Sayılar Teorisi

Sayılar Teorisi 2 — İleri Yapılar ve Analitik Araçlar

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. 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.

1.1 Çözüm Kavramı

Tanım 1.1 (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 1.1. 2 sayısı, $x^2 + 2x \equiv 0 \pmod{8}$ kongrüansının bir çözümüdür; çünkü

$$2^2 + 2 \cdot 2 = 8 \equiv 0 \pmod{8}$$

1.2 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 1.2. 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.

1.3 Çözüm Sayısı

Tanım 1.2 (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 1.3. $x^2 - 1 \equiv 0 \pmod{8}$ 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:

$$x \equiv 1, \quad x \equiv 3, \quad x \equiv 5, \quad x \equiv 7 \pmod{8}$$

1.4 Bir Kongrüansın Derecesi

Bir kongrüansın derecesi, polinomun derecesiyle karıştırılmamalıdır: baş katsayı modüle bölünüyorsa o terim kongrüansta hiçbir rol oynamaz.

Tanım 1.3 (Kongrüansın Derecesi). $f(x) = a_n x^n + \cdots + a_1 x + a_0$ olsun ($a_n \neq 0$; 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.

2. 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.

2.1 İndirgeme Teoremi

Teorem 2.1 (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 2.2 (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.

2.2 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 $(a_1, ..., a_k)$ kombinasyonları alınarak $N_1 N_2 \cdots N_k$ çözümün hepsi elde edilir.

2.3 Çözümlü Uygulamalar

Örnek 2.1. $x^2 + x + 7 \equiv 0 \pmod{189}$ 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 2.2. $f(x) = x^3 + 19x^2 - x + 23 \equiv 0 \pmod{42}$ 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 $12167 + 10051 - 23 + 23 = 22218 = 42 \cdot 529 \equiv 0$.)
■

2.4 Problemler

Alıştırma 2.1 (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.

3. 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

$$f(x) \equiv 0 \pmod{p^2}, \qquad f(x) \equiv 0 \pmod{p^3}, \qquad \dots$$

kongrüanslarını modül p^s olana dek **basamak basamak** çözeriz. Her basamakta bir önceki basamağın çözümlerini "yükseltmeye" çalışırız. Bu tekniğe **kök yükseltme (kök taşıma)** denir.

3.1 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 3.1 (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 3.1 (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 3.2 (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 3.1 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.
■

3.2 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 3.2 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.

3.3 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 3.3 (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 3.2 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 3.1 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 3.4 (Yükseltmenin Üç Hâli). *Teorem 3.3'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.

3.4 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 3.4'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.

3.5 Çözümlü Uygulamalar

Örnek 3.1. $x^3 - 3x^2 + 27 \equiv 0 \pmod{5^3}$ 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 3.2. $x^3 + x + 1 \equiv 0 \pmod{3^2}$ 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 3.3. $x^3 + x - 19 \equiv 0 \pmod{7^2}$ 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 3.4'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.

3.6 Problemler

Alıştırma 3.1 (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.

4. 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.

4.1 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 4.1 (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 4.1. $x^7 + x^3 + 2 \equiv 0 \pmod 5$ 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.

4.2 Çarpan Teoremi

Cebirden bilinen "kök $\Longleftrightarrow$ çarpan" ilkesi, modül asal olduğunda kongrüanslar için de geçerlidir.

Teorem 4.2 (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.
■

4.3 Lagrange Teoremi

Artık bu bölümün ana sonucunu ispatlayabiliriz: asal modülde çözüm sayısı dereceyi aşamaz.

Teorem 4.3 (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 4.2 gereği*

$$f(x) \equiv (x-a)\,g(x) \pmod p \qquad (*)$$

olacak şekilde tam katsayılı bir $g(x)$ polinomu vardır. Üstelik bu polinom, Teorem 4.2'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 4.2'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.

5. 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.

5.1 n. Kuvvet Rezidü Kavramı

Bir sayının belirli bir modüle göre tam kuvvetinin alınıp alınamayacağını ifade eden yapıya "rezidü (kalan)" denir.

Tanım 5.1 (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 5.1 (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.

5.2 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 5.2 (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.

5.3 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 5.1 (Mertebe ϕ'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:*

$$\phi(m) = qh + r, \qquad 0 \le r < h$$

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* $0 \le r < h$*'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 5.2 (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.

5.4 Üslerin Denkliği ve Periyodiklik

İki farklı kuvvetin modüler sistemde aynı kalanı vermesi tesadüf değildir; üsler arasındaki fark doğrudan mertebeyle bağlantılıdır.

Önerme 5.1 (Üslerin Denkliği ve Mertebe İlişkisi). *$m \ge 2$ bir tam sayı,* $\gcd(a,m) = 1$ *ve a'nın mertebesi h olsun. $j, k \ge 0$ tam sayıları için:*

$$a^j \equiv a^k \pmod{m} \Longrightarrow h \mid (j-k)$$

İspat.
Genelliği bozmadan $j \ge k$ *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.*

$$j - k = qh + r, \qquad 0 \le r < h$$

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 5.3 (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.

5.5 Bir Kuvvetin Mertebesini Hesaplama

Bir tabanın mertebesini biliyorsanız, o tabandan türetilmiş herhangi bir kuvvetin mertebesini de tek bir formülle bulabilirsiniz.

Teorem 5.2 (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:

$$t \left| \frac{h}{\gcd(h, k)} \right. \tag{$**$}$$

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 5.4 (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.

5.6 Primitif (İlkel) Kök Kavramı

Tanım 5.3 (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 5.3 (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 5.5 (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 5.4 (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 5.6 (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.

5.7 İndeks Kavramı (Ayrık Logaritma)

Klasik cebirde logaritma bir üssü bulmamızı sağlar; modüler aritmetikte de **indeks** aynı görevi üstlenir.

Tanım 5.4 (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 $\mathrm{ind}_a(b)$ ile gösterilir.

Örnek 5.7 (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:

$$\mathrm{ind}_3(4) = 4$$

5.8 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 5.5 (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.

5.9 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 5.8. $x^{20} \equiv 13 \pmod{17}$ 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 **$g = 3$, 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: $3^{20} = 3^{16} \cdot 3^4 \equiv 1 \cdot 13 = 13 \pmod{17}$ ✓
■

6. 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?

6.1 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 6.1 (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 6.1 (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

$$6x + 2 \equiv 3 \pmod{11} \Longrightarrow 6x \equiv 1 \pmod{11}$$

Modüler bölme için sağ tarafa 11 ekleyip sayıyı 6'nın katı yapalım ($1 + 11 = 12$):

$$6x \equiv 12 \pmod{11} \Longrightarrow x \equiv 2 \pmod{11}$$

Durum 2: $y \equiv 8$ için

$$6x + 2 \equiv 8 \pmod{11} \Longrightarrow 6x \equiv 6 \pmod{11} \Longrightarrow x \equiv 1 \pmod{11}$$

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 $3 + 2 + 6 = 11 \equiv 0 \pmod{11}$ ✓

■

6.2 Kuadratik Rezidü (Kalan) Kavramı

Bir sayının modüler aritmetikte karekökü alınabiliyorsa, o sayıya kuadratik rezidü denir.

Tanım 6.1 (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 6.2 (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 6.3 (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:

$$1^2 = 1 \equiv 1 \pmod{7}$$
$$2^2 = 4 \equiv 4 \pmod{7}$$
$$3^2 = 9 \equiv 2 \pmod{7}$$
$$4^2 = 16 \equiv 2 \pmod{7}$$
$$5^2 = 25 \equiv 4 \pmod{7}$$
$$6^2 = 36 \equiv 1 \pmod{7}$$

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.

7. 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**.

7.1 Legendre Sembolünün Tanımı

Tanım 7.1 (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 7.1 (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.

7.2 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 7.1 (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.

7.3 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.)

8. 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.

8.1 Gauss Lemması

Teorem 8.1 (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 $\{p-r_1,\ldots,p-r_n\}$ *ile* $\{s_1,\ldots,s_k\}$ *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:*

$$\{p-r_1,\ldots,p-r_n\}\cup\{s_1,\ldots,s_k\}=\left\{1,2,\ldots,\frac{p-1}{2}\right\}$$

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* $1a,2a,\ldots,\frac{p-1}{2}a$*'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.

8.2 Legendre Sembolü İçin Genel Formül ve 2′nin Karesel Karakteri

Teorem 8.2 (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.
$j\in\left\{1,\ldots,\frac{p-1}{2}\right\}$ *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:

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$$

■

8.3 Çözümlü Uygulamalar

İspatladığımız bu soyut teoremlerin, modüler aritmetikteki sayıların karesel karakterini bulmak için nasıl güçlü bir araca dönüştüğünü aşağıdaki örneklerle inceleyelim.

Örnek 8.1. $x^2 \equiv 22 \pmod{41}$ 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 8.2. 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 8.3. $x^2 \equiv 3 \pmod{17}$ 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 8.4. 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 8.5. 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 8.6. $m \geq 2$ 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.
■

9. 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.

9.1 Teorem ve Kafes (Lattice) İspatı

Teorem 9.1 (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:

$$K = \left\{(x,y) : 1 \leq x \leq \frac{p-1}{2}, \quad 1 \leq y \leq \frac{q-1}{2}, \quad x,y \in \mathbb{Z}\right\}$$

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 $x \leq \frac{p-1}{2} < p$ ve $y \leq \frac{q-1}{2} < q$'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:

$$K_1 = \bigcup_{x=1}^{(p-1)/2} \left\{(x,y) : 1 \leq y < \frac{qx}{p}, y \in \mathbb{Z}\right\}$$

Bu birleşime giren kümeler ikişer ikişer ayrıktır. Belirli bir x değeri için $1 \leq y < \frac{qx}{p}$ 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.

9.2 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 9.1. $x^2 \equiv -42 \pmod{61}$ 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 9.2. 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.
■

10. 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.

10.1 Jacobi Sembolünün Tanımı

Tanım 10.1 (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.

10.2 Jacobi Sembolünün Temel Özellikleri

Jacobi sembolü, Legendre sembolünün sahip olduğu çarpımsal özellikleri aynen korur.

Teorem 10.1 (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.*
■

10.3 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 10.2 (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.
■

10.4 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 10.3 (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.
■

10.5 Çözümlü Örnek

Örnek 10.1. $x^2 \equiv 105 \pmod{317}$ 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.
■

10.6 Çalışma Problemleri

Konuyu pekiştirmek için aşağıdaki problemleri; öğrendiğiniz Legendre/Jacobi sembolü kuralları, Euler kriteri ve kuadratik resiprosite teoremlerini kullanarak çözebilirsiniz.

Alıştırma 10.1 (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 10.2 (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.

11. 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.

11.1 Tanım ve Çözülebilirlik Şartı

Tanım 11.1 (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.

11.2 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 11.1 (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.
■

11.3 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 11.1. $30x + 66y = 41$ 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 11.2. $291x + 549y = 54$ 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 11.3. $312x + 51y = 9$ 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:

$$x = -24 + 17t, \qquad y = 147 - 104t \qquad (t \in \mathbb{Z})$$

■

11.4 Çalışma Problemleri

Alıştırma 11.1 (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)** $15x + 11y = 1$

