

1. Legyenek $p \neq q$ prímek és legyen k pozitív egész. Mutassuk meg, hogy a $\mathbb{Z}_{p^k}$ gyűrűben minden elem osztható q -val.
2. Megoldható-e az $x^2 \equiv 3 \pmod{4}$ kongruencia?
3. Legyen $p \geq 2$ prím. Mutassuk meg, hogy $x \equiv x^{-1} \pmod{p}$ akkor és csak akkor, ha $p|(x-1)$ vagy $p|(x+1)$.
4. Az előző feladat alapján igazoljuk Wilson tételét: ha p prím, akkor $(p-1)! \equiv -1 \pmod{p}$.
5. Számítsuk ki:
(a) $\varphi(23)$, $\varphi(21)$, $\varphi(63)$, $\varphi(6!)$,
(b) $120^{24} \pmod{23}$, $115^{21} \pmod{21}$, $68^{111} \pmod{63}$, $111^{68} \pmod{63}$ (vigyázzunk, 111 nem relatív prím a 63-hoz).
6. Mutassuk meg, hogy tetszőleges a, b pozitív egészekre $\varphi(ab) \geq \varphi(a)\varphi(b)$.
7. Legyenek n, m pozitív egészek.
(a) Mutassuk meg, hogy az $f : \mathbb{Z}_{nm} \rightarrow \mathbb{Z}_n$, $f(k/\equiv_{nm}) = k/\equiv_n$ függvény szűrjektív gyűrű-homomorfizmus.
(b) Mutassuk meg, hogy a $g : \mathbb{Z}_n \rightarrow \mathbb{Z}_{mn}$, $g(k/\equiv_n) = km/\equiv_{mn}$ függvény injektív, megőrzi az összeadást, de általában nem gyűrű-homomorfizmus (nem őrz meg a szorzást).
8. **Racionális számok konstrukciója az egész számokból.**
Legyen $P = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, és legyen

$$R = \{ \langle (a_1, b_1), (a_2, b_2) \rangle \in P^2 : a_1 b_2 = a_2 b_1 \}.$$

- (a) Igazoljuk, hogy R egy ekvivalenciareláció.
- (b) Defináljuk P/R -en (azaz R ekvivalenciaosztályain) a $+^R$ összeadást így:

$$(a_1, b_1)/R +^R (a_2, b_2)/R \stackrel{Def.}{=} (a_1 b_2 + a_2 b_1, b_1 b_2)/R.$$

Mutassuk meg, hogy $+^R$ jóldefiniált.

- (c) Mutassuk meg, hogy az

$$f : P/R \rightarrow \mathbb{Z}, f((a, b)/R) \stackrel{Def.}{=} a/b$$

függvény jóldefiniált és izomorfizmus a $\langle P/R, +^R \rangle$ és $\langle \mathbb{Q}, + \rangle$ struktúrák között.