

Megoldás. Legyen p tetszőleges, 2-nél nagyobb prím. Vizsgáljuk a

$$2^{2^1}, 2^{2^2}, 2^{2^3}, \dots$$

számok p -vel való osztási maradékát. Ezek a számok sorban egymás négyzetei, hiszen

$$(2^{2^n})^2 = 2^{2^{n+1}}.$$

Ha valamelyikük maradéka -1 , akkor a következő $(-1)^2 = 1$, és az összes többi is 1. Ebből következik, hogy a (-1) -es maradék legfeljebb egyszer fordulhat elő. Tegyük fel, hogy előfordul, azaz $2^{2^m} \equiv -1 \pmod{p}$, másszóval $p \mid 2^{2^m} + 1$. Megmutatjuk, hogy ekkor $m < p$. Tétélezzük fel ugyanis, hogy $m \geq p$. Akkor előtte legalább $p - 1$ maradék volt, de egyik sem lehet 0, (mert egy kettőhatványt nem oszthat egy páratlan prím), továbbá egyik sem lehet -1 , hiszen csak az m -edik -1 . Így az összes maradék közül csak $(p - 2)$ -féle lehet előtte, ezért a skatulyaelv miatt lesz két megegyező maradék, mondjuk az s -edik és a t -edik, ahol $1 \leq s < t < m$. Ekkor, mivel egymás után egymás négyzetei vannak, és egy szám négyzetének p -vel való maradéka a szám p -vel való maradéka négyzetének a p -vel való maradéka, azért az $(s + 1)$ -edik és a $(t + 1)$ -edik maradékok is megegyeznek egymással, ugyanezért az $(s + 2)$ -edik és a $(t + 2)$ -edik is stb. Így azonban az $m - (t - s)$ -edik maradék megegyezne az m -edikkel, vagyis mindkettő (-1) lenne, ami lehetetlen. Tehát valóban $m < p$.

Tegyük fel, hogy egy n, k számpárra $nk \mid (2^{2^n} + 1)(2^{2^k} + 1)$; szimmetria miatt feltehetjük, hogy $n \leq k$. Ha $n > 1$, akkor legyen p az n egyik prímtényezője. Nyilván $p \neq 2$, hiszen $(2^{2^n} + 1)(2^{2^k} + 1)$ páratlan. Mivel $p \leq n \leq k$, a fentiek szerint sem $2^{2^n} + 1$, sem pedig $2^{2^k} + 1$ nem lehet p -vel osztható, de akkor a szorzatuk sem, ami ellentmondás; így szükségképpen $n = 1$. Tegyük fel, hogy $k > 1$, és az egyik prímosztója p . A fenti esethez hasonlóan $p > 2$, és $p \leq k$ miatt p nem osztja a $2^{2^k} + 1$ tényezőt. Ezért $p \mid k \mid (2^{2^n} + 1)(2^{2^k} + 1)$ csak úgy lehetséges, hogy $p \mid 2^{2^n} + 1 = 5$, ezért – mivel k minden prímtényezője relatív prím $2^{2^k} + 1$ -hez – $k \mid 5$.

Tehát a lehetséges számpárok (a sorrendet is figyelembe véve): $(1, 1)$, $(1, 5)$, $(5, 1)$, amik valamennyien teljesítik is a feladat feltételét.