

Üretiler

$$\mathbb{Z}_{10} = \{0, \bar{1}, \bar{2}, \dots, \bar{9}\} \text{ içerisinde } o(\mathbb{Z}_{10}) = \phi(10) = 4$$

$$o(\mathbb{Z}_{10}) = \langle \bar{1} \rangle = \langle \bar{3} \rangle = \langle \bar{7} \rangle = \langle \bar{9} \rangle \text{ içerisinde } \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$$

olan $\phi(10) = 4$ tane üretili var mıdır?

İnceleyelim;

$$\langle \bar{3} \rangle = \{ \bar{3}, \bar{9}, \bar{7}, \bar{1} \}, \langle \bar{7} \rangle = \{ \bar{7}, \bar{9}, \bar{3}, \bar{1} \}, \langle \bar{9} \rangle = \{ \bar{9}, \bar{1} \}$$

$$\langle \bar{1} \rangle = \{ \bar{1} \}$$

burada $\langle \bar{3} \rangle$ ve $\langle \bar{7} \rangle$ $\mathbb{Z}_{10}$ 'ün üretileridir

Tanım (primitif kök) $\mathbb{Z}_m^*$ deirli cıprmsal bir grıpdır

Eğer bir $g \in \mathbb{Z}_m^*$; $\mathbb{Z}_m^* = \langle g \rangle$ ve g 'ye "mod m primitif kök veya m 'nin primitif kökü" denir.

Tanım (meretebe) p asal sayı olmak üzere $0 \neq g \in \mathbb{Z}_p^*$ olan

$o(\langle g \rangle)$ sayısına g 'nin $\mathbb{Z}_p^*$ 'deki meretebeı denir.

$$o(g) = o(\langle g \rangle) = \text{ord}_p g \text{ şeklinde yazılır}$$

~~örnek~~ $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

•) $g = \bar{4}$ olsun. $\rightarrow \langle \bar{4} \rangle = \{ \bar{4}, \bar{2}, \bar{1} \} \Rightarrow o(\bar{4}) = o(\langle \bar{4} \rangle) = \text{ord}_7 4 = 3$

•) $g = \bar{3}$ olsun. $\rightarrow \langle \bar{3} \rangle = \{ \bar{3}, \bar{2}, \bar{6}, \bar{4}, \bar{5}, \bar{1} \} = \mathbb{Z}_7^*$

$$\Rightarrow g = \bar{3}, \langle \bar{3} \rangle = \{ \bar{3}, \bar{2}, \bar{6}, \bar{4}, \bar{5}, \bar{1} \} = \mathbb{Z}_7^*$$

$$o(\bar{3}) = o(\langle \bar{3} \rangle) = \text{ord}_7 3 = 6 = o(\mathbb{Z}_7^*)$$

$$\downarrow$$

$$4^3 \equiv 1 \pmod{7}$$

Tanım (n -yüncü mertebeden rezidü) p asal, $0 < n \in \mathbb{Z}$, $a \in \mathbb{Z}$;

$x^n \equiv a \pmod{p} \rightarrow \textcircled{1}$ kongrüns denklemini verilsin. Eğer $\textcircled{1}$ denklemini çözümlü ise yani $\textcircled{1}$ 'i sağlayan $\bar{x} \in \mathbb{Z}_p$ var ise a 'ya " $\pmod{p}$, n -yüncü mertebeden rezidü"dür" denir.

NOT

- $n=1$ ve $\textcircled{1}$ çözümlü ise a , lineer rezidü
- $n=2$ ve $\textcircled{1}$ çözümlü ise a , kuadratik rezidü
- $n=3$ ve $\textcircled{1}$ çözümlü ise a , kubik rezidü
- $n=4$ ve $\textcircled{1}$ çözümlü ise a , bikuadratik rezidü
- $n > 4$ ve $\textcircled{1}$ çözümlü ise a , yüksek mert. rezidü denir

(*) Teorem p asal, $a \in \mathbb{Z}$, $p \nmid a$ olsun. Ayrıca g , $\pmod{p}$ primitif kök ve $a = g^b \pmod{p}$ olsun. Bu takdirde $\textcircled{1}$ 'in çözümlü olması için gerek ve yeter şart $((n, p-1) \mid b)$ dir.

Teorem (Euler kriteri) p asal, $a \in \mathbb{Z}$ ve $p \nmid a$ olsun. Bu takdirde $\textcircled{1}$ 'in çözümlü olması için gerek ve yeter şart $(n, p-1) = 1$ olmak üzere $a^{(p-1)/n} \equiv 1 \pmod{p}$ dir.

ALGİTİRMALAR

Soru-1 $x^7 \equiv 4 \pmod{5} \Rightarrow \bar{x} = ?$

Çözüm Teorem (*)'a göre,

$$\left. \begin{array}{l} n=7, a=4, p=5 \\ g_5 = ? \\ \mathbb{Z}_5^* = \{2, 1, 3, 4\} \\ \langle 2 \rangle = \{2, 4, 3, 1\} \end{array} \right\} \left. \begin{array}{l} \bar{2}, \mathbb{Z}_5^* \text{ de en } \\ \text{küçük } \text{primitif kök olduğundan} \\ g_5 = \bar{2} \text{ buluna} \\ a = 4 = \bar{2}^2 \rightarrow b \\ [(n, p-1) \mid b] \text{ mi} \end{array} \right\} \begin{array}{l} (7, 4) = 1 \text{ ve} \\ 1 \mid 2 \text{ olduğundan} \\ \text{çözümlüdür.} \end{array}$$

Örnek 2 (Euler kriterine göre)

$$(n, p-1) = s \quad \text{iz} \quad (7, 4) = 1 = s \Rightarrow 4 \stackrel{?}{\equiv} 1 \pmod{5}$$

$$\left. \begin{array}{l} 4^2 \equiv 1 \pmod{5} \\ 4^2 \equiv 1 \pmod{5} \end{array} \right\} \Rightarrow 4^4 \equiv 1 \pmod{5} \quad \text{Çözümüldür.}$$

$$\Rightarrow g_5 = \bar{2} \Rightarrow 4 \equiv \bar{2}^2 \pmod{5}$$

Ayrıca $x = 2^u$ diyelim. $x^7 = 2^{\overset{7u}{\circlearrowleft} \rightarrow s} \equiv 2^{\overset{2}{\circlearrowleft} \rightarrow r} \pmod{5}$ terimden

$$\Rightarrow 4 \mid (s-r) \Rightarrow 7u-2 \Rightarrow 7u-2 \equiv 0 \pmod{4}$$

$$\Rightarrow 7u \equiv 2 \pmod{4} \Rightarrow 3u \equiv 2 \pmod{4} \Rightarrow u \equiv 2 \pmod{4}$$

$$\Rightarrow \boxed{u=2} \quad u \text{ yerine yazılırsa} \quad x = 2^4 = 2^2 = 4$$

$$\Rightarrow \bar{x} \equiv 4 \pmod{5} \text{ bulunur}$$

Soru-2 $x^6 \equiv 9 \pmod{17} \Rightarrow \bar{x} = ?$

$\Rightarrow$ Çözünürlük Testi

Euler'e göre

$$(6, 16) = \overset{2}{\circlearrowleft} \rightarrow s \quad \text{ve} \quad g^{\frac{16}{2}} \stackrel{?}{\equiv} 1 \pmod{17} \quad \text{doğru ise sistem çözümlüdür.} \quad (r)$$

$$\Rightarrow g_{17} = \bar{3} \quad \text{ve} \quad g = 3^2 \rightarrow x = 3^4 \Rightarrow x^6 = 3^{6u} \Rightarrow$$

$$3^{6u} \equiv 3^2 \pmod{17} \Leftrightarrow \text{Terimden,}$$

$$6u \equiv 2 \pmod{16} \Leftrightarrow 3u \equiv 1 \pmod{8} \Leftrightarrow u \equiv 3 \pmod{8}$$

$$u=3 \rightarrow x = 3^4 = 3^3 = 27 \rightarrow \bar{x} \equiv 10 \pmod{17} \text{ bulunur}$$

Teorem (indis - indisler)

p asal, $g \bmod p$ bir primitif kök, $a \in \mathbb{Z}$ ve $p \nmid a$ olsun.

Ayrıca $a \equiv g^i \pmod{p}$ olsun. Buradan $i \in \mathbb{N}$ değere

a 'nın g primitif köküne göre $\bmod p$ indis, denir ve

$$\text{ind}_{g,p} a = i \text{ ile gösterilir.}$$

Örnekler

1) $g_{13} = 2$ idi. Mesela $a = 9$ ise

$$\bar{2}^0 = 1, \bar{2}^1 = 2, \bar{2}^2 = 4, \bar{2}^3 = 8, \bar{2}^4 = 3, \bar{2}^5 = 6, \bar{2}^6 = 12, \bar{2}^7 = 11$$

$$\bar{2}^8 = 9, \bar{2}^9 = 5, \bar{2}^{10} = 10, \bar{2}^{11} = 7, \bar{2}^{12} = 1, \bar{2}^{13} = 2$$

$$\text{Buradan } 9 = 2^8 \pmod{13} \text{ old. için } i = 8$$

$$\text{yani } \text{ind}_{g_{13}} 9 = 8.$$

$$a = 37 \Rightarrow 37 \equiv 11 \pmod{13} \rightarrow 37 \equiv 11 \equiv 2^7 \pmod{13}$$

$$\Rightarrow \text{ind}_{g_{13}} 37 = 37 = \text{ind}_{g_{13}} 11 = 7$$

$g_{13} = 2$ 'ye göre indis tablası

a	1	2	3	4	5	6	7	8	9	10	11	12
$\text{ind}_{g_{13}} a$	0	1	4	2	9	5	11	3	8	10	7	6

Teorem p asal, $a, b \in \mathbb{Z}$, $p \nmid a$ ve $p \nmid b$ olsun.

$$i) a \equiv b \pmod{p} \Rightarrow \text{ind}_{g,p} a \equiv \text{ind}_{g,p} b \pmod{p-1}$$

$$ii) \text{ind}_{g,p} ab \equiv (\text{ind}_{g,p} a + \text{ind}_{g,p} b) \pmod{p-1}$$

$$\text{sonuç } \text{ind}_{g,p} a^n \equiv n \cdot \text{ind}_{g,p} a \pmod{p-1}$$

Soru (method)

$$ax \equiv b \pmod{p} \Rightarrow \bar{x} = ?$$

$$\rightarrow \text{ind}_g ax = \text{ind}_g b \pmod{p-1}$$

$$\rightarrow \text{ind}_g a + \text{ind}_g x \equiv \text{ind}_g b \pmod{p-1}$$

$$\rightarrow \text{ind}_g x \equiv (\text{ind}_g b - \text{ind}_g a) \pmod{p-1} \text{ olur}$$

Burada $\text{ind}_g x$ ve buradan da x bulunur

Soru $10x \equiv 7 \pmod{13} \Rightarrow \bar{x} = ?$

$$\rightarrow g_{13} = 2 \text{ 'ye göre çözelim}$$

$$\text{ind}_2 10x \equiv \text{ind}_2 7 \pmod{12} \rightarrow \text{ind}_2 10 + \text{ind}_2 x \equiv \text{ind}_2 7 \pmod{12}$$

$$10 + \text{ind}_2 x \equiv 11 \pmod{12} \rightarrow \text{ind}_2 x \equiv 1 \pmod{12} \text{ (indisi 1 olan 2'dir.)}$$

$$\boxed{x=2}$$

Soru (method)

$$x^n \equiv a \pmod{p} \rightarrow \bar{x} = ?$$

$$\rightarrow \left. \begin{array}{l} \text{ind}_g x^n \equiv \text{ind}_g a \pmod{p-1} \\ n \cdot \text{ind}_g x \equiv \text{ind}_g a \pmod{p-1} \end{array} \right\} \text{ind}_g x \text{ ve buradan } x \text{ bulunur}$$

Soru $x^5 \equiv 11 \pmod{17} \Rightarrow \bar{x} = ?$

$$\rightarrow g_{17} = 3 \text{ alalım.}$$

$$\text{ind}_3 x^5 \equiv \text{ind}_3 11 \pmod{16}$$

$$\Rightarrow 5 \cdot \text{ind}_3 x \equiv \text{ind}_3 11 \pmod{16}$$

$$\rightarrow 5 \cdot \text{ind}_3 x \equiv 7 \pmod{16}$$

$$\rightarrow 13 \cdot 5 \text{ ind}_3 x \equiv 13 \cdot 7 \pmod{16}$$

$$\text{ind}_3 x \equiv 11 \pmod{16}$$

$$\boxed{x=7}$$

$$\text{SOL} \quad a^x \equiv b \pmod{p} \rightarrow \bar{x} = ?$$

$$\rightarrow \text{ind}_g a^x \equiv \text{ind}_g b \pmod{p-1}$$

$$x \cdot \text{ind}_g a \equiv \text{ind}_g b \pmod{p-1} \rightarrow x \text{ bulunur}$$

$$\text{SOL} \rightarrow 18^x \equiv 2 \pmod{13} \Rightarrow \bar{x} = ?$$

$$\Rightarrow 5^x \equiv 2 \pmod{13} \rightarrow \bar{x} = ?$$

$$x \cdot \text{ind}_2 5 \equiv \text{ind}_2 2 \pmod{12}$$

$$\begin{cases} 9x \equiv 1 \pmod{12} \end{cases}$$

$$\begin{cases} (9, 12) = 3 \nmid 1 \Rightarrow \text{no solution} \end{cases}$$

$$\text{SOL} \quad 11^x \equiv 5 \pmod{17} \Rightarrow \bar{x} = ?$$

$$\rightarrow g_{17} = 3 \text{ i\u00e7in } \text{ind}_3 11^x \equiv 5 \pmod{17}$$

$$x \cdot \text{ind}_3 11 \equiv 5 \pmod{16} \rightarrow 7x \equiv 5 \pmod{16} \rightarrow x \equiv 3 \pmod{16}$$

$$\boxed{\bar{x} = 3}$$

KUADRATİK REZİDÜLER

Tanım $1 < m \in \mathbb{Z}$, $n \in \mathbb{N}^+$, $a \in \mathbb{Z}$ olmak üzere $x^n \equiv a \pmod{m}$ ①

Eğer ① çözümlü ise " $a, \pmod{m}$ n -yinci mertebeden rezidüdür.

Aksi halde ① çözümsüz ise $a, \pmod{m}$ n -yinci mertebeden rezidü değil (veya non-rezidü) denir.

Kuadratik rezidü konusu $x^2 \equiv a \pmod{m}$ nin çözümlülüğünü araştırmaktan ibarettir.

Önce $m=p$ asal durumlarını inceleyelim.

Teorem $x^2 \equiv a \pmod{p}$ (p asal ve $p \nmid a$)

① çözümlü $\Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ 'dir.

Teorem $\mathbb{Z}_p^*$ 'in sınıfının tam yarısı, $\pmod{p}$ kuadratik rezidü, diğer yarısı non-rezidüdür.

örnek $p=11 \rightarrow \mathbb{Z}_{11}^* = \{1, 2, 3, \dots, 10\}$ de

$$K = \{1^2, 2^2, 3^2, \dots, 5^2\} = \{1, 4, 9, \bar{5}, 3\} \rightarrow K' = \{2, 6, \bar{7}, 8, 10\}$$

****** Tanım p asal olmak üzere ($p \neq 2$)

$$(-): \mathbb{Z} \rightarrow \{-1, 1, 0\} \quad \forall a \in \mathbb{Z}; (-)(a) = \begin{cases} +1; & x^2 \equiv a \pmod{p} \text{ çözümlü} \\ & (a, \pmod{p} \text{ kuadratik rezidü}) \\ -1; & x^2 \equiv a \pmod{p} \text{ çözümsüz} \\ & (a, \pmod{p} \text{ non-kuadratik rezidü}) \\ 0; & p \mid a \text{ ise} \end{cases}$$

Şeklinde tanımlı aritmetik fonksiyonu Legendre fonksiyonu denir

NOT $(-)(a), \left(\frac{a}{p}\right) \begin{cases} +1; \text{ (1) çözümü ise} \\ -1; \text{ (1) çözümü değilse} \\ 0; p|a \text{ ise} \end{cases}$

$\left(\frac{a}{p}\right)$ 'ye Legendre sembolü (göstergisi) veya değeri denir.

Sonuç $\forall a \in \mathbb{Z}$ ve $\forall p$ asal için,

$\left(\frac{a}{p}\right) = 1; \left(\frac{a}{p}\right) = -1$ ve $\left(\frac{a}{p}\right) = 0$ den yalnız biri doğrudur.

Örnekler

① $\left(\frac{3}{5}\right) = ? \longrightarrow (x^2 \equiv 3 \pmod{5} \iff \text{çözümü mü?})$
 $x^2 \equiv 3 \pmod{5} \longrightarrow \text{çözümü yoktur} \longrightarrow \left(\frac{3}{5}\right) = -1$ yazılır.

② $\left(\frac{6}{7}\right) = ? \longrightarrow x^2 \equiv 6 \pmod{7} \longrightarrow \text{çözümü yoktur} \longrightarrow \left(\frac{6}{7}\right) = -1.$

③ $\left(\frac{4}{7}\right) = ? \longrightarrow x^2 \equiv 4 \pmod{7} \longrightarrow \text{çözümü var} \longrightarrow \left(\frac{4}{7}\right) = 1.$

Teorem $p \neq 2$ asal ; $a, b \in \mathbb{Z}$ olmak üzere $p \nmid a, b$ ise

i) $a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

ii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$

iii) $\left(\frac{a^2}{p}\right) = 1$

Sonuç $\left(\frac{1}{p}\right) = +1$ dir.

$$iv) \left(\frac{a \mp b}{p} \right) = \left(\frac{a}{p} \right) \mp \left(\frac{b}{p} \right)$$

$$\boxed{\text{Sonuç}} \quad \left(\frac{a \mp np}{p} \right) = \left(\frac{a}{p} \right) \Rightarrow$$

$$v) p|c \rightarrow \left(\frac{ac^2}{p} \right) = \left(\frac{a}{p} \right)$$

$$vi) \left(\frac{a}{p} \right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

$$vii) \left(\frac{-1}{p} \right) = (-1)^{\frac{p-1}{2}} \pmod{p}$$

$$viii) \left(\frac{2}{p} \right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1; & p \equiv \mp 1 \pmod{8} \quad \text{ise} \\ -1; & p \equiv \mp 3 \pmod{8} \quad \text{ise} \end{cases}$$

$$\boxed{\text{Örnek}} \quad 1) \left(\frac{6}{5} \right) = ? \rightarrow \left(\frac{6}{5} \right) = \left(\frac{2 \cdot 3}{5} \right) = \underbrace{\left(\frac{2}{5} \right)}_{-1} \cdot \underbrace{\left(\frac{3}{5} \right)}_{-1} = +1$$

$$2) \left(\frac{12}{13} \right) = ? \rightarrow \left(\frac{2^2 \cdot 3}{13} \right) = \underbrace{\left(\frac{2^2}{13} \right)}_{+1} \cdot \left(\frac{3}{13} \right) = \left(\frac{3}{13} \right)$$

$$x^2 \equiv 3 \pmod{13} \text{ çözümlü mü?} \rightarrow \left(\frac{3}{13} \right) = 1 \text{ olur.}$$

$$\left(\frac{12}{13} \right) = \underbrace{\left(\frac{3}{13} \right)}_1 \cdot \underbrace{\left(\frac{2^2}{13} \right)}_1 = 1$$

$$3) \left(\frac{45}{7} \right) = ? \rightarrow \left(\frac{45}{7} \right) = \underbrace{\left(\frac{3^2}{7} \right)}_1 \cdot \underbrace{\left(\frac{5}{7} \right)}_{-1} = -1$$

$$x^2 \equiv 5 \pmod{7} \text{ çözümlü mü?}$$

$$4) \forall p; \left(\frac{1}{p}\right) = 1$$

$$5) \forall p; \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \Rightarrow \begin{cases} +1; p \equiv 1 \pmod{4} \\ -1; p \equiv 3 \pmod{4} \end{cases} \text{ i.e.}$$

$$6) \forall p; \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \Rightarrow \begin{cases} +1; p \equiv \pm 1 \pmod{8} \\ -1; p \equiv \pm 3 \pmod{8} \end{cases}$$

$$7) \forall p; \left(\frac{5}{p}\right) = \begin{cases} 1; p \equiv 1, 9 \pmod{10} \\ -1; p \equiv 3, 7 \pmod{10} \end{cases}$$

Teorem (Kuadratik Residua Yasası)

p ve q farklı tek asal sayılar olmak üzere,

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right) \cdot \left(\frac{q-1}{2}\right)} \text{ dir}$$

$$1) \left(\frac{10}{19}\right) = \left(\frac{2 \cdot 5}{19}\right) = \left(\frac{2}{19}\right) \cdot \left(\frac{5}{19}\right) \quad (1)$$

$$\left(\frac{5}{19}\right) \cdot \left(\frac{19}{5}\right) = (-1)^{\frac{5-1}{2} \cdot \frac{19-1}{2}} = (-1)^{2 \cdot 9} = 1$$

$$\left(\frac{5}{19}\right) \cdot \left(\frac{4}{19}\right) = 1 \rightarrow \left(\frac{5}{19}\right) \cdot \underbrace{\left(\frac{2^2}{19}\right)}_{+1} = +1 \rightarrow \left(\frac{5}{19}\right) \cdot (+1) = 1 \Rightarrow \left(\frac{5}{19}\right) = +1 \quad (2)$$

$$(1) \text{ ve } (2) \text{ den } \left(\frac{10}{19}\right) = (-1) \cdot \left(\frac{5}{19}\right) = (-1) \cdot (+1) = (-1)$$

SONUÇ $\rightarrow x^2 \equiv 10 \pmod{19}$ çözümsüzdür

$$2) \left(\frac{19}{43}\right) = ? \rightarrow \left(\frac{19}{43}\right) \cdot \left(\frac{43}{19}\right) = (-1)^{9 \cdot 21} = -1 \dots (1)$$

$$\left(\frac{43}{19}\right) = \left(\frac{5}{19}\right) = 1 \quad \left(\frac{19}{43}\right) \cdot (+1) = -1 \rightarrow \left(\frac{19}{43}\right) = -1 \text{ çözümsüz}$$

$$3) \left(\frac{110}{59} \right) = \left(\frac{0}{0} \right) \rightarrow 110 = 2 \cdot 5 \cdot 11$$

$$\text{Işık} \quad \left(\frac{110}{59} \right) = \left(\frac{2 \cdot 5 \cdot 11}{59} \right) = \left(\frac{2}{59} \right) \left(\frac{5}{59} \right) \left(\frac{11}{59} \right) = - \left(\frac{5}{59} \right) \cdot \left(\frac{11}{59} \right) \rightarrow \textcircled{1}$$

$$\left(\frac{5}{59} \right) \cdot \left(\frac{59}{5} \right) = (-1)^{2 \cdot 29} = +1$$

$$\left(\frac{5}{59} \right) \cdot \left(\frac{4}{5} \right) = +1 \rightarrow \left(\frac{5}{59} \right) = +1 \dots \textcircled{2}$$

$$\left. \begin{aligned} \left(\frac{11}{59} \right) \cdot \left(\frac{59}{11} \right) &= (-1)^{5 \cdot 29} = -1 \\ \left(\frac{59}{11} \right) &= \left(\frac{4}{11} \right) = +1 \end{aligned} \right\} \Rightarrow \left(\frac{11}{59} \right) = -1 \dots \textcircled{3}$$

② ve ③'ü ①'de yerine yazarsak

$$\left(\frac{110}{59} \right) = - \left(\frac{5}{59} \right) \cdot \left(\frac{11}{59} \right) = (-1) \cdot (+1) \cdot (-1) = +1$$

$$\Rightarrow x^2 \equiv 51 \pmod{59} \text{ çözümlü}$$

$$\text{Işık} \quad \left(\frac{110}{59} \right) = \left(\frac{51}{59} \right) = \left(\frac{3}{59} \right) \cdot \left(\frac{17}{59} \right) \dots \textcircled{1}$$

$$\left(\frac{3}{59} \right) \cdot \left(\frac{59}{3} \right) = (-1)^{1 \cdot 29} = -1 \left. \right\} \left(\frac{3}{59} \right) = +1 \dots \textcircled{2}$$

$$\left(\frac{59}{3} \right) = \left(\frac{2}{3} \right) = -1$$

$$\left(\frac{17}{59} \right) \cdot \left(\frac{59}{17} \right) = (-1)^{8 \cdot 29} = +1 \left. \right\} \left(\frac{17}{59} \right) = +1 \dots \textcircled{3}$$

$$\left(\frac{59}{17} \right) = \left(\frac{8}{17} \right) = \underbrace{\left(\frac{2}{17} \right)}_1 \cdot \underbrace{\left(\frac{2^2}{17} \right)}_1$$

② ve ③'den

$$\left(\frac{110}{59} \right) = (+1) \cdot (+1) = +1$$

$$\boxed{\text{Soru}} \left(\frac{23}{117} \right) = ?$$

$$\rightarrow 117 = 3^2 \cdot 13$$

$$\left(\frac{23}{117} \right) = \left(\frac{23}{3^2 \cdot 13} \right) = \left(\frac{23}{3^2} \right) \cdot \left(\frac{23}{13} \right) = \underbrace{\left(\frac{23}{3} \right)^2}_{+1} \cdot \left(\frac{23}{13} \right) = \left(\frac{23}{13} \right) = \left(\frac{10}{13} \right)$$

$$= \underbrace{\left(\frac{2}{13} \right)}_{-1} \cdot \left(\frac{5}{13} \right) = - \left(\frac{5}{13} \right) \dots \textcircled{1}$$

$$\left\{ \begin{aligned} \left(\frac{13}{5} \right) &= \left(\frac{3}{5} \right) \\ \left(\frac{3}{5} \right) \cdot \left(\frac{5}{3} \right) &= (-1)^{2 \cdot 1} = +1 \end{aligned} \right.$$

$$\left(\frac{5}{13} \right) \cdot \left(\frac{13}{5} \right) = (-1)^{2 \cdot 6} = +1 \dots \textcircled{2}$$

$$\left(\frac{3}{5} \right) \cdot \left(\frac{5}{3} \right) = +1$$

$$\left(\frac{3}{5} \right) = -1$$

$$\left(\frac{13}{5} \right) = -1 \dots \textcircled{3}$$

$$\left(\frac{5}{13} \right) = -1 \dots \textcircled{4}$$

$$\textcircled{4} \text{ ve } \textcircled{1} \text{ de } \text{keyesok!}$$

$$\left(\frac{23}{117} \right) = - \left(\frac{5}{13} \right) = +1$$

$$x^2 \equiv 23 \pmod{117} \quad \text{çözümler.}$$

$$\boxed{\text{Soru}} \left(\frac{38}{135} \right) = ?$$

$$\rightarrow \left(\frac{38}{135} \right) = \left(\frac{2 \cdot 19}{3^3 \cdot 5} \right) = \left(\frac{2}{3^3 \cdot 5} \right) \cdot \left(\frac{19}{3^3 \cdot 5} \right)$$

$$= \left\{ \left(\frac{2}{3} \right)^3 \cdot \left(\frac{2}{5} \right) \right\} \left\{ \left(\frac{19}{3} \right)^3 \cdot \left(\frac{19}{5} \right) \right\} \dots \textcircled{1}$$

$$\left(\frac{2}{3} \right) = -1 \rightarrow \left(\frac{2}{3} \right)^3 = -1 \dots \textcircled{2} \quad \left(\frac{2}{5} \right) = -1 \dots \textcircled{3}$$

$$\left(\frac{19}{3} \right) = \left(\frac{1}{3} \right) = +1 \rightarrow \left(\frac{19}{3} \right)^3 = 1 \dots \textcircled{4} \quad \left(\frac{19}{5} \right) = \left(\frac{4}{5} \right) = +1 \dots \textcircled{5}$$

⑤, ④, ③, ②'yi ①'de koyalım.

$$\left(\frac{38}{135}\right) = (-1) \cdot (-1) \cdot (+1) \cdot (+1) = +1.$$

Soru $\left(\frac{247}{315}\right) = ?$

$$\begin{aligned} \rightarrow \left(\frac{247}{315}\right) &= \left(\frac{13 \cdot 19}{3^2 \cdot 5 \cdot 7}\right) = \left(\frac{13}{3^2 \cdot 5 \cdot 7}\right) \cdot \left(\frac{19}{3^2 \cdot 5 \cdot 7}\right) \\ &= \left\{ \left(\frac{13}{3}\right)^2 \cdot \left(\frac{13}{5}\right) \cdot \left(\frac{13}{7}\right) \right\} \left\{ \left(\frac{19}{3}\right)^2 \cdot \left(\frac{19}{5}\right) \cdot \left(\frac{19}{7}\right) \right\} \dots \textcircled{1} \end{aligned}$$

$$\left(\frac{13}{3}\right) = \left(\frac{1}{3}\right) = +1 \rightarrow \left(\frac{13}{3}\right)^2 = +1 \quad \left(\frac{19}{3}\right) = \left(\frac{1}{3}\right) = +1 \rightarrow \left(\frac{19}{3}\right)^2 = +1$$

$$\left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) = -1 \dots \textcircled{2} \quad \left(\frac{19}{5}\right) = \left(\frac{4}{5}\right) = +1 \dots \textcircled{4}$$

$$\left(\frac{13}{7}\right) = \left(\frac{6}{7}\right) = \left(\frac{2}{7}\right) \left(\frac{3}{7}\right) \quad \left(\frac{13}{7}\right) = -1 \dots \textcircled{3}$$

$$\left(\frac{3}{7}\right) \cdot \left(\frac{7}{3}\right) = (-1)^{1 \cdot 3} = -1$$

$$\left(\frac{3}{7}\right) \cdot \left(\frac{4}{3}\right) = +1$$

$$\left\{ \begin{array}{l} \left(\frac{3}{7}\right) \cdot \left(\frac{7}{3}\right) = (-1)^{1 \cdot 3} = -1 \\ \left(\frac{3}{7}\right) \cdot \left(\frac{4}{3}\right) = +1 \end{array} \right\} \rightarrow \left(\frac{3}{7}\right) = -1$$

$$\left(\frac{19}{7}\right) = \left(\frac{5}{7}\right) \rightarrow \left(\frac{5}{7}\right) \cdot \left(\frac{7}{5}\right) = (-1)^{2 \cdot 3} = +1 \quad \left(\frac{5}{7}\right) = -1$$

$$\left(\frac{5}{7}\right) \cdot \left(\frac{2}{5}\right) = +1 \quad \rightarrow \left(\frac{19}{7}\right) = +1 \dots \textcircled{5}$$

⑤, ④, ③, ②'yi ①'de koyalım

$$\left(\frac{247}{315}\right) = \left\{ (+1) (-1) (-1) \right\} \left\{ (+1) (+1) (-1) \right\} = -1 \quad \left. \begin{array}{l} x^2 \equiv 247 \pmod{315} \\ \text{(Gauss)} \end{array} \right\}$$

Soru p , $p=8m+1$ veya $p=8m+3$ şeklinde bir asal

sayı ise bu takdirde $x^2+2 \equiv 0 \pmod{p}$ kongransasının
çözümü olduğunu gösterelim.

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

yazılıdır.

$$p=8m+1 \rightarrow \frac{p-1}{2} = 4m \rightarrow (-1)^{\frac{p-1}{2}} = (-1)^{4m} = 1 \quad \text{ve}$$

$$\frac{p^2-1}{8} = \frac{(p-1) \cdot (p+1)}{8} = \frac{8m \cdot (8m+2)}{8} = 2m \cdot (4m+1)$$

$$\rightarrow (-1)^{\frac{p^2-1}{8}} = (-1)^{2m \cdot (4m+1)} = 1 \quad \text{elde ederiz.}$$

$$\text{Şu halde} \quad \left(\frac{-2}{p} \right) = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p^2-1}{8}} = 1 \cdot 1 = 1 \quad \text{olduğundan}$$

$x^2+2 \equiv 0 \pmod{p}$ kongransı çözümlüdür. Diğer taraftan eğer,

$$p=8m+3 \text{ ise} \quad \frac{p-1}{2} = 4m+1 \rightarrow (-1)^{\frac{p-1}{2}} = (-1)^{4m+1} = -1 \quad \text{ve}$$

$$\frac{p^2-1}{8} = \frac{(p-1)(p+1)}{8} = \frac{(8m+2)(8m+4)}{8} = (4m+1) \cdot (2m+1)$$

$$\rightarrow (-1)^{\frac{p^2-1}{8}} = (-1)^{\overbrace{(4m+1) \cdot (2m+1)}^{\text{tek}}} = -1 \quad \text{elde ederiz buradan}$$

$$\left(\frac{-2}{p} \right) = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p^2-1}{8}} = (-1) \cdot (-1) = +1. \quad \text{çözümlüdür}$$

Soru $p=8m \pm 1$ için $\left(\frac{2}{p} \right) = +1$, $p=8m \pm 3$ için $\left(\frac{2}{p} \right) = -1$

olduğunu gösteriniz.

$\rightarrow$

$$\rightarrow \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \text{ olduğundan eğer } p=8m \pm 1 \text{ ise ;}$$

$$\frac{p^2-1}{8} = \frac{(8m \pm 1)^2 - 1}{8} = 8m^2 \pm 2m \text{ olduğundan}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{8m^2 \pm 2m} = 1 \text{ dir. Eğer } p=8m \pm 3 \text{ ise ;}$$

$$\frac{p^2-1}{8} = \frac{(8m \pm 3)^2 - 1}{8} = 8m^2 \pm 6m + 1 \text{ olduğundan}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{8m^2 \pm 6m + 1} = -1 \text{ dir.}$$

$$\boxed{\text{Soru}} \left(\frac{-22}{73}\right) = ?$$

$$\begin{aligned} \rightarrow \left(\frac{-22}{73}\right) &= \left(\frac{-1}{73}\right) \cdot \left(\frac{2}{73}\right) \cdot \left(\frac{11}{73}\right) = (-1)^{\frac{73-1}{2}} \cdot (-1)^{\frac{73^2-1}{8}} \cdot (-1)^{\frac{11-1}{2} \cdot \frac{73-1}{2}} \cdot \left(\frac{73}{11}\right) \\ &= (-1)^{36} \cdot (-1)^{\frac{72 \cdot 74}{8}} \cdot (-1)^{5 \cdot 36} \cdot \left(\frac{73}{11}\right) = \left(\frac{7}{11}\right) = \left(\frac{-4}{11}\right) = \left(\frac{-1}{11}\right) \cdot \left(\frac{4}{11}\right) \\ &= (-1)^{\frac{11-1}{2}} = (-1)^5 = -1 \text{ elde edilir.} \end{aligned}$$

$$\boxed{\text{Soru}} \left(\frac{365}{1847}\right) = ?$$

$$\begin{aligned} \rightarrow \left(\frac{365}{1847}\right) &= \left(\frac{5}{1847}\right) \cdot \left(\frac{73}{1847}\right) = \underbrace{(-1)^{\frac{4}{2} \cdot \frac{1846}{2}}}_{+1} \cdot \left(\frac{1847}{5}\right) \underbrace{(-1)^{\frac{73}{2} \cdot \frac{1846}{2}}}_{+1} \cdot \left(\frac{1847}{73}\right) \\ &= \left(\frac{2}{5}\right) \left(\frac{22}{73}\right) = (-1)^{\frac{(5-1) \cdot (5+1)}{8}} \cdot \left(\frac{2}{73}\right) \cdot \left(\frac{11}{73}\right) \\ &= (-1)^{\frac{72 \cdot 74}{8}} \cdot (-1)^{\frac{10}{2} \cdot \frac{72}{2}} \cdot \left(\frac{73}{11}\right) = -\left(\frac{-4}{11}\right) \\ &= -\left(\frac{-1}{11}\right) \left(\frac{4}{11}\right) = -(-1)^{\frac{11-1}{2}} = -(-1)^5 = 1, \text{ çözümlüdür.} \end{aligned}$$

Soru $\left(\frac{3}{p}\right) = 1$ koşulunu sağlayan p tek asal sayılarını bulunuz

→ $x^2 \equiv 3 \pmod{p}$ kongrüansının hangi p asal sayıları için çözümü olduğunu araştırmalıyız. Kuadratik Resiprosite Teoreminden,

$$\left(\frac{3}{p}\right) = (-1)^{\frac{3-1}{2} \cdot \frac{p-1}{2}} \left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{p}{3}\right) \text{ olduğunu biliyoruz.}$$

$\left(\frac{3}{p}\right) = 1$ olması için

$$a) \left(\frac{p}{3}\right) = 1 \text{ ve } (-1)^{\frac{p-1}{2}} = 1 \text{ veya } b) \left(\frac{p}{3}\right) = -1 \text{ ve } (-1)^{\frac{p-1}{2}} = -1$$

gerçeklenmelidir. Bu iki durumu inceleyelim.

a) $\left(\frac{p}{3}\right) = 1$ ise p , 3'ün bir kR sene kongrüent olmalıdır.

$x^2 \equiv 1 \pmod{3}$ kongrüansı için $1^2 \equiv 1 \pmod{3}$, $2^2 \equiv 1 \pmod{3}$ olduğundan 1, 3'ün tek kR südür. Buradan

$$\left(\frac{p}{3}\right) = 1 \Rightarrow p \equiv 1 \pmod{3} \text{ yazabiliriz.}$$

$$(-1)^{\frac{p-1}{2}} = 1 \Rightarrow \frac{p-1}{2} = 2k, k \in \mathbb{Z} \Rightarrow p-1 = 4k \Rightarrow p = 4k+1$$

$$\Rightarrow p \equiv 1 \pmod{4} \text{ bulunur. Buradan}$$

$p \equiv 1 \pmod{4}$ ve $p \equiv 1 \pmod{3}$ aynı anda gerçekleşmelidir.

Bu iki kongrüans sisteminin çözümü $p \equiv 1 \pmod{12}$ bulunur.

b) $\left(\frac{p}{3}\right) = -1$ ise p , 3'ün bir kNR sene kongrüent olmalıdır.

3'ün tek kNR s 2 olduğundan $p \equiv 2 \pmod{3}$ olmalıdır.

$$(-1)^{\frac{p-1}{2}} = -1 \Rightarrow \frac{p-1}{2} = 2k+1, k \in \mathbb{Z} \Rightarrow p-1 = 4k+2 \Rightarrow p = 4k+3 \Rightarrow p \equiv 3 \pmod{4}$$

bulunur. Şu halde $p \equiv 3 \pmod{4}$ ve $p \equiv 2 \pmod{3}$ çözümlere

$$p \equiv 11 \pmod{12} \text{ bulunur}$$

Soru p tek asal sayı olsun.

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{eğer } p \equiv 1 \text{ veya } 7 \pmod{8} \\ -1, & \text{eğer } p \equiv 3 \text{ veya } 5 \pmod{8} \end{cases}$$

veya $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ veya 2'nin p modunda kaç kalas olması için $p \equiv \pm 1 \pmod{8}$ gerek ve yeter şarttır.

→ $p \equiv 1$ veya $p \equiv 5 \pmod{8}$ olsun.

$$\begin{aligned} 2 \cdot 4 \cdot 6 \cdots (p-1) &= 2 \cdot 1 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdots 2 \cdot \frac{p-1}{2} \\ &= 2^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \cdots (1) \end{aligned}$$

Diğer taraftan

$$2 \cdot 4 \cdot 6 \cdots (p-1) = 2 \cdot 4 \cdot 6 \cdots \left(\frac{p-1}{2}\right) \cdot \left(\frac{p-3}{2}\right) \cdots (-5) \cdot (-3) \cdot (-1) \pmod{p}$$

Yani

$$2 \cdot 4 \cdot 6 \cdots (p-1) \equiv (-1)^{\frac{p-1}{4}} \left(\frac{p-1}{2}\right)! \cdots (2)$$

$$\Rightarrow 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{4}} \pmod{p}$$

$$\Rightarrow \left(\frac{2}{p}\right) \equiv (-1)^{\frac{p-1}{4}} \Rightarrow p \equiv 1 \pmod{8} \text{ ise } \left(\frac{2}{p}\right) = 1$$

$p \equiv 5 \pmod{8}$ ise $\left(\frac{2}{p}\right) = -1$ bulun Benzer olarak

$p \equiv 3$ veya $p \equiv 7 \pmod{8}$ olsun

$$2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv 2 \cdot 4 \cdot 6 \cdots \frac{p-3}{2} \cdots \left(-\frac{p-1}{2}\right) \cdots (-5) \cdot (-3) \cdot (-1)$$

$$\equiv (-1)^{\frac{p+1}{4}} \left(\frac{p-1}{2}\right)! \pmod{8}$$

$$\Rightarrow 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p+1}{4}} \pmod{p}$$

$$\Rightarrow \left(\frac{2}{p}\right) = -1 \rightarrow p \equiv 3 \pmod{8}$$

$$\rightarrow \left(\frac{2}{p}\right) = -1 \rightarrow p \equiv 3 \pmod{8}$$

Soru $p > 3$ tek asal sayı olsun. -3 , hangi p 'ler için
kare kalıdır?

$$\rightarrow \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{3}{p}\right) = 1 \Rightarrow \left(\frac{3}{p}\right) \cdot \left(\frac{p}{3}\right) = (-1)^{\left(\frac{p-1}{2}\right) \cdot \left(\frac{3-1}{2}\right)}$$

$$\rightarrow \left(\frac{3}{p}\right) \cdot \left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}} = \left(\frac{-1}{p}\right)$$

$$\rightarrow \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) \left(\frac{-1}{p}\right)^2 = \left(\frac{p}{3}\right)$$

$$\rightarrow \left(\frac{p}{3}\right) = 1 \Leftrightarrow p^{\frac{3-1}{2}} \equiv 1 \pmod{3} \Leftrightarrow p \equiv 1 \pmod{3}$$

ama $p \not\equiv 4 \pmod{6}$ olma $\Rightarrow p \equiv 1 \pmod{6}$