

Megmutatjuk, hogy végtelen sok ilyen n létezik.

Legyen tetszőleges pozitív egész k -ra f_k az a polinom, amelynek gyökei a primitív k -adik komplex egységgyökök, főegyütthatója pedig 1. (Ezt a polinomot hívják a k -adik körosztási polinomnak. Az $f_1(x)$ polinomot $x - 1$ -nek definiáljuk.)

Az f_k polinomoknak két fontos tulajdonságára lesz szükségünk:

(1) f_k egész együtthatós;

(2) Tetszőleges k pozitív egészre $\prod_{d|k} f_d(x) = x^k - 1$.

Először a (2) tulajdonságot bizonyítjuk. Mindkét oldalon a polinomok főegyütthatója 1, ezért elég azt igazolnunk, hogy ugyanazok a gyökeik is. A jobb oldalon álló $x^k - 1$ polinom gyökei a k -adik komplex egységgyökök (mindegyik egyszeres gyök). Tekintsünk egy ε n -edik egységgyököt. Azt kell belátnunk, hogy ε a bal oldalon szereplő tényezők közül pontosan egynek gyöke. Az f_k polinomok definíciója szerint egyetlen olyan d pozitív egész létezik, amelyre ε gyöke f_d -nek: a legkisebb olyan szám, amelyre $\varepsilon^d = 1$. Könnyű megmondolni, hogy azok az m számok, amelyekre $\varepsilon^m = 1$, d többszörösei; speciálisan n többszöröse d -nek. Az f_d polinom tehát szerepel (2) bal oldalán.

Az (1) tulajdonságot teljes indukcióval igazolhatjuk, a (2) tulajdonság felhasználásával. $k = 1$ -re az állítás igaz. Ha f_1, \dots, f_{k-1} mind egész együtthatós, akkor (2) alapján

$$f_k(x) = \frac{x^k - 1}{\prod_{d|k, d < k} f_d(x)}.$$

A számláló és a nevező is egész együtthatós, továbbá a nevező főegyütthatója 1. Ebből a jól ismert polinomosztási algoritmus alapján következik, hogy a két polinom hányadosa, $f_k(x)$ is egész együtthatós.

Keressük ezután az n számot $q_1 q_2 \dots q_s$ alakban, ahol q_1, q_2, \dots, q_s az első s darab 1997-nél nagyobb prímszám. A (2) tulajdonság szerint

$$2^n - 1 = \prod_{d|n} f_d(2),$$

és az (1) tulajdonság miatt a jobb oldalon mindegyik tényező egész. Ha mindegyik abszolút értéke kisebb lenne $2^{\frac{n}{1997}}$ -nél, kész volnánk.

Ha d egy valódi osztója n -nek, azaz $d < n$, akkor $2^d - 1 = \prod_{\delta|d} f_\delta(2)$, emiatt $f_d(2)$ osztója $2^d - 1$ -nek, ezért

$$|f_d(2)| \leq 2^d - 1 < 2^{\frac{n}{1997}}.$$

Azt kell tehát csak megvizsgálnunk, hogy $|f_n(2)| < 2^{\frac{n}{1997}}$ teljesül-e. Legyenek az n -edik primitív egységgyökök $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{\varphi(n)}$. Ekkor

$$|f_n(2)| = \prod_{j=1}^{\varphi(n)} |2 - \varepsilon_j| < 3^{\varphi(n)}.$$

Ha sikerülne n -et úgy választani, hogy $3^{\varphi(n)} < 2^{\frac{n}{1997}}$, azaz $\frac{\varphi(n)}{n} < \frac{1}{1997 \cdot \log_2 3}$ teljesüljön, kész volnánk.

A φ függvény egy jól ismert felírása szerint (lásd pl. *Szalay Mihály: Számelmélet*, 117. old.)

$$\frac{\varphi(n)}{n} = \prod_{j=1}^s \left(1 - \frac{1}{q_j}\right).$$

Az is ismert (ugyanott, 153. old.), hogy tetszőleges $x \geq 2$ valós számra

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right) \leq \frac{1}{\sum_{k \leq x} \frac{1}{k}} < \frac{1}{\log x}.$$

(A szorzat az x -nél nem nagyobb prímszámokon fut végig.) Ezt $x = q_s$ -re alkalmazva

$$\prod_{p \leq q_s} \left(1 - \frac{1}{p}\right) = \prod_{p \leq 1997} \left(1 - \frac{1}{p}\right) \cdot \prod_{j=1}^s \left(1 - \frac{1}{q_j}\right) < \frac{1}{\log q_s},$$

vagyis

$$\frac{\varphi(n)}{n} = \prod_{j=1}^s \left(1 - \frac{1}{q_j}\right) < \frac{1}{\prod_{p \leq 1997} \left(1 - \frac{1}{p}\right) \cdot \log q_s}.$$

Ebből látszik, hogy s -et elég nagynak választva $\frac{\varphi(n)}{n}$ tetszőlegesen kicsivé tehető.