

1. Az Euler-féle φ függvény

1.1. Definíció. Jelöljük $\varphi(n)$ -nel az n -nél nem nagyobb pozitív egész számok közül azoknak a számát, amelyek n -hez relatív prímek:

$$\varphi(n) = |\{a : 1 \leq a \leq n \text{ és } \text{Inko}(a, n) = 1\}|.$$

Az így kapott függvényt **Euler-féle φ függvénynek** nevezzük. Ha megállapodunk abban, hogy $\mathbb{Z}_1^*$ egyelemű halmaz, akkor tömörebben is megfogalmazhatjuk a definíciót:

$$\varphi: \mathbb{N} \rightarrow \mathbb{N}, n \mapsto |\mathbb{Z}_n^*|.$$

1.2. Példa. Számítsuk ki közvetlenül a definíció alapján φ néhány értékét:

(a) $\varphi(6) = |\mathbb{Z}_6^*| = |\{1, 2, 3, 4, 5, 6\}| = |\{1, 5\}| = 2$
 $= |\{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}| = |\{\overline{1}, \overline{5}\}| = 2$ $\mathbb{Z}_6 \setminus \{0\}$

(b) $\varphi(7) = |\mathbb{Z}_7^*| = |\{1, 2, 3, 4, 5, 6, 7\}| = 6$ $\varphi(p) = p-1 = |\mathbb{Z}_p^*|$

(c) $\varphi(8) = |\mathbb{Z}_8^*| = |\{1, 2, 3, 4, 5, 6, 7, 8\}| = 4$

(d) $\varphi(1024) = |\mathbb{Z}_{1024}^*| = |\{1, 2, 3, 4, \dots, 1023, 1024\}| = \frac{1024}{2} = 512 = 1024 \cdot (1 - \frac{1}{2})$

p_1 - (e) $\varphi(81) = |\mathbb{Z}_{81}^*| = |\{1, 2, 3, 4, 5, 6, \dots, 78, 79, 80, 81\}| = 81 - \frac{81}{3} = 81 \cdot (1 - \frac{1}{3}) = 54$
 3^4

1.3. Tétel. Tetszőleges p prím és α pozitív egész kitevő esetén

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1) = p^\alpha \cdot \left(1 - \frac{1}{p}\right).$$

Bizonyítás. Az $\{1, \dots, p^\alpha\}$ halmaz minden p -edik eleme osztható p -vel (ezek száma $p^{\alpha-1}$), a többiek viszont relatív prímek p^α -hoz (ugye?).

Így tehát $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$. □

1.4. Példa. Számítsuk ki közvetlenül a definíció alapján $\varphi(100)$ értékét.

Mivel $n = 2^2 \cdot 5^2$, egy szám akkor és csak akkor nem relatív prím n -hez, ha osztható 2-vel vagy 5-tel. Ezeket a „rossz” számokat fogjuk „kiszitálni” az $\{1, 2, \dots, 100\}$ halmazból.

$$U = \{1, 2, \dots, 100\}$$

$$|U| = 100$$

$$A_1 = \{a \in U : 2 \mid a\}$$

$$|A_1| = \frac{100}{2} = 50$$

$$A_2 = \{a \in U : 5 \mid a\}$$

$$|A_2| = \frac{100}{5} = 20$$

$$A_1 \cap A_2 = \{a \in U : 10 \mid a\}$$

$$|A_1 \cap A_2| = \frac{100}{2 \cdot 5} = 10$$



$$\begin{aligned} \varphi(100) &= |U| - |A_1| - |A_2| + |A_1 \cap A_2| = 100 - \frac{100}{2} - \frac{100}{5} + \frac{100}{10} = \\ &= 100 \cdot \left(1 - \frac{1}{2} - \frac{1}{5} + \frac{1}{2 \cdot 5}\right) = 100 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) \end{aligned}$$

1.5. Tétel. Legyen az n pozitív egész szám prímszaktényezős felbontása $n = \prod_{i=1}^k p_i^{\alpha_i}$. Ekkor

$$\varphi(n) = n \cdot \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^k \overbrace{(p_i^{\alpha_i} - p_i^{\alpha_i-1})}^{\varphi(p_i^{\alpha_i})} = \prod_{i=1}^k p_i^{\alpha_i-1} (p_i - 1).$$

Bizonyítás. Ha n -nek csak két prímszaktója van, azaz $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2}$, akkor az előző példában használt szita-formulát alkalmazhatjuk:

$$U = \{1, \dots, n\}$$

$$|U| = n$$

$$A_1 = \{a \in U : p_1 \mid a\}$$

$$|A_1| = \frac{n}{p_1}$$

$$A_2 = \{a \in U : p_2 \mid a\}$$

$$|A_2| = \frac{n}{p_2}$$

$$A_1 \cap A_2 = \{a \in U : p_1 p_2 \mid a\}$$

$$|A_1 \cap A_2| = \frac{n}{p_1 p_2}$$

$$\varphi(n) = |\overline{A_1 \cup A_2}| = |U| - |A_1| - |A_2| + |A_1 \cap A_2| =$$

$$= n - \frac{n}{p_1} - \frac{n}{p_2} + \frac{n}{p_1 p_2} = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right)$$

Ha n -nek k darab prímszaktója van, akkor k darab halmazra kell felírni a szita-formulát. A gondolatmenet a fentihez hasonló, csak a formulák nagyobbak. $\square$

1.6. Feladat. Számítsuk ki a tanult képlet alapján φ néhány értékét:

$$(a) \varphi(1000) = \varphi(2^3 \cdot 5^3) = \varphi(2^3) \cdot \varphi(5^3) = (2^3 - 2^2) \cdot (5^3 - 5^2) = 4 \cdot 100 = 400$$

$$(b) \varphi(360) = \varphi(2^3 \cdot 3^2 \cdot 5) = (2^3 - 2^2) \cdot (3^2 - 3^1) \cdot (5^1 - 5^0) = 4 \cdot 6 \cdot 4 = 96$$

$$(c) \varphi(2025) = \varphi(3^4 \cdot 5^2) = (3^4 - 3^3) \cdot (5^2 - 5^1) = 54 \cdot 20 = 1080$$

1.7. Tétel. A primitív n -edik egységgyökök száma $\varphi(n)$ minden n pozitív egész szám esetén.

Bizonyítás. Tudjuk, hogy az n -edik egységgyökök csoportja ciklikus:

$$E_n = \{\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{n-1}\} = [\varepsilon_1], \quad \text{ahol } \varepsilon_k = \varepsilon_1^k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}.$$

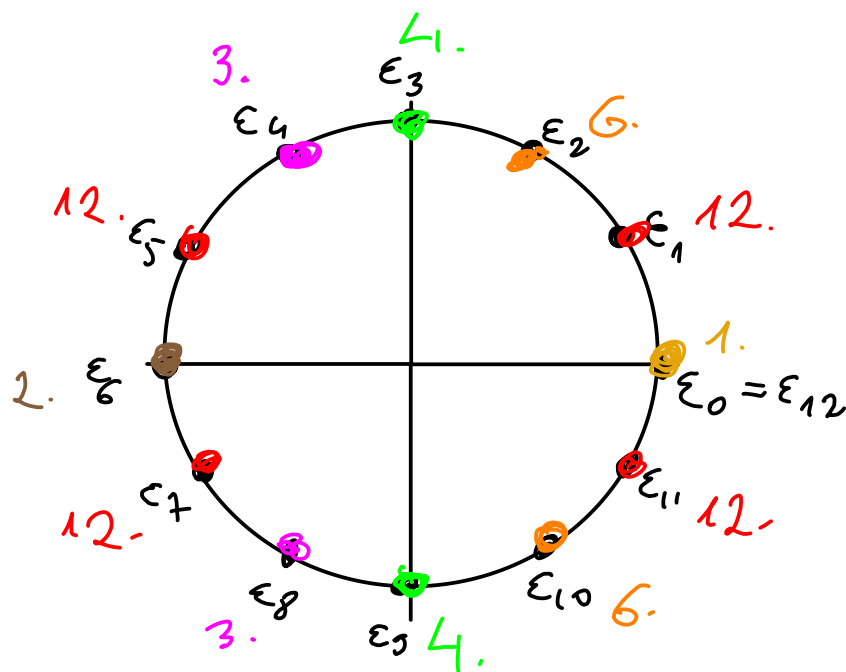
Az ε_k egységgyök akkor és csak akkor primitív n -edik egységgyök, ha rendje n . Alkalmazzuk a hatvány rendjére vonatkozó képletet:

$$o(\varepsilon_k) = o(\varepsilon_1^k) = \frac{o(\varepsilon_1)}{\text{Inko}(o(\varepsilon_1), k)} = \frac{n}{\text{Inko}(n, k)} = n \iff \text{Inko}(n, k) = 1$$

Tehát a primitív n -edik egységgyökök halmaza

$$P_n = \{\varepsilon_k : 0 \leq k \leq n-1 \text{ és } \text{Inko}(k, n) = 1\},$$

ennek a halmaznak pedig éppen $\varphi(n)$ eleme van (ugye?). □



$$|P_{12}| = 4 = \varphi(12)$$

$$|P_6| = 2 = \varphi(6)$$

$$|P_4| = 2 = \varphi(4)$$

$$|P_3| = 2 = \varphi(3)$$

$$|P_2| = 1 = \varphi(2)$$

$$|P_1| = 1 = \varphi(1)$$

$$12 = \sum_{d|12} \varphi(d)$$

1.8. Tétel. Minden n pozitív egész számra $\sum_{d|n} \varphi(d) = n$.

Bizonyítás. Jelölje E_n az n -edik egységgyökök halmazát, P_n pedig a primitív n -edik egységgyökök halmazát:

$$E_n = \{z \in \mathbb{C}^* : z^n = 1\}, \quad P_n = \{z \in \mathbb{C}^* : o(z) = n\}.$$

$$|E_n| = n$$

$$|P_n| = \varphi(n)$$

A bizonyítás kulcsa az alábbi megfigyelés:

$$z \in E_n \iff o(z) \mid n$$

$$z \in E_n \iff z^n = 1 = z^0 \iff n = 0 \pmod{o(z)} \iff o(z) \mid n$$

Látjuk tehát, hogy E_n felbontható a P_d ($d \mid n$) halmazok egyesítésére, és ezek a halmazok páronként diszjunktak (miért?):

$$E_n = \bigcup_{d|n} P_d.$$

Diszjunkt halmazok egyesítésénél az elemszámok összeadódnak, tehát

$$n = |E_n| = \left| \bigcup_{d|n} P_d \right| = \sum_{d|n} |P_d|.$$

Az előző tételből tudjuk, hogy $|P_d| = \varphi(d)$, tehát a fenti egyenlőség igazolja, hogy $n = \sum_{d|n} \varphi(d)$. □

2. Az Euler–Fermat-tétel

2.1. Definíció. Ha $a \in \mathbb{Z}$ és $m \geq 2$ relatív prímek, akkor az a szám **modulo m rendjén** a $\mathbb{Z}_m^*$ csoport $\bar{a}$ elemének rendjét értjük:

$$o_m(a) = o_{\mathbb{Z}_m^*}(\bar{a}) := \min \{k \in \mathbb{N} : a^k \equiv 1 \pmod{m}\}.$$

Ha a nem relatív prím m -hez, akkor $o_m(a)$ nem értelmezett.

2.2. Példa. Határozzuk meg $o_{18}(7)$ értékét. Ehhez kezdjük el hatványozni a $\bar{7} \in \mathbb{Z}_{18}^*$ elemet:

k	1	2	3	4	5	6	7	8	...	1001
$\bar{7}^k$	$\bar{7}$	$\bar{13}$	$\bar{1}$	$\bar{7}$	$\bar{13}$	$\bar{1}$	$\bar{7}$	$\bar{13}$	...	$\bar{13}$

A harmadik hatványra jött ki először $\bar{1}$, ezért $o(\bar{7}) = 3 = o_{18}(7)$.

2.3. Példa. Mit ad 18-cal osztva maradékul 7^{1001} ?

Fent megállapítottuk, hogy $o_{18}(7) = 3$, és ez azt jelenti, hogy $\mathbb{Z}_{18}^* \geq [\bar{7}] \cong \mathbb{Z}_3$, vagyis 7 modulo 18 hatványozásakor a kitevő modulo 3 „számít”:

$$1001 \equiv 2 \pmod{3} \implies \bar{7}^{1001} = \bar{7}^2 = \bar{13}.$$

Tehát $7^{1001} \equiv 13 \pmod{18}$.

2.4. Tétel (Euler–Fermat-tétel). Ha az a egész szám relatív prím az m modulushoz, akkor

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Bizonyítás.

- Ha a és m relatív prímek, akkor $\bar{a}$ eleme a $G := (\mathbb{Z}_m^*, \cdot)$ csoportnak.
- **LAGRANGE** tételének egyik következménye szerint $\bar{a}^{|G|} = \bar{1}$.
- Definíció szerint $|G| = \varphi(m)$

Tehát $\bar{a}^{\varphi(m)} = \bar{1}$, és épp ezt kellett bizonyítani. □

2.5. Következmény (kis Fermat-tétel). Ha p prímszám és a nem osztható p -vel, akkor $a^{p-1} \equiv 1 \pmod{p}$.

Más (ekvivalens) megfogalmazásban: Ha p prímszám, akkor minden a egész számra $a^p \equiv a \pmod{p}$.

Bizonyítás.

- Ha p prímszám, akkor $\varphi(p) = p - 1$.
- Ha p prímszám, akkor $\text{Inko}(a, p) = 1 \iff p \nmid a$.

Tehát az Euler–Fermat-tételt az $m = p$ esetben ezt adja:

$$p \nmid a \implies a^{p-1} \equiv 1 \pmod{p}.$$

Ha beszorozzuk mindkét oldalt a -val, akkor az $a^p \equiv a \pmod{p}$ kongruenciát kapjuk, ami még akkor is igaz, ha $p \mid a$ (miért?). $\square$

2.6. Példa. Mit ad 18-cal osztva maradékul 7^{1001} ?

Ezt a feladatot már egyszer megoldottuk, de most az Euler–Fermat-tétel segítségével úgy is meg tudjuk oldani, hogy nem készítünk táblázatot 7 hatványaiból.

Osszuk el a kitevőt maradékosan $\varphi(18) = 6$ -tal: $1001 = 166 \cdot 6 + 5$. A hatványt átalakítva és az Euler–Fermat-tételt használva a következőképpen számolhatunk:

$$7^{1001} \equiv 7^{166 \cdot 6 + 5} \equiv (7^6)^{166} \cdot 7^5 \equiv 1^{166} \cdot 7^5 \equiv 7^5 \equiv 13 \pmod{18}.$$

$\begin{array}{c} \text{E-F} \\ 1 \\ \text{mod } 18 \end{array}$

2.7. Következmény. Ha $a \in \mathbb{Z}$ relatív prím az $m \geq 2$ modulushoz, akkor tetszőleges $k, \ell \in \mathbb{Z}$ kitevők esetén

$$(1) \text{ } o_m(a) \mid \varphi(m);$$

$\begin{array}{c} \text{H} \\ \parallel \\ \text{G} \end{array}$

$$(2) k \equiv \ell \pmod{\varphi(m)} \implies a^k \equiv a^\ell \pmod{m}.$$

Bizonyítás.

(1) Ez rögtön következik Lagrange tételéből, ha a $G = \mathbb{Z}_m^*$ csoport $H = [\bar{a}]$ részcsoportjára alkalmazzuk.

$$(2) k \equiv \ell \pmod{\varphi(m)} \implies k \equiv \ell \pmod{o_m(a)} \iff \bar{a}^k = \bar{a}^\ell.$$

$\begin{array}{c} \parallel \\ 6 \end{array} \quad \begin{array}{c} \parallel \\ 3 \end{array}$

$\square$

2.8. Példa. Mit ad 18-cal osztva maradékul 7^{1001} ?

A második megoldásunk tömörebb leírása (vegyük észre, hogy a 166-os számnak semmi szerepe nem volt): $\varphi(18)$

$$1001 \equiv 5 \pmod{6} \xRightarrow{(2)} 7^{1001} \equiv 7^5 \equiv 13 \pmod{18}.$$

2.9. Feladat. Mit ad 11-gyel osztva maradékul 123^{765} ?

$$\bullet 123 \equiv 2 \pmod{11} \Rightarrow 123^{765} \equiv 2^{765} \pmod{11}$$

$$\bullet \varphi(11) = 10$$

$$\bullet \ell_6(2, 11) = 1 \checkmark \varphi(11)$$

$$\bullet 765 \equiv 5 \pmod{10} \xRightarrow{(2)} 2^{765} \equiv 2^5 \equiv 10 \pmod{11}$$

$$\begin{array}{l} 123 \equiv 2 \pmod{11} \\ \vdots \\ 123 \equiv 2 \pmod{11} \end{array} \left. \vphantom{\begin{array}{l} 123 \equiv 2 \pmod{11} \\ \vdots \\ 123 \equiv 2 \pmod{11} \end{array}} \right\} 765 \\ \hline 123^{765} \equiv 2^{765} \pmod{11} \\ \equiv 2 \pmod{11}$$

Összefoglalva:

$$123^{765} \equiv 2^{765} \equiv 2^5 \equiv 10 \pmod{11}.$$

Mit felejtettünk el?

2.10. Feladat. Mit ad 44-gyel osztva maradékul 4447^{2018} ?

$$1. 4447 \equiv 3 \pmod{44}$$

$$2. \varphi(44) = \varphi(2^2 \cdot 11) = (2^2 - 2^1) \cdot (11 - 1) = 2 \cdot 10 = 20$$

$$3. \text{Inko}(3, 44) = 1 \checkmark$$

$$4. 2018 \equiv 18 \pmod{20}$$

A fentiekből következik, hogy

$$4447^{2018} \equiv 3^{2018} \equiv 3^{18} \equiv 3^{-2} \equiv 3^{-1} \equiv x \equiv 5 \pmod{44}.$$

$$9x \equiv 1 \pmod{44}$$

$$9x \equiv 45 \pmod{44} \quad | :9 \quad \ell_6(9, 44) = 1$$

$$x \equiv 5 \pmod{44}$$

$$3^{18} \equiv 3^9 \cdot 3^9 \cdot 3^4 \cdot 3^1 \cdot 3^2 \equiv (-1)(-1)(-1)(-1) \cdot 9 \equiv 49 \cdot 49 \cdot 9 \equiv 5 \cdot 5 \cdot 9 \equiv 5 \cdot 1 \cdot 5$$

3. Primitív gyök, index

3.1. Definíció. Azt mondjuk, hogy a g egész szám **primitív gyök** modulo m , ha rendje éppen $\varphi(m)$.

3.2. Tétel. A g egész szám akkor és csak akkor primitív gyök modulo m , ha az összes mod m redukált maradékosztály megkapható $\bar{g}$ hatványaként.

Bizonyítás. A $\mathbb{Z}_m^*$ csoportban $\bar{g}$ hatványai a $[\bar{g}]$ részcsoporthot alkotják, melynek $o_m(g)$ eleme van. Ez akkor és csak akkor teszi ki a teljes $\mathbb{Z}_m^*$ csoportot, ha $o_m(g) = \varphi(m)$. $\square$

3.3. Példa.

$m=5$ $\mathbb{Z}_5^* = \{1, \bar{2}, \bar{3}, \bar{4}\} = [\bar{g}]$ pr. mőköd

$\bar{2}^0$	1	2	3	4
$\bar{2}^1$	$\bar{2}$	$\bar{4}$	$\bar{3}$	$\bar{1}$

$\sigma(\bar{2}) = 4 = \varphi(5) \Leftrightarrow [\bar{2}] = \mathbb{Z}_5^*$

$\bar{3}^0$	1	2	3	4
$\bar{3}^1$	$\bar{3}$	$\bar{4}$	$\bar{2}$	$\bar{1}$

$\sigma(\bar{3}) = 4 = \varphi(5) \Leftrightarrow [\bar{3}] = \mathbb{Z}_5^*$

$\bar{4}^0$	1	2	3	4
$\bar{4}^1$	$\bar{4}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

$\sigma(\bar{4}) = 2$
 $[\bar{4}] = \{1, \bar{4}\} \neq \mathbb{Z}_5^*$

3.4. Tétel. Akkor és csak akkor létezik primitív gyök, ha a modulus 2, 4, páratlan prímhatvány vagy páratlan prímhatvány kétszerese:

$$m = 2, 4, p^\alpha, 2p^\alpha \quad (p \text{ páratlan prím}, \alpha \in \mathbb{N}).$$

$a^k = b \quad k = \log_a b \quad \bar{3} = \bar{2}^? \in \mathbb{Z}_5^* \quad ? = \log_{\bar{2}} \bar{3} = 3$

3.5. Definíció. Tegyük fel, hogy g primitív gyök az m modulushoz. Az a egész szám **indexén** (az m modulusra és a g primitív gyökre nézve) olyan i kitevőt értünk, amelyre $g^i \equiv a \pmod{m}$.

~~$\text{ind}_4 3$ nem definiált~~

Jelölés. A moduluszt az egyszerűség kedvéért nem írjuk ki (ez többnyire amúgy is világos a szövegkörnyezetből), tehát a indexét röviden $\text{ind}_g a$ jelöli.

3.6. Megjegyzés. Világos, hogy ha a és m nem relatív prím, akkor $\text{ind}_g a$ nem értelmezett (ugyanis g^i mindig relatív prím m -hez). Ha viszont a és m relatív prím, akkor a 3.2. Tétel szerint a előáll g hatványaként modulo m , tehát ekkor $\text{ind}_g a$ értelmezett.

3.7. Megjegyzés. Az index nem egyértelmű, csak modulo $\varphi(m)$ van meghatározva.

$$g^i \equiv g^{i'} \pmod{m} \Leftrightarrow i \equiv i' \pmod{\sigma_m(g)} \quad \sigma_m(g) = \varphi(m)$$

3.8. Tétel. Legyen g primitív gyök modulo m , legyen k tetszőleges egész szám, a és b pedig relatív prímek m -hez. Ekkor érvényesek az alábbi azonosságok:

- (1) $\text{ind}_g 1 \equiv 0 \pmod{\varphi(m)}$;
- (2) $\text{ind}_g(ab) \equiv \text{ind}_g a + \text{ind}_g b \pmod{\varphi(m)}$;
- (3) $\text{ind}_g a^k \equiv k \cdot \text{ind}_g a \pmod{\varphi(m)}$;
- (4) $\text{ind}_g(ab^{-1}) \equiv \text{ind}_g a - \text{ind}_g b \pmod{\varphi(m)}$.

Bizonyítás.

- (1) $g^0 \equiv 1 \pmod{m} \implies \text{ind}_g 1 \equiv 0 \pmod{\varphi(m)}$.
- (2) $ab \equiv g^{\text{ind}_g(a)} g^{\text{ind}_g(b)} \equiv g^{\text{ind}_g(a) + \text{ind}_g(b)} \pmod{m} \implies \text{ind}_g(ab) \equiv \text{ind}_g a + \text{ind}_g b \pmod{\varphi(m)}$.
- (3) $a^k \equiv (g^{\text{ind}_g(a)})^k \equiv g^{k \cdot \text{ind}_g(a)} \pmod{m} \implies \text{ind}_g a^k \equiv k \cdot \text{ind}_g a \pmod{\varphi(m)}$;
- (4) $ab^{-1} \equiv g^{\text{ind}_g(a)} (g^{\text{ind}_g(b)})^{-1} \equiv g^{\text{ind}_g(a) - \text{ind}_g(b)} \pmod{m} \implies \text{ind}_g(ab^{-1}) \equiv \text{ind}_g a - \text{ind}_g b \pmod{\varphi(m)}$.

□

3.9. Feladat. Ellenőrizzük, hogy $g = 2$ primitív gyök a $p = 11$ modulushoz.

Ehhez számítsuk ki 2 hatványainak modulo 11 maradékait:

$\sigma_{11}(2)$

$10 = \varphi(11)$

$\text{ind}_{11} a = i$	0	1	2	3	4	5	6	7	8	9	
$(\text{ind}_{11}) a \equiv 2^i$	1	2	4	8	5	10	9	7	3	6	1

10 = 2 + 8

A táblázatból látható, hogy $\sigma_{11}(2) = 10 = \varphi(11)$, tehát 2 valóban primitív gyök modulo 11. Az is látszik a táblázatból, hogy minden modulo 11 redukált maradékosztály megkapható $\bar{2}$ hatványaként. A táblázatban minden szám fölött az indexe található. Ha megcseréljük a két sort, és a felső számok szerint rendezzük az oszlopokat, akkor kapjuk az alábbi **indextáblázatot**:

$(\text{ind}_{11}) 2^i = a$	1	2	3	4	5	6	7	8	9	10
$(\text{ind}_{11}) i \equiv \text{ind}_g a$	0	1	8	2	4	9	7	3	6	5

A megoldást kereshetjük $x \equiv 2^i \pmod{11}$ alakban (miért?), és a jobb oldali 5-öst is felírhatjuk 2 hatványaként. Így az $i = \text{ind}_2 x$ ismeretlenre egy lineáris kongruenciát kapunk, amit könnyen meg tudunk oldani:

$$\begin{aligned} X^6 &\equiv 5 \pmod{11} \\ 2^6 &\equiv 2^4 \pmod{11} \\ \Uparrow \\ 6i &\equiv 4 \pmod{10} \\ 6i &\equiv 2^4 \pmod{10} \\ i &\equiv 4 \pmod{5} \\ i &\equiv 4, 9 \pmod{10} \end{aligned}$$

$$x \equiv \begin{matrix} 2^4 & 2^9 \\ || & || \\ 5 & 6 \end{matrix} \pmod{11}$$

Eredményünk így is megfogalmazható: a $\mathbb{Z}_{11}$ testben $\bar{5}$ -nak két hatodik gyöke van, mégpedig $\bar{5}$ és $\bar{6}$.

3.11. Definíció. Azt mondjuk, hogy az a egész szám **n -edik hatványmaradék** modulo m , ha az $x^n \equiv a \pmod{m}$ kongruenciának van megoldása.

3.12. Tétel. Legyen g primitív gyök modulo m , és legyen a relatív prím m -hez. Ekkor a pontosan akkor n -edik hatványmaradék modulo m , ha

$$\text{Inko}(n, \varphi(m)) \mid \text{ind}_g a.$$

Bizonyítás.

$$x \equiv g^i \pmod{m} \quad i = \text{ind}_g x$$

$$a \equiv g^{\text{ind}_g a} \pmod{m}$$

$$x^n \equiv a \pmod{m}$$

$$g^{ni} \equiv g^{\text{ind}_g a} \pmod{m}$$

$$\Updownarrow$$

$$ni \equiv \text{ind}_g a \pmod{\varphi(m)}$$

$$\text{van } n \Leftrightarrow \text{Inko}(n, \varphi(m)) \mid \text{ind}_g a$$

$$100 \dots 001 = x^2 \equiv 2 \pmod{3}$$

$$x^2 \equiv 0^2 \equiv 0$$

$$x^2 \equiv 1^2 \equiv 1 \pmod{3}$$

$$x^2 \equiv 2^2 \equiv 1$$

□

4. Négyzetes maradékok, Legendre-szimbólum

4.1. Definíció. Az a egész számot **négyzetes maradéknak** nevezzük modulo m , ha az $x^2 \equiv a \pmod{m}$ kongruenciának van megoldása. Ellenkező esetben azt mondjuk, hogy a **négyzetes nemmaradék** modulo m .

4.2. Tétel. Legyen p páratlan prímszám, g primitív gyök modulo p . Ekkor $a \in \mathbb{Z}$ pontosan akkor négyzetes maradék modulo p , ha $p \mid a$ vagy $\text{ind}_g a$ páros.

Bizonyítás.

- Ha $p \mid a$, akkor $a \equiv 0 \pmod{p}$, és a 0 nyilván négyzetes maradék.
- Ha $p \nmid a$, akkor $\text{Inko}(a, p) = 1$, így alkalmazható a 3.12. Tétel:

$$a \text{ négyzetes maradék} \iff \underbrace{\text{Inko}(2, \underbrace{\varphi(p)}_{p-1})}_{2} \mid \text{ind}_g a.$$

□

4.3. Definíció. Tetszőleges p páratlan prímszám és p -vel nem osztható a egész szám esetén értelmezzük az $\left(\frac{a}{p}\right)$ **Legendre-szimbólumot** a következőképpen:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{ha } a \text{ négyzetes maradék mod } p; \\ -1, & \text{ha } a \text{ négyzetes nemmaradék mod } p. \end{cases}$$

4.4. Tétel (Euler-kritérium). Ha p páratlan prímszám és $p \nmid a$, akkor

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

Bizonyítás. Legyen g primitív gyök modulo p és $i := \text{ind}_g a$.

1. lépés: $g^{\frac{p-1}{2}} \equiv x \equiv -1 \pmod{p}$

$$x^2 = g^{p-1} \equiv 1 \pmod{p} \Rightarrow p \mid x^2 - 1 = (x-1)(x+1) \Rightarrow p \mid x-1 \vee p \mid x+1$$

$\Rightarrow x \equiv 1 \pmod{p} \vee x \equiv -1 \pmod{p}$
 $\sigma(g) \leq \frac{p-1}{2} < g^{p-1}$

2. lépés: $a^{\frac{p-1}{2}} \equiv (g^i)^{\frac{p-1}{2}} \equiv (g^{\frac{p-1}{2}})^i \equiv (-1)^i \equiv \left(\frac{a}{p}\right) \pmod{p}$

□

4.5. Tétel. Tetszőleges p páratlan prímszám és p -vel nem osztható a, b egész számok esetén teljesülnek az alábbiak:

$$\tau (1) a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right);$$

$$\mu (2) \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right). \quad \left. \begin{array}{l} \exists x: x^2 \equiv a \\ \exists y: y^2 \equiv b \end{array} \right\} \implies \exists z: z^2 \equiv ab$$

$1 \quad (-1)(1)$

Bizonyítás.

(1) Triviális.

$$(2) \left(\frac{ab}{p}\right) \stackrel{E-K}{=} (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \stackrel{E-K}{=} \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \pmod{p}.$$

$$1 \not\equiv -1 \pmod{p}, \text{ mert } p > 2$$

□

4.6. Tétel (a négyzetes reciprocitási tétel első kiegészítő tétele).

Tetszőleges p páratlan prímszám esetén

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{ha } p \equiv 1 \pmod{4}; \\ -1, & \text{ha } p \equiv 3 \pmod{4}. \end{cases}$$

4.7. Feladat. Számítsuk ki az alábbi Legendre-szimbólumokat.

$$(a) \left(\frac{8}{79}\right) = \left(\frac{2 \cdot 2 \cdot 2}{79}\right) \stackrel{\mu}{=} \left(\frac{2}{79}\right) \cdot \left(\frac{2}{79}\right) \cdot \left(\frac{2}{79}\right) \stackrel{\tau}{=} \left(\frac{2}{79}\right)^3 \stackrel{\tau}{=} \left(\frac{81}{79}\right)^3 \stackrel{\tau}{=} 1^3 = 1$$

Teljesen $\exists x: x^2 \equiv 8 \pmod{79}.$

$$(b) \left(\frac{19}{23}\right) \stackrel{\tau}{=} \left(\frac{-4}{23}\right) \stackrel{\mu}{=} \left(\frac{-1}{23}\right) \cdot \left(\frac{4}{23}\right) \stackrel{\tau}{=} (-1) \cdot 1 = -1$$

$\begin{array}{cc} \parallel & \parallel \\ -1 & 1 \end{array}$

$$\text{Teljesen } \exists x: x^2 \equiv 19 \pmod{23}$$

4.8. Tétel (négyzetes reciprocitási tétel).

$\mathcal{R}$ Tetszőleges p, q különböző páratlan prímszámok esetén

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \begin{cases} 1, & \text{ha } p \equiv 1 \pmod{4} \text{ vagy } q \equiv 1 \pmod{4}; \\ -1, & \text{ha } p \equiv 3 \pmod{4} \text{ és } q \equiv 3 \pmod{4}. \end{cases}$$

4.9. Tétel (a négyzetes reciprocitási tétel második kiegészítő tétele).

Tetszőleges p páratlan prímszám esetén

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

4.10. Feladat. Számítsuk ki az alábbi Legendre-szimbólumokat.

$$(a) \quad \left(\frac{7}{17}\right) \stackrel{\mathcal{R}}{=} \left(\frac{17}{7}\right)^T = \left(\frac{3}{7}\right) \stackrel{\mathcal{R}}{=} -\left(\frac{7}{3}\right)^T = -\left(\frac{1}{3}\right) \stackrel{\parallel}{=} -(-1) \cdot 1 = -1$$

$$(b) \quad \left(\frac{77}{101}\right) = \left(\frac{101}{77}\right)^M = \left(\frac{7}{101}\right) \cdot \left(\frac{11}{101}\right) \stackrel{\mathcal{R}}{=} \left(\frac{101}{7}\right) \cdot \left(\frac{101}{11}\right)^T = \left(\frac{3}{7}\right) \cdot \left(\frac{2}{11}\right)^T =$$

$$= -\left(\frac{7}{3}\right) \cdot \left(\frac{7}{2}\right)^T = -\left(\frac{7}{3}\right) \cdot (-1)^T = +\left(\frac{1}{3}\right) \stackrel{\parallel}{=} 1$$

$$(c) \quad \left(\frac{69}{83}\right) \stackrel{M}{=} \left(\frac{3}{83}\right) \cdot \left(\frac{23}{83}\right) \stackrel{\mathcal{R}}{=} -\left(\frac{83}{3}\right) \cdot \left(\frac{83}{23}\right)^T = \left(\frac{2}{3}\right) \cdot \left(\frac{14}{23}\right) = -\left(\frac{2}{23}\right) \cdot \left(\frac{7}{23}\right) =$$

$$\stackrel{199.}{=} -\left(\frac{7}{23}\right) \stackrel{\mathcal{R}}{=} +\left(\frac{23}{7}\right)^T = \left(\frac{2}{7}\right) = 1$$

$$\left(\frac{69}{83}\right)^T = \left(\frac{-14}{83}\right) = \left(\frac{-1}{83}\right) \cdot \left(\frac{2}{83}\right) \cdot \left(\frac{7}{83}\right) = -\left(\frac{83}{7}\right) = -\left(\frac{-1}{7}\right) = 1$$