AZ EULER-FÉLE φ FÜGGVÉNY

Waldhauser Tamás

SZTE Bolyai Intézet

Tartalom

Definíció

Tetszőleges n természetes szám esetén $\varphi(n)$ jelöli azt, hogy 1-től n-ig hány olyan szám van, ami relatív prím n-hez:

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

Az így kapott $\varphi\colon \mathbb{N} \to \mathbb{N},\ n \mapsto \varphi(n)$ függvényt Euler-féle φ függvénynek nevezzük.

Megjegyzés

Nyilván $\varphi(1) = 1$, és $m \geq 2$ esetén $\varphi(m) = |\mathbb{Z}_m^*|$.

Példák

- $\varphi(29) = |\{1, 2, \ldots, 28, 29\}| = 29 - 1 = 28$ $\qquad \varphi(p) = p - 1$
- $\varphi(32) = |\{1, 2, 3, 4, \ldots, 31, 32\}| = 32 - \frac{32}{2} = 32 - 16 = 16$
- $\varphi(81) = |\{1, 2, 3, 4, 5, 6, 7, \ldots, 80, 81\}| = 81 - \frac{81}{3} = 81 - 27 = 54$

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

Példa

Számítsuk ki $\varphi(1000)$ értékét.

$$\varphi(1000) = |\{a : 1 \leq a \leq 1000 \text{ és } 2 \nmid a \text{ és } 5 \nmid a\}| = \left| \overline{R_1 \cup R_2} \right|$$

$$U = \{1, \ldots, 1000\} \qquad |U| = 1000$$

$$R_1 = \{a \in U : 2 \mid a\} \qquad |R_1| = 500$$

$$R_2 = \{a \in U : 5 \mid a\} \qquad |R_2| = 200$$

$$R_1 \cap R_2 = \{a \in U : 10 \mid a\} \qquad |R_1 \cap R_2| = 100$$

$$\varphi(1000) = |U| - |R_1| - |R_2| + |R_1 \cap R_2| = 1000 - 500 - 200 + 100 = 400$$

$$= 1000 - \frac{1000}{2} - \frac{1000}{5} + \frac{1000}{2 \cdot 5} = 1000 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right)$$

Példa

Számítsuk ki $\varphi(n)$ értékét, ha $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2}$.

$$\varphi(n) = |\{a : 1 \leq a \leq n \text{ és } p_1 \nmid a \text{ és } p_2 \nmid a\}| = \left|\overline{R_1 \cup R_2}\right|$$

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

$$R_1 = \{a \in U : p_1 \mid a\} \qquad |R_1| = \frac{n}{p_1}$$

$$R_2 = \{a \in U : p_2 \mid a\} \qquad |R_2| = \frac{n}{p_2}$$

$$R_1 \cap R_2 = \{a \in U : p_1 p_2 \mid a\} \qquad |R_1 \cap R_2| = \frac{n}{p_1 p_2}$$

$$\varphi(n) = |U| - |R_1| - |R_2| + |R_1 \cap R_2| = n - \frac{n}{p_1} - \frac{n}{p_2} + \frac{n}{p_1 p_2}$$

$$= n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \cdot \left(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}\right)$$

$\varphi(360)$ kiszámítása

Mivel 360 prímfelbontása $360 = 2^3 \cdot 3^2 \cdot 5$, az univerzum és a „szitálandó” halmazok ebben az esetben a következők lesznek:

$$U = \{1, 2, \ldots, 360\}, \quad R_1 = \{a \in U : 2 \mid a\}, \quad R_2 = \{a \in U : 3 \mid a\}, \quad R_3 = \{a \in U : 5 \mid a\}.$$

Minden második szám osztható 2-vel, minden harmadik szám osztható 3-mal, és minden ötödik szám osztható 5-tel, ezért a fenti halmazok elemszáma

$$|U| = 360, \quad |R_1| = \frac{360}{2} = 180, \quad |R_2| = \frac{360}{3} = 120, \quad |R_3| = \frac{360}{5} = 72.$$

Pontosan azok a számok relatív prímek 360-hoz, amelyek se 2-vel, se 3-mal, se 5-tel nem oszthatóak, tehát $\varphi(360) = \left|\overline{R_1 \cup R_2 \cup R_3}\right|$. Erre a szita-formula a következőképpen fest:

$$\left|\overline{R_1 \cup R_2 \cup R_3}\right| = |U| - |R_1| - |R_2| - |R_3| + |R_1 \cap R_2| + |R_1 \cap R_3| + |R_2 \cap R_3| - |R_1 \cap R_2 \cap R_3|.$$

Ki kell tehát számítanunk a halmazok páronkénti metszeteinek, valamint a három halmaz metszetének elemszámát. Lévén 2 és 3 relatív prím, $R_1 \cap R_2$ pontosan azokat az U-beli számokat tartalmazza, amelyek 6-tal oszthatóak, ilyenből pedig $\frac{360}{6} = 60$ van. Hasonló meggondolással kapjuk az $R_1 \cap R_3, R_2 \cap R_3$ és az $R_1 \cap R_2 \cap R_3$ halmazokat illetve elemszámukat:

$$R_1 \cap R_2 = \{a \in U : 2 \mid a \text{ és } 3 \mid a\} = \{a \in U : 6 \mid a\}, \qquad |R_1 \cap R_2| = \tfrac{360}{6} = 60;$$

$$R_1 \cap R_3 = \{a \in U : 2 \mid a \text{ és } 5 \mid a\} = \{a \in U : 10 \mid a\}, \qquad |R_1 \cap R_3| = \tfrac{360}{10} = 36;$$

$$R_2 \cap R_3 = \{a \in U : 3 \mid a \text{ és } 5 \mid a\} = \{a \in U : 15 \mid a\}, \qquad |R_2 \cap R_3| = \tfrac{360}{15} = 24;$$

$$R_1 \cap R_2 \cap R_3 = \{a \in U : 2 \mid a \text{ és } 3 \mid a \text{ és } 5 \mid a\} = \{a \in U : 30 \mid a\}, \quad |R_1 \cap R_2 \cap R_3| = \tfrac{360}{30} = 12.$$

Mindezeket behelyettesítve a szita-formulába, megkapjuk $\varphi(360)$ értékét:

$$\varphi(360) = 360 - 180 - 120 - 72 + 60 + 36 + 24 - 12 = 96.$$

Ha nem számolunk ki mindent, akkor megfigyelhetjük, hogyan alakul $\varphi(m)$ képlete ebben a speciális esetben:

$$\begin{aligned}\varphi(360) &= 360 - \frac{360}{2} - \frac{360}{3} - \frac{360}{5} + \frac{360}{2\cdot 3} + \frac{360}{2\cdot 5} + \frac{360}{3\cdot 5} - \frac{360}{2\cdot 3\cdot 5} = \\ &= 360 \cdot \left(1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{5} + \frac{1}{2\cdot 3} + \frac{1}{2\cdot 5} + \frac{1}{3\cdot 5} - \frac{1}{2\cdot 3\cdot 5}\right) = \\ &= 360 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right).\end{aligned}$$

A legutolsó lépés, a szorzattá alakítás, egy kicsit trükkösnek tűnhet. Könnyebb követni, ha jobbról balra olvassuk: az $\left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right)$ szorzatban bontsuk fel a zárójeleket (szorozzunk össze „mindenkit mindenkivel”), és figyeljük meg, hogy valóban a középső sorban álló kifejezést kapjuk. Ha ez már stimmel, akkor gondolkodjunk el azon, hogy hogyan fest az $\left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right)$ szorzat hasonló kifejtése. (Hány tagja lesz, és hogy néz ki egy tipikus tag?)

Tétel

Tetszőleges $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ prímhatványtényezős alakban megadott természetes szám esetén

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdot \ldots \cdot (p_k^{\alpha_k} - p_k^{\alpha_k - 1}).$$

Megjegyzés

Annak a valószínűsége, hogy az $U = \{1, \ldots, n\}$ halmaz egy véletlenszerűen kiválasztott eleme relatív prím n-hez:

$$\frac{\varphi(n)}{n} = \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right).$$

Ez nem meglepő, mert $1 - \frac{1}{p_i}$ annak a valószínűsége, hogy az adott elem nem osztható p_i-vel, és az „n-hez relatív prímnek lenni” esemény épp ezeknek az eseményeknek a szorzata.

$\{1,2,3,4,5,6,7\} = U$

2-vel osztva: $\frac{3}{7}$

3-mal osztva: $\frac{2}{7}$

6-tal osztva: $\frac{1}{7} \neq \frac{3}{7} \cdot \frac{2}{7}$

Példák

- $\varphi(1000) = \varphi(2^3 \cdot 5^3) = (2^3 - 2^2) \cdot (5^3 - 5^2) = 4 \cdot 100 = 400$
- $\varphi(360) = \varphi(2^3 \cdot 3^2 \cdot 5) = (2^3 - 2^2) \cdot (3^2 - 3) \cdot (5 - 1) = 4 \cdot 6 \cdot 4 = 96$
- $\varphi(2021) = \varphi(43 \cdot 47) = (43 - 1) \cdot (47 - 1) = 42 \cdot 46 = 1932$

Tétel

A komplex számok körében a primitív n-edik egységgyökök száma $\varphi(n)$.

Bizonyítás.

Az n-edik egységgyökök a következők:

$$\varepsilon_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} \qquad (k = 0, \ldots, n-1).$$

Tudjuk, hogy ε_k akkor és csak akkor primitív n-edik egységgyök, ha k relatív prím n-hez. Az ilyen k értékek száma pedig éppen $\varphi(n)$. ■

Tétel

Ha n gyöngyből fűzünk nyakláncot és k-féle különböző színű gyöngyből választhatunk, akkor a lehetséges nyaklánok száma:

$$\frac{1}{n}\sum_{d|n}\varphi(d)k^{\frac{n}{d}}.$$

Tartalom

Euler–Fermat-tétel

Ha az a egész szám relatív prím az m modulushoz, akkor

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

Kis Fermat-tétel

Ha p prímszám, akkor

- $p \nmid a$ esetén $a^{p-1} \equiv 1 \pmod{p}$;
- minden a egész számra $a^p \equiv a \pmod{p}$.

Következmény

Tetszőleges $\overline{a} \in \mathbb{Z}_m^*$ redukált maradékosztályra $o(\overline{a}) \mid \varphi(m)$.

Példa

Mennyit ad 11-gyel osztva maradékul 123^{765}?

$123 \equiv 2 \pmod{11} \Longrightarrow 123^{765} \equiv 2^{765} \pmod{11}$

$\gcd(2,11) = 1$ ✓ $\quad \varphi(11) = 10$

$765 = 5 + 76 \cdot 10$

$2^{765} \equiv 2^{5+76\cdot 10} \equiv 2^5 \cdot (2^{10})^{76} \equiv 2^5 \cdot 1^{76} \equiv 2^5 \equiv 32 \equiv 10 \pmod{11}$

$765 \equiv 5 \pmod{\varphi(11)}$

$2^{10} \equiv 1 \pmod{11}$ (Fermat)

Következmény

Ha az a egész szám relatív prím az m modulushoz, akkor tetszőleges $k, \ell \in \mathbb{Z}$ kitevők esetén

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

Biz:

$k \equiv \ell \pmod{\varphi(m)} \Rightarrow k = \ell + \varphi(m) \cdot t \quad (\exists t \in \mathbb{Z})$

$a^k \equiv a^{\ell + \varphi(m) \cdot t} \equiv a^\ell \cdot \underbrace{\left(a^{\varphi(m)}\right)^t}_{\text{III EF}} \equiv a^\ell \cdot 1^t \equiv a^\ell \pmod{m}$ ∎

1

Példa

Mennyit ad 44-gyel osztva maradékul 4447^{2018}?

$4447 = 4444 + 3 \equiv 3 \pmod{44} \Rightarrow 4447^{2018} \equiv 3^{2018} \pmod{44}$

$\text{lnko}(3,44) = 1$ ✓ $\quad \varphi(44) = \varphi(2^2 \cdot 11) = (2^2 - 2) \cdot (11 - 1) = 20$

$2018 \equiv 18 \equiv -2 \pmod{20} \Rightarrow 3^{2018} \equiv 3^{18} \equiv 3^{-2} \equiv 9^{-1} \equiv 5 \pmod{44}$

9^{-1} = x

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

$9x \equiv 45 \pmod{44} \quad / : 9 \quad \text{lnko}(9,44) = 1$

$x \equiv 5 \pmod{44}$

Tartalom

Euler–Fermat-tétel

Minden $\overline{a} \in \mathbb{Z}_m^*$ esetén $\overline{a}^{\varphi(m)} = \overline{1}$.

Példa

Legyen $m = 9$ és $a = 2$. Soroljuk fel $\mathbb{Z}_9^*$ elemeit:

$$\{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\} = \mathbb{Z}_9^*.$$

Szorozzuk meg mindegyik elemet $\overline{2}$-sal:

$$\{\overline{2}, \overline{4}, \overline{8}, \overline{1}, \overline{5}, \overline{7}\} = \mathbb{Z}_9^*.$$

A két halmaz megegyezik, ezért elemeik szorzatai is megegyeznek:

$$\overline{1} \cdot \overline{2} \cdot \overline{4} \cdot \overline{5} \cdot \overline{7} \cdot \overline{8} = \overline{2} \cdot \overline{4} \cdot \overline{8} \cdot \overline{1} \cdot \overline{5} \cdot \overline{7} = (\overline{2} \cdot \overline{1}) \cdot (\overline{2} \cdot \overline{2}) \cdot (\overline{2} \cdot \overline{4}) \cdot (\overline{2} \cdot \overline{5}) \cdot (\overline{2} \cdot \overline{7}) \cdot (\overline{2} \cdot \overline{8}).$$

Egyszerűsítés után kapjuk, hogy

$$\overline{1} = \overline{2} \cdot \overline{2} \cdot \overline{2} \cdot \overline{2} \cdot \overline{2} \cdot \overline{2} = \overline{2}^6 = \overline{2}^{\varphi(9)}.$$

Euler–Fermat-tétel

Minden $\overline{a} \in \mathbb{Z}_m^*$ esetén $\overline{a}^{\varphi(m)} = \overline{1}$.

Bizonyítás.

Az alábbi két leképezés egymás inverze, ezért mindkettő bijekció:

$$\mathbb{Z}_m^* \to \mathbb{Z}_m^*,\ \overline{x} \to \overline{a} \cdot \overline{x}; \qquad \mathbb{Z}_m^* \to \mathbb{Z}_m^*,\ \overline{x} \to \overline{a}^{-1} \cdot \overline{x}.$$

Ebből következik, hogy ha $\mathbb{Z}_m^*$ elemeit rendre megszorozzuk $\overline{a}$-sal, akkor ugyanazokat az elemeket kapjuk, csak esetleg más sorrendben. Mivel a szorzás kommutatív és asszociatív, az elemek szorzata ugyanaz marad:

$$\prod_{\overline{x} \in \mathbb{Z}_m^*} \overline{x} = \prod_{\overline{x} \in \mathbb{Z}_m^*} (\overline{a} \cdot \overline{x}) = \overline{a}^{\varphi(m)} \cdot \prod_{\overline{x} \in \mathbb{Z}_m^*} \overline{x}.$$

Egyszerűsítés után kapjuk, hogy

$$\overline{1} = \overline{a}^{\varphi(m)}.$$

■