MBLK13E: Számelmélet - Hatványozás modulo m

(előadásvázlat, 2024. április 7.)

Kátai-Urbán Kamilla

1. Az Euler-féle φ függvény

1. Definíció. Tetszőleges n természetes szám esetén legyen $\varphi(n) = |\mathbb{Z}_n^*|$, ahol $\mathbb{Z}_n^*$ a mod n redukált maradékosztályok halmazát jelöli, ahogy ezt már korábban bevezettük. Azaz a következőképpen is felírható: $\varphi(n) = |\{a \in \mathbb{N} : 1 \leq a \leq n \text{ és } \operatorname{lnko}(a,n) = 1\}|$. Az így definiált $\varphi\colon \mathbb{N} \to \mathbb{N}$ függvényt Euler-féle φ függvénynek nevezzük.

2. Példa. A definíció alapján:

(a) $\varphi(5) = |\mathbb{Z}_5^*| = |\{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}| = 4$;
(b) $\varphi(6) = |\mathbb{Z}_6^*| = |\{\overline{1}, \overline{5}\}| = 2$;
(c) $\varphi(8) = |\mathbb{Z}_8^*| = |\{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}| = 4$;
(d) $\varphi(1024) = |\mathbb{Z}_{1024}^*| = |\{\overline{1}, \overline{3}, \overline{5}, \ldots \overline{1023}\}| = 1024/2 = 512$.

3. Tétel. Az Euler-féle φ függvény gyengén multiplikatív, azaz $\operatorname{lnko}(m,n) = 1$ esetén $\varphi(mn) = \varphi(m)\varphi(n)$.

4. Tétel. Legyen az n természetes szám prímtényezős felbontása $n = \prod_{i=1}^{k} p_i^{\alpha_i}$. Ekkor

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

5. Példa. A második számolási szabályt használva:

(a) $\varphi(100) = \varphi(2^2 \cdot 5^2) = (2^2 - 2) \cdot (5^2 - 5) = 2 \cdot 20 = 40$;
(b) $\varphi(2023) = \varphi(7 \cdot 17^2) = (7-1) \cdot (17^2 - 17) = 6 \cdot 272 = 1632$.

6. Tétel. Minden n természetes szám esetén $\sum_{d|n} \varphi(d) = n$.

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

8. Tétel (Euler–Fermat-tétel). Ha az a egész szám és $\operatorname{lnko}(a,m) = 1$, akkor $a^{\varphi(m)} \equiv 1 \pmod{m}$.

9. Következmény. Ha $a \in \mathbb{Z}$ relatív prím az m modulushoz és $k, \ell \in \mathbb{Z}$, akkor $k \equiv \ell \pmod{\varphi(m)} \Longrightarrow a^k \equiv a^\ell \pmod{m}$.

10. Példa. A 7. és 8. Tételek segítségével könnyebben tudunk nagy hatványokat számolni. Például, ha meg szeretnénk határozni a 3^{204} szám utolsó két számjegyét, azaz meg szeretnénk oldani a $3^{204} \equiv x \pmod{100}$ kongruenciát, akkor alkalmazhatjuk a 8. Tételt, hiszen $\operatorname{lnko}(3,100) = 1$. Az 5. Példában kiszámoltuk, hogy $\varphi(100) = 40$, tehát az Euler–Fermat tétel szerint $3^{40} \equiv 1 \pmod{100}$. Mivel a kitevő $204 = 40 \cdot 5 + 4$, így a hatványozás azonosságait és az Euler–Fermat tételt felhasználva:

$$3^{204} = 3^{40 \cdot 5 + 4} = (3^{40})^5 \cdot 3^4 \equiv 1^5 \cdot 3^4 = 3^4 = 81 \pmod{100}.$$

Tehát 3^{204} szám utolsó két számjegye 81.

2. Primitív gyök, index

11. Definíció. Legyen $a \in \mathbb{Z}$ relatív prím az m modulushoz. Ekkor az a szám modulo m rendjén az $\overline{a} \in \mathbb{Z}_m^*$ maradékosztály rendjét értjük (a $\mathbb{Z}_m^*$ multiplikatív csoportban). Jelölés: $o_m(a)$.

12. Állítás. Tetszőleges $a \in \mathbb{Z}$ és $m \geq 2$ természetes szám esetén, ha $\operatorname{lnko}(a,m) = 1$, akkor $o_m(a) \mid \varphi(m)$.

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

14. Állítás. A g egész szám akkor és csak akkor primitív gyök modulo m, ha az összes modulo m redukált maradékosztály megkapható $\overline{g}$ hatványaként.

15. Példa. Meghatározzuk az $1, 3, 7, 9$ elemek rendjét modulo 10. Természetesen az 1 rendje 1. Mivel $[\overline{3}] = \mathbb{Z}_{10}^*$, így $o_{10}(3) = 4 = \varphi(10)$, hasonlóan $o_{10}(7) = 4 = \varphi(10)$. Továbbá $\overline{9}^2 = \overline{1}$, így $o_{10}(9) = 2$. Tehát 3 és 7 primitív gyökök modulo 10. Mivel találtunk primitív gyököt, amelynek hatványaiként $\mathbb{Z}_{10}^*$ minden eleme megkapható, így $\mathbb{Z}_{10}^*$ ciklikus csoport. A következő tétel leírja, hogy mely m-ek esetén találnuk primitív gyököt modulo m, azaz mikor lesz $\mathbb{Z}_m^*$ ciklikus csoport.

16.* Tétel. Akkor és csak akkor létezik primitív gyök az m modulushoz (vagyis a $\mathbb{Z}_m^*$ csoport akkor és csak akkor ciklikus), ha $m = 2$, 4, p^α, $2p^\alpha$, ahol p páratlan prímszám és $\alpha \in \mathbb{N}$.

17. 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: $\operatorname{ind}_g a$ (a modulus többnyire világos a szövegkörnyezetből).

18. 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 az 14. Állítás szerint a előáll g hatványaként modulo m, tehát ekkor $\operatorname{ind}_g a$ értelmezett.

19. Példa. A 2 szám primitív gyök modulo 11, tehát $\mathbb{Z}_{11}^*$ elemei felírhatók $\overline{2}$ hatványaiként. Például $a = 5$ esetén $\overline{2}^4 = \overline{16} = \overline{5}$, tehát $\operatorname{ind}_2 5 = 4$. Hasonlóan $a = 10$ esetén $\overline{2}^5 = \overline{2}^4 \cdot \overline{2} = \overline{5} \cdot \overline{2} = \overline{10}$, tehát $\operatorname{ind}_2 10 = 5$. Ha az összes a értékhez meghatározzuk az index értékét, és táblázatba fogalaljuk, akkor megkapjuk a következő úgynevezett indextáblázatot:

a	1	2	3	4	5	6	7	8	9	10
$\operatorname{ind}_2 a$	10	1	8	2	4	9	7	3	6	5

Megfigyelhető, hogy az index hasonlóan számolható, mint a logaritmus, így nem véletlen, hogy a következő tételben az indexre vonatkozó azonosságok nagyon emlékeztetnek a logaritmusnál tanult azonosságokra.

20. 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) $\operatorname{ind}_g a^n \equiv n \cdot \operatorname{ind}_g a \pmod{\varphi(m)}$.

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

22. Tétel. Legyen g primitív gyök modulo m, és legyen a relatív prím m-hez. Ekkor a pontosan akkor n-edik hatványmaradék modulo m, ha $\operatorname{lnko}(n, \varphi(m)) \mid \operatorname{ind}_g a$.

23. Példa. Megoldjuk az $x^8 \equiv 4 \pmod{11}$ kongruenciát. A 19. Példában felírtuk a 2 primitív gyök indextáblázatát (modulo 11), ahonnan leolvasható, hogy $\operatorname{ind}_2 4 = 2$, tehát a 22. Tétel alapján megoldható a kongruencia, hiszen $\operatorname{lnko}(8, \varphi(11)) = 2 \mid \operatorname{ind}_2 4 = 2$. Tehát a kongruencia mindkét oldalát felírtuk 2 hatványként, mivel $\overline{2}^2 = \overline{4}$ és $x^8 = (2^y)^8 = 2^{8y}$, tehát a kongruencia $2^{8y} \equiv 2^2 \pmod{11}$ alakú. Mivel 2 primitív gyök modulo 11, így a rendje $\varphi(11) = 10$, a rendnél tanult tétel alapján az előző kongruencia pontosan akkor teljesül, ha a kitevőkre érvényes, hogy $8y \equiv 2 \pmod{10}$, ahol a modulus $\varphi(11) = 10$. Megfigyelhetjük, hogy a 22. Tételben éppen ennek a kongruenciának a megoldhatósága szerepel feltételként. Az előző kongruenciát megoldva kapjuk, hogy $y \equiv 4 \pmod{5}$, figyeljünk arra, hogy változott a modulus. Visszaírva modulo 10, $y \equiv 4 \pmod{10}$, $y \equiv 9 \pmod{10}$ a megoldások. Tehát $x \equiv 2^4 \pmod{11}$, $x \equiv 2^9 \pmod{11}$. Az x értéke a 19. Példában szereplő indextáblázatból leolvasható, ugyanis a 4 felett az 5 szerepel, és a 9 felett pedig 6, tehát $x \equiv 5 \pmod{11}$, $x \equiv 6 \pmod{11}$.

3. Négyzetes maradékok, Legendre-szimbólum

24. 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 nem-maradék modulo m.

25. Tétel. Legyen p páratlan prímszám és 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.

26. 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:

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

(Szóban az $\left(\frac{a}{p}\right)$ formulát „a per p Legendre-szimbólum”-nak olvassuk ki.)

27. Megjegyzés. Ha p páratlan prím és $p \nmid a$, akkor $\left(\frac{a^2}{p}\right) = 1$, jól látszik, hogy a megoldása az $x^2 \equiv a^2 \pmod p$ kongruenciának.

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

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

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

30. Tétel. Tetszőleges p páratlan prímszám esetén

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

31.* Tétel. Tetszőleges p páratlan prímszámra

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

32.* Tétel (Négyzetes reciprocitási tétel). Tetszőleges p, q különböző páratlan prímszámok esetén

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

33. Megjegyzés. Az $\left(\frac{a}{p}\right)$ Legendre-szimbólum meghatározásakor a következő lépéseket hajtjuk végre.

- 1. lépés: Ha $a > p$ akkor a redukáljuk a 29. Tétel (1) része segítségével a-t modulo p.
- 2. lépés: Ha $a = -1$, $a = 2$, használjuk a 30. és 31. Tételt. Ha a négyzetszám, akkor a 27. Megjegyzés szerint számolunk.
- 3. lépés: Ha a összetett szám, akkor bontsuk szorzattá a 29. Tétel (2) része alapján, és számoljuk ki külön a tényezőket.
- 4. lépés: Ha a prímszám, akkor a 32. Tétel segítségével „fordítsuk fejre” (ld. 34. Példa).
- 5. lépés: Kezdjük előről az eljárást.

34. Példa. Határozzuk meg a $\left(\frac{75}{53}\right)$ Legendre-szimbólumot. Alkalmazzuk előaszőr az előző megjegyzés 1. lépését: $75 \equiv 22 \pmod{53}$, majd a 3. lépést, tehát $\left(\frac{75}{53}\right) = \left(\frac{22}{53}\right) = \left(\frac{2}{53}\right)\left(\frac{11}{53}\right)$. A 31. Tétel alapján $\left(\frac{2}{53}\right) = (-1)^{\frac{53^2-1}{8}} = -1$. A $\left(\frac{11}{53}\right)$ tényező esetén pedig használhatjuk a 4. lépést, azaz a 32. Tétel (Négyzetes reciprocitási tétel) alapján $\left(\frac{11}{53}\right)\left(\frac{53}{11}\right) = (-1)^{\frac{11-1}{2}\frac{53-1}{2}} = 1$. Tehát $\left(\frac{11}{53}\right) = \left(\frac{53}{11}\right)$, ezt hívtuk úgy a 4. lépésben, hogy „fordítsuk fejre”. (Természetesen, ha $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1$, akkor $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.) Összegezve az eddigieket $\left(\frac{75}{53}\right) = -\left(\frac{53}{11}\right)$, így ismét használhatjuk az 1. lépést. Mivel $53 \equiv 9 \pmod{11}$, és a 9 négyzetszám, a 27. Megjegyzés szerint $\left(\frac{53}{11}\right) = \left(\frac{9}{11}\right) = 1$. Így $\left(\frac{75}{53}\right) = -\left(\frac{53}{11}\right) = -1$, tehát 75 négyzetes nemmaradék modulo 53.