitif tam sayıları ve $\gcd(a, mn) = 1$ olsun.
a) $a^{\operatorname{lcm}(\phi(m), \phi(n))} \equiv 1 \pmod{mn}$ olduğunu gösteriniz *(*$\gcd(m, n) = 1$ *varsayarak).*
b) Bu üssün, Teorem 21.2'in verdiği $\phi(mn) = \phi(m)\phi(n)$ üssünden küçük olabileceğini bir örnekle gösteriniz.
İpucu (b): $m = 8$, $n = 5$ deneyiniz.

22. Kongrüansların Çözümleri

Sayılar Teorisi I dersinde birinci dereceden (lineer) kongrüansları incelemiştik. Bu derse, yüksek dereceden kongrüanslarla başlamadan önce "çözüm", "çözüm sayısı" ve "derece" kavramlarını kesin biçimde tanımlamamız gerekiyor.

22.1 Çözüm Kavramı

Tanım 22.1 (Kongrüansın Çözümü). $n \in \mathbb{N}$, $n \geq 1$ ve

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

olsun ($a_n \neq 0$; $a_n, a_{n-1}, \ldots, a_1, a_0 \in \mathbb{Z}$). $m \geq 2$ bir tam sayı olsun.
Eğer bir u tam sayısı için $f(u) \equiv 0 \pmod{m}$ oluyorsa, u tam sayısına $f(x) \equiv 0 \pmod{m}$ kongrüansının bir **çözümü** denir.

Örnek 22.1. 2 sayısı, $x^2 + 2x \equiv 0 \pmod{8}$ kongrüansının bir çözümüdür; çünkü

$$2^2 + 2 \cdot 2 = 8 \equiv 0 \pmod{8}$$

22.2 Hangi Çözümler "Aynı" Sayılır?

u tam sayısı $f(x) \equiv 0 \pmod{m}$ kongrüansının bir çözümü olsun. v bir tam sayı olmak üzere $v \equiv u \pmod{m}$ ise, bu durumda

$$f(v) \equiv f(u) \equiv 0 \pmod{m}$$

elde edilir; yani v de aynı kongrüansın bir çözümüdür.
O hâlde bir kongrüansın tek bir u çözümü varsa, $x \equiv u \pmod{m}$ koşulunu sağlayan **sonsuz sayıda** tam sayı da bu kongrüansın çözümüdür. Bu yüzden çözümleri tek tek saymak anlamsızdır; çözümleri denklik sınıfları düzeyinde ele almak gerekir.

> **i** Anlaşma
>
> u ve v tam sayıları, $f(x) \equiv 0 \pmod{m}$ kongrüansının iki çözümü olsun.
>
> - Eğer $u \not\equiv v \pmod{m}$ ise, u ve v'yi **iki ayrı çözüm** olarak sayarız.
> - Eğer $u \equiv v \pmod{m}$ ise, u ve v'yi **aynı çözüm** olarak sayarız.

Örnek 22.2. 3 ve 8 sayıları, $x^2 - x + 4 \equiv 0 \pmod{10}$ kongrüansının çözümleridir:

$$3^2 - 3 + 4 = 10 \equiv 0, \qquad 8^2 - 8 + 4 = 60 \equiv 0 \pmod{10}$$

$3 \not\equiv 8 \pmod{10}$ olduğundan bunlar kongrüansın **iki ayrı** çözümüdür.

22.3 Çözüm Sayısı

Tanım 22.2 (Çözüm Sayısı). $r_1, \ldots, r_m$ sayıları modülo m'ye göre bir **tam kalanlar sistemi** olsun. $f(x) \equiv 0 \pmod{m}$ kongrüansının **çözüm sayısı**,

$$f(r_i) \equiv 0 \pmod{m}$$

koşulunu sağlayan r_i ($i \in \{1, \ldots, m\}$) tam sayılarının adedidir.

> **i** İki temel gözlem
>
> - Bir $f(x) \equiv 0 \pmod{m}$ kongrüansının çözüm sayısı, seçilen tam kalanlar sisteminden **bağımsızdır**.
> - Bir $f(x) \equiv 0 \pmod{m}$ kongrüansının çözüm sayısı m'yi **geçemez**; çünkü modülo m'de yalnızca m tane denklik sınıfı vardır.

Örnek 22.3. $x^2 - 1 \equiv 0 \pmod{8}$ kongrüansının çözüm sayısını bulunuz.

Çözüm.
$0, 1, 2, \ldots, 7$ tam sayıları modülo 8'e göre bir tam kalanlar sistemidir. $f(x) = x^2 - 1$ diyelim ve her birini tek tek deneyelim:

x	0	1	2	3	4	5	6	7
$f(x) \bmod 8$	7	0	3	0	7	0	3	0

$f(1) \equiv f(3) \equiv f(5) \equiv f(7) \equiv 0 \pmod{8}$ ve diğerleri sıfırdan farklı olduğundan, kongrüansın **çözüm sayısı 4'tür**.
Tüm çözümler:

$$x \equiv 1, \quad x \equiv 3, \quad x \equiv 5, \quad x \equiv 7 \pmod{8}$$

22.4 Bir Kongrüansın Derecesi

Bir kongrüansın derecesi, polinomun derecesiyle karıştırılmamalıdır: baş katsayı modüle bölünüyorsa o terim kongrüansta hiçbir rol oynamaz.

Tanım 22.3 (Kongrüansın Derecesi). $f(x) = a_n x^n + \cdots + a_1 x + a_0$ olsun ($a_n \not\equiv 0$; katsayılar tam sayı).

- Eğer $a_n \not\equiv 0 \pmod{m}$ ise, $f(x) \equiv 0 \pmod{m}$ kongrüansının **derecesi n** olarak tanımlanır.
- Eğer $a_n \equiv 0 \pmod{m}$ ise, kongrüansın derecesi; $a_j \not\equiv 0 \pmod{m}$ koşulunu sağlayan **en büyük** j tam sayısıdır ($j \in \{0, \ldots, n-1\}$).
- Eğer $a_j \not\equiv 0 \pmod{m}$ koşulunu sağlayan hiçbir j yoksa — yani bütün katsayılar m ile bölünüyorsa — kongrüansın derecesi **tanımsızdır**.

> **⚠** Derece, polinomun derecesiyle aynı olmayabilir
>
> $f(x) = 6x^3 + 5x^2 + 1$ polinomunun derecesi 3'tür.
> Ancak modülo 6'da $6 \equiv 0$ olduğundan baş terim düşer; bir sonraki katsayı $5 \not\equiv 0 \pmod{6}$'dır. Dolayısıyla
>
> $$f(x) \equiv 0 \pmod{6}$$
>
> kongrüansının derecesi **2**'dir.

23. Yüksek Dereceden Kongrüanslar

$n \geq 1$ bir tam sayı ve

$$f(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0$$

olsun ($c_n \neq 0$; $c_n, \ldots, c_0 \in \mathbb{Z}$). Amacımız, $m \geq 2$ bir doğal sayı olmak üzere

$$f(x) \equiv 0 \pmod{m}$$

kongrüansını çözmektir.
Doğrudan modülo m'de çalışmak, m büyüdükçe elverişsizleşir. Bunun yerine problemi, m'nin asal kuvvet çarpanlarına göre daha küçük parçalara ayırırız.

23.1 İndirgeme Teoremi

Teorem 23.1 (Asal Kuvvetlere İndirgeme). *m sayısının asal çarpanlara ayrılışı $m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ olsun. Bu durumda $f(x) \equiv 0 \pmod{m}$ kongrüansını çözme problemi,*

$$\begin{aligned} &f(x) \equiv 0 \pmod{p_1^{e_1}} \\ &f(x) \equiv 0 \pmod{p_2^{e_2}} \\ &\quad\vdots \\ &f(x) \equiv 0 \pmod{p_k^{e_k}}\} \end{aligned} \qquad (*)$$

*kongrüans sistemini çözme problemine **denktir**.*

İspat.
($\Rightarrow$) Kongrüans çözülebilirse sistem de çözülebilirdir.
$f(x) \equiv 0 \pmod{m}$ çözülebilir olsun; yani $f(u) \equiv 0 \pmod{m}$ olacak şekilde bir u tam sayısı vardır. Her i için $p_i^{e_i} \mid m$ olduğundan

$$f(u) \equiv 0 \pmod{p_i^{e_i}}, \qquad i = 1, \ldots, k$$

bulunur. Yani $(*)$ sistemindeki her kongrüans da çözülebilirdir.
($\Leftarrow$) Sistem çözülebilirse kongrüans da çözülebilirdir.
$(*)$ sistemindeki kongrüansların hepsi çözülebilir olsun. Bu durumda

$$f(a_1) \equiv 0 \pmod{p_1^{e_1}}, \quad f(a_2) \equiv 0 \pmod{p_2^{e_2}}, \quad \ldots, \quad f(a_k) \equiv 0 \pmod{p_k^{e_k}}$$

olacak şekilde $a_1, \ldots, a_k$ tam sayıları vardır.
Farklı asal kuvvetler aralarında asal olduğundan

$$\left(\frac{m}{p_i^{e_i}}, p_i^{e_i} \right) = 1, \qquad i = 1, \ldots, k$$

olur. Dolayısıyla her i için

$$\frac{m}{p_i^{e_i}} x \equiv 1 \pmod{p_i^{e_i}}$$

lineer kongrüansı çözülebilirdir; yani

$$\frac{m}{p_i^{e_i}} b_i \equiv 1 \pmod{p_i^{e_i}}$$

olacak şekilde $b_1, ..., b_k$ tam sayıları vardır. Şimdi

$$u = \frac{m}{p_1^{e_1}} b_1 a_1 + \frac{m}{p_2^{e_2}} b_2 a_2 + \cdots + \frac{m}{p_k^{e_k}} b_k a_k \in \mathbb{Z}$$

diyelim. Toplamdaki $j \neq i$ terimlerinin her biri $p_i^{e_i}$ ile bölündüğünden, modülo $p_i^{e_i}$'de yalnızca i. terim kalır:

$$u \equiv \frac{m}{p_i^{e_i}} b_i a_i \equiv 1 \cdot a_i = a_i \pmod{p_i^{e_i}}$$

O hâlde $u \equiv a_1 \pmod{p_1^{e_1}}$,...,$u \equiv a_k \pmod{p_k^{e_k}}$ olur. Buradan

$$\begin{aligned} f(u) &\equiv f(a_1) \equiv 0 \pmod{p_1^{e_1}} \\ f(u) &\equiv f(a_2) \equiv 0 \pmod{p_2^{e_2}} \\ &\vdots \\ f(u) &\equiv f(a_k) \equiv 0 \pmod{p_k^{e_k}} \end{aligned}$$

elde edilir. Bir sayı, her biri diğerleriyle aralarında asal olan sayıların hepsine bölünüyorsa en küçük ortak katlarına da bölünür:

$$f(u) \equiv 0 \pmod{\left[p_1^{e_1}, ..., p_k^{e_k}\right]}$$

$(p_i^{e_i}, p_j^{e_j}) = 1$ $(i \neq j)$ olduğundan

$$\left[p_1^{e_1}, ..., p_k^{e_k}\right] = p_1^{e_1} \cdots p_k^{e_k} = m$$

olur. Sonuç olarak $f(u) \equiv 0 \pmod{m}$, yani asıl kongrüans da çözülebilirdir.
■

Bu teoremin iki doğrudan sonucu vardır ve pratikte sürekli kullanılır.

! Çözümsüzlük ölçütü

$f(x) \equiv 0 \pmod{p_i^{e_i}}$ kongrüanslarından **herhangi birinin** çözümü yoksa, $f(x) \equiv 0 \pmod{m}$ kongrüansının da çözümü yoktur.
Bu, çözümsüzlüğü göstermenin en hızlı yoludur: tek bir küçük asal kuvvet yeter.

Teorem 23.2 (Çözüm Sayısının Çarpımsallığı). *$f(x) \equiv 0 \pmod{p_i^{e_i}}$ kongrüansının çözüm sayısı N_i olsun $(i = 1, ..., k)$. Bu durumda $f(x) \equiv 0 \pmod{m}$ kongrüansının çözüm sayısı*

$$N = N_1 \cdot N_2 \cdots N_k$$

dır.

23.2 Çözüm Algoritması

1. m sayısını asal çarpanlarına ayırın: $m = p_1^{e_1} \cdots p_k^{e_k}$.
2. Her $p_i^{e_i}$ için $f(x) \equiv 0 \pmod{p_i^{e_i}}$ kongrüansının çözümlerini bulun. Modüller küçük olduğundan bu adım genellikle deneme yoluyla yapılabilir.
3. Herhangi biri çözümsüzse durun: asıl kongrüans da çözümsüzdür.
4. Her i için $\frac{m}{p_i^{e_i}} b_i \equiv 1 \pmod{p_i^{e_i}}$ denkliğinden b_i değerlerini hesaplayın.
5. Çözümleri şu formülle birleştirin:

$$x \equiv \sum_{i=1}^{k} \frac{m}{p_i^{e_i}} \, b_i \, a_i \pmod{m}$$

Burada a_i, i. alt kongrüansın çözümlerinden biridir. Tüm $(a_1, \ldots, a_k)$ kombinasyonları alınarak $N_1 N_2 \cdots N_k$ çözümün hepsi elde edilir.

23.3 Çözümlü Uygulamalar

Örnek 23.1. $x^2 + x + 7 \equiv 0 \pmod{189}$ kongrüansını çözünüz.

Çözüm.
$189 = 3^3 \cdot 7 = 27 \cdot 7$ olduğundan $x^2 + x + 7 \equiv 0 \pmod{27}$ ve $x^2 + x + 7 \equiv 0 \pmod{7}$ kongrüanslarının çözümlerini bulalım.
Alt kongrüanslar.
Modülo 27'de çözümler:

$$x \equiv 4, \quad x \equiv 13, \quad x \equiv -5 \pmod{27}$$

(Sağlama: $4^2 + 4 + 7 = 27$, $13^2 + 13 + 7 = 189 = 7 \cdot 27$, $(-5)^2 - 5 + 7 = 27$.*)*
Modülo 7'de çözümler:

$$x \equiv 0, \quad x \equiv -1 \pmod{7}$$

(Sağlama: $0 + 0 + 7 = 7$, $1 - 1 + 7 = 7$.*)*
Buna göre çözüm sayısı $N = 3 \cdot 2 = 6$ olacaktır.
Birleştirme katsayıları.
$\frac{189}{27} = 7$ ve $7b_1 \equiv 1 \pmod{27}$: $7 \cdot 4 = 28 \equiv 1$ olduğundan $b_1 \equiv 4 \pmod{27}$.
$\frac{189}{7} = 27$ ve $27b_2 \equiv 1 \pmod{7}$: $27 \equiv -1$ olduğundan $b_2 \equiv -1 \pmod{7}$.
O hâlde çözümler

$$x \equiv 7 \cdot 4 \cdot a_1 + 27 \cdot (-1) \cdot a_2 = 28a_1 - 27a_2 \pmod{189}$$

biçimindedir; burada $a_1 \in \{4, 13, -5\}$ ve $a_2 \in \{0, -1\}$'dir.

a_1	a_2	$28a_1 - 27a_2$	mod 189
4	0	112	112
4	-1	139	139
13	0	364	175
13	-1	391	13
-5	0	-140	49
-5	-1	-113	76

Sonuç. $x^2 + x + 7 \equiv 0 \pmod{189}$ kongrüansının tüm çözümleri:

$$x \equiv 13{,}49{,}76{,}112{,}139{,}175 \pmod{189}$$

(Sağlama örneği: $13^2 + 13 + 7 = 189 \equiv 0$; $49^2 + 49 + 7 = 2457 = 189 \cdot 13 \equiv 0$.*)*
■

Örnek 23.2. $f(x) = x^3 + 19x^2 - x + 23 \equiv 0 \pmod{42}$ kongrüansını çözünüz.

Çözüm.
$42 = 2 \cdot 3 \cdot 7$ olduğundan üç alt kongrüansı ayrı ayrı çözelim. Katsayıları her modülde indirgemek işi kolaylaştırır.
Modülo 2. $19 \equiv 1$, $23 \equiv 1$ olduğundan

$$f(x) \equiv x^3 + x^2 + x + 1 \equiv 0 \pmod{2}$$

Çözüm: $x \equiv 1 \pmod{2}$. *(Tek çözüm,* $N_1 = 1$.*)*

Modülo 3. $19 \equiv 1$, $23 \equiv 2$ olduğundan

$$f(x) \equiv x^3 + x^2 - x + 2 \equiv 0 \pmod 3$$

Çözümler: $x \equiv 1$ ve $x \equiv -1 \pmod 3$. *($N_2 = 2$.)*
Modülo 7. $19 \equiv 5$, $23 \equiv 2$ olduğundan

$$f(x) \equiv x^3 + 5x^2 - x + 2 \equiv 0 \pmod 7$$

Çözümler: $x \equiv 1$, $x \equiv 2$ ve $x \equiv -1 \pmod 7$. *($N_3 = 3$.)*
O hâlde çözüm sayısı $N = 1 \cdot 2 \cdot 3 = 6$'dır.
Birleştirme katsayıları.
$\frac{42}{2} = 21$ ve $21b_1 \equiv 1 \pmod 2$: $21 \equiv 1$ olduğundan $b_1 \equiv 1 \pmod 2$.
$\frac{42}{3} = 14$ ve $14b_2 \equiv 1 \pmod 3$: $14 \equiv 2$, $2 \cdot 2 = 4 \equiv 1$ olduğundan $b_2 \equiv -1 \pmod 3$.
$\frac{42}{7} = 6$ ve $6b_3 \equiv 1 \pmod 7$: $6 \equiv -1$ olduğundan $b_3 \equiv -1 \pmod 7$.
Çözümler:

$$x \equiv 21a_1 - 14a_2 - 6a_3 \pmod{42}$$

burada $a_1 = 1$; $a_2 \in \{1, -1\}$; $a_3 \in \{1, 2, -1\}$.

a_1	a_2	a_3	$21a_1 - 14a_2 - 6a_3$
1	1	1	1
1	1	2	$-5 \equiv 37$
1	1	-1	13
1	-1	1	29
1	-1	2	23
1	-1	-1	41

Sonuç. Kongrüansın tüm çözümleri:

$$x \equiv 1{,}13{,}23{,}29{,}37{,}41 \pmod{42}$$

(Sağlama örneği: $x = 1$ için $1 + 19 - 1 + 23 = 42 \equiv 0$; $x = 23$ için $12167 + 10051 - 23 + 23 = 22218 = 42 \cdot 529 \equiv 0$.)
■

23.4 Problemler

Alıştırma 23.1 (Kongrüansları Çözme). Aşağıdaki kongrüansları çözünüz.
a) $x^3 + 2x - 3 \equiv 0 \pmod 9$ **b)** $x^3 + 2x - 3 \equiv 0 \pmod 5$
c) $x^3 + 2x - 3 \equiv 0 \pmod{45}$ **d)** $x^3 + 4x + 8 \equiv 0 \pmod{15}$
İpucu: (c) şıkkında $45 = 9 \cdot 5$ olduğundan (a) ve (b) şıklarının sonuçlarını birleştirmeniz yeterlidir.

24. Asal Kuvvet Modüllerde Kök Yükseltme

Bir önceki bölümde $f(x) \equiv 0 \pmod{m}$ kongrüansını çözme problemini, p asal ve $s \geq 1$ olmak üzere

$$f(x) \equiv 0 \pmod{p^s}$$

biçimindeki kongrüanslara indirgemiştik. Şimdi bu kongrüansın nasıl çözüleceğini göreceğiz.
Yöntemin çıkış noktası basit bir gözlemdir: u tam sayısı $f(x) \equiv 0 \pmod{p^s}$ kongrüansının bir çözümü ise, $p \mid p^s$ olduğundan $f(u) \equiv 0 \pmod{p}$ de sağlanır. Yani

> ! Temel gözlem
>
> $f(x) \equiv 0 \pmod{p^s}$ kongrüansının **her** çözümü, aynı zamanda $f(x) \equiv 0 \pmod{p}$ kongrüansının da bir çözümüdür.

Demek ki modülo p^s çözümlerini, modülo p çözümlerinin arasında aramamız yeterlidir. Bu yüzden $f(x) \equiv 0 \pmod{p}$ kongrüansından yola çıkıp

$$f(x) \equiv 0 \pmod{p^2}, \qquad f(x) \equiv 0 \pmod{p^3}, \qquad \ldots$$

kongrüanslarını modül p^s olana dek **basamak basamak** çözeriz. Her basamakta bir önceki basamağın çözümlerini "yükseltmeye" çalışırız. Bu tekniğe **kök yükseltme (kök taşıma)** denir.

24.1 Analizden Hatırlatmalar

Yükseltme adımının kalbinde, polinomların sonlu Taylor açılımı yatar. Bu açılımın burada kullanılabilmesi için katsayıların tam sayı olması gerekir; aşağıdaki üç hatırlatma tam olarak bunu güvenceye alır.

Teorem 24.1 (Binom Teoremi). *n bir pozitif tam sayı olsun. Bu durumda her a ve b için*

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n}b^n$$

*olur. Burada $0 \leq k \leq n$ olmak üzere **binom katsayıları***

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{1 \cdot 2 \cdots k} = \frac{n!}{k!\,(n-k)!} = \binom{n}{n-k}$$

*biçiminde tanımlanır ve **tam sayıdır**.*

i Kuvvet fonksiyonunun türevleri

p bir pozitif tam sayı ve $f(x) = x^p$ olsun. O hâlde

$$f'(x) = px^{p-1}, \qquad f''(x) = p(p-1)x^{p-2}, \qquad \dots$$

ve genel olarak $0 < n \leq p$ için

$$f^{(n)}(x) = p(p-1)\cdots(p-n+1)\,x^{p-n}$$

olur. Her iki tarafı $n!$'e bölersek

$$\frac{f^{(n)}(x)}{n!} = \binom{p}{n} x^{p-n}, \qquad 0 \leq n \leq p$$

elde edilir (eşitlik $n = 0$ için de doğrudur). Özel olarak $f^{(p)}(x) = p!$ ve $n > p$ için $f^{(n)}(x) = 0$'dır.

Buradan, tam katsayılı bir polinomun türevleri hakkında kilit sonucu okuyabiliriz.

Lemma 24.1 (Bölünmüş Türevler Tam Katsayılıdır). *$g(x) = a_p x^p + a_{p-1}x^{p-1} + \cdots + a_1 x + a_0$ tam katsayılı bir polinom olsun ($a_p \neq 0$). Bu durumda her $0 \leq n \leq p$ tam sayısı için*

$$\frac{g^{(n)}(x)}{n!} = a_p\binom{p}{n}x^{p-n} + a_{p-1}\binom{p-1}{n}x^{p-1-n} + \cdots + a_n\binom{n}{n}$$

*olur; yani $\frac{g^{(n)}(x)}{n!}$, $(p-n)$. dereceden **tam katsayılı** bir polinomdur. Ayrıca $n > p$ için $g^{(n)}(x) = 0$'dır.*

Neden önemli?

$\frac{g^{(n)}(x)}{n!}$ tam katsayılı olduğu için, her a tam sayısında aldığı değer de tam sayıdır:

$$\frac{g^{(n)}(a)}{n!} \in \mathbb{Z}$$

Taylor açılımının terimlerini modülo p^k incelerken tam da bu kullanılacak.

Teorem 24.2 (Taylor Teoremi (Polinomlar İçin)). *p bir pozitif tam sayı ve $g(x) = a_p x^p + \cdots + a_1 x + a_0$ tam katsayılı bir polinom olsun. x_0 ve h herhangi iki sayı olmak üzere*

$$g(x_0 + h) = g(x_0) + \frac{g'(x_0)}{1!}h + \frac{g''(x_0)}{2!}h^2 + \cdots + \frac{g^{(p)}(x_0)}{p!}h^p$$

*eşitliği geçerlidir. Polinomlarda açılım **sonludur**: kalan terim yoktur.*

İspat.
$g(x_0 + h)$ ifadesindeki $(x_0 + h)$ kuvvetlerini Binom Teoremi'ne göre açalım:

$$\begin{aligned} g(x_0+h) =& a_p x_0^p + \binom{p}{1}a_p x_0^{p-1}h + \binom{p}{2}a_p x_0^{p-2}h^2 + \cdots + a_p h^p \\ &+ a_{p-1}x_0^{p-1} + \binom{p-1}{1}a_{p-1}x_0^{p-2}h + \cdots + a_{p-1}h^{p-1} \\ &+ \vdots \\ &+ a_1 x_0 + a_1 h \\ &+ a_0 \end{aligned}$$

Şimdi bu ifadeyi h'nin kuvvetlerine göre yeniden düzenleyelim. h^k ile çarpılan terimlerin toplamı

$$\left[\binom{p}{k}a_p x_0^{p-k} + \binom{p-1}{k}a_{p-1}x_0^{p-1-k} + \cdots + \binom{k+1}{k}a_{k+1}x_0 + \binom{k}{k}a_k\right]h^k$$

olur. Köşeli parantezin içi, Lemma 24.1 gereği tam olarak $\frac{g^{(k)}(x_0)}{k!}$ ifadesidir. O hâlde

$$g(x_0+h)=\sum_{k=0}^{p}\frac{g^{(k)}(x_0)}{k!}h^k$$

bulunur. Son olarak $n>p$ için $g^{(n)}(x_0)=0$ olduğundan, toplama istenildiği kadar sıfır terim eklenebilir; açılımın değeri değişmez.
■

24.2 Modülo p'den Modülo p^2'ye

Önce en küçük adımı ayrıntısıyla inceleyelim: elimizde $f(x)\equiv 0 \pmod p$ kongrüansının çözümleri var; bunları modülo p^2'ye taşımak istiyoruz.
$f(x)\equiv 0 \pmod p$ kongrüansı için iki durum söz konusudur.
1. durum. Kongrüans çözümsüzdür. Bu durumda $f(x)\equiv 0 \pmod{p^s}$ kongrüansı da çözümsüzdür (temel gözlem).
2. durum. Kongrüans çözülebilirdir; çözümleri

$$x\equiv a_1,\quad x\equiv a_2,\quad \ldots,\quad x\equiv a_t \pmod p$$

olsun. $f(x)\equiv 0 \pmod{p^2}$ kongrüansının çözümlerini bu t tane sınıfın içinde arayacağız.
Bir $j\in\{1,\ldots,t\}$ sabitleyip $x\equiv a_j \pmod p$ koşulunu sağlayan çözümleri arayalım. Bu koşul

$$x\equiv a_j \pmod p \Leftrightarrow x=a_j+py,\qquad y\in\mathbb{Z}$$

demektir. O hâlde

$$f(x)\equiv 0 \pmod{p^2} \Leftrightarrow f(a_j+py)\equiv 0 \pmod{p^2}$$

olur. Şimdi $f(a_j+py)$ ifadesini Teorem 24.2 ile açalım:

$$f(a_j+py)=f(a_j)+\frac{f'(a_j)}{1!}(py)+\underbrace{\frac{f''(a_j)}{2!}}_{\in\mathbb{Z}}(py)^2+\cdots+\underbrace{\frac{f^{(n)}(a_j)}{n!}}_{\in\mathbb{Z}}(py)^n$$

Üçüncü terimden itibaren her terim p^2 ile bölünür ve katsayıları tam sayıdır; dolayısıyla modülo p^2'de düşerler:

$$f(a_j+py)\equiv 0 \pmod{p^2} \Leftrightarrow f(a_j)+f'(a_j)\,py\equiv 0 \pmod{p^2}$$

a_j modülo p'de bir çözüm olduğundan $p\mid f(a_j)$, yani $\frac{f(a_j)}{p}\in\mathbb{Z}$'dir. Her iki tarafı ve modülü p'ye bölebiliriz:

$$ax\equiv ay \pmod m \Leftrightarrow x\equiv y\left(\bmod \frac{m}{(a,m)}\right)$$

kuralı gereği

$$\boxed{\frac{f(a_j)}{p}+f'(a_j)\,y\equiv 0 \pmod p}$$

elde edilir. Bu, y bilinmeyenine göre **birinci dereceden** bir kongrüanstır; onu çözmeyi zaten biliyoruz.

24.3 Genel Yükseltme Adımı

Yukarıdaki hesabın $p\to p^2$ geçişine özel hiçbir yanı yoktur. $\alpha\geq 1$ olmak üzere $p^\alpha\to p^{\alpha+1}$ geçişi de aynı biçimde yürür: $x=b+yp^\alpha$ yazıldığında Taylor açılımının üçüncü terimi $p^{2\alpha}$ ile bölünür ve $\alpha\geq 1$ için

$$2\alpha\geq\alpha+1$$

olduğundan bu terim modülo $p^{\alpha+1}$'de yok olur. Bu gözlemi bir teorem olarak toplayalım.

Teorem 24.3 (Yükseltme Lemması). *$f(x)$ tam katsayılı bir polinom, p bir asal sayı ve $\alpha \geq 1$ bir tam sayı olsun. b tam sayısı*

$$f(b) \equiv 0 \pmod{p^{\alpha}}$$

kongrüansının bir çözümü olsun. Bu durumda $f(x) \equiv 0 \pmod{p^{\alpha+1}}$ kongrüansının $x \equiv b \pmod{p^{\alpha}}$ koşulunu sağlayan çözümleri, tam olarak

$$x \equiv b + y\,p^{\alpha} \pmod{p^{\alpha+1}}$$

biçimindeki sayılardır; burada y,

$$\frac{f(b)}{p^{\alpha}} + f'(b)\,y \equiv 0 \pmod{p} \qquad (*)$$

lineer kongrüansının çözümleridir.

> ***İspat.***
> $x \equiv b \pmod{p^{\alpha}}$ *koşulu* $x = b + yp^{\alpha}$ *($y \in \mathbb{Z}$) demektir. Teorem 24.2 ile*
>
> $$f(b + yp^{\alpha}) = f(b) + f'(b)\,yp^{\alpha} + \frac{f''(b)}{2!}(yp^{\alpha})^2 + \cdots + \frac{f^{(n)}(b)}{n!}(yp^{\alpha})^n$$
>
> *yazılır. Lemma 24.1 gereği tüm $\frac{f^{(k)}(b)}{k!}$ katsayıları tam sayıdır. Üçüncü terimden itibaren her terim $p^{2\alpha}$ ile bölünür ve $2\alpha \geq \alpha + 1$ olduğundan bu terimler modülo $p^{\alpha+1}$'de sıfırdır. Böylece*
>
> $$f(b + yp^{\alpha}) \equiv 0 \pmod{p^{\alpha+1}} \Leftrightarrow f(b) + f'(b)\,y\,p^{\alpha} \equiv 0 \pmod{p^{\alpha+1}}$$
>
> *olur. $f(b) \equiv 0 \pmod{p^{\alpha}}$ olduğundan $\frac{f(b)}{p^{\alpha}} \in \mathbb{Z}$'dir ve*
>
> $$ax \equiv ay \pmod{m} \Leftrightarrow x \equiv y \left(\bmod \frac{m}{(a,m)} \right)$$
>
> *kuralı $a = p^{\alpha}$, $m = p^{\alpha+1}$ ile uygulanırsa $(*)$ elde edilir.*
> ■

$(*)$ kongrüansı y'ye göre lineer olduğundan, çözüm sayısı $f'(b)$ ile p'nin ortak bölenine bağlıdır. Üç seçenek vardır.

Teorem 24.4 (Yükseltmenin Üç Hâli). *Teorem 24.3'nin varsayımları altında:*
i) *$(f'(b), p) = 1$, yani $p \nmid f'(b)$ ise: $(*)$ kongrüansının **bir tek** $y \equiv y_0 \pmod{p}$ çözümü vardır. Dolayısıyla $f(x) \equiv 0 \pmod{p^{\alpha+1}}$ kongrüansının, $x \equiv b \pmod{p^{\alpha}}$ koşulunu sağlayan **bir tek** çözümü vardır:*

$$x \equiv b + p^{\alpha} y_0 \pmod{p^{\alpha+1}}$$

ii) *$p \mid f'(b)$ ve $\frac{f(b)}{p^{\alpha}} \not\equiv 0 \pmod{p}$ ise: $(*)$ kongrüansını sağlayan hiçbir y tam sayısı yoktur. Dolayısıyla $x \equiv b \pmod{p^{\alpha}}$ koşulunu sağlayan **hiçbir** çözüm yoktur; kök bu basamakta **ölür**.*
iii) *$p \mid f'(b)$ ve $\frac{f(b)}{p^{\alpha}} \equiv 0 \pmod{p}$ ise: $(*)$ kongrüansı $0 \equiv 0$ hâline gelir ve $y \equiv 0, 1, \ldots, p-1 \pmod{p}$ değerlerinin hepsi çözümdür. Dolayısıyla **tam p tane** çözüm doğar:*

$$x \equiv b, \quad b + p^{\alpha}, \quad b + 2p^{\alpha}, \quad \ldots, \quad b + (p-1)p^{\alpha} \pmod{p^{\alpha+1}}$$

(i) hâli, klasik olarak **Hensel lemması** adıyla anılır: türevin modülo p'de sıfırdan farklı olduğu (yani **basit**, tekrarlı olmayan) bir kök, her basamakta tek türlü ve kesintisiz biçimde yükselir.

i Hensel lemması

$f(a) \equiv 0 \pmod{p}$ ve $p \nmid f'(a)$ olsun. Bu durumda her $s \geq 1$ için $f(x) \equiv 0 \pmod{p^s}$ kongrüansının $x \equiv a \pmod{p}$ koşulunu sağlayan **bir tek** çözümü vardır.
Nedeni basittir: yükseltilen kök her adımda $b \equiv a \pmod{p}$ kaldığından $f'(b) \equiv f'(a) \not\equiv 0 \pmod{p}$ olur; yani (i) hâli sonsuza kadar korunur.

24.4 Çözüm Algoritması

$f(x) \equiv 0 \pmod{p^s}$ kongrüansını çözmek için:

1. $f(x) \equiv 0 \pmod{p}$ kongrüansını, modülo p'ye göre bir tam kalanlar sistemini deneyerek çözün. Çözüm yoksa durun: asıl kongrüans da çözümsüzdür.
2. $f'(x)$ türevini hesaplayın.
3. $\alpha = 1$ ile başlayın. Elinizdeki her b çözümü için $\frac{f(b)}{p^\alpha} + f'(b)y \equiv 0 \pmod{p}$ kongrüansını çözün; Teorem 24.4'a göre bu b'den 0, 1 veya p tane yeni çözüm doğar.
4. α'yı bir artırıp 3. adımı tekrarlayın; $\alpha = s - 1$ basamağı bitince modülo p^s çözümlerinin tamamı elde edilmiş olur.

24.5 Çözümlü Uygulamalar

Örnek 24.1. $x^3 - 3x^2 + 27 \equiv 0 \pmod{5^3}$ kongrüansının çözümlerini araştırınız.

Çözüm.
$f(x) = x^3 - 3x^2 + 27$ ve $f'(x) = 3x^2 - 6x$ olsun.
1. basamak: modülo 5. $0, \pm 1, \pm 2$ sayıları modülo 5'e göre bir tam kalanlar sistemidir.

x	0	1	-1	2	-2
$f(x)$	27	25	23	23	7
$f(x) \bmod 5$	2	0	3	3	2

Yalnızca $f(1) \equiv 0 \pmod{5}$ olduğundan kongrüansın bir tek çözümü vardır: $x \equiv 1 \pmod{5}$.
2. basamak: modülo 5^2. $\alpha = 1$ ve $b = 1$ için

$$\frac{f(1)}{5} + f'(1)\, y \equiv 0 \pmod{5}$$

kongrüansını çözelim. $f(1) = 1 - 3 + 27 = 25$ ve $f'(1) = 3 - 6 = -3$ olduğundan

$$5 - 3y \equiv 0 \pmod{5} \Leftrightarrow -3y \equiv 0 \pmod{5}$$

olur. $(-3, 5) = 1$ olduğundan bir tek çözüm vardır: $y \equiv 0 \pmod{5}$. O hâlde

$$x \equiv 1 + 5 \cdot 0 = 1 \pmod{5^2}$$

3. basamak: modülo 5^3. Şimdi $\alpha = 2$ ve $b = 1$ için

$$\frac{f(1)}{5^2} + f'(1)\, y \equiv 0 \pmod{5}$$

kongrüansını çözelim. $\frac{25}{25} = 1$ olduğundan

$$1 - 3y \equiv 0 \pmod{5} \Leftrightarrow 2y \equiv 1 \pmod{5} \Leftrightarrow 2y \equiv 6 \pmod{5} \Leftrightarrow y \equiv 3 \cdot 2 \equiv 2 \pmod{5}$$

(Ara adım: $(2, 5) = 1$ *olduğundan sadeleştirme yapılabilir.)* Buradan

$$x \equiv 1 + 5^2 \cdot 2 = 51 \pmod{5^3}$$

Sonuç. Kongrüansın bir tek çözümü vardır: $x \equiv 51 \pmod{125}$.
Sağlama. $x = 51$ değeri için kongrüansın sol tarafı 125'in katıdır:

$$51^3 - 3 \cdot 51^2 + 27 = 132651 - 7803 + 27 = 124875 = 125 \cdot 999$$

Dikkat edilirse $p = 5 \nmid f'(1) = -3$ olduğundan bu, Hensel lemmasının tipik bir uygulamasıdır: kök her basamakta tek türlü yükselmiştir.
■

Örnek 24.2. $x^3 + x + 1 \equiv 0 \pmod{3^2}$ kongrüansını çözünüz.

Çözüm.
$f(x) = x^3 + x + 1$ ve $f'(x) = 3x^2 + 1$ olsun.
1. basamak: modülo 3. $0, \pm 1$ sayıları modülo 3'e göre bir tam kalanlar sistemidir. $f(0) = 1 \not\equiv 0$, $f(-1) = -1 \not\equiv 0$ ve $f(1) = 3 \equiv 0 \pmod{3}$ olduğundan bir tek çözüm vardır: $x \equiv 1 \pmod{3}$.
2. basamak: modülo 3^2. $f(1) = 3$ ve $f'(1) = 4$ olduğundan

$$\frac{f(1)}{3} + f'(1)\, y \equiv 0 \pmod{3} \Leftrightarrow 1 + 4y \equiv 0 \pmod{3}$$

olur. $(4, 3) = 1$ olduğundan bir tek çözüm vardır: $4y \equiv -1$, yani $y \equiv -1 \pmod{3}$.
Sonuç. $x^3 + x + 1 \equiv 0 \pmod{3^2}$ kongrüansının bir tek çözümü vardır:

$$x \equiv 1 + 3 \cdot (-1) = -2 \equiv 7 \pmod{9}$$

(Sağlama: $7^3 + 7 + 1 = 351 = 9 \cdot 39$*.)*
■

Örnek 24.3. $x^3 + x - 19 \equiv 0 \pmod{7^2}$ kongrüansını çözünüz.

Çözüm.
$f(x) = x^3 + x - 19$ ve $f'(x) = 3x^2 + 1$ olsun.
1. basamak: modülo 7. $0, \pm 1, \pm 2, \pm 3$ sayıları modülo 7'ye göre bir tam kalanlar sistemidir.

x	0	1	-1	2	-2	3	-3
$f(x)$	-19	-17	-21	-9	-29	11	-49
$f(x) \bmod 7$	2	4	0	5	6	4	0

O hâlde $f(x) \equiv 0 \pmod{7}$ kongrüansının **iki** çözümü vardır: $x \equiv -1$ ve $x \equiv -3 \pmod{7}$. Her ikisini ayrı ayrı yükseltelim.
i) $a_1 = -1$ için. $f(-1) = -21$ ve $f'(-1) = 4$ olduğundan

$$\frac{f(-1)}{7} + f'(-1)\, y \equiv 0 \pmod{7} \Leftrightarrow -3 + 4y \equiv 0 \pmod{7}$$

olur. $(4, 7) = 1$ olduğundan bir tek çözüm vardır:

$$4y \equiv 3 \equiv 24 \pmod{7} \Leftrightarrow y \equiv 6 \equiv -1 \pmod{7}$$

Buradan $x \equiv -1 + 7 \cdot (-1) = -8 \equiv 41 \pmod{7^2}$ bulunur. *(Bu, (i) hâli: kök tek türlü yükseldi.)*
ii) $a_2 = -3$ için. $f(-3) = -27 - 3 - 19 = -49$ ve $f'(-3) = 28$ olduğundan

$$\frac{f(-3)}{7} + f'(-3)\, y \equiv 0 \pmod{7} \Leftrightarrow -7 + 28y \equiv 0 \pmod{7}$$

olur. Burada $7 \mid 28 = f'(-3)$ ve $\frac{f(-3)}{7} = -7 \equiv 0 \pmod{7}$'dir; yani Teorem 24.4'un (iii) hâlindeyiz. Kongrüans her y için sağlanır ve **tam 7 tane** çözüm doğar: $y \equiv 0, 1, \ldots, 6 \pmod{7}$. Bunlara karşılık gelen $x \equiv -3 + 7y \pmod{7^2}$ çözümleri:

y	0	1	2	3	4	5	6
$x \bmod 49$	46	4	11	18	25	32	39

Sonuç. $x^3 + x - 19 \equiv 0 \pmod{7^2}$ kongrüansının **sekiz** çözümü vardır:

$$x \equiv 4{,}11{,}18{,}25{,}32{,}39{,}41{,}46 \pmod{49}$$

(Sağlama örneği: $4^3 + 4 - 19 = 49$*;* $11^3 + 11 - 19 = 1323 = 49 \cdot 27$*;* $41^3 + 41 - 19 = 68943 = 49 \cdot 1407$*.)*
■

⚠ Çözüm sayısı derecenin üstüne çıkabilir

Son örnekte kongrüansın derecesi 3 olmasına rağmen modülo 49'da **sekiz** çözüm çıktı. Bu bir çelişki değildir: çözüm sayısının dereceyi aşamaması yalnızca **asal** modüller için geçerlidir. Bu sonucu bir sonraki bölümde ispatlayacağız.

24.6 Problemler

Alıştırma 24.1 (Asal Kuvvet Modülleri). Aşağıdaki kongrüansları çözünüz.
a) $x^5 + x^4 + 1 \equiv 0 \pmod{3^3}$ **b)** $x^3 + x + 57 \equiv 0 \pmod{5^3}$
c) $x^3 + x^2 - 5 \equiv 0 \pmod{7^3}$ **d)** $x^3 + 10x^2 + x + 2 \equiv 0 \pmod{3^3}$
İpucu: Her şıkta önce modülo p çözümlerini bulun, sonra yükseltme adımını basamak basamak uygulayın. Türevin modülo p'de sıfır olduğu basamaklara özellikle dikkat edin: orada kök ya ölür ya da p kola ayrılır.

25. Asal Modüllü Kongrüanslar

Bir polinom kongrüansını çözme problemini önce asal kuvvet modüllerine, oradan da kök yükseltme yoluyla asal modüllere indirgemiştik. Zincirin son halkası, yani

$$f(x) \equiv 0 \pmod{p} \qquad (p \ \text{ asal})$$

biçimindeki kongrüanslar, aslında zincirin **en düzenli** halkasıdır: modül asal olunca $\mathbb{Z}_p$ bir cisim gibi davranır ve polinomların bildiğimiz cebirsel özellikleri hemen hemen olduğu gibi geçerli kalır.
Bu kongrüansın çözümleri, modülo p'ye göre bir $a_1, a_2, ..., a_p$ tam kalanlar sistemi denenerek her zaman bulunabilir. Bu bölümde asıl amacımız bu aramayı **kısaltmak** ve çözüm sayısı hakkında bir üst sınır elde etmektir.

25.1 Dereceyi p'nin Altına İndirme

Modülo p'de x^p ile x aynı değeri aldığından ($u^p \equiv u$), derecesi p veya daha yüksek olan bir kongrüansı her zaman daha düşük dereceli bir kongrüansla değiştirebiliriz.

Teorem 25.1 (Derece İndirgeme). *$f(x)$ tam katsayılı bir polinom, p bir asal sayı ve $f(x) \equiv 0 \pmod{p}$ kongrüansının derecesi p olsun. Bu durumda aşağıdakilerden biri gerçekleşir:*

- *ya **her** x tam sayısı $f(x) \equiv 0 \pmod{p}$ kongrüansının bir çözümüdür;*
- *ya da $g(x) \equiv 0 \pmod{p}$ kongrüansının derecesi p'den küçük, baş katsayısı modülo p'ye göre 1'e kongrüan ve çözüm kümesi $f(x) \equiv 0 \pmod{p}$ kongrüansınınkiyle **aynı** olan tam katsayılı bir $g(x)$ polinomu vardır.*

İspat.
$f(x)$ polinomunu $x^p - x$ polinomuna bölelim. $x^p - x$ polinomunun baş katsayısı 1 olduğundan, bölme işlemi tam katsayılar içinde yapılabilir:

$$f(x) = q(x)\,(x^p - x) + r(x)$$

Burada $q(x)$ ve $r(x)$ tam katsayılı polinomlardır; ayrıca $r(x)$ ya sıfır polinomudur ya da

$$\partial r(x) < \partial(x^p - x) = p$$

sağlanır.
Fermat teoremi gereği her u tam sayısı için $u^p \equiv u \pmod{p}$, yani $u^p - u \equiv 0 \pmod{p}$'dir. O hâlde yukarıdaki eşitlikte $x = u$ yazılırsa

$$f(u) \equiv r(u) \pmod{p}, \qquad \forall u \in \mathbb{Z}$$

bulunur. Şimdi iki durum söz konusudur.
***i) $r(x) \equiv 0$ ise.** Yani $r(x)$ ya sıfır polinomudur ya da bütün katsayıları p ile bölünür. Bu durumda her $u \in \mathbb{Z}$ için $r(u) \equiv 0 \pmod{p}$, dolayısıyla*

$$f(u) \equiv 0 \pmod{p}, \qquad \forall u \in \mathbb{Z}$$

olur; yani her tam sayı kongrüansın bir çözümüdür.
***ii) $r(x) \not\equiv 0$ ise.** Yani $r(x)$ sıfır polinomundan farklıdır ve en az bir katsayısı p ile bölünmez. Bu durumda $r(x)$ polinomu*

$$r(x) = r_m x^m + r_{m-1} x^{m-1} + \cdots + r_1 x + r_0$$

biçimindedir; burada $r_m \not\equiv 0 \pmod{p}$ ve $\partial r(x) = m < p$'dir.
$(r_m, p) = 1$ olduğundan $r_m x \equiv 1 \pmod{p}$ kongrüansı çözülebilirdir ve bir tek çözümü vardır; bu çözüm $x \equiv b \pmod{p}$ olsun.
Artık üç kongrüansın çözüm kümeleri arasındaki ilişkiyi kurabiliriz:

- $f(x) \equiv 0 \pmod p$ *ile* $r(x) \equiv 0 \pmod p$ *kongrüanslarının çözümleri* ***aynıdır*** *(çünkü her* u *için* $f(u) \equiv r(u)$*).*
- $(b, p) = 1$ *olduğundan* $r(x) \equiv 0 \pmod p$ *ile* $b\,r(x) \equiv 0 \pmod p$ *kongrüanslarının çözümleri de* ***aynıdır****.*

O hâlde aranan polinom olarak

$$g(x) = b\,r(x)$$

alınabilir: derecesi $m < p$*'dir ve baş katsayısı* $b\,r_m \equiv 1 \pmod p$*'dir.*
■

Örnek 25.1. $x^7 + x^3 + 2 \equiv 0 \pmod 5$ kongrüansını, derecesi 5'ten küçük ve baş katsayısı 1 olan bir kongrüansa indirgeyiniz.

Çözüm.
$f(x) = x^7 + x^3 + 2$ polinomunu $x^5 - x$ polinomuna bölelim:

$$x^7 + x^3 + 2 = x^2\,(x^5 - x) + \underbrace{2x^3 + 2}_{r(x)}$$

O hâlde her u tam sayısı için $f(u) \equiv r(u) \pmod 5$'tir ve $\partial r(x) = 3 < 5$'tir.
Baş katsayıyı 1 yapmak için $r_3 x \equiv 1 \pmod 5$, yani $2x \equiv 1 \pmod 5$ kongrüansını çözelim: $b \equiv 3 \pmod 5$. Buradan

$$g(x) = 3\,r(x) = 6x^3 + 6 \equiv x^3 + 1 \pmod 5$$

bulunur. Demek ki $x^7 + x^3 + 2 \equiv 0 \pmod 5$ ile $x^3 + 1 \equiv 0 \pmod 5$ kongrüanslarının çözümleri aynıdır.
Sağlama. $x^3 + 1 \equiv 0 \pmod 5$ kongrüansının tek çözümü $x \equiv 4 \pmod 5$'tir ($4^3 + 1 = 65$). Gerçekten de $4^7 + 4^3 + 2 = 16450 = 5 \cdot 3290$'dır ve $x = 0, 1, 2, 3$ değerlerinin hiçbiri asıl kongrüansı sağlamaz.
■

> **i** Pratikte ne işe yarar?
>
> Teorem, modülo p'de çalışırken derecenin her zaman p'nin altına çekilebileceğini söyler. Bu hem elle arama alanını küçültür hem de bir sonraki teoremin vereceği "çözüm sayısı $\leq$ derece" sınırını keskinleştirir.

25.2 Çarpan Teoremi

Cebirden bilinen "kök $\Longleftrightarrow$ çarpan" ilkesi, modül asal olduğunda kongrüanslar için de geçerlidir.

Teorem 25.2 (Çarpan Teoremi). *$f(x)$ tam katsayılı bir polinom, $\partial f(x) \geq 1$ ve p bir asal sayı olsun. Bir a tam sayısının $f(x) \equiv 0 \pmod p$ kongrüansının çözümü olması için gerek ve yeter koşul,*

$$f(x) \equiv (x - a)\,\rho(x) \pmod p$$

olacak şekilde tam katsayılı bir $\rho(x)$ polinomunun var olmasıdır.

İspat.
Gereklik. *a tam sayısı $f(x) \equiv 0 \pmod p$ kongrüansının bir çözümü olsun. $f(x)$ polinomunu $x - a$ polinomuna bölelim. $x - a$ polinomunun baş katsayısı 1 olduğundan bölme tam katsayılar içinde yapılabilir ve kalan bir sabittir:*

$$f(x) = (x - a)\,\rho(x) + r \qquad (*)$$

Burada $\rho(x)$ tam katsayılı bir polinom, r ise bir tam sayıdır. $(*)$'da $x = a$ yazılırsa $f(a) = r$ bulunur. a bir çözüm olduğundan $f(a) \equiv 0 \pmod p$, yani

$$r \equiv 0 \pmod p$$

olur. Bunu $(*)$'da kullanırsak

$$f(x) \equiv (x-a)\,\rho(x) \pmod p$$

elde edilir.
Yeterlik. *$f(x) \equiv (x-a)\rho(x) \pmod p$ olacak şekilde tam katsayılı bir $\rho(x)$ polinomu var olsun. Bu kongrüansta $x = a$ yazılırsa*

$$f(a) \equiv (a-a)\,\rho(a) = 0 \pmod p$$

bulunur; yani a tam sayısı $f(x) \equiv 0 \pmod p$ kongrüansının bir çözümüdür.
■

25.3 Lagrange Teoremi

Artık bu bölümün ana sonucunu ispatlayabiliriz: asal modülde çözüm sayısı dereceyi aşamaz.

Teorem 25.3 (Lagrange Teoremi). *p bir asal sayı olmak üzere*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod p$$

*kongrüansının derecesi n olsun; yani $a_n \neq 0$ ve $a_n \not\equiv 0 \pmod p$ olsun. Bu durumda kongrüansın **en fazla n tane** çözümü vardır.*

İspat.
İspatı n üzerinden tümevarımla yapalım.
Başlangıç adımı ($n = 1$). *$a_1 x + a_0 \equiv 0 \pmod p$ kongrüansında $p \nmid a_1$, yani $(a_1, p) = 1$'dir. Birinci dereceden kongrüanslar hakkında bildiklerimize göre bu kongrüansın tam olarak bir çözümü vardır; özel olarak en fazla 1 çözümü vardır. Teorem $n = 1$ için doğrudur.*
Tümevarım hipotezi. *Teoremin $n = k-1$ için doğru olduğunu kabul edelim ($k > 1$, $k \in \mathbb{N}$); yani $(k-1)$. dereceden bir $g(x) \equiv 0 \pmod p$ kongrüansının en fazla $k-1$ tane çözümü olduğunu varsayalım.*
Tümevarım adımı. *$f(x) \equiv 0 \pmod p$, k. dereceden bir kongrüans olsun. İki durum söz konusudur.*
i) *Kongrüansın hiç çözümü yoktur. Bu durumda ispatlanacak bir şey yoktur; $0 \leq k$ olduğundan teorem $n = k$ için doğrudur.*
ii) *Kongrüansın bir çözümü vardır; bu çözüm $x \equiv a \pmod p$ olsun. Teorem 25.2 gereği*

$$f(x) \equiv (x-a)\,g(x) \pmod p \qquad (*)$$

olacak şekilde tam katsayılı bir $g(x)$ polinomu vardır. Üstelik bu polinom, Teorem 25.2'ın ispatındaki bölme işleminin bölümüdür: $f(x)$ derecesi k olan bir polinom, $x - a$ ise baş katsayısı 1 olan birinci dereceden bir polinom olduğundan $g(x)$'in derecesi $k-1$ ve baş katsayısı a_k'dır. $a_k \not\equiv 0 \pmod p$ olduğundan $g(x) \equiv 0 \pmod p$ kongrüansının derecesi de $k-1$'dir.
Tümevarım hipotezine göre $g(x) \equiv 0 \pmod p$ kongrüansının en fazla $k-1$ tane çözümü vardır. Bu çözümler

$$x \equiv c_1, \quad x \equiv c_2, \quad \ldots, \quad x \equiv c_r \pmod p, \qquad r \leq k-1$$

olsun.
Şimdi d tam sayısı, $f(x) \equiv 0 \pmod p$ kongrüansının herhangi bir çözümü olsun; yani $f(d) \equiv 0 \pmod p$. $(*)$'da $x = d$ yazılırsa

$$(d-a)\,g(d) \equiv 0 \pmod p$$

*bulunur. **p asal olduğu için** bir çarpımın p ile bölünmesi, çarpanlardan en az birinin p ile bölünmesini gerektirir:*

- *Eğer $g(d) \equiv 0 \pmod p$ ise, $x \equiv d \pmod p$ çözümü $c_1, \ldots, c_r$ çözümlerinden biridir.*

- *Eğer* $g(d) \not\equiv 0 \pmod{p}$ *ise,* $d - a \equiv 0 \pmod{p}$*, yani* $d \equiv a \pmod{p}$ *olur; bu çözüm* $x \equiv a$ *çözümüyle aynıdır.*

O hâlde $f(x) \equiv 0 \pmod{p}$ *kongrüansının çözümleri*

$$x \equiv a, \quad x \equiv c_1, \quad x \equiv c_2, \quad \ldots, \quad x \equiv c_r \pmod{p}$$

listesinden ibarettir ve çözüm sayısı en fazla $r + 1$*'dir.* $r \leq k - 1$ *olduğundan*

$$r + 1 \leq k$$

bulunur. Yani teorem $n = k$ *için de doğrudur.*
Tümevarım ilkesi gereği teorem her $n \geq 1$ *doğal sayısı için doğrudur.*
■

⚠ Modülün asal olması şart

Lagrange teoreminin ispatında asallık **iki kez** kullanıldı: hem Teorem 25.2'da, hem de "$(d-a)g(d) \equiv 0$ ise çarpanlardan biri $\equiv 0$" adımında.
Modül asal değilse sonuç bozulur. Kongrüansların çözümleri bölümündeki

$$x^2 - 1 \equiv 0 \pmod{8}$$

kongrüansının derecesi 2'dir, ama $x \equiv 1, 3, 5, 7$ olmak üzere **dört** çözümü vardır. Benzer biçimde kök yükseltme bölümünde $x^3 + x - 19 \equiv 0 \pmod{49}$ kongrüansının derecesi 3 iken sekiz çözümü çıkmıştı.

💡 Bir sonraki adım

Lagrange teoremi, primitif kök teorisinin de temel taşıdır: $x^d - 1 \equiv 0 \pmod{p}$ kongrüansının en fazla d çözümü olması, modülo p'de belirli mertebeden eleman sayısını sınırlar. Bunu bir sonraki bölümde kullanacağız.

26. Mertebe, Primitif Kökler ve İndeks

Önceki bölümlerde bir kongrüansın **çözüm sayısını** kuşatan araçları geliştirdik. Şimdi ise sorunun kendisine dönüyoruz: $x^n \equiv a \pmod{m}$ kongrüansı ne zaman çözülebilir ve çözümleri nasıl bulunur? Bu soruyu yanıtlamak için modüler yapılardaki döngüsel periyotları ölçen kavramları kuracağız.

26.1 n. Kuvvet Rezidü Kavramı

Bir sayının belirli bir modüle göre tam kuvvetinin alınıp alınamayacağını ifade eden yapıya "rezidü (kalan)" denir.

Tanım 26.1 (n. Kuvvet Rezidü). n pozitif bir tam sayı ve $m \geq 2$ bir modül olsun. Eğer

$$x^n \equiv a \pmod{m}$$

kongrüansının bir x çözümü varsa, a sayısına modülo m'ye göre bir ***n*. kuvvet rezidüsü** denir.

Örnek 26.1 (Rezidü Kavramı). $x^3 \equiv 2 \pmod{5}$ denklemini inceleyelim. $x \equiv 3 \pmod{5}$ denediğimizde:

$$3^3 = 27 \equiv 2 \pmod{5}$$

Denklem sağlandığı için **2 sayısı, modülo 5'e göre bir 3. kuvvet rezidüsüdür.**

Rezidüler bize bir denklemin kökü olup olmadığını söyler. Ancak modüler aritmetikteki asıl sihir, bir sayının kuvvetlerini almaya devam ettiğimizde ortaya çıkan döngüselliktir: sayılar sonsuza kadar büyümez, modüle ulaştığında başa sarar. Bu "başa sarma" noktasını ölçmek için yeni bir kavrama ihtiyacımız var.

26.2 Mertebe (Eksponent) Nedir?

Euler-Fermat teoreminden biliyoruz ki $\gcd(a, m) = 1$ ise $a^{\phi(m)} \equiv 1 \pmod{m}$'dir. Yani a'nın kuvvetlerini almaya devam ettiğimizde *eninde sonunda* sonucu 1 yapan bir üs karşımıza çıkar. Peki döngüyü tamamlayıp 1 sonucunu veren **en küçük** üs hangisidir?

Tanım 26.2 (Mertebe (Eksponent)). $m \geq 2$ bir tam sayı ve $\gcd(a, m) = 1$ olsun.

$$a^x \equiv 1 \pmod{m}$$

koşulunu sağlayan **en küçük pozitif x tam sayısına**, a'nın modülo m'ye göre **mertebesi** denir ve $\mathrm{ord}_m(a)$ ile gösterilir.

26.3 Mertebe ve Euler Phi İlişkisi

Bir sayının modüler döngü uzunluğu rastgele bir değer değildir; o modülün Euler phi değeriyle kusursuz bir bölünme ilişkisi içindedir.

Teorem 26.1 (Mertebe $\(m \)$'i Böler). *$m \geq 2$ bir tam sayı, $\gcd(a, m) = 1$ ve a'nın modülo m'ye göre mertebesi h olsun. Bu durumda h, $\phi(m)$'i tam böler:*

$$h \mid \phi(m)$$

> ***İspat.***

*Bu teoremi ispatlamak için **bölme algoritmasını** kullanacağız. $\phi(m)$ sayısını h'ye bölelim; bölüm q ve kalan r olmak üzere:*

$$\phi(m) = qh + r, \qquad 0 \leq r < h$$

Euler-Fermat teoremi gereği $\gcd(a, m) = 1$ olduğundan $a^{\phi(m)} \equiv 1 \pmod{m}$'dir. $\phi(m)$ yerine yukarıdaki eşitliği yazalım:

$$a^{qh+r} \equiv 1 \pmod{m} \Longrightarrow (a^h)^q \cdot a^r \equiv 1 \pmod{m}$$

Mertebe tanımı gereği $a^h \equiv 1 \pmod{m}$'dir; yerine koyalım:

$$1^q \cdot a^r \equiv 1 \pmod{m} \Longrightarrow a^r \equiv 1 \pmod{m}$$

***Kritik adım.** Elimizde $a^r \equiv 1 \pmod{m}$ şartını sağlayan bir r kaldı ve bölme algoritması gereği $0 \leq r < h$'dir. Fakat h'yi, bu şartı sağlayan **en küçük pozitif** tam sayı olarak tanımlamıştık. Eğer $r > 0$ olsaydı, h'den küçük pozitif bir sayı bu şartı sağlamış olurdu — mertebe tanımıyla çelişki.*
Çelişkiden kaçınmanın tek yolu $r = 0$ olmasıdır. Bölme denklemine dönersek:

$$\phi(m) = qh \Longrightarrow h \mid \phi(m)$$

■

Örnek 26.2 (Mertebenin $phi.alt \(m \)$'i Bölmesi). $m = 7$ ve $a = 2$ olsun; $\gcd(2, 7) = 1$ ve $\phi(7) = 6$'dır.
2'nin modülo 7'ye göre mertebesini bulmak için kuvvetlerini sırasıyla alalım:

$$2^1 \equiv 2 \pmod{7}$$
$$2^2 \equiv 4 \pmod{7}$$
$$2^3 = 8 \equiv 1 \pmod{7}$$

Sonucu 1 yapan en küçük pozitif üs 3 olduğundan $\mathrm{ord}_7(2) = 3$'tür. Teoremin ifade ettiği üzere $3 \mid 6$, yani mertebe gerçekten $\phi(7)$'yi böler.

26.4 Üslerin Denkliği ve Periyodiklik

İki farklı kuvvetin modüler sistemde aynı kalanı vermesi tesadüf değildir; üsler arasındaki fark doğrudan mertebeyle bağlantılıdır.

Önerme 26.1 (Üslerin Denkliği ve Mertebe İlişkisi). *$m \geq 2$ bir tam sayı, $\gcd(a, m) = 1$ ve a'nın mertebesi h olsun. $j, k \geq 0$ tam sayıları için:*

$$a^j \equiv a^k \pmod{m} \Longrightarrow h \mid (j - k)$$

İspat.
Genelliği bozmadan $j \geq k$ olduğunu kabul edebiliriz. Başlangıç denkliğimiz:

$$a^j \equiv a^k \pmod{m}$$

$\gcd(a, m) = 1$ olduğundan a'nın her pozitif kuvveti de m ile aralarında asaldır; bu sayede her iki tarafı güvenle a^k'ya bölebiliriz:

$$a^{j-k} \equiv 1 \pmod{m}$$

Şimdi bölme algoritmasını tekrar kullanalım: $(j - k)$ tam sayısını h'ye bölelim.

$$j - k = qh + r, \qquad 0 \leq r < h$$

Bu eşitliği denklemde yerine yazalım:

$$(a^h)^q \cdot a^r \equiv 1 \pmod{m}$$

Mertebe tanımı gereği $a^h \equiv 1$ olduğundan $a^r \equiv 1 \pmod{m}$ elde ederiz. Yine aynı çelişki argümanına ulaştık: $0 \leq r < h$ iken h bu denkliği sağlayan en küçük pozitif tam sayıydı. O hâlde $r = 0$ olmalıdır:

$$j - k = qh \Longrightarrow h \mid (j - k)$$

■

Örnek 26.3 (Üslerin Denkliği ve Mertebe İlişkisi). Bir önceki örnekten devam edelim: $m = 7$, $a = 2$ ve $h = 3$'tür. Üsler olarak $j = 8$ ve $k = 2$ seçelim:

$$2^8 = 256 \equiv 4 \pmod{7}$$
$$2^2 = 4 \equiv 4 \pmod{7}$$

Görüldüğü üzere $2^8 \equiv 2^2 \pmod{7}$ sağlanmaktadır. Önermeye göre mertebemiz $h = 3$, üslerin farkı olan $8 - 2 = 6$ sayısını tam bölmelidir; gerçekten de $3 \mid 6$'dır.

26.5 Bir Kuvvetin Mertebesini Hesaplama

Bir tabanın mertebesini biliyorsanız, o tabandan türetilmiş herhangi bir kuvvetin mertebesini de tek bir formülle bulabilirsiniz.

Teorem 26.2 (Bir Kuvvetin Mertebesi). *$m \geq 2$ bir tam sayı, $\gcd(a, m) = 1$, $k \in \mathbb{Z}^+$ ve a'nın modülo m'ye göre mertebesi h olsun. Bu durumda a^k tam sayısının mertebesi:*

$$\operatorname{ord}_m(a^k) = \frac{h}{\gcd(h, k)}$$

İspat.
$\gcd(a, m) = 1$ olduğundan $\gcd(a^k, m) = 1$'dir. a^k'nın mertebesi t olsun; tanım gereği:

$$(a^k)^t = a^{kt} \equiv 1 \pmod{m}$$

Bir önceki önermeden biliyoruz ki bir kuvvet 1'e denkse tabanın mertebesi o kuvveti tam böler:

$$h \mid kt$$

Her iki tarafı $\gcd(h, k)$ değerine bölelim:

$$\frac{h}{\gcd(h, k)} \left| \left(\frac{k}{\gcd(h, k)} \cdot t \right) \right.$$

Bir sayıyı en büyük ortak bölenine böldüğümüzde elde edilen bölümler daima aralarında asaldır:

$$\gcd\left(\frac{h}{\gcd(h, k)}, \frac{k}{\gcd(h, k)} \right) = 1$$

***Öklid lemması** gereği, bir tam sayı bir çarpımı bölüyorsa ve çarpanlardan biriyle aralarında asalsa, diğer çarpanı bölmek zorundadır:*

$$\frac{h}{\gcd(h, k)} \left| t \right. \tag{$*$}$$

Öte yandan a^k'nın $\frac{h}{\gcd(h,k)}$. kuvvetini alalım:

$$(a^k)^{\frac{h}{\gcd(h,k)}} = a^{\frac{kh}{\gcd(h,k)}} = (a^h)^{\frac{k}{\gcd(h,k)}} \equiv 1^{\frac{k}{\gcd(h,k)}} \equiv 1 \pmod{m}$$

Mertebenin tanımı gereği t, 1 sonucunu veren her kuvveti tam bölmek zorundadır:

$$t \left| \frac{h}{\gcd(h,k)} \right. \qquad (**)$$

Hem t hem de $\frac{h}{\gcd(h,k)}$ pozitif tam sayı olduğundan, $(*)$ ve $(**)$'ın aynı anda sağlanabilmesi için bu iki ifadenin eşit olması zorunludur.
■

Örnek 26.4 (Bir Kuvvetin Mertebesini Bulma). $m = 11$ ve $a = 2$ olsun; $\gcd(2, 11) = 1$'dir.
Hesaplandığında $2^{10} \equiv 1 \pmod{11}$ olduğu ve daha küçük bir kuvvette 1 sonucuna ulaşılamadığı görülür; yani $\text{ord}_{11}(2) = 10$'dur.
Şimdi $k = 4$. kuvvet olan $2^4 \equiv 16 \equiv 5 \pmod{11}$ sayısının mertebesini arayalım:

$$\frac{h}{\gcd(h,k)} = \frac{10}{\gcd(10,4)} = \frac{10}{2} = 5$$

Sağlaması için 5'in modülo 11'deki kuvvetlerine bakalım:

$$5^1 \equiv 5 \pmod{11}$$
$$5^2 = 25 \equiv 3 \pmod{11}$$
$$5^3 \equiv 15 \equiv 4 \pmod{11}$$
$$5^4 \equiv 20 \equiv 9 \pmod{11}$$
$$5^5 \equiv 45 \equiv 1 \pmod{11}$$

Görüldüğü üzere 2^4'ün mertebesi gerçekten de formülün verdiği gibi tam olarak 5'tir.

26.6 Primitif (İlkel) Kök Kavramı

Tanım 26.3 (Primitif Kök). $m \geq 2$ bir tam sayı ve $\gcd(a, m) = 1$ olsun. Eğer a'nın modülo m'ye göre mertebesi tam olarak $\phi(m)$ ise, a'ya modülo m'ye göre bir **primitif kök (ilkel kök)** denir.

Her modülün bir primitif kökü olmak zorunda değildir. Hangi modüllerin primitif kök barındırdığı kesin olarak sınıflandırılmıştır.

Teorem 26.3 (Primitif Köklerin Varlığı). *$m \geq 2$ bir tam sayı olsun. Modülo m'ye göre bir primitif kökün var olabilmesi için gerek ve yeter şart m'nin şu formlardan birinde olmasıdır:*

$$m \in \{2, 4, p^n, 2p^n\}$$

Burada p herhangi bir tek asal, n ise herhangi bir pozitif tam sayıdır. m'nin başka hiçbir değeri için modülo m'ye göre primitif kök yoktur.

Örnek 26.5 (Primitif Kökün Varlığı ve Yokluğu). 1. Primitif kökü olan bir modül ($m = 7$). 7 asaldır, yani p^1 formuna uyar ve $\phi(7) = 6$'dır. $a = 3$ bir primitif kök müdür?

$$3^1 \equiv 3, \quad 3^2 \equiv 2, \quad 3^3 \equiv 6 \pmod{7}$$
$$3^4 \equiv 4, \quad 3^5 \equiv 5, \quad 3^6 \equiv 1 \pmod{7}$$

1 sonucunu veren en küçük pozitif üs 6'dır; yani 3'ün mertebesi tam olarak $\phi(7) = 6$'ya eşittir. Dolayısıyla **3, modülo 7'ye göre bir primitif köktür.**
2. Primitif kökü olmayan bir modül ($m = 8$). $8 = 2^3$ olduğundan varlık teoreminin izin verdiği kümelerden hiçbirine uymaz. $\phi(8) = 4$'tür ve 8 ile aralarında asal sayılar $\{1, 3, 5, 7\}$'dir:

$$1^1 \equiv 1 \pmod 8$$
$$3^2 = 9 \equiv 1 \pmod 8$$
$$5^2 = 25 \equiv 1 \pmod 8$$
$$7^2 = 49 \equiv 1 \pmod 8$$

Hiçbir elemanın mertebesi $\phi(8) = 4$'e ulaşamaz; maksimum mertebe 2'de kalır. Bu nedenle **modülo 8'in hiçbir primitif kökü yoktur.**

Elimizde bir primitif kök varsa, bu kök o modüldeki bütün çarpımsal yapıyı tek başına üretebilir.

Teorem 26.4 (Primitif Köklerin Özellikleri). *a, modülo m'ye göre bir primitif kök olsun. Bu durumda:*

1. *Her $j, k \geq 0$ tam sayısı için: $a^j \equiv a^k \pmod m \Leftrightarrow j \equiv k \pmod{\phi(m)}$*
2. *Her $j \geq 0$ tam sayısı için: $a^j \equiv 1 \pmod m \Leftrightarrow \phi(m) \mid j$*
3. *$a, a^2, a^3, \ldots, a^{\phi(m)}$ tam sayıları, modülo m'ye göre bir **asal kalanlar sistemi** oluşturur.*

> ***İspat.***
> ***1) Birinci özellik.***
> Gereklilik ($\Longrightarrow$). *$a^j \equiv a^k \pmod m$ olsun. a primitif kök olduğundan mertebesi $\phi(m)$'dir. Üslerin denkliği önermesinden, mertebe üslerin farkını böler:*
>
> $$\phi(m) \mid (j-k) \Longrightarrow j \equiv k \pmod{\phi(m)}$$
>
> Yeterlilik ($\Longleftarrow$). *$j \equiv k \pmod{\phi(m)}$ olsun; bu durumda $j = k + r\phi(m)$ olacak şekilde bir $r \geq 0$ tam sayısı vardır:*
>
> $$a^j = a^{k+r\phi(m)} = a^k \cdot \left(a^{\phi(m)}\right)^r \equiv a^k \cdot 1^r \equiv a^k \pmod m$$
>
> ***2) İkinci özellik.*** *Birinci ispatta $k = 0$ alırsak, $a^0 = 1$ olduğundan:*
>
> $$a^j \equiv 1 \pmod m \Leftrightarrow j \equiv 0 \pmod{\phi(m)} \Leftrightarrow \phi(m) \mid j$$
>
> ***3) Üçüncü özellik.*** *$\gcd(a, m) = 1$ olduğundan a'nın tüm pozitif kuvvetleri de m ile aralarında asaldır ve bu kümenin eleman sayısı tam olarak $\phi(m)$'dir.*
> *Geriye bu elemanlardan hiçbir ikisinin birbirine denk olmadığını göstermek kalıyor. Aksini varsayalım: $1 \leq j, k \leq \phi(m)$ için $a^j \equiv a^k \pmod m$ olsun. Birinci özellik gereği $\phi(m) \mid (j-k)$ olmalıdır. Ancak j ve k her ikisi de 1 ile $\phi(m)$ arasında olduğundan $\mid j - k \mid < \phi(m)$'dir. $\phi(m)$'den küçük olup $\phi(m)$'e tam bölünen tek sayı 0'dır; dolayısıyla $j = k$ olmak zorundadır.*
> *Sonuç olarak $j \neq k$ iken $a^j \not\equiv a^k$'dir. Bu kümedeki elemanlar birbirinden farklı ve hepsi m ile aralarında asal olduğundan bir **asal kalanlar sistemi** oluştururlar.*
> ■

Örnek 26.6 (Asal Kalanlar Sisteminin Üretilmesi). $m = 7$ modülünün primitif kökü olan $a = 3$ sayısını kullanalım. Teoremin üçüncü maddesine göre 3'ün $\phi(7) = 6$'ya kadar olan kuvvetleri tüm asal kalanlar sistemini üretmelidir:

$$3^1 \equiv 3, \quad 3^2 \equiv 2, \quad 3^3 \equiv 6 \pmod 7$$
$$3^4 \equiv 4, \quad 3^5 \equiv 5, \quad 3^6 \equiv 1 \pmod 7$$

Elde ettiğimiz küme $\{3, 2, 6, 4, 5, 1\}$'dir. Görüldüğü gibi primitif kök olan 3, modülo 7'de sıfır hariç tüm sayıları **eksiksiz biçimde** üretmiştir; hiçbir değer kendini tekrar etmeden tüm kümeyi taramıştır.

26.7 İndeks Kavramı (Ayrık Logaritma)

Klasik cebirde logaritma bir üssü bulmamızı sağlar; modüler aritmetikte de **indeks** aynı görevi üstlenir.

Tanım 26.4 (İndeks (Ayrık Logaritma)). a, modülo m'ye göre bir primitif kök ve b, $\gcd(b, m) = 1$ koşulunu sağlayan herhangi bir tam sayı olsun.

$$a^j \equiv b \pmod{m}$$

koşulunu sağlayan ve $1 \leq j \leq \phi(m)$ aralığında bulunan yegâne j doğal sayısına, ***b*'nin *a* primitif köküne göre indeksi** denir ve $\text{ind}_a(b)$ ile gösterilir.

Örnek 26.7 (İndeks (Ayrık Logaritma) Hesaplama). Modülümüz $m = 7$ ve primitif kökümüz $a = 3$ olsun. $b = 4$ sayısının indeksini arıyoruz; $\gcd(4, 7) = 1$'dir.
Sorduğumuz soru şudur: *"3'ün modülo 7'de kaçıncı kuvveti 4'e denktir?"*

$$3^j \equiv 4 \pmod{7}$$

Yukarıda ürettiğimiz asal kalanlar tablosuna bakarsak $3^4 \equiv 4 \pmod{7}$ olduğunu görürüz. Dolayısıyla:

$$\text{ind}_3(4) = 4$$

26.8 n. Kuvvetten Kongrüansların Çözülebilirliği

Bir $x^n \equiv a \pmod{m}$ denkleminin çözümünün olup olmadığını deneme yanılmayla bulmak, modül büyüdükçe imkânsızlaşır. Ancak modül bir asal sayı ise, primitif kökler ve indeksler sayesinde çözülebilirliği tek bir hesaplamayla test edebiliriz.

Teorem 26.5 (n. Kuvvetten Kongrüanslar (Euler Kriteri Genellemesi)). *p bir asal sayı, n pozitif bir tam sayı ve $\gcd(a, p) = 1$ olsun. $x^n \equiv a \pmod{p}$ kongrüansı için şu iki durum geçerlidir:*

1. *Eğer $a^{(p-1)/\gcd(n,\,p-1)} \not\equiv 1 \pmod{p}$ ise, kongrüansın **hiçbir çözümü yoktur**.*
2. *Eğer $a^{(p-1)/\gcd(n,\,p-1)} \equiv 1 \pmod{p}$ ise, kongrüansın **çözümü vardır** ve modülo p'deki çözüm sayısı tam olarak $\gcd(n, p-1)$ tanedir.*

İspat.
1. kısım — çözümsüzlük. *Aksini varsayalım ve denklemin bir u çözümü olduğunu kabul edelim: $u^n \equiv a \pmod{p}$. Denkliğin her iki tarafının $\frac{p-1}{\gcd(n,p-1)}$. kuvvetini alalım:*

$$a^{\frac{p-1}{\gcd(n,p-1)}} \equiv (u^n)^{\frac{p-1}{\gcd(n,p-1)}} \equiv \left(u^{p-1}\right)^{\frac{n}{\gcd(n,p-1)}} \pmod{p}$$

$\gcd(a, p) = 1$ olduğundan u da p ile aralarında asaldır; Fermat'nın küçük teoremi gereği $u^{p-1} \equiv 1 \pmod{p}$'dir:

$$a^{\frac{p-1}{\gcd(n,p-1)}} \equiv 1 \pmod{p}$$

*O hâlde ifade 1'e denk değilse, "bir u çözümü vardır" varsayımımız çöker; yani **çözüm yoktur**.*
2. kısım — çözümün varlığı ve sayısı. *$a^{(p-1)/\gcd(n,p-1)} \equiv 1 \pmod{p}$ olduğunu kabul edelim. g, modülo p'ye göre bir primitif kök ve a'nın indeksi j olsun: $g^j \equiv a \pmod{p}$. Kabulümüze yerleştirirsek:*

$$g^{\frac{j(p-1)}{\gcd(n,p-1)}} \equiv 1 \pmod{p}$$

g primitif kök olduğundan mertebesi $p-1$'dir. "Bir kuvvet 1'e denkse tabanın mertebesi o üssü böler" kuralı gereği:

$$(p-1) \,\Big|\, \frac{j(p-1)}{\gcd(n, p-1)}$$

Sadeleştirdiğimizde $\frac{j}{\gcd(n,p-1)}$ ifadesinin tam sayı olması gerektiği ortaya çıkar:

$$\gcd(n, p-1) \mid j \qquad (*)$$

Öte yandan aradığımız x çözümü de p ile aralarında asal olacağından $x \equiv g^y \pmod{p}$ formatında yazılabilir. Denklemimize dönersek:

$$(g^y)^n \equiv g^j \pmod{p} \Longrightarrow g^{yn} \equiv g^j \pmod{p}$$

Primitif köklerin üs denkliği özelliğinden, üsleri modülo $p-1$'de eşitleriz:

$$ny \equiv j \pmod{p-1}$$

*Bu, bilinmeyeni y olan bir **lineer kongrüanstır**. Lineer kongrüans teorisinden biliyoruz ki $Ay \equiv B \pmod{M}$ denkleminin çözümü olması için gerek ve yeter şart $\gcd(A, M) \mid B$ olmasıdır ve çözüm sayısı $\gcd(A, M)$ kadardır.*
Bizim denklemimizde $A = n$, $M = p-1$, $B = j$'dir ve $(*)$ adımında $\gcd(n, p-1) \mid j$ olduğunu kanıtlamıştık. Bu nedenle modülo $p-1$'de y için tam olarak $\gcd(n, p-1)$ tane çözüm vardır; bu çözümler de $x \equiv g^{y_i} \pmod{p}$ şeklinde ana denklemin köklerini üretir.
■

i Hatırlatma: lineer kongrüans çözümleri

Birinci dereceden $ax \equiv b \pmod{m}$ şeklindeki denklemlerin çözülebilir olması için $\gcd(a, m) \mid b$ şartı sağlanmalıdır. Bu şart sağlanıyorsa denklemin modülo m'de tam olarak $\gcd(a, m)$ adet farklı çözümü vardır.

26.9 Adım Adım Çözüm Algoritması

Yüksek mertebeden bir modüler denklemi çözmek için, problemi karmaşık kuvvetlerden kurtarıp birinci dereceden kongrüansa indirgeyen şu altı adımlı algoritma uygulanır.

1. **Çözülebilirlik kontrolü.** $d = \gcd(n, p-1)$ hesaplayın ve $a^{(p-1)/d} \equiv 1 \pmod{p}$ şartını test edin. Sonuç 1'e denk değilse denklem çözümsüzdür. Denkse, modülo p'de tam olarak d adet farklı çözüm olduğu garantilenir.
2. **Primitif kök seçimi.** Modülo p'ye göre mertebesi tam olarak $p-1$ olan bir g primitif kökü tespit edin.
3. **İndeks bulma.** $g^j \equiv a \pmod{p}$ eşitliğini sağlayan j üssünü hesaplayın. Aranan kökü de $x \equiv g^y \pmod{p}$ şeklinde tanımlayın.
4. **Lineer kongrüansa çevirme.** Denklemi $(g^y)^n \equiv g^j$ olarak yazıp üsleri modülo $p-1$'de eşitleyin:
$$ny \equiv j \pmod{p-1}$$
5. **Çözüm kümesini üretme.** Denklemin sağını, solunu ve modülünü d'ye bölerek sadeleştirin, temel y_0 çözümünü bulun ve diğer kökleri şu formülle elde edin:
$$y_k = y_0 + k \cdot \frac{p-1}{d}, \qquad k = 0, 1, \ldots, d-1$$
6. **Orijinal köklere dönüş.** Bulduğunuz tüm y_k üslerini $x \equiv g^{y_k} \pmod{p}$ denkleminde yerine koyun.

Örnek 26.8. $x^{20} \equiv 13 \pmod{17}$ denkleminin çözümü var mıdır; varsa çözümleri nelerdir?

Çözüm.
Verilenler: $p = 17$, $a = 13$, $n = 20$ ve $\gcd(13, 17) = 1$'dir.
1. adım — çözülebilirlik testi.
$d = \gcd(20, 16) = 4$'tür. Test kuvvetimizi hesaplayalım:

$$a^{\frac{p-1}{d}} = 13^{\frac{16}{4}} = 13^4 \pmod{17}$$

Modüler indirgeme yapalım:

$$13 \equiv -4 \pmod{17} \Longrightarrow 13^2 \equiv 16 \equiv -1 \pmod{17} \Longrightarrow 13^4 \equiv (-1)^2 \equiv 1 \pmod{17}$$

Sonuç 1 çıktığı için **çözüm vardır ve çözüm sayısı $d = 4$ tanedir**.
2. adım — primitif kök bulma.
$\phi(17) = 16$'dır; mertebesi 16 olan bir sayı arıyoruz. $g = 3$ deneyelim. Mertebe 16'yı bölmek zorunda olduğundan yalnızca $1, 2, 4, 8, 16$ kuvvetlerini kontrol etmek yeterlidir:

$$3^1 = 3, \qquad 3^2 = 9$$
$$3^4 = 81 \equiv 13 \equiv -4 \pmod{17}$$
$$3^8 \equiv (-4)^2 = 16 \equiv -1 \pmod{17}$$
$$3^{16} \equiv (-1)^2 = 1 \pmod{17}$$

Sonucu 1 yapan en küçük üs 16 olduğundan $\boldsymbol{g = 3}$**, modülo 17'nin bir primitif köküdür**.
3. adım — indeks hesaplama ve lineer denkleme geçiş.
13'ün 3 primitif köküne göre indeksini arıyoruz. Yukarıdaki hesaplamada $3^4 \equiv 13 \pmod{17}$ bulmuştuk; yani $j = 4$'tür.
Bilinmeyeni $x \equiv 3^y \pmod{17}$ olarak ifade edersek:

$$(3^y)^{20} \equiv 3^4 \pmod{17} \Longrightarrow 3^{20y} \equiv 3^4 \pmod{17}$$

Primitif kök kuralı gereği üsleri modülo 16'da eşitleriz:

$$20y \equiv 4 \pmod{16}$$

4. adım — çözümleri elde etme.
$20 \equiv 4 \pmod{16}$ olduğundan denklem şu hâle gelir:

$$4y \equiv 4 \pmod{16}$$

Her iki tarafı ve modülü $\gcd(4, 16) = 4$'e bölelim:

$$y \equiv 1 \pmod{4} \Leftrightarrow y = 1 + 4t$$

$t = 0, 1, 2, 3$ vererek modülo 16'daki dört çözümü buluruz:

$$y \in \{1{,}5{,}9{,}13\}$$

Bu üsleri $x \equiv 3^y \pmod{17}$ formatına yerleştirelim:

$$x_1 \equiv 3^1 \equiv 3 \pmod{17}$$
$$x_2 \equiv 3^5 = 3^4 \cdot 3 \equiv 13 \cdot 3 = 39 \equiv 5 \pmod{17}$$
$$x_3 \equiv 3^9 = 3^8 \cdot 3 \equiv 16 \cdot 3 \equiv (-1) \cdot 3 \equiv 14 \pmod{17}$$
$$x_4 \equiv 3^{13} = (3^4)^3 \cdot 3 \equiv (-4)^3 \cdot 3 = -64 \cdot 3 \equiv 4 \cdot 3 = 12 \pmod{17}$$

Sonuç: $x^{20} \equiv 13 \pmod{17}$ denkleminin dört farklı çözümü vardır:

$$x \in \{3{,}5{,}12{,}14\}$$

Sağlama: $3^{20} = 3^{16} \cdot 3^4 \equiv 1 \cdot 13 = 13 \pmod{17}$ ✓
■

27. Kuadratik (İkinci Dereceden) Rezidüler

Yüksek mertebeden kongrüansları ($x^n \equiv a \pmod{p}$) genel hatlarıyla inceledikten sonra, sayılar teorisinin en önemli özel durumu olan $n = 2$ hâline, yani **ikinci dereceden (kuadratik) kongrüanslara** geçiş yapıyoruz.
Modüler aritmetikte kök bulma problemlerinin temelini oluşturan bu konu, en temelde şu soruyla başlar: genel bir ikinci dereceden modüler denklemi nasıl çözeriz?

27.1 Genel İkinci Dereceden Denklemlerin İndirgenmesi

p bir asal sayı ve $a, b, c \in \mathbb{Z}$ olmak üzere, $a \not\equiv 0 \pmod{p}$ şartını sağlayan genel ikinci dereceden kongrüans şudur:

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

Eğer $p = 2$ ise denklem $ax^2 + bx + c \equiv 0 \pmod{2}$ hâlini alır ve yalnızca $x = 0$ ile $x = 1$ değerleri denenerek çözümler kolayca bulunur. Dolayısıyla asıl problem, $p > 2$ olan **tek asal sayılar** için çözümlerin aranmasıdır.
Aşağıdaki teorem, modül $p > 2$ tek asalı olduğunda karmaşık görünen bu genel denklemin basit bir $y^2 \equiv d \pmod{p}$ formatına nasıl denk olduğunu gösterir.

Teorem 27.1 (Kuadratik İndirgeme ve Tam Kareye Tamamlama). *$p > 2$ bir tek asal sayı ve $\gcd(a, p) = 1$ olmak üzere;*

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

kongrüansını çözmek, diskriminantı $d = b^2 - 4ac$ olan

$$y^2 \equiv d \pmod{p}$$

kongrüansını çözmeye denk bir problemdir.

> ***İspat.***
> *$f(x) = ax^2 + bx + c \equiv 0 \pmod{p}$ diyelim.*
> *p bir tek asal ($p > 2$) ve $a \not\equiv 0 \pmod{p}$ olduğundan, $4a$ sayısı da p ile aralarında asaldır:* $\gcd(4a, p) = 1$. *Bu sayede kongrüansın çözüm kümesini değiştirmeden her iki tarafı $4a$ ile çarpabiliriz:*
>
> $$4a \cdot f(x) \equiv 0 \pmod{p}$$
>
> $$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{p}$$
>
> *Şimdi bu ifadeyi klasik cebirdeki gibi tam kareye tamamlayalım. İlk iki terim $(2ax + b)^2$ açılımına çok benzemektedir:*
>
> $$(2ax + b)^2 = 4a^2x^2 + 4abx + b^2$$
>
> *Eşitliği yakalamak için denklemimize b^2 ekleyip çıkaralım:*
>
> $$(4a^2x^2 + 4abx + b^2) - b^2 + 4ac \equiv 0 \pmod{p}$$
>
> $$(2ax + b)^2 \equiv b^2 - 4ac \pmod{p}$$
>
> *Bu aşamada değişken değişimi yapıyoruz: $y = 2ax + b$ diyelim. Denklem şu sade forma dönüşür:*
>
> $$y^2 \equiv b^2 - 4ac \pmod{p}$$
>
> ***Birebir eşleme.***

- *Eğer $f(x) \equiv 0 \pmod{p}$ denkleminin bir x_0 çözümü varsa, $y_0 \equiv 2ax_0 + b \pmod{p}$ değeri de $y^2 \equiv b^2 - 4ac \pmod{p}$ denkleminin bir çözümüdür.*
- *Tersine, eğer $y^2 \equiv b^2 - 4ac \pmod{p}$ denkleminin bir y_0 çözümü varsa, $\gcd(2a, p) = 1$ olduğundan $2ax_0 \equiv y_0 - b \pmod{p}$ lineer kongrüansını sağlayan **tek bir x_0 çözümü** kesin olarak vardır ve bu x_0, asıl $f(x) \equiv 0 \pmod{p}$ denklemini sağlar.*

O hâlde bu iki denklemin çözümleri arasında birebir bir eşleme vardır ve problemi başarıyla $y^2 \equiv d \pmod{p}$ formatına indirgemiş olduk.
■

Bu indirgeme bize gösteriyor ki; ikinci dereceden karmaşık bir denklemi çözmenin bütün sırrı, aslında basit bir sayının **karekökünün** modüler aritmetikte var olup olmadığını belirlemekten geçmektedir.

Örnek 27.1 (İkinci Dereceden Denklemi İndirgeme ve Çözme). $3x^2 + 2x + 6 \equiv 0 \pmod{11}$ kongrüansını ele alalım. Burada $p = 11$ (tek asal), $a = 3$, $b = 2$ ve $c = 6$'dır; $\gcd(3, 11) = 1$ koşulu sağlanmaktadır.

Çözüm.
1. adım — diskriminantı hesaplama.
Teoreme göre denklemin diskriminantı:

$$d = b^2 - 4ac = 2^2 - 4(3)(6) = 4 - 72 = -68$$

Bu değeri modülo 11'de indirgersek:

$$-68 = -77 + 9 \equiv 9 \pmod{11}$$

2. adım — indirgenmiş denklemi kurma ve çözme.
Karmaşık denklemimiz artık $y^2 \equiv 9 \pmod{11}$ gibi çok daha basit bir forma dönüşmüştür. Hangi sayıların karesi modülo 11'de 9 verir?

$$y \equiv 3 \pmod{11} \quad \text{veya} \quad y \equiv -3 \equiv 8 \pmod{11}$$

3. adım — orijinal x değişkenine dönüş.
Değişken dönüşümümüz $y = 2ax + b$ şeklindeydi; değerleri yerine koyarsak $y = 6x + 2$ olur. Bulduğumuz y değerlerini tek tek lineer denklemlere eşitleyelim.
Durum 1: $y \equiv 3$ için

$$6x + 2 \equiv 3 \pmod{11} \implies 6x \equiv 1 \pmod{11}$$

Modüler bölme için sağ tarafa 11 ekleyip sayıyı 6'nın katı yapalım ($1 + 11 = 12$):

$$6x \equiv 12 \pmod{11} \implies x \equiv 2 \pmod{11}$$

Durum 2: $y \equiv 8$ için

$$6x + 2 \equiv 8 \pmod{11} \implies 6x \equiv 6 \pmod{11} \implies x \equiv 1 \pmod{11}$$

Sonuç: Başlangıçtaki kongrüansın çözüm kümesi $x \in \{1, 2\}$ olarak elde edilmiştir.
Sağlama: $x = 2$ için $3(4) + 2(2) + 6 = 22 \equiv 0 \pmod{11}$ ✓ ve $x = 1$ için $3 + 2 + 6 = 11 \equiv 0 \pmod{11}$ ✓
■

27.2 Kuadratik Rezidü (Kalan) Kavramı

Bir sayının modüler aritmetikte karekökü alınabiliyorsa, o sayıya kuadratik rezidü denir.

Tanım 27.1 (Kuadratik Rezidü ve Non-Rezidü). $m \geq 2$ bir tam sayı ve $\gcd(a, m) = 1$ olsun.
Eğer $x^2 \equiv a \pmod{m}$ kongrüansının en az bir çözümü varsa, a tam sayısına modülo m'ye göre bir **kuadratik rezidü (karesel kalan)** denir.

Eğer $x^2 \equiv a \pmod{m}$ kongrüansının hiçbir çözümü yoksa, a tam sayısına modülo m'ye göre bir **kuadratik non-rezidü** denir.

> **i** Notasyon anlaşması
>
> Notlarımızın devamında ve ilerleyen ispatlarda, terim tekrarlarını önlemek adına şu standart kısaltmaları kullanacağız:
>
> - Kuadratik rezidü yerine $\Longrightarrow$ **KR**
> - Kuadratik non-rezidü yerine $\Longrightarrow$ **KNR**

Örnek 27.2 (Kuadratik Rezidü Tespiti). $x^2 \equiv 3 \pmod{13}$ kongrüansını inceleyelim: $a = 3$ sayısı modülo 13'e göre bir KR midir yoksa KNR midir?
Modülo 13'teki sayıların karelerini test ettiğimizde

$$x = 4 \Longrightarrow 4^2 = 16 \equiv 3 \pmod{13}$$

olduğunu görürüz. Denklemi sağlayan bir x değeri bulunduğu için **3 sayısı, modülo 13'e göre bir kuadratik rezidüdür (KR)**.

> **i** Denklik sınıfları üzerinde çalışmak
>
> Eğer a, modülo m'ye göre bir kuadratik rezidü ise ve $a \equiv b \pmod{m}$ denkliği sağlanıyorsa, b tam sayısı da modülo m'ye göre bir kuadratik rezidüdür.
> Dolayısıyla kuadratik rezidüleri ararken sonsuz tam sayı kümesini değil, yalnızca modülo m'ye göre **birbirine denk olmayan** sayıları inceleriz.

Örnek 27.3 (Modülo 7 İçin KR ve KNR Kümeleri). Modülo 7 sistemini ele alalım. Tüm denklik sınıflarını taramak için $1 \leq x < 7$ aralığındaki sayıların karelerini inceleyelim:

$$\begin{aligned}
1^2 &= 1 \equiv 1 \pmod{7} \\
2^2 &= 4 \equiv 4 \pmod{7} \\
3^2 &= 9 \equiv 2 \pmod{7} \\
4^2 &= 16 \equiv 2 \pmod{7} \\
5^2 &= 25 \equiv 4 \pmod{7} \\
6^2 &= 36 \equiv 1 \pmod{7}
\end{aligned}$$

Kare alma işlemi sonucunda elde ettiğimiz birbirinden farklı kalanlar yalnızca 1, 2 ve 4'tür. 7'den küçük diğer pozitif tam sayılar (3, 5 ve 6) hiçbir sayının karesi olarak elde edilememiştir. Bu durumda modülo 7 için kümelerimiz şöyledir:

- **Kuadratik rezidüler (KR):** $\{1, 2, 4\}$
- **Kuadratik non-rezidüler (KNR):** $\{3, 5, 6\}$

Dikkat edilirse x ve $-x$ aynı kareyi verdiğinden ($1 \leftrightarrow 6$, $2 \leftrightarrow 5$, $3 \leftrightarrow 4$), tek asal p için KR sayısı tam olarak $\frac{p-1}{2}$ olmaktadır.

28. Legendre Sembolü ve Euler Kriteri

Bir önceki bölümde bir sayının kuadratik rezidü (KR) veya kuadratik non-rezidü (KNR) olma durumunu denklemler üzerinden tanımlamıştık. Ancak sayılar büyüdükçe her defasında "acaba modülo p'de karesi a'yı veren bir sayı var mıdır?" diye tek tek kare alarak kontrol etmek imkânsızlaşır.
Bu durumu çok daha kompakt ve işlevsel bir forma sokan gösterim **Legendre sembolüdür**.

28.1 Legendre Sembolünün Tanımı

Tanım 28.1 (Legendre Sembolü). p bir tek asal sayı ve a herhangi bir tam sayı olsun. a'nın modülo p'ye göre kuadratik karakterini belirten **Legendre sembolü** $\left(\frac{a}{p}\right)$ ile gösterilir ve şöyle tanımlanır:
$$ \left(\frac{a}{p} \right) = \begin{cases} \hphantom{-}1, & a,\ \bmod p \text{'de kuadratik rezidü ise} \ \[0.3em] -1, & a,\ \bmod p \text{'de kuadratik non-rezidü ise} \\[0.3em] \hphantom{-}0, & p \mid a \text{ ise} \end{cases} $$

Örnek 28.1 (Legendre Sembolü Değerleri). **1. Kuadratik rezidü örneği.** $x^2 \equiv 1 \pmod 7$ kongrüansının çözülebilir olduğu bariz ($x = 1$). Bu durumda 1, modülo 7'ye göre bir KR olduğundan sembolün değeri 1'dir:

$$\left(\frac{1}{7}\right) = 1$$

2. Kuadratik non-rezidü örneği. $x^2 \equiv 3 \pmod 5$ kongrüansını inceleyelim. Modülo 5'te kareler $\{1, 4\}$ olduğundan 3 bir KNR'dir; dolayısıyla:

$$\left(\frac{3}{5}\right) = -1$$

Tanımı basit görünse de, Legendre sembolünün asıl gücü sahip olduğu çarpımsal özelliklerden ve **Euler kriterinden** gelir.

28.2 Euler Kriteri ve Sembolün Özellikleri

Aşağıdaki teorem, Legendre sembolü ile modüler üs alma işlemi arasında kusursuz bir köprü kurar. Kriptografide büyük asallarla çalışırken, bir sayının KR olup olmadığını tespit etmek için çözülebilirlik testleri yapmak yerine yalnızca Euler kriteri kullanılır.

Teorem 28.1 (Euler Kriteri ve Legendre Sembolünün Özellikleri). *p bir tek asal sayı; a ve b tam sayılar ve $\gcd(a, p) = \gcd(b, p) = 1$ olsun. Bu durumda aşağıdaki dört özellik geçerlidir:*

1. ***Euler kriteri:*** $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$
2. ***Çarpımsallık kuralı:*** $\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$
3. ***Periyodiklik:*** $a \equiv b \pmod p \Longrightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
4. ***Özel değerler:*** $\left(\frac{a^2}{p}\right) = 1$, $\left(\frac{1}{p}\right) = 1$, $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$

> ***İspat.***
> ***1) Euler kriterinin ispatı.*** *Bu ispatı, daha önce işlediğimiz n. kuvvetten kongrüanslar teoreminin $n = 2$ olan özel durumu üzerinden yapacağız.*
> KR durumu. *a modülo p'ye göre bir KR olsun; bu durumda kongrüansın çözümü vardır ve önceki teoremimiz gereği $a^{(p-1)/2} \equiv 1 \pmod p$ olmalıdır. Legendre tanımı gereği $\left(\frac{a}{p}\right) = 1$ olduğundan:*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$$

KNR durumu. *a modülo p'ye göre bir KNR olsun. Çözüm yoktur ve önceki teorem gereği $a^{(p-1)/2} \not\equiv 1 \pmod{p}$'dir.*
Öte yandan Fermat'nın küçük teoreminden $a^{p-1} \equiv 1 \pmod{p}$ olduğunu biliyoruz. İki kare farkı olarak açarsak:

$$\left(a^{(p-1)/2} - 1 \right) \left(a^{(p-1)/2} + 1 \right) \equiv 0 \pmod{p}$$

p asal olduğu için bu çarpanlardan birini tam bölmek zorundadır. $a^{(p-1)/2} \not\equiv 1 \pmod{p}$ olduğunu bildiğimizden birinci çarpanı bölemez; o hâlde mecburen ikinciyi böler:

$$a^{(p-1)/2} \equiv -1 \pmod{p}$$

Legendre tanımı gereği KNR için $\left(\frac{a}{p}\right) = -1$ olduğundan eşitlik yine sağlanır.
2) Çarpımsallık kuralının ispatı. *Euler kriterini a yerine ab alarak yazalım:*

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2} \cdot b^{(p-1)/2} \pmod{p}$$

Yine Euler kriterinden $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right)$ ve $b^{(p-1)/2} \equiv \left(\frac{b}{p}\right)$ olduğunu biliyoruz; yerlerine yazarsak:

$$\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \pmod{p}$$

Sembollerin alabileceği değerler yalnızca 1 ve -1'dir. $p > 2$ tek asal olduğundan modülo p'de $1 \not\equiv -1$'dir; dolayısıyla denklik ancak tam eşitlikle mümkündür:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$$

3) Periyodikliğin ispatı. *$a \equiv b \pmod{p}$ olsun. Her iki tarafın $\frac{p-1}{2}$. kuvvetini alırsak:*

$$a^{(p-1)/2} \equiv b^{(p-1)/2} \pmod{p}$$

Euler kriteri gereği bu kuvvetler Legendre sembollerine denktir:

$$\left(\frac{a}{p}\right) \equiv \left(\frac{b}{p}\right) \pmod{p}$$

İkinci ispattaki mantıkla, yalnızca ± 1 olabilen bu sembollerin modülo $p > 2$'de denk olması birbirlerine eşit olduklarını kanıtlar.
4) Özel değerlerin ispatı.

- *$a = 1$ için Euler kriterini uygularsak:*

$$\left(\frac{1}{p}\right) \equiv 1^{(p-1)/2} = 1 \pmod{p} \Longrightarrow \left(\frac{1}{p}\right) = 1$$

- *Çarpımsallık özelliğini kullanarak:*

$$\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{a}{p}\right) = (\pm 1)^2 = 1$$

- *$a = -1$ için Euler kriterini uygularsak, sayılar teorisinde ve soyut cebirde çok sık karşılaşacağımız meşhur özdeşliği elde ederiz:*

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod{p}$$

Değerler ± 1 aralığında olduğu için eşitlik kesindir.

■

$\left(\frac{-1}{p}\right)$ ne anlama gelir?

Dördüncü özellik pratikte şu anlama gelir: -1 sayısı, ancak ve ancak $p \equiv 1 \pmod 4$ olduğunda modülo p'de bir kuadratik rezidüdür.
Çünkü $p \equiv 1 \pmod 4$ iken $\frac{p-1}{2}$ çifttir ve sembol $+1$ olur; $p \equiv 3 \pmod 4$ iken $\frac{p-1}{2}$ tektir ve sembol -1 olur.

28.3 İnteraktif Legendre Hesaplayıcısı

Legendre sembolünün tanımını ve özelliklerini öğrendikten sonra, farklı a ve p değerleri için sembolün nasıl davrandığını gözlemlemek faydalı olacaktır. Aşağıdaki araç, herhangi bir a ve tek asal p değeri için $\left(\frac{a}{p}\right)$ değerini Euler kriteriyle hesaplar.
(Bu etkileşimli bileşen yalnızca web sürümünde çalışır.)

29. Gauss Lemması ve 2'nin Karesel Karakteri

Legendre sembolünün değerini hesaplamak için her zaman Euler kriterine başvurmak zorunda değiliz. Carl Friedrich Gauss, modüler sistemin yalnızca yarısını —1'den $\frac{p-1}{2}$'ye kadar olan kısmı— inceleyerek sembolün değerini veren son derece zarif bir sayma yöntemi ispatlamıştır.

29.1 Gauss Lemması

Teorem 29.1 (Gauss Lemması). *p bir tek asal sayı, a bir tam sayı ve $\gcd(a,p)=1$ olsun. $a, 2a, 3a, \ldots, \left(\frac{p-1}{2}\right)a$ tam sayılarını p ile bölüp kalanları bulalım. Eğer $\frac{p}{2}$'den büyük olan kalanların sayısı n ise:*

$$\left(\frac{a}{p}\right) = (-1)^n$$

İspat.
$a, 2a, \ldots, \frac{p-1}{2}a$ tam sayılarını p ile bölüp kalanları bulalım ve bu kalanları büyüklüklerine göre ikiye ayıralım:

- *$\frac{p}{2}$'den **büyük** olan kalanların sayısı n olsun; bunları $r_1, \ldots, r_n$ ile gösterelim.*
- *$\frac{p}{2}$'den **küçük** olan kalanların sayısı k olsun; bunları $s_1, \ldots, s_k$ ile gösterelim.*

Başlangıçtaki sayılar $\gcd(a,p)=1$ olduğundan modülo p'de birbirine denk olamaz; dolayısıyla elde edilen tüm kalanlar birbirinden farklıdır ve

$$n + k = \frac{p-1}{2}$$

Kalanların sınırları şöyledir:

$$0 < s_1, \ldots, s_k \leq \frac{p-1}{2} < \frac{p}{2}$$

$$\frac{p}{2} < \frac{p+1}{2} \leq r_1, \ldots, r_n < p$$

Şimdi büyük kalanları modül değerinden çıkararak yeni bir küme oluşturalım: $p - r_1, \ldots, p - r_n$. Bu sayılar da birbirinden farklıdır ve $0 < p - r_i < \frac{p}{2}$ aralığına düşerler.
***Kritik soru:** Herhangi bir $p - r_i$ değeri, küçük kalanlardan bir s_j değerine eşit olabilir mi?*
Aksini varsayalım ve $p - r_i = s_j$ olsun. Modüler aritmetiğe geçersek:

$$p - r_i \equiv s_j \pmod{p} \Longrightarrow r_i + s_j \equiv 0 \pmod{p}$$

Tanımımız gereği $r_i \equiv t_1 a$ ve $s_j \equiv t_2 a \pmod{p}$ olacak şekilde $1 \leq t_1, t_2 \leq \frac{p-1}{2}$ tam sayıları vardır:

$$(t_1 + t_2)a \equiv 0 \pmod{p}$$

$\gcd(a,p)=1$ olduğundan sadeleştirme yapabiliriz:

$$t_1 + t_2 \equiv 0 \pmod{p}$$

*Ancak $1 \leq t_1, t_2 \leq \frac{p-1}{2}$ olduğundan toplamları en fazla $p-1$ olabilir. $0 < t_1 + t_2 < p$ iken bu toplam modülo p'de sıfıra denk olamaz — **çelişki**.*

Demek ki $\{p-r_1,\dots,p-r_n\}$ *ile* $\{s_1,\dots,s_k\}$ *kümelerinin ortak elemanı yoktur. Her iki kümenin elemanları toplam* $\frac{p-1}{2}$ *adettir ve hepsi* 1 *ile* $\frac{p-1}{2}$ *arasındadır. O hâlde birleşimleri tam olarak şu kümedir:*

$$\{p-r_1,\dots,p-r_n\}\cup\{s_1,\dots,s_k\}=\left\{1,2,\dots,\frac{p-1}{2}\right\}$$

Tüm elemanları çarpalım:

$$(p-r_1)\cdots(p-r_n)\cdot s_1\cdots s_k=\left(\frac{p-1}{2}\right)!$$

Bu eşitliğin modülo p*'deki durumuna bakalım (*$p\equiv 0$ *olduğundan* $p-r_i\equiv -r_i$*):*

$$(-1)^n\ (\ r_1\cdots r_n\cdot s_1\cdots s_k\ )\equiv\left(\frac{p-1}{2}\right)!\pmod p$$

r_i *ve* s_j*'lerin orijinal hâlleri* $1a,2a,\dots,\frac{p-1}{2}a$*'nın kalanlarıydı; yerlerine koyarsak:*

$$(-1)^n\cdot a^{(p-1)/2}\cdot\left(1\cdot 2\cdots\frac{p-1}{2}\right)\equiv\left(\frac{p-1}{2}\right)!\pmod p$$

$$(-1)^n\cdot a^{(p-1)/2}\cdot\left(\frac{p-1}{2}\right)!\equiv\left(\frac{p-1}{2}\right)!\pmod p$$

Faktöriyelli ifade p *ile aralarında asal olduğu için her iki taraftan sadeleştirebiliriz:*

$$(-1)^n\cdot a^{(p-1)/2}\equiv 1\pmod p$$

Her iki tarafı $(-1)^n$ *ile çarparsak (çünkü* $(-1)^n\cdot(-1)^n=1$*):*

$$a^{(p-1)/2}\equiv(-1)^n\pmod p$$

Euler kriterinden $\left(\frac{a}{p}\right)\equiv a^{(p-1)/2}\pmod p$ *olduğunu biliyoruz; öyleyse*

$$\left(\frac{a}{p}\right)\equiv(-1)^n\pmod p$$

Her iki taraf da yalnızca ± 1 *olabileceği ve* $p>2$ *olduğu için denklik doğrudan eşitliğe dönüşür.*
■

Gauss lemması, tek başına bir hesaplama yönteminden ziyade arkasından gelecek büyük teoremleri kanıtlamak için bir köprüdür. Aşağıdaki teorem, Gauss lemmasını kullanarak a'nın ve özel olarak 2'nin karesel durumunu çok daha pratik bir formüle bağlar.

29.2 Legendre Sembolü İçin Genel Formül ve 2′nin Karesel Karakteri

Teorem 29.2 (Karesel Karakterlerin Hesabı). *p bir tek asal sayı ve* $\gcd(a,2p)=1$ *olsun (yani a tek bir tam sayı ve p ile aralarında asal). Bu durumda:*

1. $t=\sum_{j=1}^{(p-1)/2}\left\lfloor\frac{ja}{p}\right\rfloor$ *olmak üzere* $\left(\frac{a}{p}\right)=(-1)^t$*'dir.*
2. $\left(\frac{2}{p}\right)=(-1)^{(p^2-1)/8}$*'dir.*

Burada $\lfloor x\rfloor$ *sembolü x'in tam kısmını ifade eder.*

İspat.
1) Birinci kısmın ispatı.
$j\in\left\{1,\dots,\frac{p-1}{2}\right\}$ *olmak üzere ja sayılarına p modülünde bölme algoritmasını uygulayalım:*

$$ja=q_j\cdot p+\ell_j,\qquad 0<\ell_j<p$$

Burada bölüm $q_j=\left\lfloor\frac{ja}{p}\right\rfloor$ *şeklinde ifade edilebilir. Bu eşitliği* $j=1$*'den* $\frac{p-1}{2}$*'ye kadar toplayalım:*

$$a\sum j = p\sum\left\lfloor\frac{ja}{p}\right\rfloor + \sum \ell_j$$

Kalanlar dizisi ℓ_j, Gauss lemması ispatındaki r_i (büyük kalanlar) ve s_j (küçük kalanlar) dizilerinin ta kendisidir:

$$a\sum j = p\sum\left\lfloor\frac{ja}{p}\right\rfloor + \sum r_j + \sum s_j \qquad (*)$$

Öte yandan Gauss lemması ispatında 1'den $\frac{p-1}{2}$'ye kadar olan sayıların toplamını iki parçaya ayırmıştık:

$$\sum j = \sum_{j=1}^{n}(p - r_j) + \sum_{j=1}^{k} s_j = np - \sum r_j + \sum s_j \qquad (**)$$

$(*)$ *denkleminden* $(**)$ *denklemini taraf tarafa çıkaralım; $\sum s_j$ terimleri birbirini götürür:*

$$(a-1)\sum j = p\sum\left\lfloor\frac{ja}{p}\right\rfloor - np + 2\sum r_j$$

Ardışık sayıların toplam formülünden $\sum j = \frac{\frac{p-1}{2}\left(\frac{p-1}{2}+1\right)}{2} = \frac{p^2-1}{8}$'dir. Yerine yazarsak:

$$(a-1)\frac{p^2-1}{8} = p\left(\sum\left\lfloor\frac{ja}{p}\right\rfloor - n\right) + 2\sum r_j \qquad (***)$$

*Bu denklemi **modülo 2**'de inceleyelim. p tek asal olduğundan $p \equiv 1 \pmod 2$; a tek kabul edildiği için $(a-1)$ çifttir. Denklem şu hâle gelir:*

$$0 \equiv \sum\left\lfloor\frac{ja}{p}\right\rfloor - n \pmod 2 \Longrightarrow n \equiv \sum\left\lfloor\frac{ja}{p}\right\rfloor \pmod 2$$

$t = \sum\left\lfloor\frac{ja}{p}\right\rfloor$ dersek $n \equiv t \pmod 2$ bulunur. Gauss lemması gereği $\left(\frac{a}{p}\right) = (-1)^n$ olduğundan ve üslerin mod 2'deki denkliği işareti değiştirmeyeceğinden:

$$\left(\frac{a}{p}\right) = (-1)^t$$

2) İkinci kısmın ispatı — 2'nin karesel karakteri.
$(***)$ *denkleminde $a = 2$ alalım. Önce toplamı inceleyelim:*

$$t = \sum_{j=1}^{(p-1)/2}\left\lfloor\frac{2j}{p}\right\rfloor$$

j'nin alabileceği en büyük değer $\frac{p-1}{2}$ olduğundan $2j$'nin en büyük değeri $p-1$'dir. $2j < p$ olduğu için $\frac{2j}{p}$ kesri daima 1'den küçüktür ve tam kısmı sıfırdır:

$$\left\lfloor\frac{2j}{p}\right\rfloor = 0 \Longrightarrow t = 0$$

Şimdi $(***)$ denkleminde $a = 2$ ve toplam yerine 0 yazalım:

$$(2-1)\frac{p^2-1}{8} = p(0-n) + 2\sum r_j \Longrightarrow \frac{p^2-1}{8} = -pn + 2\sum r_j$$

*Bu denklemi yine **modülo 2**'de okuyalım; p tek olduğundan $-p \equiv 1 \pmod 2$:*

$$\frac{p^2-1}{8} \equiv n \pmod 2$$

Gauss lemmasına dönersek $\left(\frac{2}{p}\right) = (-1)^n$ olduğunu biliyoruz. Mod 2'deki denklik üslerde işareti etkilemediğinden:

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$$

■

29.3 Çözümlü Uygulamalar

İspatladığımız bu soyut teoremlerin, modüler aritmetikteki sayıların karesel karakterini bulmak için nasıl güçlü bir araca dönüştüğünü aşağıdaki örneklerle inceleyelim.

Örnek 29.1. $x^2 \equiv 22 \pmod{41}$ kongrüansının çözümünün olup olmadığını **Gauss lemması** ve **Euler kriteri** olmak üzere iki farklı yolla inceleyiniz.

Çözüm.
Burada $p = 41$ (tek asal) ve $a = 22$'dir; $\gcd(22, 41) = 1$ sağlanmaktadır.
1. yol — Gauss lemması.
$\frac{p-1}{2} = 20$'dir. 22'nin 1'den 20'ye kadar olan katlarının modülo 41'deki kalanlarını yazalım:

j	1	2	3	4	5	6	7	8	9	10
$22j \bmod 41$	**22**	3	**25**	6	**28**	9	**31**	12	**34**	15

j	11	12	13	14	15	16	17	18	19	20
$22j \bmod 41$	**37**	18	**40**	**21**	2	**24**	5	**27**	8	**30**

Koyu yazılan değerler $\frac{p}{2} = 20$, 5'ten büyük olanlardır: $22, 25, 28, 31, 34, 37, 40, 21, 24, 27, 30$ — toplam $n = 11$ adet.
Gauss lemmasına göre:

$$\left(\frac{22}{41}\right) = (-1)^{11} = -1$$

Sonuç -1 çıktığı için 22 bir KNR'dir ve denklemin çözümü yoktur.
2. yol — Euler kriteri.
$\left(\frac{22}{41}\right) \equiv 22^{20} \pmod{41}$ olmalıdır:

$$\begin{aligned} 22^2 &= 484 = 41 \cdot 11 + 33 \equiv 33 \equiv -8 \pmod{41} \\ 22^4 &\equiv (-8)^2 = 64 \equiv 23 \equiv -18 \pmod{41} \\ 22^8 &\equiv (-18)^2 = 324 = 41 \cdot 7 + 37 \equiv 37 \equiv -4 \pmod{41} \\ 22^{16} &\equiv (-4)^2 = 16 \pmod{41} \end{aligned}$$

$20 = 16 + 4$ olduğundan:

$$22^{20} = 22^{16} \cdot 22^4 \equiv 16 \cdot (-18) = -288 \pmod{41}$$

$41 \cdot 8 = 328$ olduğundan $-288 + 328 = 40 \equiv -1 \pmod{41}$.
Sonuç yine -1 (KNR) olarak bulunur; iki yöntem birbirini doğrulamaktadır.
■

Örnek 29.2. Euler kriteriyle bulduğumuz $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ özel değer formülünün doğruluğunu **Gauss lemmasını** kullanarak ispatlayınız.

Çözüm.
$a = -1$ alalım. Gauss lemması gereği -1'in katlarını yazarsak:

$$-1, \quad 2(-1), \quad \ldots, \quad \frac{p-1}{2}(-1)$$

Bu negatif sayıların modülo p'deki asıl kalanlarını (modül ekleyerek) bulalım:

$$p-1, \quad p-2, \quad \ldots, \quad p-\frac{p-1}{2} = \frac{p+1}{2}$$

Bu dizideki en küçük eleman olan $\frac{p+1}{2}$ bile $\frac{p}{2}$ değerinden büyüktür; yani kalanların **hepsi** $\frac{p}{2}$'den büyüktür. Dolayısıyla büyük kalanların sayısı doğrudan dizinin eleman sayısına eşittir:

$$n = \frac{p-1}{2}$$

Gauss lemmasına göre $\left(\frac{a}{p}\right) = (-1)^n$ olduğundan ispat tamamlanır:

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$$

■

Örnek 29.3. $x^2 \equiv 3 \pmod{17}$ kongrüansının çözülebilirliğini ***t*-toplam formülü** ve **Gauss lemması** olmak üzere iki yolla analiz ediniz.

Çözüm.
Verilenler: $p = 17$, $a = 3$ ve $\frac{p-1}{2} = 8$.
1. yol — *t*-toplam formülü.

$$t = \sum_{j=1}^{8} \left\lfloor \frac{3j}{17} \right\rfloor$$

Tam kısımları tek tek hesaplayalım:

j	1	2	3	4	5	6	7	8
$3j$	3	6	9	12	15	18	21	24
$\lfloor 3j/17 \rfloor$	0	0	0	0	0	1	1	1

Toplam $t = 3$'tür. Buradan:

$$\left(\frac{3}{17}\right) = (-1)^3 = -1 \quad \text{(çözüm yok)}$$

2. yol — Gauss lemması.
3'ün ilk sekiz katının modülo 17'deki değerleri:

$$3, 6, 9, 12, 15, 1, 4, 7$$

Bu sayılardan $\frac{p}{2} = 8$, 5'ten büyük olanlar yalnızca $9, 12, 15$'tir; yani $n = 3$. Yine

$$\left(\frac{3}{17}\right) = (-1)^3 = -1$$

bulunur. Nitekim modülo 17'deki kareler kümesi $\{1, 2, 4, 8, 9, 13, 15, 16\}$ olup 3 bu kümede yer almaz.
■

Örnek 29.4. Legendre sembolünün özelliklerini kullanarak $x^2 \equiv -2 \pmod{61}$ kongrüansının çözümünün olup olmadığını bulunuz.

Çözüm.
$p = 61$ ve $a = -2$'dir. Legendre sembolünün çarpımsallık özelliğini kullanarak sayıyı parçalayalım:

$$\left(\frac{-2}{61}\right) = \left(\frac{-1}{61}\right) \cdot \left(\frac{2}{61}\right)$$

Özel değer formüllerinden her iki parçayı ayrı ayrı hesaplayalım:

1. $\left(\frac{-1}{61}\right) = (-1)^{(61-1)/2} = (-1)^{30} = 1$
2. $\left(\frac{2}{61}\right) = (-1)^{(61^2-1)/8}$. Üssü hesaplayalım: $\frac{3721-1}{8} = 465$. Bu tek bir sayı olduğundan $(-1)^{465} = -1$.

Bu iki sonucu çarptığımızda:

$$\left(\frac{-2}{61}\right) = 1 \cdot (-1) = -1$$

Sonuç -1 (KNR) olduğundan denklemin çözümü yoktur.
Kontrol: $61 \equiv 5 \pmod 8$ olduğundan, bir sonraki örnekte göreceğimiz kural gereği 2 modülo 61'de bir non-rezidüdür — bulduğumuz sonuçla tutarlıdır.
■

Örnek 29.5. p tek asal sayı olmak üzere, $x^2 \equiv 2 \pmod p$ denkleminin çözülebilir olması için gerek ve yeter koşul nedir?

Çözüm.
Denklemin çözülebilmesi için 2'nin KR olması, yani $\left(\frac{2}{p}\right) = 1$ olması zorunludur. 2'nin karesel karakter formülünü hatırlayalım:

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = 1$$

Bu eşitliğin sağlanabilmesi için üs olan $\frac{p^2-1}{8}$ ifadesinin **çift** olması gerekir:

$$\frac{p^2-1}{8} = 2k \Longrightarrow p^2 - 1 = 16k \Longrightarrow p^2 \equiv 1 \pmod{16}$$

Tek asalları mod 8'e göre inceleyelim:

$p \bmod 8$	$p^2 \bmod 16$	$\frac{p^2-1}{8}$	$\left(\frac{2}{p}\right)$
1	1	çift	$+1$
3	9	tek	-1
5	9	tek	-1
7	1	çift	$+1$

Sonuç: $x^2 \equiv 2 \pmod p$ denklemi ancak ve ancak $p \equiv \pm 1 \pmod 8$, yani $p \equiv 1$ veya $p \equiv 7 \pmod 8$ olduğunda çözülebilirdir.
■

Örnek 29.6. $m \geq 2$ bir tam sayı ve $\gcd(r, m) = 1$ olsun. Eğer r, modülo m'ye göre bir kuadratik rezidü ise, $r^{\phi(m)/2} \equiv 1 \pmod m$ olduğunu gösteriniz.

Çözüm.
r bir KR olduğundan $x^2 \equiv r \pmod m$ denklemini sağlayan en az bir a tam sayısı vardır:

$$a^2 \equiv r \pmod m$$

$\gcd(r, m) = 1$ olduğundan $\gcd(a^2, m) = 1$ ve dolayısıyla a da modülle aralarında asaldır. Kongrüansın her iki tarafının $\frac{\phi(m)}{2}$. kuvvetini alalım:

$$r^{\phi(m)/2} \equiv (a^2)^{\phi(m)/2} \equiv a^{\phi(m)} \pmod{m}$$

a ve m aralarında asal olduğu için **Euler teoremi** devreye girer ve $a^{\phi(m)} \equiv 1 \pmod{m}$ olur. Yerine yazdığımızda ispat tamamlanır:

$$r^{\phi(m)/2} \equiv 1 \pmod{m}$$

Bu sonuç, Euler kriterinin asal olmayan modüllere yönelik bir genellemesidir; ancak dikkat: tersi doğru değildir — $r^{\phi(m)/2} \equiv 1$ olması r'nin KR olmasını garanti etmez.
■

30. Kuadratik Resiprosite (Karesel Karşılıklılık) Teoremi

Şu ana kadar Legendre sembolünün özelliklerini, Euler kriterini ve Gauss lemmasını kullanarak sayıların karesel karakterlerini belirledik. Ancak asallar büyüdükçe (örneğin $\left(\frac{7}{61}\right)$ gibi ifadelerde) üs alma işlemleri veya Gauss saymaları bile hantallaşır.
Gauss'un **"altın teorem"** adını verdiği **kuadratik resiprosite teoremi**, iki farklı tek asal sayının birbirine göre karesel durumlarının doğrudan bağlantılı olduğunu kanıtlar. Bu teorem, büyük modüller altındaki denklemlerin çözülebilirliğini çok kısa sürede tespit etmemizi sağlar.

30.1 Teorem ve Kafes (Lattice) İspatı

Teorem 30.1 (Kuadratik Resiprosite Teoremi). *p ve q birbirinden farklı iki tek asal sayı olsun. Bu durumda*

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

eşitliği sağlanır.

İspat.
Bu ispat, kartezyen koordinat sistemindeki tam sayı koordinatlı noktaların (kafes noktalarının) sayılması mantığına dayanır.
İlk olarak, birinci bölgede yer alan ve sınırları belirli bir K dikdörtgensel tam sayı kümesi tanımlayalım:

$$K=\left\{(x,y):1\le x\le\frac{p-1}{2},\quad 1\le y\le\frac{q-1}{2},\quad x,y\in\mathbb{Z}\right\}$$

Bu kümenin eleman sayısı, x ve y'nin alabileceği değerlerin çarpımı kadardır:

$$s(K)=\frac{p-1}{2}\cdot\frac{q-1}{2}$$

Şimdi K kümesini $qx=py$ doğrusu yardımıyla iki alt kümeye ayıralım:

- *Doğrunun bir tarafında kalanlar: $K_1=\{(x,y)\in K:qx>py\}$*
- *Diğer tarafında kalanlar: $K_2=\{(x,y)\in K:qx<py\}$*

Kritik ayrıntı. *K kümesindeki hiçbir nokta tam olarak $qx=py$ doğrusunun üzerinde olamaz. Çünkü $\gcd(p,q)=1$ olduğundan bu eşitliğin sağlanması için $p\mid x$ ve $q\mid y$ olması gerekirdi; oysa kümemizin sınırlarında $x\le\frac{p-1}{2}<p$ ve $y\le\frac{q-1}{2}<q$'dur.*
Dolayısıyla $K_1\cap K_2=\emptyset$ ve $K_1\cup K_2=K$'dır:

$$s(K_1)+s(K_2)=\frac{p-1}{2}\cdot\frac{q-1}{2}$$

Şimdi K_1 kümesinin eleman sayısını sütun sütun bulalım:

$$K_1=\bigcup_{x=1}^{(p-1)/2}\left\{(x,y):1\le y<\frac{qx}{p},y\in\mathbb{Z}\right\}$$

Bu birleşime giren kümeler ikişer ikişer ayrıktır. Belirli bir x değeri için $1\le y<\frac{qx}{p}$ şartını sağlayan y tam sayılarının adedi, $\left\lfloor\frac{qx}{p}\right\rfloor$ sayısına eşittir. O hâlde:

$$s(K_1) = \sum_{x=1}^{(p-1)/2} \left\lfloor \frac{qx}{p} \right\rfloor$$

Tamamen simetrik bir düşünceyle K_2 kümesinin eleman sayısı da y ekseni üzerinden toplanarak bulunur:

$$s(K_2) = \sum_{y=1}^{(q-1)/2} \left\lfloor \frac{py}{q} \right\rfloor$$

Bu değerleri toplam denkleminde yerine yazalım:

$$\sum_{x=1}^{(p-1)/2} \left\lfloor \frac{qx}{p} \right\rfloor + \sum_{y=1}^{(q-1)/2} \left\lfloor \frac{py}{q} \right\rfloor = \frac{p-1}{2} \cdot \frac{q-1}{2}$$

Eşitliğin her iki tarafını (-1)'in üssü olarak yazalım:

$$(-1)^{\sum \lfloor qx/p \rfloor} \cdot (-1)^{\sum \lfloor py/q \rfloor} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

Bir önceki bölümde Gauss lemması üzerinden kanıtladığımız t-toplam formülü gereği

$$\left(\frac{q}{p}\right) = (-1)^{\sum \lfloor qx/p \rfloor}, \qquad \left(\frac{p}{q}\right) = (-1)^{\sum \lfloor py/q \rfloor}$$

olduğunu biliyoruz. Bu değerleri yerine yazdığımızda ispat tamamlanır.
■

Teoremin pratik anlamı: ters çevirme kuralı

Kuadratik resiprosite teoremi aslında şunu söyler: $\left(\frac{p}{q}\right)$ sembolünü hesaplamak zorsa, onu ters çevirip $\left(\frac{q}{p}\right)$ sembolünü hesaplayabilirsiniz.

- Eğer p ve q asallarından **en az biri** $4k+1$ formundaysa, sembol işaret değiştirmeden aynen ters çevrilir:

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

- Eğer p ve q asallarının **her ikisi de** $4k+3$ formundaysa, sembol ters çevrildiğinde eksi işareti alır:

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$$

i Mantık köprüsü: çarpımdan asıl değere nasıl geçiyoruz?

Kuadratik resiprosite teoreminde hesapladığımız şey iki sembolün **çarpımıdır**. Peki bu çarpımdan asıl aradığımız sembolü tek başına nasıl çekiyoruz?
Legendre sembolleri yalnızca 1 veya -1 değerini alabilir; dolayısıyla iki senaryo vardır.
1. senaryo (çarpım 1 ise). İki sayı ya $(1 \cdot 1)$ ya da $((-1) \cdot (-1))$ olmak zorundadır. Her iki durumda da semboller **birbirine eşittir**:

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

2. senaryo (çarpım -1 ise). Sayılardan biri 1 iken diğeri zorunlu olarak -1'dir; yani semboller birbirinin **zıt işaretlisidir**:

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$$

İşte bu basit işaret mantığı sayesinde, üstteki büyük sayıyı aşağıya atıp modüler indirgemeyle küçültme işlemine devam edebiliriz.

30.2 Çözümlü Uygulamalar

Resiprosite teoreminin gücü, çok büyük sayılar içeren kongrüansları basit modüler indirgemeler ve sembolü sürekli ters çevirme ("takla attırma") yoluyla çok küçük sayılara düşürmesinde yatar.

Örnek 30.1. $x^2 \equiv -42 \pmod{61}$ kongrüansının çözülebilir olup olmadığını araştırınız.

Çözüm.
Problemi çözmek için $\left(\frac{-42}{61}\right)$ değerini hesaplamalıyız (61 bir asal sayıdır). İlk adım olarak -42 sayısını çarpanlarına ayırıp Legendre'nin çarpımsallık kuralını uygulayalım:

$$\left(\frac{-42}{61}\right) = \left(\frac{-1}{61}\right) \cdot \left(\frac{2}{61}\right) \cdot \left(\frac{3}{61}\right) \cdot \left(\frac{7}{61}\right)$$

1. parça — $\left(\frac{-1}{61}\right)$:

$$\left(\frac{-1}{61}\right) = (-1)^{\frac{61-1}{2}} = (-1)^{30} = 1$$

2. parça — $\left(\frac{2}{61}\right)$:

$$\left(\frac{2}{61}\right) = (-1)^{\frac{61^2-1}{8}} = (-1)^{465} = -1$$

3. parça — $\left(\frac{3}{61}\right)$: Her iki sayı da tek asaldır; resiprosite formülünü uygulayalım.

$$\left(\frac{3}{61}\right) \cdot \left(\frac{61}{3}\right) = (-1)^{\frac{3-1}{2} \cdot \frac{61-1}{2}} = (-1)^{1 \cdot 30} = 1$$

Çarpımları 1 olduğu için semboller eşittir. Şimdi 61'i modülo 3'te indirgeyelim ($61 \equiv 1 \pmod{3}$):

$$\left(\frac{3}{61}\right) = \left(\frac{61}{3}\right) = \left(\frac{1}{3}\right) = 1$$

4. parça — $\left(\frac{7}{61}\right)$:

$$\left(\frac{7}{61}\right) \cdot \left(\frac{61}{7}\right) = (-1)^{\frac{7-1}{2} \cdot \frac{61-1}{2}} = (-1)^{3 \cdot 30} = (-1)^{90} = 1$$

Yine çarpımları 1 çıktığından sembol işaretsiz çevrilir. Modülo 7'ye indirgeyelim ($61 \equiv 5 \pmod{7}$):

$$\left(\frac{7}{61}\right) = \left(\frac{61}{7}\right) = \left(\frac{5}{7}\right)$$

Karşımıza yine iki tek asal çıktı; teoremi bir kez daha uygulayıp "takla" attıralım:

$$\left(\frac{5}{7}\right) \cdot \left(\frac{7}{5}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{7-1}{2}} = (-1)^{2\cdot 3} = 1 \Longrightarrow \left(\frac{5}{7}\right) = \left(\frac{7}{5}\right)$$

7'yi modülo 5'e indirgeyelim ($7 \equiv 2 \pmod 5$):

$$\left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = (-1)^3 = -1$$

Zincirleme geriye dönersek:

$$\left(\frac{7}{61}\right) = \left(\frac{61}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = -1$$

Sonuçların birleştirilmesi.

$$\left(\frac{-42}{61}\right) = 1 \cdot (-1) \cdot 1 \cdot (-1) = 1$$

Genel sonuç 1 çıktığı için -42 sayısı modülo 61'e göre bir **kuadratik rezidüdür** ve $x^2 \equiv -42 \pmod{61}$ kongrüansı **kesin olarak çözülebilirdir**.
■

Örnek 30.2. Hangi p tek asal sayıları için 3, modülo p'ye göre bir kuadratik rezidüdür? Yani $x^2 \equiv 3 \pmod p$ kongrüansı hangi asallarda çözülebilirdir?

Çözüm.
Soru bizden $\left(\frac{3}{p}\right) = 1$ koşulunu sağlayan tüm p tek asallarını bulmamızı istiyor. Kuadratik resiprosite teoreminden faydalanalım:

$$\left(\frac{3}{p}\right) \cdot \left(\frac{p}{3}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}}$$

Denklemi düzenlersek:

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) \cdot (-1)^{\frac{p-1}{2}}$$

Sonucun 1 çıkması için iki çarpanın da 1 ya da ikisinin de -1 olması gerekir; böylece iki durum ortaya çıkar.
Durum 1: $\left(\frac{p}{3}\right) = 1$ **ve** $(-1)^{\frac{p-1}{2}} = 1$

- $(-1)^{\frac{p-1}{2}} = 1 \Longrightarrow \frac{p-1}{2}$ çift $\Longrightarrow p \equiv 1 \pmod 4$
- $\left(\frac{p}{3}\right) = 1 \Longrightarrow p$, mod 3'e göre bir KR'dir. Modülo 3'te kareler yalnızca $\{1\}$ olduğundan $\Longrightarrow p \equiv 1 \pmod 3$

Durum 2: $\left(\frac{p}{3}\right) = -1$ **ve** $(-1)^{\frac{p-1}{2}} = -1$

- $(-1)^{\frac{p-1}{2}} = -1 \Longrightarrow \frac{p-1}{2}$ tek $\Longrightarrow p \equiv 3 \pmod 4$
- $\left(\frac{p}{3}\right) = -1 \Longrightarrow p$, mod 3'e göre bir KNR'dir $\Longrightarrow p \equiv 2 \pmod 3$

Aradığımız asallar şu iki kongrüans sisteminden birini sağlamalıdır:

1. $p \equiv 1 \pmod 3$ ve $p \equiv 1 \pmod 4$
2. $p \equiv 2 \pmod 3$ ve $p \equiv 3 \pmod 4$

Şimdi **Çin kalan teoreminden** yararlanarak bu sistemleri çözelim.

1. sistemin çözümü. $p \equiv 1 \pmod 3 \Longrightarrow p = 1 + 3y$. Bunu ikinci denklemde yerine koyalım:

$$1 + 3y \equiv 1 \pmod 4 \Longrightarrow 3y \equiv 0 \pmod 4 \Longrightarrow y \equiv 0 \pmod 4 \Longrightarrow y = 4z$$

Başa dönersek $p = 1 + 12z$, yani $p \equiv 1 \pmod{12}$.
2. sistemin çözümü. $p \equiv 2 \pmod 3 \Longrightarrow p = 2 + 3y$. İkinci denklemde yerine koyalım:

$$2 + 3y \equiv 3 \pmod 4 \Longrightarrow 3y \equiv 1 \pmod 4$$

Modüler bölme için sağ tarafa 8 ekleyelim (9, 3'e tam bölünür):

$$3y \equiv 9 \pmod 4 \Longrightarrow y \equiv 3 \pmod 4 \Longrightarrow y = 3 + 4z$$

Başa dönersek $p = 2 + 3(3 + 4z) = 11 + 12z$, yani $p \equiv 11 \pmod{12}$.
Genel sonuç. $\left(\frac{3}{p}\right) = 1$ olması için p tek asalının modülo 12'ye göre 1 veya 11 kalanını vermesi gerekir; kısaca $p \equiv \pm 1 \pmod{12}$.
Kontrol: Bir önceki örnekte $\left(\frac{3}{61}\right) = 1$ bulmuştuk. Gerçekten de $61 = 5 \cdot 12 + 1 \equiv 1 \pmod{12}$'dir.
■

31. Jacobi Sembolü

Legendre sembolü yalnızca tek asal modüller için tanımlıydı. Ancak pratikte ve ileri düzey kriptografik algoritmalarda, asal çarpanlarına ayrılmamış büyük kompozit sayılarla çalışmamız gerekir. Carl Gustav Jacob Jacobi, Legendre sembolünün özelliklerini kullanarak bu kavramı tüm tek tam sayılara genelleştirmiştir.

31.1 Jacobi Sembolünün Tanımı

Tanım 31.1 (Jacobi Sembolü). P bir tam sayı, $Q > 1$ bir **tek tam sayı** ve $\gcd(P, Q) = 1$ olsun. Eğer Q sayısının asal çarpanlarına ayrılmış hâli $Q = q_1 q_2 \cdots q_s$ ise (q_i'ler tek asallar), P'nin Q'ya göre **Jacobi sembolü** şöyle tanımlanır:

$$\left(\frac{P}{Q}\right) = \left(\frac{P}{q_1}\right) \cdot \left(\frac{P}{q_2}\right) \cdots \left(\frac{P}{q_s}\right)$$

Buradaki q_i asallarının birbirinden farklı olması gerekmez; aynı asal çarpandan birden fazla varsa çarpımda o kadar kez tekrar edilir.

Bu tanımdan iki temel çıkarım elde ederiz:

1. Eğer Q zaten bir tek asal sayı ise, Jacobi sembolü doğrudan **Legendre sembolüyle çakışır**.
2. Sağ taraftaki Legendre sembollerinin her biri yalnızca ± 1 alabildiğinden, **Jacobi sembolünün alabileceği değerler de yalnızca 1 veya -1'dir**.

> ⚠ Jacobi sembolünün tuzağı
>
> Jacobi sembolü, Legendre sembolünün görünümünü taklit etse de "çözülebilirlik" konusunda aynı garantiyi vermez.
>
> - Eğer $\left(\frac{P}{Q}\right) = -1$ ise, $x^2 \equiv P \pmod{Q}$ kongrüansının **çözümü kesinlikle yoktur**.
> - Ancak $\left(\frac{P}{Q}\right) = 1$ olması, denklemin **çözülebilir olduğunu garanti etmez.**
>
> **Örnek:** $9 = 3 \cdot 3$ olduğundan
>
> $$\left(\frac{2}{9}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{3}\right) = (-1) \cdot (-1) = 1$$
>
> Sembolün değeri 1 çıkmasına rağmen $x^2 \equiv 2 \pmod{9}$ kongrüansının hiçbir çözümü yoktur; modülo 9'daki kareler $\{0, 1, 4, 7\}$ kümesidir. Çözümün var olması için sağ taraftaki *tüm* Legendre sembollerinin ayrı ayrı 1 olması gerekir.

31.2 Jacobi Sembolünün Temel Özellikleri

Jacobi sembolü, Legendre sembolünün sahip olduğu çarpımsal özellikleri aynen korur.

Teorem 31.1 (Jacobi Sembolünün Cebirsel Özellikleri). *$Q > 1$ ve $Q' > 1$ tek tam sayılar; P ve P' tam sayılar olsun.* $\gcd(PP', QQ') = 1$ *koşulu altında aşağıdaki özellikler geçerlidir:*

1. $\left(\frac{P}{Q}\right) \cdot \left(\frac{P}{Q'}\right) = \left(\frac{P}{QQ'}\right)$
2. $\left(\frac{P}{Q}\right) \cdot \left(\frac{P'}{Q}\right) = \left(\frac{PP'}{Q}\right)$
3. $\left(\frac{P^2}{Q}\right) = \left(\frac{P}{Q^2}\right) = 1$
4. $\left(\frac{P'P^2}{Q'Q^2}\right) = \left(\frac{P'}{Q'}\right)$

5. $P \equiv P' \pmod{Q}$ *ise* $\left(\frac{P}{Q}\right) = \left(\frac{P'}{Q}\right)$

İspat.
Q ve Q' sayılarını tek asal çarpanlarına ayıralım: $Q = q_1 \cdots q_s$ ve $Q' = q'_1 \cdots q'_t$.
1) Birinci özellik. *Sol tarafı Jacobi tanımına göre açalım:*

$$\left(\frac{P}{Q}\right) \cdot \left(\frac{P}{Q'}\right) = \left[\left(\frac{P}{q_1}\right) \cdots \left(\frac{P}{q_s}\right)\right] \cdot \left[\left(\frac{P}{q'_1}\right) \cdots \left(\frac{P}{q'_t}\right)\right]$$

Bu çarpım, QQ' sayısının tüm asal çarpanlarına ait Legendre sembollerinin çarpımıdır; dolayısıyla $\left(\frac{P}{QQ'}\right)$ ifadesine eşittir.
2) İkinci özellik.

$$\left(\frac{P}{Q}\right) \cdot \left(\frac{P'}{Q}\right) = \left[\left(\frac{P}{q_1}\right) \cdots \left(\frac{P}{q_s}\right)\right] \cdot \left[\left(\frac{P'}{q_1}\right) \cdots \left(\frac{P'}{q_s}\right)\right]$$

Terimleri aynı q_i'lere göre gruplayalım ve Legendre sembolünün çarpımsallık özelliğini uygulayalım:

$$= \left(\frac{PP'}{q_1}\right) \cdots \left(\frac{PP'}{q_s}\right) = \left(\frac{PP'}{Q}\right)$$

3) Üçüncü özellik. *İkinci özelliği kullanarak $\left(\frac{P^2}{Q}\right) = \left(\frac{P}{Q}\right)^2 = (\pm 1)^2 = 1$; birinci özelliği kullanarak $\left(\frac{P}{Q^2}\right) = \left(\frac{P}{Q}\right)^2 = 1$.*
4) Dördüncü özellik. *İlk üç özelliğin doğrudan birleşimidir:*

$$\left(\frac{P'P^2}{Q'Q^2}\right) = \left(\frac{P'}{Q'}\right) \cdot \underbrace{\left(\frac{P'}{Q^2}\right)}_{=1} \cdot \underbrace{\left(\frac{P^2}{Q'}\right)}_{=1} \cdot \underbrace{\left(\frac{P^2}{Q^2}\right)}_{=1} = \left(\frac{P'}{Q'}\right)$$

5) Beşinci özellik. *$P \equiv P' \pmod{Q}$ ise, Q'nun her q_i asal çarpanı için de $P \equiv P' \pmod{q_i}$ geçerlidir. Legendre sembolü modüler denkliği koruduğundan her i için $\left(\frac{P}{q_i}\right) = \left(\frac{P'}{q_i}\right)$ olur; çarpımları da eşittir.*
■

31.3 Jacobi Sembolü İçin Özel Değerler

Jacobi sembolü, asal modüller için bulduğumuz -1 ve 2'nin karesel karakteri formüllerini **birebir aynı şekilde** korur. Ancak ispatı, asal çarpanlar üzerinde zarif bir modüler tümevarım gerektirir.

Teorem 31.2 (Jacobi Sembolünde Özel Değerler). *$Q > 1$ bir tek tam sayı olsun. Bu durumda:*

1. $\left(\frac{-1}{Q}\right) = (-1)^{\frac{Q-1}{2}}$
2. $\left(\frac{2}{Q}\right) = (-1)^{\frac{Q^2-1}{8}}$

İspat.
$Q = q_1 q_2 \cdots q_s$ şeklinde tek asal çarpanlarına ayrılmış olsun.
1) Birinci formülün ispatı. *Jacobi tanımını kullanarak açalım:*

$$\left(\frac{-1}{Q}\right) = \left(\frac{-1}{q_1}\right) \cdots \left(\frac{-1}{q_s}\right) = (-1)^{\frac{q_1-1}{2} + \cdots + \frac{q_s-1}{2}} \qquad (*)$$

Yardımcı cebirsel gerçek. *a ve b iki tek tam sayı olsun:*

$$\frac{ab-1}{2} - \left(\frac{a-1}{2} + \frac{b-1}{2}\right) = \frac{(a-1)(b-1)}{2}$$

a ve b tek olduğundan $(a-1)$ ve $(b-1)$ çifttir; iki çift sayının çarpımı 4'ün katıdır ve 2'ye bölündüğünde sonuç yine çifttir. O hâlde modülo 2'de bu fark sıfıra denktir:

$$\frac{ab-1}{2} \equiv \frac{a-1}{2} + \frac{b-1}{2} \pmod 2$$

Bu mantığı tümevarımla tüm q_i'lere genellersek:

$$\frac{q_1-1}{2} + \cdots + \frac{q_s-1}{2} \equiv \frac{q_1 \cdots q_s - 1}{2} = \frac{Q-1}{2} \pmod 2$$

Modülo 2'deki denklik, (-1)'in üssündeki teklik/çiftlik durumunu değiştirmeyeceğinden $(*)$ denklemindeki toplamı bu sonuca eşitleyebiliriz.
2) İkinci formülün ispatı. *Yine Jacobi tanımını açalım:*

$$\left(\frac{2}{Q}\right) = \left(\frac{2}{q_1}\right) \cdots \left(\frac{2}{q_s}\right) = (-1)^{\frac{q_1^2-1}{8} + \cdots + \frac{q_s^2-1}{8}} \qquad (**)$$

Yardımcı cebirsel gerçek. *a ve b iki tek tam sayı olsun:*

$$\frac{a^2b^2-1}{8} - \left(\frac{a^2-1}{8} + \frac{b^2-1}{8}\right) = \frac{(a^2-1)(b^2-1)}{8}$$

Her tek sayının karesi modülo 8'de 1'e denktir; yani $8 \mid a^2-1$ ve $8 \mid b^2-1$. Dolayısıyla çarpım 64'ün katıdır ve 8'e bölündüğünde sonuç hâlâ çifttir. O hâlde:

$$\frac{a^2b^2-1}{8} \equiv \frac{a^2-1}{8} + \frac{b^2-1}{8} \pmod 2$$

Bu mantığı tümevarımla tüm q_i'lere uygularsak:

$$\frac{q_1^2-1}{8} + \cdots + \frac{q_s^2-1}{8} \equiv \frac{(q_1 \cdots q_s)^2 - 1}{8} = \frac{Q^2-1}{8} \pmod 2$$

Bu sonucu $(**)$ denklemindeki üsse yazdığımızda ispat tamamlanır.
■

31.4 Jacobi Sembolü İçin Karşılıklılık Teoremi

Legendre sembolü için ispatladığımız altın teorem, Jacobi sembolü için de birebir aynı formda geçerlidir. Bu teorem, devasa kompozit sayılarla çalışırken **asal çarpanlara ayırma zahmetinden kurtulup** doğrudan ters çevirme işlemi yapmamıza olanak tanır — Jacobi sembolünün asıl pratik değeri buradadır.

Teorem 31.3 (Jacobi Sembolü İçin Karşılıklılık Teoremi). *$P > 1$ ve $Q > 1$ iki **tek tam sayı** ve $\gcd(P, Q) = 1$ olsun. Bu durumda*

$$\left(\frac{P}{Q}\right) \cdot \left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}}$$

eşitliği sağlanır.

İspat.
P ve Q tek tam sayılarını asal çarpanlarına ayıralım: $P = p_1 \cdots p_r$ ve $Q = q_1 \cdots q_s$.
Jacobi sembolünün tanımı ve çarpımsallık özelliğinden:

$$\left(\frac{P}{Q}\right) = \prod_{j=1}^{s} \left(\frac{P}{q_j}\right) = \prod_{j=1}^{s} \prod_{i=1}^{r} \left(\frac{p_i}{q_j}\right)$$

*Buradaki $\left(\frac{p_i}{q_j}\right)$ sembolleri, tabanlar asal olduğu için doğrudan **Legendre sembolleridir**; onlara klasik kuadratik resiprosite teoremini uygulayabiliriz:*

$$\left(\frac{p_i}{q_j}\right) = \left(\frac{q_j}{p_i}\right) \cdot (-1)^{\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}$$

Bu eşitliği çarpımın içine yerleştirip sembolleri ve işaretleri ayıralım:

$$\left(\frac{P}{Q}\right) = \left[\prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{q_j}{p_i}\right)\right] \cdot (-1)^{\sum_i \sum_j \frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}$$

Köşeli parantezin içi tam olarak $\left(\frac{Q}{P}\right)$ Jacobi sembolünün açılımıdır. Üsteki çift toplamı ise çarpanlarına ayırabiliriz:

$$\left(\frac{P}{Q}\right) = \left(\frac{Q}{P}\right) \cdot (-1)^{\left(\sum_i \frac{p_i-1}{2}\right)\cdot\left(\sum_j \frac{q_j-1}{2}\right)}$$

Bir önceki teoremde kullandığımız yardımcı cebirsel gerçek gereği:

$$\sum_{i=1}^{r}\frac{p_i-1}{2} \equiv \frac{P-1}{2} \pmod 2, \qquad \sum_{j=1}^{s}\frac{q_j-1}{2} \equiv \frac{Q-1}{2} \pmod 2$$

Bu denklikleri üsse yazıp her iki tarafı $\left(\frac{Q}{P}\right)$ ile çarptığımızda ispat tamamlanır.
■

31.5 Çözümlü Örnek

Örnek 31.1. $x^2 \equiv 105 \pmod{317}$ kongrüansının çözümü var mıdır? Başka bir deyişle, 105 sayısı modülo 317'ye göre bir KR midir?

Çözüm.
Hatırlatma (asallık testi). Asal olmayan bir $t > 1$ doğal sayısının, $p \le \sqrt{t}$ koşuluna uyan en az bir p asal böleni vardır. Dolayısıyla bu koşula uyan hiçbir asala bölünemeyen bir sayı kesinlikle asaldır.
$17 < \sqrt{317} < 18$ olduğundan kontrol etmemiz gereken asallar $2, 3, 5, 7, 11, 13, 17$'dir. Bunların hiçbiri 317'yi tam bölmediğinden **317 bir asal sayıdır**.
O hâlde 105 tek bir tam sayı, 317 tek bir asal ve $\gcd(105, 317) = 1$'dir. 317 asal olduğu için Jacobi ve Legendre sembolleri burada çakışır; bulacağımız sonuç kesin bir çözülebilirlik yanıtı verir.
Jacobi karşılıklılık teoremini uygulayıp "takla" attıralım:

$$\left(\frac{105}{317}\right) \cdot \left(\frac{317}{105}\right) = (-1)^{\frac{105-1}{2}\cdot\frac{317-1}{2}} = (-1)^{52\cdot 158}$$

Üs çift olduğundan sonuç $+1$'dir; yani işaret değişmez:

$$\left(\frac{105}{317}\right) = \left(\frac{317}{105}\right)$$

Şimdi 317'yi modülo 105'e indirgeyelim. $105 \cdot 3 = 315$ olduğundan $317 \equiv 2 \pmod{105}$:

$$\left(\frac{317}{105}\right) = \left(\frac{2}{105}\right)$$

Karşımıza 2'nin karesel karakteri çıktı; özel değer formülünü uygulayalım:

$$\left(\frac{2}{105}\right) = (-1)^{\frac{105^2-1}{8}}$$

Üssü hesaplayalım: $105^2 = 11025$ ve $\frac{11024}{8} = 1378$. Bu çift bir sayı olduğundan:

$$\left(\frac{2}{105}\right) = 1$$

Sonuç: Zincirleme eşitliklerden $\left(\frac{105}{317}\right) = 1$ elde edilir. 317 asal olduğundan bu, 105'in modülo 317'ye göre kesin bir **kuadratik rezidü** olduğu anlamına gelir; dolayısıyla $x^2 \equiv 105 \pmod{317}$ kongrüansı **çözülebilirdir**.
Sağlama (çarpanlara ayırarak). $105 = 3 \cdot 5 \cdot 7$ olduğundan:

- $317 \equiv 5 \pmod{12}$ olduğundan $\left(\frac{3}{317}\right) = -1$
- $317 \equiv 1 \pmod{4}$ olduğundan $\left(\frac{5}{317}\right) = \left(\frac{317}{5}\right) = \left(\frac{2}{5}\right) = -1$
- Benzer şekilde $\left(\frac{7}{317}\right) = \left(\frac{317}{7}\right) = \left(\frac{2}{7}\right) = +1$

Çarpım: $(-1)(-1)(+1) = 1$ ✓ İki yöntem birbirini doğrulamaktadır.
■

31.6 Çalışma Problemleri

Konuyu pekiştirmek için aşağıdaki problemleri; öğrendiğiniz Legendre/Jacobi sembolü kuralları, Euler kriteri ve kuadratik resiprosite teoremlerini kullanarak çözebilirsiniz.

Alıştırma 31.1 (Sembol Değerleri). Aşağıdaki sembollerin değerlerini hesaplayınız:

$$\left(\frac{-23}{83}\right), \qquad \left(\frac{51}{71}\right), \qquad \left(\frac{71}{73}\right), \qquad \left(\frac{-35}{97}\right)$$

Alıştırma 31.2 (Çözülebilirlik Analizi). Aşağıdaki kongrüansların hangileri çözülebilirdir?
a) $x^2 \equiv 10 \pmod{127}$
b) $x^2 \equiv 234 \pmod{401}$
c) $x^2 \equiv -73 \pmod{143}$
d) $x^2 \equiv 45 \pmod{101}$
İpucu: $143 = 11 \cdot 13$ asal değildir; bu şıkta Jacobi sembolünün tuzağını hatırlayın.

32. Doğrusal (Lineer) Diofant Denklemleri

Sayılar teorisinde katsayıları ve aranan çözümleri yalnızca **tam sayılar** olan denklemlere Diofant denklemleri denir. Bu bölümde yüksek dereceli karmaşık yapılar yerine, modüler aritmetik ve Öklid algoritmasıyla doğrudan bağlantılı olan birinci dereceden denklemleri inceleyeceğiz.

32.1 Tanım ve Çözülebilirlik Şartı

Tanım 32.1 (Birinci Dereceden İki Bilinmeyenli Diofant Denklemi). $a, b, c \in \mathbb{Z} \setminus \{0\}$ olmak üzere,

$$ax + by = c$$

şeklinde ifade edilen ve yalnızca tam sayılı x ve y çözümleri aranan denklemlere **birinci dereceden iki bilinmeyenli Diofant denklemi** denir.

Bu denklemleri çözmek, daha önce öğrendiğimiz lineer kongrüansları çözmekle birebir aynı şeydir; çünkü

$$ax + by = c \Leftrightarrow ax \equiv c \pmod{b}$$

denkliği vardır. Dolayısıyla $ax + by = c$ denklemini çözme problemi, $ax \equiv c \pmod{b}$ kongrüansını çözme problemine denktir.

i Çözülebilirlik ve sadeleştirme kuralı

1. **Çözülebilirlik şartı.** Bir $ax + by = c$ Diofant denkleminin tam sayılı çözümünün olabilmesi için gerek ve yeter koşul $\gcd(a, b) \mid c$ olmasıdır.
2. **Sadeleştirme.** Bu şart sağlanıyorsa, işlemleri kolaylaştırmak adına denklemin her iki tarafını ortak bölene böleriz:
$$\frac{a}{\gcd(a,b)}x + \frac{b}{\gcd(a,b)}y = \frac{c}{\gcd(a,b)}$$
3. Bu sadeleştirme sonucunda yeni katsayılar daima aralarında asal olur. Bu yüzden Diofant denklemlerini incelerken genel olarak $\gcd(a, b) = 1$ olan sadeleştirilmiş formlar üzerinde çalışmak yeterlidir.

32.2 Genel Çözüm Teoremi

Elimizde denklemi sağlayan tek bir başlangıç çözümü varsa, bu çözümü kullanarak sonsuz sayıdaki diğer tüm çözümleri nasıl bulacağımızı aşağıdaki teorem söyler.

Teorem 32.1 (Diofant Denkleminin Genel Çözümü). *$a, b, c \in \mathbb{Z} \setminus \{0\}$ ve $\gcd(a, b) = 1$ olsun. $ax + by = c$ Diofant denkleminin bir tam sayılı özel çözümü (x_0, y_0) ise, denklemin **bütün** tam sayılı çözümleri $t \in \mathbb{Z}$ olmak üzere şöyledir:*

$$x = x_0 + bt, \qquad y = y_0 - at$$

> ***İspat.***
> *(x, y), $ax + by = c$ denkleminin herhangi bir tam sayılı çözümü olsun. (x_0, y_0) da özel bir çözüm olduğundan $ax_0 + by_0 = c$'dir. Bu iki denklemi taraf tarafa çıkaralım:*
>
> $$a(x - x_0) + b(y - y_0) = 0$$
>
> *Terimlerden birini karşıya atalım:*

$$a(x - x_0) = -b(y - y_0)$$

Bu eşitlikten b sayısının sol tarafı, yani $a(x - x_0)$ çarpımını tam böldüğünü anlıyoruz:

$$b \mid a(x - x_0)$$

Teoremin başında $\gcd(a, b) = 1$ kabul etmiştik. Öklid lemması gereği, b bir çarpımı bölüyorsa ve çarpanlardan biriyle (a) aralarında asalsa, diğer çarpanı bölmek zorundadır:

$$b \mid (x - x_0) \Longrightarrow x - x_0 = bt \quad (t \in \mathbb{Z}) \Longrightarrow x = x_0 + bt$$

Şimdi $(x - x_0) = bt$ ifadesini asıl denklemde yerine yazalım:

$$a(bt) + b(y - y_0) = 0$$

Her iki tarafı $b \neq 0$'a bölersek:

$$at + y - y_0 = 0 \Longrightarrow y = y_0 - at$$

Tersine, bulduğumuz $x = x_0 + bt$ ve $y = y_0 - at$ tam sayıları denklemde yerine konulduğunda denklemi her zaman sağlar; dolayısıyla tüm çözümleri bulmuş oluruz.
■

32.3 Genişletilmiş Öklid Algoritmasıyla Çözümlü Örnekler

Katsayılar küçükse deneme yanılmayla bir (x_0, y_0) bulunabilir. Ancak katsayılar büyükse, **genişletilmiş Öklid algoritması** kullanarak en büyük ortak böleni geriye doğru açar ve ilk çözümü algoritmik olarak buluruz.

Örnek 32.1. $30x + 66y = 41$ Diofant denkleminin çözümünü araştırınız.

Çözüm.
Çözülebilirlik şartını kontrol edelim: $\gcd(a, b) \mid c$ olmalıdır.

$$\gcd(30, 66) = 6$$

Ancak 6 sayısı 41'i tam bölmez ($6 \nmid 41$). Bu nedenle verilen Diofant denklemi **çözümsüzdür**; hiçbir tam sayı çözümü yoktur.
Sezgisel olarak: sol taraftaki her terim 6'nın katı olduğundan toplam da daima 6'nın katı olmak zorundadır, oysa 41 değildir.
■

Örnek 32.2. $291x + 549y = 54$ Diofant denkleminin tüm tam sayı çözümlerini bulunuz.

Çözüm.
1. Çözülebilirlik ve sadeleştirme.
$\gcd(291, 549) = 3$ ve $3 \mid 54$ olduğundan denklemin sonsuz çözümü vardır. Her iki tarafı 3'e bölelim:

$$97x + 183y = 18$$

Artık aralarında asal olan 97 ve 183 ile çalışacağız.
2. Öklid algoritması.

$$\begin{aligned} 183 &= 1 \cdot 97 + 86 \Longrightarrow 86 = 183 - 97 \\ 97 &= 1 \cdot 86 + 11 \Longrightarrow 11 = 97 - 86 \\ 86 &= 7 \cdot 11 + 9 \ \ \Longrightarrow 9 = 86 - 7 \cdot 11 \end{aligned}$$

Algoritmayı 1 kalanına kadar indirmeye gerek yoktur: 9 sayısı, aradığımız 18'in tam yarısıdır. İşlemi burada kesip 9'u yalnız bırakıyoruz.
3. Geriye doğru yerine koyma.

$$\begin{aligned} 9 &= 86 - 7 \cdot 11 \\ &= 86 - 7(97 - 86) \\ &= 8 \cdot 86 - 7 \cdot 97 \\ &= 8(183 - 97) - 7 \cdot 97 \\ &= 8 \cdot 183 - 15 \cdot 97 \end{aligned}$$

Doğrusal birleşimimizi bulduk: $97 \cdot (-15) + 183 \cdot 8 = 9$. *(Sağlama:* $-1455 + 1464 = 9$ ✓*)*
4. Hedef denkleme ulaşma.
Sadeleşmiş denklemimizin sağ tarafı 9 değil 18'di; eşitliğin her iki tarafını 2 ile çarpalım:

$$97 \cdot (-30) + 183 \cdot 16 = 18$$

(Sağlama: $-2910 + 2928 = 18$ ✓*)* O hâlde özel çözümümüz:

$$x_0 = -30, \qquad y_0 = 16$$

5. Genel çözüm.
Sadeleşmiş denklemde $a = 97$ ve $b = 183$ olduğundan:

$$x = -30 + 183t, \qquad y = 16 - 97t \qquad (t \in \mathbb{Z})$$

■

Örnek 32.3. $312x + 51y = 9$ Diofant denklemini çözünüz.

Çözüm.
1. Sadeleştirme. $\gcd(312, 51) = 3$ ve $3 \mid 9$ olduğundan çözüm vardır. Üçe bölelim:

$$104x + 17y = 3$$

2. Öklid algoritması (104 ve 17 için).

$$\begin{aligned} 104 &= 6 \cdot 17 + 2 \\ 17 &= 8 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

3. Geriye dönüş.

$$\begin{aligned} 1 &= 17 - 8 \cdot 2 \\ &= 17 - 8(104 - 6 \cdot 17) \\ &= 17 - 8 \cdot 104 + 48 \cdot 17 \\ &= 104 \cdot (-8) + 17 \cdot 49 \end{aligned}$$

(Sağlama: $-832 + 833 = 1$ ✓*)*
4. Hedef denkleme genişletme. Denklemin sağ tarafı 3 olduğu için eşitliğin iki tarafını 3 ile çarpalım:

$$3 = 104 \cdot (-24) + 17 \cdot 147$$

(Sağlama: $-2496 + 2499 = 3$ ✓*)* Buradan özel çözüm: $x_0 = -24$, $y_0 = 147$.
5. Genel çözüm. $a = 104$ ve $b = 17$ kullanılarak:

$$x = -24 + 17t, \qquad y = 147 - 104t \qquad (t \in \mathbb{Z})$$

■

32.4 Çalışma Problemleri

Alıştırma 32.1 (Diofant Denklemleri). Aşağıdaki Diofant denklemlerinin bütün tam sayılı çözümlerini bulunuz. Önce çözülebilirlik şartı olan $\gcd(a, b) \mid c$ kuralını kontrol etmeyi unutmayın.
a) $3x + 5y = 1$ **b)** $5x + 3y = 52$ **c)** $40x + 63y = 521$ **d)** $330x + 175y = 50$

e) $15x - 7y = 111$ **f)** $12x + 501y = 1$ **g)** $10x - 7y = 17$ **h)** $15x + 11y = 1$

