Számelmélet 2.

Kovács Benedek szakköre

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

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

F/1. Legyen $n \geq 1$ egész, és $p > n+1$ prím. Igazoljuk, hogy $p \mid 1^n + 2^n + ... + (p-1)^n$.

F/2. Bizonyítsuk be primitív gyök segítségével, hogy ha p páratlan prím, akkor $x^2 \equiv -1 \pmod{p}$ pontosan akkor oldható meg, ha $p \equiv 1 \pmod{4}$.

F/3. 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/4. **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/5. 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 maradékrendszert alkotnak mod 2^α.

F/6. 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/7. Legyen $f : \mathbb{Z}^+ \to \mathbb{Z}^+$ egy olyan függvény, amire:

(1) $(m, n) = 1 \Rightarrow (f(m), f(n)) = 1$, és

(2) minden n-re $n \leq f(n) \leq n + 2023$.

Bizonyítsuk be, hogy minden $n \geq 1$ egészre és p prímre teljesül, hogy ha $p \mid f(n)$, akkor $p \mid n$.

2023. december 9.

Szakkörvezető: Kovács Benedek (benoke981@gmail.com)

Az Olimpiai Iskola email címe: olimpiai.iskola@gmail.com

OLIMPIAI ISKOLA

SZAKKÖR

Számelmélet 2.

Kovács Benedek szakköre

Házi feladatok

Beadási határidő: 2023. december 17. (vasárnap)

HF/1. (=október 28-i feladatsor, **F/26.**) Bizonyítsd be, hogy ha p prím, akkor $2^p - 1$ minden prímosztója p-nél nagyobb.

HF/2. Legyenek $n \geq 1$ és $k \geq 2$ egészek, valamint $a_1, a_2, ..., a_k$ különböző 1 és n közti egészek. Tudjuk, hogy minden i-re ($1 \leq i \leq k-1$) teljesül, hogy $n \mid a_i(a_{i+1} - 1)$. Mutassuk meg, hogy $n \nmid a_k(a_1 - 1)$.

HF/3. Anna és Balázs játszanak. Anna kezd, és felváltva választanak 1 és 9 közti számjegyeket, amíg a végén ki nem jön egy hétjegyű szám: $\overline{A_1B_2A_3B_4A_5B_6A_7}$, ahol A-val az Anna és B-vel a Balázs által választott számjegyeket jelöltük. Anna nyer, ha a kapott hétjegyű szám egy teljes hetedik hatvány utolsó hét számjegyével egyezik meg. Különben pedig Balázs nyer. Kinek van nyerő stratégiája?

HF/4. (=**F/6.**) Legyen $p \geq 11$ prím. Bizonyítsuk be, hogy léteznek $m, n \geq 1$ egészek úgy, hogy $m + n < p$ és $p \mid 5^m 7^n - 1$.

2023. december 9.
Szakkörvezető: Kovács Benedek (benoke981@gmail.com)
Az Olimpiai Iskola email címe: olimpiai.iskola@gmail.com