

Rend és primitív gyök

Kovács Benedek foglalkozása

Rend

Definíció — Adott a és n egészek esetén legyen a rendje modulo n az a legkisebb m pozitív egész, amire $a^m \equiv 1 \pmod{n}$. Jelölés: $\text{ord}_n(a)$.

Állítás. $\text{ord}_n(a)$ pontosan akkor létezik, ha $(a, n) = 1$. És ekkor $\text{ord}_n(a) \mid \varphi(n)$.

- F/1.** Legyen p prímszám. Mutassuk meg, hogy $2^p - 1$ minden prímosztója nagyobb p -nél.
- F/2.** Legyenek $a \geq 2$ és $n \geq 1$ egészek. Bizonyítsd be, hogy n osztja $\varphi(a^n - 1)$ -et.
- F/3.** Legyen $n \geq 1$ egész. Mutassuk meg, hogy $2^{2^n} + 1$ minden osztója $k \cdot 2^{n+1} + 1$ alakú valamilyen egész k -ra.
- F/4.** Legyen $p = 4k - 1$ prím és $k \in \mathbb{N}$. Mutassuk meg, hogy ha az a egészre van megoldása az $x^2 \equiv a \pmod{p}$ kongruenciának, akkor a megoldásai $x = \pm a^k$.
- F/5.** Legyen p prím és $n \geq 1$ egész. Bizonyítsuk be, hogy ha $p \mid 2^n - 1$, akkor $p \mid 2^{p-1} - 1$.
Azt mondjuk egy A egészre és $k \geq 0$ kitevőre, hogy $p^k \mid A$ (azaz p^k pontosan osztja A -t), ha $p^k \mid A$ és $p^{k+1} \nmid A$.
- F/6.** * Határozzuk meg az összes olyan, prímekből álló (p, q, r) számhármast, melyre teljesül $p \mid q^r + 1$, $q \mid r^p + 1$ és $r \mid p^q + 1$.
- F/7.** * Határozzuk meg azokat az (n, k) pozitív egészekből álló számpárokat, amelyekre

$$\frac{(2^{2^n} + 1)(2^{2^k} + 1)}{nk} \in \mathbb{Z}.$$

- F/8.** * (IMO 1990/3.) Mely $n \geq 1$ egészekre teljesül, hogy $n^2 \mid 2^n + 1$?

Primitív gyök

Definíció — Ha adott egy n pozitív egész, akkor *primitív gyöknek* nevezünk egy g redukált maradékosztályt modulo n , ha az $1, g, g^2, \dots, g^{\varphi(n)-1}$ felsorolás a modulo n redukált maradékkrendszer összes eleméből áll.

Ezzel ekvivalensen: g primitív gyök mod $n \Leftrightarrow \text{ord}_n(g) = \varphi(n)$.

- F/9.** Mik a primitív gyökök modulo 7? És modulo 8? Ha létezik primitív gyök mod n , akkor hány darab van?

2025. október 24.

Szakkörvezető: Kovács Benedek (benoke981@gmail.com)

- F/10.** Legyen $n \geq 1$ egész, és $p > n + 1$ prím. Igazoljuk, hogy $p \mid 1^n + 2^n + \dots + (p-1)^n$.
- F/11.** Primitív gyök felhasználásával lássuk be a Wilson-tételt.
- F/12.** Legyen $p \geq 11$ prím. Bizonyítsuk be, hogy léteznek $m, n \geq 1$ egészek úgy, hogy $m+n < p$ és $p \mid 5^m 7^n - 1$.
- F/13.** (Lekötő) **a)** Legyen $p \geq 3$ prím, $k \geq 1$ egész és $y \in \mathbb{Z}$. Igazoljuk, hogy ha $x \equiv 1 + p^k y \pmod{p^{k+1}}$, akkor $x^p \equiv 1 + p^{k+1} y \pmod{p^{k+2}}$.
- b)** * Legyen $p \geq 3$ prím. Bizonyítsuk be, hogy ha g primitív gyök mod p és $g^{p-1} \not\equiv 1 \pmod{p^2}$, akkor g primitív gyök mod p^k minden $k \geq 1$ egészre.
- F/14.** (Lekötő) Legyen $\alpha \geq 3$ egész. Igazoljuk, hogy
- a)** $\text{ord}_{2^\alpha}(5) = 2^{\alpha-2}$,
- b)** a $\pm 5^k$ ($0 \leq k < 2^{\alpha-2}$) számok redukált maradékrendszer alkotnak mod 2^α .

Tétel. Pontosán akkor létezik primitív gyök mod n , ha $n = 2, 4, p^k, 2p^k$. (Ahol p páratlan prím és $k \geq 1$ egész.)

Kvadratikus maradékok

Definíció — Legyen $p \geq 3$ prím, a redukált maradékosztály mod p . Azt mondjuk, hogy a *kvadratikus maradék* mod p , ha létezik x egész, melyre $x^2 \equiv a \pmod{p}$. Különben a *kvadratikus nemmaradék* mod p .

- F/15.** Legyen $p \geq 3$ prím.
- a)** Számoljuk meg a kvadratikus maradékokat és nemmaradékokat mod p .
- b)** Bizonyítsuk be, hogy két kvadratikus maradék szorzata kvadratikus maradék; maradék és nemmaradék szorzata nemmaradék; két nemmaradék szorzata maradék.
- F/16.** Bizonyítsuk be primitív gyök segítségével, hogy ha p páratlan prím, akkor -1 pontosan akkor kvadratikus maradék mod p , ha $p \equiv 1 \pmod{4}$.
- F/17.** Mely p prímszámok és n pozitív egészek esetén igaz, hogy mod p minden maradékosztályból lehet n -edik gyököt vonni (azaz minden $x \in \{0, 1, \dots, p-1\}$ -re létezik $y \in \{0, 1, \dots, p-1\}$, melyre $y^n \equiv x \pmod{p}$)?
- F/18.** * (IMO 2003/6.) Adott egy p prím. Bizonyítsuk be, hogy létezik q prím, melyre nincs a egész, hogy $q \mid a^p - p$.

2025. október 24.

Szakkörvezető: Kovács Benedek (benoke981@gmail.com)