

Tétel. Ha $n > 4$ összetett szám, akkor $(n - 1)!$ osztható n -nel.

Biz. Tekintsük n prímszámhatványtényezős felbontását: $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_k^{e_k}$. Célunk az, hogy az $1 \cdot 2 \cdot 3 \cdot \dots \cdot (n - 1)$ szorzatban találjunk néhány tényezőt, amelyek szorzata n , vagy többszöröse n -nek. (Fontos, hogy ezek *különböző* számok legyenek. Például az $1 \cdot 2 \cdot 3$ szorzatban hiába van ott a 2 és a 2 is, ettől még a szorzat nem lesz osztható $2 \cdot 2$ -vel!)

Ha $k \geq 2$, azaz n -nek legalább két különböző prímszótója van, akkor a következő k db szám megfelelő lesz: Ezek mind kisebbek n -nél (és páronként különbözők), és szorzatuk éppen n .

Ha $k = 1$, akkor $n = p_1^{e_1}$, vagyis n prímszámhatvány. A jelölést egyszerűsítendő, hagyjuk az indexeket: $n = p^e$. Ekkor $e \geq 2$, mert n Vizsgáljuk külön az $e \geq 3$ és $e = 2$ eseteket.

Ha $e \geq 3$, akkor tekintsük a következő két számot: Ez két különböző szám, mindkettő kisebb n -nél, és szorzatuk éppen n .

Ha $e = 2$, azaz $n = p^2$, akkor a fenti gondolatmenet nem működik, mert ekkor fent megadott két szám egyenlő. Mivel, a p prímszám legalább 3, és emiatt a következő két szám megfelelő lesz: Ez két különböző szám, szorzatuk $2n$, és $p \geq 3$ miatt mindkettő kisebb, mint n .

□

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

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