

Megoldás. (Bodor Mátyás) Megmutatjuk, hogy c legkisebb lehetséges értéke a 4.

Bármely p prímszámra és nemnulla x egészre jelöljük $v_p(x)$ -szel az x prímtényező felbontásában a p kitevőjét. A megoldás során többször is használni fogjuk a *Lifting The Exponent (LTE)* lemmát:

- Ha p páratlan prímszám és x, y egészek úgy, hogy $p \nmid x, y$ és $p \mid x - y$, akkor tetszőleges n pozitív egészre

$$v_p(x^n - y^n) = v_p(x - y) + v_p(n).$$

- $p = 2$ -re: ha x, y páratlanok és n páros, akkor

$$v_2(x^n - y^n) = v_2(x - y) + v_2(x + y) + v_2(n) - 1.$$

(Bővebben lásd például a https://en.wikipedia.org/wiki/Lifting-the-exponent_lemma oldalt.)

Nekünk csak a $p = 2$ az esetre lesz szükségünk.

Először megmutatjuk, hogy $c \geq 4$. Ehhez tekintsük a következő függvényt:

$$g(x) = \begin{cases} 1, & \text{ha } x \text{ páratlan,} \\ 2, & \text{ha } x = 2, \\ 2^{v_2(x)+2}, & \text{ha } x \text{ páros és } x > 2. \end{cases}$$

A g függvény pöpec, mert:

- Ha a páratlan, akkor $g(a) = 1 \mid b^a - g(b)$.
- Ha $a = 2$, akkor az kell, hogy $g(a) = 2 \mid b^2 - g(b)^2$, ami igaz, mert a konstrukcióból látható, hogy b és $g(b)$ paritása mindig megegyezik.
- Ha a páros, $a \geq 4$ és b páros, akkor az kell, hogy $g(a) = 2^{v_2(a)+2} \mid b^a - g(b)^{2^{v_2(a)+2}}$. Mivel $2 \mid g(b)$ páros, $v_2(g(b)^{2^{v_2(a)+2}}) \geq 2^{v_2(a)+2} > v_2(a) + 2$, ezért $2^{v_2(a)+2} \mid g(b)^{2^{v_2(a)+2}}$; másrészt $2 \mid b$ miatt $v_2(b^a) \geq a \geq v_2(a) + 2$ (például a 2, 3, ..., a számok között legfeljebb $a - 2$ darab 2-hatvány lehet, mert a 3 nem 2-hatvány, ezért $v_2(a) \leq a - 2$). Vagyis $2^{v_2(a)+2} \mid b^a$, ahonnan következik a kívánt oszthatóság.
- Végül, ha a páros, $a \geq 4$ és b páratlan, akkor a feltétel $g(a) = 2^{v_2(a)+2} \mid b^a - 1$, ez pedig következik az LTE lemmából: $v_2(b^a - 1) = v_2(b + 1) + v_2(b - 1) + v_2(a) - 1 \geq v_2(a) + 2$, hiszen $b + 1$ és $b - 1$ mindegyike páros, és pontosan az egyik osztható 4-gyel is, tehát 2-es kitevője legalább 2.

Összegezve, a g függvény valóban pöpec. Emellett $g(4) = 2^{2+2} = 16$, így $4c \geq g(4) = 16$, tehát biztosan $c \geq 4$.

Most pedig megmutatjuk, hogy $c = 4$ eleget tesz a feltételeknek.

Tekintsünk egy tetszőleges pöpec f függvényt. Belátjuk, hogy minden pozitív egész n -re $f(n) \leq 4n$, innen készen leszünk. Tetszőleges a, b pozitív egészre legyen $P(a, b)$ az oszthatósági feltétel, tehát $P(a, b)$ annak a rövidítése, hogy $f(a) \mid b^a - f(b)^{f(a)}$.

A $P(a, a)$ szerint $f(a) \mid a^a - f(a)^{f(a)}$, ezért $f(a) \mid a^a$. Ha most $a = p$ prímszám, akkor $f(p) \mid p^p$. Ezért $f(p)$ értéke vagy 1, vagy pedig p -hatvány minden p prímre. Legyen $f(p) = p^{i_p}$, ahol $i_p \geq 0$ egész.

Tegyük fel, hogy van végtelen sok olyan p prím, hogy $i_p > 0$. Legyen emellett b tetszőleges pozitív egész. Válasszunk egy olyan nagy p prímet, hogy $i_p > 0$ és $p > |b - f(b)|$; ilyen van a feltevésünk miatt. Így $P(p, b)$ -ből $p \mid p^{i_p} = f(p) \mid b^p - f(b)^{f(p)}$. De mind p , mind $f(p)$ egy p -hatvány, ezért a kis Fermat-tételből $b^p \equiv b \pmod{p}$ és $f(b)^{f(p)} \equiv f(b) \pmod{p}$. A fentiek alapján $p \mid b - f(b)$ és $p > |b - f(b)|$, ami csak úgy lehetséges, ha $b - f(b) = 0$, vagyis $f(b) = b$. De b tetszőlegesen volt megválasztva, tehát $f(b) = b \leq 4b$ minden b -re.

Marad az az eset, amikor nincs végtelen sok olyan p prím, hogy $i_p > 0$, vagyis véges sok van, legyenek ezek $p_1 < p_2 < \dots < p_k$, és ekkor minden $p > p_k$ prímszámra $f(p) = 1$.

Ha egyáltalán nincsenek ilyen $p_1 < \dots < p_k$ prímek, akkor $f(p) = 1$, minden p prímre. Ha van olyan a , amelyre $f(a) > 1$, akkor legyen p az $f(a)$ egyik prímosztója. $P(a, p)$ -ből $p \mid f(a) \mid p^a - 1^{f(a)} = p^a - 1$ miatt $p \mid 1$, ellentmondás. Tehát ilyen a nem létezhet; $f(n) = 1 \leq 4n$ minden n -re.

Ha $k \geq 1$, és $p_k > 2$, akkor válasszunk egy $p > p_k$ prímet a $p \equiv 2 \pmod{p_k}$ tulajdonsággal; ezt meg tudjuk tenni a Dirichlet-tétel miatt, hiszen p_k és a 2 relatív prímek. De $P(p_k, p)$ miatt $p_k \mid f(p_k) \mid p^{p_k} - f(p)^{p_k} = p^{p_k} - 1$, de $p^{p_k} - 1 \equiv p - 1 \equiv 1 \pmod{p_k}$ a kis Fermat-tételből, ami ellentmondás.

Az az eset marad, amikor $k = 1$, $f(2)$ páros, és $f(p) = 1$ minden $p > 2$ prímre.

Ha van olyan a , hogy $p \mid f(a)$ valamilyen páratlan p prímre, akkor $P(a, p)$ miatt $p \mid f(a) \mid p^a - 1^{f(a)} = p^a - 1$, ellentmondás. Ez azzal egyenértékű, hogy $f(a)$ minden a -ra vagy 1, vagy pedig 2-hatvány.

A $P(a, 3)$ -ból $f(a) \mid 3^a - f(3)^{f(a)} = 3^a - 1$, így páratlan a -ra $4 \nmid 3^a - 1$ miatt $f(a) \leq 2 < 4a$. Ha pedig a páros, akkor az LTE lemmából $v_2(3^a - 1) = v_2(3 - 1) + v_2(3 + 1) + v_2(a) - 1 = v_2(a) + 2$, ezért $v_2(a) + 2 \geq v_2(f(a)) = \log_2 f(a)$, ezért $f(a) \leq 2^{v_2(a)+2} = 4 \cdot 2^{v_2(a)} \leq 4a$.

Tehát az $f(n) \leq 4n$ egyenlőtlenség minden $n \in \mathbb{N}$ számra fennáll, és ez igazolja, hogy $c = 4$ megfelelő.