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:

$$\varphi(n) = \left|\left\{a : 1 \leq a \leq n \text{ és } \operatorname{lnko}(a, n) = 1\right\}\right|.$$

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

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

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

(a) $\varphi(6) = |\mathbb{Z}_6^*| =$

(b) $\varphi(7) = |\mathbb{Z}_7^*| =$

(c) $\varphi(8) = |\mathbb{Z}_8^*| =$

(d) $\varphi(1024) = |\mathbb{Z}_{1024}^*| =$

(e) $\varphi(81) = |\mathbb{Z}_{81}^*| =$

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 $\{1, \ldots, p^\alpha\}$ 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 $\{1, 2, \ldots, 100\}$ halmazból.

$$U = \{1, 2, \ldots, 100\} \qquad |U| =$$

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

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

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

$\varphi(100) =$

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

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

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

$$U = \{1, \ldots, n\} \qquad |U| = n$$

$$A_1 = \{a \in U : p_1 \mid a\} \qquad |A_1| = \tfrac{n}{p_1}$$

$$A_2 = \{a \in U : p_2 \mid a\} \qquad |A_2| = \tfrac{n}{p_2}$$

$$A_1 \cap A_2 = \{a \in U : p_1 p_2 \mid a\} \qquad |A_1 \cap A_2| = \tfrac{n}{p_1 p_2}$$

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

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

Ha n-nek k darab prímosztója van, akkor k darab halmazra kell felírni a szita-formulát. A gondolatmenet a fentihez hasonló, csak a formulák nagyobbak. □

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

(a) $\varphi(1000) = \varphi(2^3 \cdot 5^3) =$

(b) $\varphi(360) = \varphi(2^3 \cdot 3^2 \cdot 5) =$

(c) $\varphi(2025) = \varphi(3^4 \cdot 5^2) =$

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:

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

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

$$o(\varepsilon_k) = o(\varepsilon_1^k) = \frac{o(\varepsilon_1)}{\text{lnko}(o(\varepsilon_1), k)} = \frac{n}{\text{lnko}(n, k)}.$$

Tehát a primitív n-edik egységgyökök halmaza

$$\big\{\varepsilon_k : 0 \le k \le n-1 \text{ és } \text{lnko}(k, n) = 1\big\},$$

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

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 primitiv n-edik egységgyökök halmazát:

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

A bizonyítás kulcsa az alábbi megfigyelés:

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

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 $\overline{a}$ elemének rendjét értjük:

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

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 $\overline{7} \in \mathbb{Z}_{18}^*$ elemet:

k	1	2	3	4	5	6	7	8	$\cdots$
$\overline{7}^k$									$\cdots$

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

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

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

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

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 $\overline{a}$ eleme a $G := \ldots\ldots\ldots\ldots$ csoportnak.
- $\ldots\ldots\ldots\ldots\ldots\ldots\ldots$ tételének egyik következménye szerint $\overline{a}^{|G|} = \overline{1}$.
- Definíció szerint $|G| = \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$

Tehát $\overline{a}^{\varphi(m)} = \overline{1}$, 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 $\operatorname{lnko}(a, p) = 1 \iff p \nmid a$.

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?). □

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:

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

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) $o_m(a) \mid \varphi(m)$;

(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 $H = [\overline{a}]$ részcsoportjára alkalmazzuk.

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

□

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):

$$1001 \equiv 5 \pmod{6} \implies 7^{1001} \equiv 7^5 \equiv 13 \pmod{18}.$$

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

- $123 \equiv 2 \pmod{11} \implies 123^{765} \equiv 2^{765} \pmod{11}$
- $\varphi(11) = 10$
- $765 \equiv 5 \pmod{10} \implies 2^{765} \equiv 2^5 \equiv 10 \pmod{11}$

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. $4447 \equiv \qquad \pmod{44}$

2. $\varphi(44) =$

3. $\text{lnko}(3, 44) = 1$✓

4. $2018 \equiv \qquad \pmod{\qquad}$

A fentiekből következik, hogy

$$4447^{2018} \equiv 3^{2018} \equiv 3^{18} \equiv \qquad\qquad\qquad \pmod{44}.$$

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 $\overline{g}$ hatványaként.

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

3.3. Példa.

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

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

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 $g^i \equiv a \pmod{m}$.

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

3.6. Megjegyzés. Világos, hogy ha a és m nem relatív prím, akkor $\operatorname{ind}_g a$ 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 $\operatorname{ind}_g a$ értelmezett.

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

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) $\operatorname{ind}_g 1 \equiv 0 \pmod{\varphi(m)}$;

(2) $\operatorname{ind}_g(ab) \equiv \operatorname{ind}_g a + \operatorname{ind}_g b \pmod{\varphi(m)}$;

(3) $\operatorname{ind}_g a^k \equiv k \cdot \operatorname{ind}_g a \pmod{\varphi(m)}$;

(4) $\operatorname{ind}_g(ab^{-1}) \equiv \operatorname{ind}_g a - \operatorname{ind}_g b \pmod{\varphi(m)}$.

Bizonyítás.

(1) $g^0 \equiv 1 \pmod{m} \implies \operatorname{ind}_g 1 \equiv 0 \pmod{\varphi(m)}$.

(2) $ab \equiv g^{\operatorname{ind}_g(a)} g^{\operatorname{ind}_g(b)} \equiv g^{\operatorname{ind}_g(a)+\operatorname{ind}_g(b)} \pmod{m} \implies$
$\implies \operatorname{ind}_g(ab) \equiv \operatorname{ind}_g a + \operatorname{ind}_g b \pmod{\varphi(m)}$.

(3) $a^k \equiv (g^{\operatorname{ind}_g(a)})^k \equiv g^{k \operatorname{ind}_g(a)} \pmod{m} \implies \operatorname{ind}_g a^k \equiv k \cdot \operatorname{ind}_g a \pmod{\varphi(m)}$;

(4) $ab^{-1} \equiv g^{\operatorname{ind}_g(a)} (g^{\operatorname{ind}_g(b)})^{-1} \equiv g^{\operatorname{ind}_g(a)-\operatorname{ind}_g(b)} \pmod{m} \implies$
$\implies \operatorname{ind}_g(ab^{-1}) \equiv \operatorname{ind}_g a - \operatorname{ind}_g b \pmod{\varphi(m)}$.

□

3.9. Feladat. Ellenőrizzük, hogy $g = 2$ primitív gyök a $p = 11$ modulushoz. Ehhez számítsuk ki 2 hatványainak modulo 11 maradékait:

i	0	1	2	3	4	5	6	7	8	9	10
2^i											

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

a	1	2	3	4	5	6	7	8	9	10
$\operatorname{ind}_g a$										

3.10. Feladat. Oldjuk meg a fenti példában konstruált indextáblázat segítségével az $x^6 \equiv 5 \pmod{11}$ kongruenciát.

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

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

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

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

Bizonyítás.

□

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 $\operatorname{ind}_g a$ páros.

Bizonyítás.

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

$$a \text{ négyzetes maradék} \iff \operatorname{lnko}(2, \varphi(p)) \mid \operatorname{ind}_g a.$$

□

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:

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

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 $i := \operatorname{ind}_g a$.

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

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

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

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

(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Bizonyítás.

(1) Triviális.

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

□

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) $\left(\frac{8}{79}\right) =$

(b) $\left(\frac{19}{23}\right) =$

4.8. Tétel (**négyzetes reciprocitási tétel**).
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) $\left(\frac{7}{17}\right) =$

(b) $\left(\frac{77}{101}\right) =$

(c) $\left(\frac{69}{83}\right) =$