

Kongruenciák, kvadratikus maradékok

Kovács Benedek foglalkozása

Kongruenciák

Definíció • Legyenek a, b, m egész számok, $m \geq 1$. Azt mondjuk, hogy a és b *kongruens* modulo m , ha a és b ugyanazt a maradékot adják m -mel osztva. Jelölése: $a \equiv b \pmod{m}$, vagy röviden: $a \equiv b \pmod{m}$.

- $a \equiv b \pmod{m}$ pontosan akkor, ha $m \mid a - b$.

Definíció Legyen $m \geq 1$ egész. $\varphi(m)$ az olyan $1 \leq a \leq m$ számok száma, amire $(a, m) = 1$.

Definíció • Legyen $m \geq 1$. Modulo m *teljes maradékrendszernek* (TMR_m) nevezünk egy olyan m elemű számhalmazt, melynek elemei mind különböző maradékot adnak m -mel osztva.

- Legyen $m \geq 1$. Modulo m *redukált maradékrendszernek* (RMR_m) nevezünk egy olyan $\varphi(m)$ elemű számhalmazt, amelynek tagjai mind relatív prímek m -hez, és mind különböző maradékot adnak m -mel osztva.

Például $\{1, 15, 20, 26\}$ egy TMR_4 , és $\{-7, 61\}$ egy RMR_6 .

F/1. Tegyük fel, hogy az $\overline{abc}$ háromjegyű szám osztható 37-tel. Mutassuk meg, hogy ekkor $\overline{bca}$ is osztható 37-tel.

F/2. a) Legyen $a \equiv b \pmod{m}$ és $c \equiv d \pmod{m}$. Igazoljuk, hogy $a + c \equiv b + d \pmod{m}$, $a - c \equiv b - d \pmod{m}$ és $ac \equiv bd \pmod{m}$.

b) Miért nem igaz, hogy $ac \equiv bc \pmod{m} \Rightarrow a \equiv b \pmod{m}$? Javítsuk meg az állítást.

F/3. a) Ha $\{t_1, t_2, \dots, t_m\}$ TMR_m , és $(a, m) = 1$, akkor $\{at_1, at_2, \dots, at_m\}$ is TMR_m .

b) Ha $\{t_1, t_2, \dots, t_{\varphi(m)}\}$ RMR_m és $(a, m) = 1$, akkor $\{at_1, at_2, \dots, at_{\varphi(m)}\}$ is RMR_m .

c) Adjunk szükséges és elégséges feltételt arra, hogy a -nak létezzen *inverze* modulo m , vagyis létezik olyan b , hogy $ab \equiv 1 \pmod{m}$. (Ekkor b helyett írhatunk a^{-1} -et, vagy $\frac{1}{a}$ -t.)

d) Legyen $(b, m) = (d, m) = 1$. Igazoljuk, hogy $\frac{a}{b} \cdot \frac{c}{d} \equiv \frac{ac}{bd} \pmod{m}$ és $\frac{a}{b} + \frac{c}{d} \equiv \frac{ad+bc}{bd} \pmod{m}$.

F/4. a) Minden $n > 2$ -re $\varphi(n)$ páros.

b) Ha $(m, n) = 1$, akkor $\varphi(mn) = \varphi(m)\varphi(n)$.

c) Mennyi $\varphi(1200)$?

d) Igazoljuk, hogy $\sum_{d|n} \varphi(d) = n$.

F/5. Mennyi $7!$ maradéka mod 17? Hogyan számolnád ki "gyorsan" 7^{21} maradékát mod 101?

2025. december 28.

Szakkörvezető: Kovács Benedek (benoke981@gmail.com)

F/6. Bizonyítsuk az alábbi tételeket.

- Tétel.**
- (Euler-Fermat-tétel) Legyen $a \in \mathbb{Z}$, $m \in \mathbb{Z}^+$, $(a, m) = 1$. Ekkor $a^{\varphi(m)} \equiv 1 \pmod{m}$.
 - (kis Fermat-tétel) Legyen $a \in \mathbb{Z}$, p prím, $(a, p) = 1$. Ekkor $a^{p-1} \equiv 1 \pmod{p}$.

F/7. Mennyi $2^{61} \pmod{13}$? És $2^{67} \pmod{71}$? Hogyan számolnád ki "gyorsan" $7^{521} \pmod{101}$?

F/8. * Legyen $p \geq 5$ prím. Bizonyítsuk be, hogy $1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{p-1}$ legegyszerűbb alakjában a számláló osztható p^2 -tel.

F/9. * Legyen P a pozitív prímek halmaza. Tudjuk, hogy $M \subseteq P$ egy legalább 3 elemű halmaz, melynek minden $A \subsetneq M$ véges valódi részhalmazára $n_A := -1 + \prod_{p \in A} p$ minden prímosztója M -beli. Lássuk be, hogy $M = P$.

F/10. * (IMO SL 2015/N3) Legyenek $m > n \geq 1$ egészek. Legyen minden $k \in \{1, 2, \dots, n+1\}$ -re $x_k = \frac{m+k}{n+k}$. Igazoljuk, hogy ha $x_1, x_2, \dots, x_{n+1}$ mind egészek, akkor $x_1 x_2 \dots x_{n+1} - 1$ nem lehet 2-hatvány.

Lineáris kongruenciák

F/11. Oldjuk meg az alábbi kongruenciákat:

(a) $3x \equiv 7 \pmod{16}$, (b) $26x \equiv 39 \pmod{46}$, (c) $24x + 5 \equiv 65 \pmod{51}$.

F/12. Határozzuk meg 5 inverzét mod 26.

F/13. Adjunk szükséges és elégséges feltételt arra, hogy $ax \equiv b \pmod{m}$ megoldható! ($a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$.) Ha megoldható, hány megoldása van mod m ?

Kvadratikus maradékok

Definíció Legyen $p \geq 3$ prím, $(a, p) = 1$. 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/14. Adjuk meg a kvadratikus maradékokat modulo 3, 5, 7, 11, 13.

F/15. Legyen $p \geq 3$ prím.

a) Számoljuk meg a kvadratikus maradékokat és nemmaradókat mod p .

b) Két kvadratikus maradék szorzata kvadratikus maradék; maradék és nemmaradék szorzata nemmaradék; két nemmaradék szorzata maradék. Maradék inverze maradék, nemmaradék inverze nemmaradék.

2025. december 28.

Szakkörvezető: Kovács Benedek (benoke981@gmail.com)

F/16. Legyen $p \geq 5$ prím. Mutassuk meg, hogy mod p a legkisebb kvadratikus nemmaradék értéke $< \sqrt{p} + 1$.

F/17. Az x és y egész számokra $x^2 + xy + y^2$ osztható 10-zel. Mutassuk meg, hogy ekkor 100-zal is osztható.

F/18. * Bizonyítsuk be, hogy -1 pontosan akkor kvadratikus maradék mod p , ha $p \equiv 1 \pmod{4}$.

Az alábbi feladatokhoz felhasználhatod, hogy minden p prímre létezik *primitív gyök* mod p , azaz olyan $g \in \mathbb{Z}$, melyre $\{g^0, g^1, \dots, g^{p-2}\} \equiv \{1, 2, \dots, p-1\} \pmod{p}$:

F/19. 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/20. * Legyen $p \geq 3$ prím. Hány (x, y) számpár teljesíti az $x^2 + y^2 \equiv -1 \pmod{p}$ kongruenciát, ahol $0 \leq x, y \leq p-1$?

2025. december 28.

Szakkörvezető: Kovács Benedek (benoke981@gmail.com)