I. megoldás. Definiáljuk a következő sorozatot:

$$n_0 = 11; \qquad n_{i+1} = 2^{n_i} - 1.$$

Erről a sorozatról a következőt állítjuk:

a) $n_i \mid 2^{n_i} - 2$ minden $i = 0, 1, 2, \ldots$ esetén;

b) n_i összetett, ha $i \geq 1$.

Mindkét állítást teljes indukcióval bizonyítjuk:

a) Könnyen ellenőrizhető, hogy $n_0 \mid 2^{n_0} - 2$:

$$2^{11} - 2 = 2046 = 11 \cdot 186$$

(de a Fermat-tétel szerint is igaz). Tegyük most fel, hogy $n_i \mid 2^{n_i} - 2$. Ekkor

$$2^{n_{i+1}} - 2 = 2\left(2^{n_{i+1}-1} - 1\right) = 2\left(2^{2^{n_i}-2} - 1\right) = 2\left(2^{\frac{2^{n_i}-2}{n_i}\cdot n_i} - 1\right) =$$
$$= 2\left(2^{n_i} - 1\right)\left(1 + 2^{n_i} + 2^{2n_i} + \cdots + 2^{2^{n_i}-2-n_i}\right) = n_{i+1} \cdot 2\left(1 + 2^{n_i} + \cdots + 2^{2^{n_i}-2-n_i}\right).$$

Tehát $2^{n_{i+1}} - 2$ osztható n_{i+1}-gyel. Ezzel az a) állítást igazoltuk.

b) Az n_1 összetett, mert $n_1 = 2^{11} - 1 = 2047 = 23 \cdot 89$.

Ha n_i összetett – mondjuk $n_i = p \cdot q$, ahol p, $q > 1$ –, akkor

$$n_{i+1} = 2^{n_i} - 1 = 2^{pq} - 1 = \left(2^p - 1\right)\left(1 + 2^p + 2^{2p} + \cdots + 2^{(q-1)p}\right).$$

Itt mindkét tényező nagyobb, mint 1, tehát n_{i+1} is összetett.

Ezzel a b) állítást is bebizonyítottuk.

Az n_1, n_2, $\ldots$ számok tehát mind megfelelők. Ez a sorozat szigorúan monoton nő. (n_i osztója $2^{n_i} - 2$-nek, $n_i \leq 2^{n_i} - 2 < n_{i+1}$), ezért csupa különböző elemből áll.

A sorozat tehát végtelen sok megfelelő n-et szolgáltat.

II. megoldás. Legyen p 3-nál nagyobb prím, és legyen $n = \dfrac{4^p - 1}{3}$. Ez egész, mert $4^p \equiv 1^p = 1 \pmod 3$.

Megmutatjuk, hogy n összetett, és $n \mid 2^n - 2$. Mivel végtelen sok prímszám van, ebből az állítás következik.

Az n összetett, mert $n = \dfrac{2^p + 1}{3}\left(2^p - 1\right)$, és $2^p \equiv (-1)^p \equiv -1 \pmod 3$ miatt az első tényező is egész, továbbá $\dfrac{2^p + 1}{3} > \dfrac{2^3 + 1}{3} = 3$, $2^p - 1 > 2^3 - 1 = 7$, vagyis mindkét tényező 1-nél nagyobb.

Mivel $p > 2$, a Fermat-tétel szerint $4^p - 4$ osztható p-vel. Ez a szám páros, és 3-mal is osztható. Mivel p, 2 és 3 páronként relatív prímek, ebből következik, hogy

$$k = \frac{n-1}{2p} = \frac{4^p - 4}{2 \cdot 3 \cdot p}$$

egész szám.

Az n definíciója alapján $2^{2p} \equiv 1 \pmod n$. Ha ezt a kongruenciát k-adik hatványra emeljük, és 2-vel megszorozzuk, azt kapjuk, hogy

$$2 \cdot \left(2^{2p}\right)^k \equiv 2 \pmod n; 2^n \equiv 2 \pmod n,$$

azaz $2^n - 2$ osztható n-nel.

Ezzel az állítást bebizonyítottuk.

Szeidl Ádám (Miskolc, Földes F. Gimn., IV. o.t.)

Megjegyzés. A Fermat-tétel szerint, ha p prím, akkor tetszőleges p-hez relatív prím a-ra

$$a^{p-1} \equiv 1 \pmod p.$$

Ez azonban nemcsak prímekre, hanem néhány összetett p-re is igaz. Az ilyen számokat univerzális pszeudoprímeknek nevezzük. A legkisebb ilyen szám az 561.