

A Wilson-tétel megfordításának bizonyítása:

Néhány számot kipróbálva hamar kialakul az a sejtésünk, hogy ha $n \neq 4$ összetett szám, akkor $(n-1)! \equiv 0 \pmod{n}$, azaz $n \mid (n-1)!$. A sejtés bizonyításához tekintsük n prímtényezőszorzat felbontását: $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$.

(1) Ha $k \geq 2$, azaz n -nek legalább két különböző prímosztója van, akkor azért lesz $(n-1)!$ osztható n -nel, mert az $1 \cdot 2 \cdot \dots \cdot (n-1)$ szorzatban fellépnek a ____, ____, ..., ____ számok, amelyek szorzata éppen n .

(2) Ha $k = 1$, azaz $n = p_1^{\alpha_1}$ prímtényező, akkor $\alpha_1 \geq 2$, mert n összetett szám. Vizsgáljuk külön az $\alpha_1 \geq 3$ és $\alpha_1 = 2$ eseteket.

(a) Ha $\alpha_1 \geq 3$, akkor azért lesz $(n-1)!$ osztható n -nel, mert az $1 \cdot 2 \cdot \dots \cdot (n-1)$ szorzatban fellép ____ és ____; ezen két szám szorzata pedig éppen $p_1^{\alpha_1} = n$.

(b) Ha $\alpha_1 = 2$, akkor a fenti gondolatmenet nem működik, mert ekkor $p_1 = p_1^{\alpha_1-1}$.

Két alesetet különböztetünk meg aszerint, hogy $p_1 > 2$ vagy $p_1 = 2$.

(i) Ha p_1 páratlan prím, akkor azért lesz $(n-1)!$ osztható n -nel, mert az $1 \cdot 2 \cdot \dots \cdot (n-1)$ szorzatban fellép ____ és ____; ezen két szám szorzata pedig $2p_1^2 = 2n$.

(ii) Végül, ha $p_1 = 2$, akkor $n = 4$, de ezt az esetet nem kell néznünk, mert feltettük, hogy $n \neq 4$. Ebben az esetben egyébként $(n-1)! \equiv 2 \pmod{4}$.

A fentieket Wilson tételével összekapcsolva a következőt kapjuk tetszőleges $n \geq 2$ természetes számra:

$$(n-1)! \equiv \begin{cases} -1, & \text{ha } n \text{ prímszám} \\ 0, & \text{ha } n \neq 4 \text{ összetett szám} \\ 2, & \text{ha } n = 4 \end{cases} \pmod{n}.$$