

I. megoldás. Felhasználjuk a következő ismert tételt (lásd az 1. megjegyzést): ha m pozitív egész, és a, b, c egész számok, amelyekre teljesül, hogy $a^b \equiv 1 \pmod{m}$ és $a^c \equiv 1 \pmod{m}$, akkor $a^{(b,c)} \equiv 1 \pmod{m}$ is teljesül ((b, c) a b és c legnagyobb közös osztóját jelöli).

Legyen p az n legkisebb prímosztója ($n > 1$, tehát van neki). Megmutatjuk, hogy $p = 5$; ebből az állítás azonnal következik.

A feltétel szerint $6^n \equiv 1 \pmod{n}$; ebből csak annyit fogunk felhasználni, hogy $6^n \equiv 1 \pmod{p}$.

Mivel p nem osztója a 6-nak (ha osztója lenne, akkor nem lehetne $6^n - 1$ osztója), felírhatjuk a Fermat-tételt: $6^{p-1} \equiv 1 \pmod{p}$. Mivel, mint láttuk, $6^n \equiv 1 \pmod{p}$ is teljesül, az idézett tétel szerint $6^{(p-1, n)} \equiv 1 \pmod{p}$.

Azonban $p - 1$ és n relatív prímek, hiszen n legkisebb prímosztója p , míg $(p - 1)$ -nek csak p -nél kisebb osztói lehetnek.

Kaptuk tehát, hogy $6^1 \equiv 1 \pmod{p}$, vagyis p osztója $6^1 - 1 = 5$ -nek, ez pedig csak úgy lehetséges, ha $p = 5$.

Ezzel a bizonyítást befejeztük.

II. megoldás. Felhasználjuk a Fermat-tétel ugyancsak közismert általánosítását, az Euler–Fermat-tételt: ha a és m egymáshoz relatív prímek, akkor $a^{\varphi(m)} \equiv 1 \pmod{m}$, ahol $\varphi(m)$ az m -nél nem nagyobb, m -hez relatív prím pozitív egészek száma (pl. $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(10) = 4$). Ezt a függvényt Euler-féle φ függvénynek nevezik. Szükségünk lesz a φ függvénynek arra az egyszerű tulajdonságára is, hogy ha $m > 1$, akkor $\varphi(m) < m$, hiszen az m önmagához nem relatív prím, rajta kívül pedig csak $m - 1$ olyan pozitív egész van, amelyik m -nél nem nagyobb.

Tegyük fel, hogy a feladat állítása hamis, azaz van olyan n , 1-nél nagyobb egész, amelyik 5-tel nem osztható, de $6^n - 1$ -nek osztója. Legyen n_0 a legkisebb ilyen szám. A feltétel szerint $6^{n_0} \equiv 1 \pmod{n_0}$. Ebből következik, hogy n_0 a 6-hoz relatív prím; így az Euler–Fermat tétel szerint

$$6^{\varphi(n_0)} \equiv 1 \pmod{n_0}.$$

Legyen n_0 és $\varphi(n_0)$ legnagyobb közös osztója d . Mivel $\varphi(n_0) < n_0$, nyilván $d < n_0$. Másrészt az I. megoldásban idézett tétel szerint $6^d \equiv 1 \pmod{n_0}$ és – mivel d osztója az n_0 -nak – $6^d \equiv 1 \pmod{d}$. Az is igaz, hogy d nem osztható 5-tel, mert n_0 sem osztható 5-tel. Végül $d \neq 1$, mert $6^d \equiv 1 \pmod{n_0}$ teljesül, de $6^1 \equiv 1 \pmod{n_0}$, azaz $n_0 | 6 - 1$ nem.

A következőket tudjuk tehát d -ről: d 1-nél nagyobb és n_0 -nál kisebb egész szám, osztója $6^d - 1$ -nek, de nem osztható 5-tel. Ez azt jelenti, hogy d egy n_0 -nál kisebb ellenpélda a feladat állítására. Ez viszont ellentmondás, mert a legkisebb ellenpélda az n_0 .

Az indirekt feltevésből ellentmondásra jutottunk, és ezzel igazoltuk az állítást.

Megjegyzések. 1. Mindkét idézett tétel megtalálható Niven-Zuckermann: Bevezetés a számelméletbe című könyvében (29. oldal). A tételek bizonyítása nem nehéz, több természetes bizonyítás adható az első tételre, a második tétel pedig a Fermat-tételhez hasonlóan bizonyítható.

2. A második megoldásban látott módszert „végtelen leszállásnak” nevezik. Ez a teljes indukció indirekt változata, amikor nem azt bizonyítjuk be, hogy ha egy természetes számokra vonatkozó állítás igaz valamennyi az n -nél kisebb számra, akkor igaz az n -re is, hanem azt, hogy ha az n -re nem teljesül az állítás, akkor van egy n -nél kisebb pozitív egész is, amire nem teljesül. Sok esetben kényelmesebb a végtelen leszállás módszere, mint a teljes indukció.