Bebizonyítjuk, hogy a $P(x) = (x^3+3)(x^2+1)(x^2+2)(x^2-2)$ polinom, amelynek főegyütthatója 1, kielégíti a feladat feltételeit. Látható, hogy nincs egész gyöke, így elég bebizonyítani, hogy minden n-re van gyöke mod n.

Használni fogjuk az ún. Legendre-féle szimbólumot: ha p 2-nél nagyobb prím és a egész, akkor

$$\left(\frac{a}{p}\right) = 0, ha$$

p| a 1,ha $p \not| a$ és az $x^2 \equiv a \pmod p$ megoldható -1,ha az $x^2 \equiv a \pmod p$ nem oldható meg.

$$Ismert, hogy$$

$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$ (a bizonyítás megtalálható Szalay Mihály: Számelmélet c. spec. mat. tankönyvének 95–96. oldalán, Tankönyvkiadó, 1991). Így

$$\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{-2}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot 2^{\frac{p-1}{2}} \cdot (-2)^{\frac{p-1}{2}} = (-2)^{p-1} \equiv 1 \pmod p$$

minden páratlan p prímre. Tehát $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$, $\left(\frac{-2}{p}\right)$ közül valamelyik $+1$, azaz az $x^2 \equiv -1$, $x^2 \equiv 2$, $x^2 \equiv -2$ valamelyike megoldható mod p.

Belátjuk, hogy ha $x^2 \equiv a \pmod p$ megoldható (p páratlan prím, $p \not| a$), akkor $x^2 \equiv a \pmod{p^k}$ is megoldható minden $k \geq 1$-re. Teljes indukcióval bizonyítunk.

$k = 1$-re az állítás igaz. Tegyük fel, hogy valamilyen $k \geq 1$ egészre $x^2 \equiv a \pmod p$ megoldható, legyen egy megoldása $x \equiv x_1 \pmod{p^k}$. Ekkor

$$(p^k l + x_1)^2 = p^{2k} l^2 + 2p^k l x_1 + x_1^2 \equiv (2lx_1)p^k + x_1^2 \pmod{p^{k+1}},$$

azaz

$$(p^k \cdot l + x_1)^2 - a \equiv (2lx_1)p^k + x_1^2 - a = (2lx_1)p^k + bp^k \pmod{p^{k+1}}$$

valamely b egészre. $p \not| 2x_1$ miatt van olyan l egész, amelyre $p \mid 2lx_1 + b$, így valamilyen $y = p^k \cdot l = x_1$ számra $y^2 - a \equiv 0 \pmod{p^{k+1}}$, tehát $y^2 \equiv a \pmod{p^{k+1}}$. Ezt akartuk bizonyítani.

Ezzel beláttuk, hogy minden páratlan p prímre és $k \geq 1$ egészre az $x^2 \equiv -1$, $x^2 \equiv 2$, $x^2 \equiv -2$ valamelyike megoldható mod p^k. Ekkor nyilván a $p(x)$ polinomnak is van gyöke modulo p^k.

Vizsgáljuk most a $p = 2$ esetet. Bebizonyítjuk, hogy az $x^3 + 3 \equiv 0$-nak van gyöke mod 2^k, minden $k \geq 1$-re.

Teljes indukcióval bizonyítunk. $k = 1$ esetén $x \equiv 1 \pmod 2$ megoldás. Tegyük fel, hogy $x^3 + 3 \equiv 0 \pmod{2^k}$ megoldható, legyen egy megoldás x_1. Keressük a modulo 2^{k+1} megoldást $y = 2^k \cdot l + x_1$ alakban.

$$(2^k \cdot l + x_1)^3 \equiv 2^{3k} + 3 \cdot 2^{2k} l^2 x_1 + 3 \cdot 2^k l x_1^2 + x_1^3 \equiv 3 \cdot 2^k l x_1 + x_1^3,$$

azaz

$$(2^k \cdot l + x_1)^3 + 3 \equiv (3lx_1^2)2^k + x_1^3 + 3 = (3lx_1^2) \cdot 2^k + b \cdot 2^k \pmod{2^{k+1}},$$

valamilyen b egészre. Az x_1 biztosan páratlan (mert $2^k \mid x_1^3+3$), így valamilyen l-re $2 \mid 3lx_1^2+b$, és ekkor $y = 2^k \cdot l + x_1$-re $y^2 + 3 \equiv 0 \pmod{2^{k+1}}$.

Ezzel bebizonyítottuk, hogy tetszőleges p^k prímhatványra a $P(x)$ polinomnak van gyöke modulo p^k.

Legyen az n prímtényezős felbontása $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$. Tudjuk, hogy van a polinomnak x_i gyöke modulo $p_i^{\alpha_i}$ minden $1 \leq i \leq r$-re.

A kínai maradéktétel alapján az

$$x \equiv x_1 \bmod p_1^{\alpha_1}, \quad x \equiv x_2 \bmod p_2^{\alpha_2}, \quad \dots, \quad x \equiv x_r \bmod p_r^{\alpha_r}$$

kongruencia-rendszernek van egy x megoldása. Erre az x-re $P(x)$ osztható lesz $p_i^{\alpha_i}$-vel minden $1 \leq i \leq r$-re, tehát osztható lesz n-nel is.

Ezzel a feladat állítását bebizonyítottuk.

Megjegyzés. A feladat szövegéből kimaradt az a feltétel, hogy a polinom főegyütthatója legyen 1. Ennek a feltételnek a hiányában könnyebb olyan polinomot mutatni, amely kielégíti a feladat feltételeit (és főegyütthatója nem 1). Pl. a $(2x+1)(3x+1)$ polinomnak nincs egész gyöke, és – ugyancsak a kínai maradéktétel segítségével – egyszerűen belátható, hogy van gyöke modulo n, minden $n > 1$ természetes számra.