

A feladatot először abban a speciális esetben oldjuk meg, amikor c és d relatív prímek. Az a , b , c , d számok különbözősége helyett csupán annyit kötünk ki, hogy nem lehet c és d értéke is 1.

Tegyük fel, hogy az $ac^n + bd^n$ alakú pozitív egészeknek összesen csak véges sok prímosztója van. Legyenek ezek p_1, p_2, \dots, p_m . Válasszunk mindegyik p_i -hez egy olyan α_i pozitív egészet, hogy a , b és $a + b$ egyike se legyen osztható $p_i^{\alpha_i}$ -vel.

Azt állítjuk, hogy ha n elég nagy és osztható $\varphi(p_i^{\alpha_i})$ -vel, akkor $ac^n + bd^n$ nem osztható $p_i^{\alpha_i}$ -vel. (φ az Euler-féle függvény: $\varphi(n)$ az n -nél nem nagyobb, n -hez relatív prím pozitív egészek száma.) A lehetséges eseteket két részre osztjuk.

I. eset: ha sem c , sem d nem osztható p_i -vel. Legyen $n = k\varphi(p_i^{\alpha_i})$. Az Euler–Fermat tétel szerint

$$c^n = (c^k)^{\varphi(p_i^{\alpha_i})} \equiv 1 \pmod{p_i^{\alpha_i}} \quad \text{és} \quad d^n = (d^k)^{\varphi(p_i^{\alpha_i})} \equiv 1 \pmod{p_i^{\alpha_i}},$$

ezért

$$ac^n + bd^n \equiv a + b \pmod{p_i^{\alpha_i}}.$$

Az α_i definíciója szerint $a + b$ nem osztható $p_i^{\alpha_i}$ -nel.

II. eset: ha c vagy d osztható p_i -vel. Az állítás szimmetriája miatt feltehetjük, hogy c osztható p_i -vel. Mivel c és d relatív prímek, ebben az esetben d nem osztható p_i -vel. Ha $n \geq \alpha_i$, akkor c^n osztható $p_i^{\alpha_i}$ -nel, és – ismét felhasználva az Euler–Fermat tételt –

$$ac^n + bd^n \equiv a \cdot 0 + b \cdot 1 = b \pmod{p_i^{\alpha_i}}.$$

Mivel b nem osztható $p_i^{\alpha_i}$ -nel, kész vagyunk.

Legyen most $P = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\dots\varphi(p_m^{\alpha_m})$. Ha n elég nagy és osztható P -vel, akkor $ac^n + bd^n$ nem osztható $p_i^{\alpha_i}$ -nel semmilyen i -re sem, tehát prímtényezői felbontásában a p_i kitevője kisebb, mint α_i . Mivel az indirekt feltevés szerint más prímosztója nincs, ebből következik, hogy

$$ac^n + bd^n \leq p_1^{\alpha_1-1} p_2^{\alpha_2-1} \dots p_m^{\alpha_m-1}.$$

Ez azonban ellentmondás, mert c és d közül valamelyik legalább 2, így az $ac^n + bd^n$ sorozat szigorúan monoton nő, és végtelenhez tart.

Hátravan még az általános eset vizsgálata, amikor c és d különböző, nem feltétlenül relatív prím számok. Legyen c és d legnagyobb közös osztója q ; $c = c_1q$, $d = d_1q$, ahol c_1 és d_1 relatív prímek. Ezekkel a jelölésekkel

$$ac^n + bd^n = q^n (ac_1^n + bd_1^n).$$

Mivel c_1 és d_1 relatív prímek, a második tényező lehetséges értékeinek, mint láttuk, összesen végtelen sok prímosztója van.

Gyarmati Katalin (Fazekas M. Főv. Gyak. Gimn., III. o.t.)