Föltehető, hogy $n > 1$, hiszen $n = 1$ tetszőleges p prímmel megoldás. Legyen q az n *legkisebb* prímosztója, azaz $n = q^\alpha \cdot m$, ahol $q \not| m$. q választásából látszik, hogy $(q,\ m) = 1$, és az is, hogy az m páratlan. Ekkor $q \mid n \mid (p-1)^n + 1$, azaz

$$(p-1)^{q^\alpha \cdot m} \equiv -1 \pmod{q}.$$

A kis Fermat-tétel szerint $(p-1)^q \equiv p-1 \pmod{q}$. Ennek ismételt alkalmazásával

$$(p-1)^n \equiv (p-1)^m \pmod{q}, \qquad \text{és így} (p-1)^m \equiv -1 \pmod{q}. \quad (1)$$

Ebből az is következik, hogy $(q,\ p-1) = 1$, tehát ismét felhasználva a kis Fermat-tételt

$$(p-1)^{q-1} \equiv 1 \pmod{q}. \quad (2)$$

(1)-et négyzetre emelve

$$(p-1)^{2m} \equiv 1 \pmod{q} \quad (3)$$

Ha d jelöli $q-1$ és $2m$ legnagyobb közös osztóját, akkor az euklideszi algoritmus felhasználásával (2)-ből és (3)-ból $(p-1)^d \equiv 1 \pmod{q}$ következik.

A d meghatározásához vegyük észre, hogy q választása szerint az m minden prímosztója nagyobb q-nál, így $(q-1)$-nek és m-nek nincs közös prímosztója. Így $d = (q-1,\ 2m)$ vagy 1, vagy pedig 2. Így mindenképpen $(p-1)^2 \equiv 1 \pmod{q}$.

Ez pontosan akkor teljesül, ha $p - 1 \equiv 1 \pmod{q}$, vagy pedig $p - 1 \equiv -1 \pmod{q}$.

Az első esetben (1)-ből $(p-1)^m \equiv 1 \equiv -1 \pmod{q}$, azaz $q = 2$ és így $p \equiv 2 \pmod{q}$ miatt $p = 2$. Ekkor a feltételből $n = 2$ következik, és így a $p = 2$, $n = 2$ megoldást kapjuk.

A második esetben $p - 1 \equiv -1 \pmod{q}$, azaz $q \mid p$, és így $q = p > 2$, $n = p^\alpha \cdot m$, a feltételből pedig

$$p^{\alpha(p-1)} \mid (p-1)^n + 1 \quad (4)$$

következik.

Megmutatjuk, hogy p kitevője $(p-1)^n + 1$ prímtényezős felbontásában pontosan $\alpha + 1$. Ebből aztán (4) szerint $\alpha(p-1) \le \alpha + 1$, azaz $\alpha \cdot (p-2) \le 1$, tehát $\alpha = 1$ és $p = 3$ adódik.

$1 + (p-1)^n$ a binomiális tétel szerint (az n páratlan):

$$1 + \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} p^k = \underbrace{1 - 1}_{0} + \binom{n}{1} p + \sum_{k=2}^{n} (-1)^{n-k} \cdot \binom{n}{k} \cdot p^k.$$

Az összeg első tagja $\binom{n}{1} p = p^{\alpha+1} \cdot m$, és tudjuk, hogy $p \not| m$. Azt állítjuk, hogy a további tagok valamennyien oszthatók $p^{\alpha+2}$-vel, és így $1 + (p-1)^n = p^{\alpha+1}(m + p \cdot K)$ alakú, és így a második tényező valóban nem osztható p-vel.

Legyen tehát $k \ge 2$, és tekintsük a k-adik tagot ($n = p^\alpha \cdot m$):

$$\binom{n}{k} p^k = \frac{n}{k} \binom{n-1}{k-1} \cdot p^k = \frac{p^{\alpha+k} \cdot m}{k} \binom{n-1}{k-1}.$$

Ha $p \ge 3$ és $k \ge 2$, akkor $p^{k-1} > k$ (ez k-ra vonatkozó indukcióval nyilvánvaló), és így a p prímszám kitevője a k nevezőben legfeljebb $k-2$. Mivel a $p^{\alpha+k} \cdot m \cdot \binom{n-1}{k-1}$ szorzatban csak a k-val való osztás csökkentheti a p kitevőjét, azért ez a kitevő valóban legalább $\alpha + k - (k-2) = \alpha + 2$.

A második esetben tehát arra jutottunk, hogy a p prímszám csak 3 lehet, a feltétel pedig így

$$n^2 \mid 2^n + 1.$$

Ismeretes, hogy ez csak az $n = 1$ és $n = 3$ esetben teljesül. Ez volt az 1990. évi pekingi Matematikai Diákolimpia 3. feladata. Megoldása megtalálható *Reiman István:* Nemzetközi Matematikai Diákolimpiák 1959–1994 (Typotex Kiadó, Budapest, 1997) című könyvének 442–444. oldalán.

Megjegyzés. Az $n \le 2p$ feltétel felhasználásával természetesen nincs szükség erre a hivatkozásra.

Zábrádi Gergely megoldása