

Megmutatjuk, hogy nincsenek ilyen polinomok. Indirekt bizonyítunk, tegyük fel, hogy

$$(2) \quad f(x)^3 - g(x)^2 = ax + b, \quad \text{ahol } a \neq 0.$$

Ez a formula akkor volna jól kezelhető, ha a jobb oldalon teljes négyzet ellentettje állna. Ennek érdekében bevezetjük az y változót, és alkalmazzuk az $x = (-y^2 - b)/a$ helyettesítést. Ekkor

$$f(x) = f\left(\frac{-y^2 - b}{a}\right) = F(y^2), \quad \text{illetve} \quad g(x) = G(y^2)$$

teljesül alkalmas F és G polinomokra, ahonnan

$$(3) \quad F(y^2)^3 = G(y^2)^2 - y^2 = (G(y^2) - y) \cdot (G(y^2) + y)$$

adódik. A bal oldali polinom foka 6-tal osztható, ezért G nem lehet konstans. Ha F konstans tagja 0, akkor ugyanez G -re is igaz. Ám ekkor a bal oldalon álló polinom legalacsonyabb fokú tagjának foka 6-tal osztható, míg a jobb oldalon álló esetében ez a fok pontosan 2. Ezért a G polinom nem konstans, de van konstans tagja. A jobb oldali két tényező relatív prím, hiszen ha egy polinom mindkettőt osztja, akkor a különbségüket és az összegüket, a $2y$ és a $2G(y^2)$ polinomokat is osztja, ám ez utóbbi polinomok relatív prímek, hisz $2G(y^2)$ konstans tagja nem nulla.

A valós együtthatós polinomok körében érvényes a számelmélet alaptétele, ezért (3) jobboldalának mindkét tényezője egy-egy valós együtthatós polinom köbének konstansszorozosa. Mivel minden valós konstans előáll valós szám köbeként, azt kapjuk, hogy vannak olyan, valós együtthatós $p(y)$ és $q(y)$ polinomok, amelyekre

$$(4) \quad p(y)^3 = G(y^2) - y, \quad \text{illetve} \quad q(y)^3 = G(y^2) + y$$

teljesül. Láttuk, hogy G nem konstans. Ezért a (4) két jobb oldalán álló polinom legmagasabb fokú tagja megegyezik és legalább másodfokú. Ugyanez igaz tehát a két bal oldalon álló polinomra is: $p(y)$ és $q(y)$ legmagasabb fokú nemnulla tagja ugyanaz a cy^n monom, ahol $n \geq 1$. Ekkor azonban a

$$(5) \quad 2y = q(y)^3 - p(y)^3 = (q(y) - p(y)) \cdot (q(y)^2 + q(y)p(y) + p(y)^2)$$

egyenlőség jobb oldalán a második tényezőben y^{2n} együtthatója $3c^2 \neq 0$, ezért a jobb oldal nem lehet elsőfokú. A kapott ellentmondás a megoldás elején kimondott állítást bizonyítja. $\square$

II. megoldás. Ismét indirekt bizonyítunk, tegyük fel tehát, hogy

$$(6) \quad f(x)^3 = g(x)^2 + r(x), \quad \text{ahol } r(x) = ax + b \text{ és } a \neq 0.$$

Nyilván sem f , sem g nem lehet konstans, ezért $\deg f = 2k$ és $\deg g = 3k$ valamilyen pozitív egész k -ra. Legyen $d = \gcd(f, g)$. Ekkor persze $d^2 \mid f^3 - g^2 = r$, ám mivel r elsőfokú, d csak konstans lehet, vagyis f és g egymáshoz relatív prímek. Most (6) mindkét oldalát deriválva az

$$(7) \quad 3f(x)^2 f'(x) = 2g(x)g'(x) + r'$$

egyenlőséget kapjuk, ahonnan a (6) r' -szereséből kivonva a (7) r -szeresét,

$$f^2(fr' - 3f'r) = g(gr' - 2g'r)$$

adódik. A bal oldal osztható azzal az f^2 polinommal, amihez a jobb oldalon álló g relatív prím, tehát

$$(8) \quad f^2 \mid gr' - 2g'r.$$

Ekkor azonban $\deg f^2 = 4k$, míg $gr' - 2g'r$ foka legfeljebb $3k$. Ráadásul ha a g főegyütthatója d , akkor $(gr' - 2g'r)$ -ben a $3k$ -adfokú tag együtthatója

$$da - 6kda = (1 - 6k)da \neq 0.$$

Vagyis a $gr' - 2g'r$ polinom nem lehet a nulla polinom, és a foka pontosan $3k$.

Tehát a (8) szerint a $4k$ -adfokú f^2 osztója a pontosan $3k$ -adfokú, nemnulla $gr' - 2g'r$ polinomnak, ez pedig lehetetlen. $\square$

Megjegyzések. 1. Vannak olyan nem konstans f és g polinomok, amelyekre $f^3 - g^2$ másodfokú, például $(x^2 + 2)^3 - (x^3 + 3x)^2 = 3x^2 + 8$. Igazolható, hogy ez csak úgy lehetséges, ha egyrészt f és g relatív prímek, másrészt pedig ha a fokaik $\deg f = 2$ és $\deg g = 3$.

2. A feladat szorosan kapcsolódik az ún. abc-sejtéshez, ami az alábbi mondja ki. Minden pozitív ε -ra van olyan C_ε konstans, hogy ha a, b, c relatív prím pozitív egészek és $a + b = c$, akkor $c < C_\varepsilon \cdot \text{rad}(abc)^{1+\varepsilon}$. Itt $\text{rad}(n)$ az n radikálját jelöli, azaz az n különböző prímosztóinak szorzatát. (Pl. $\text{rad}(2016) = 42$, $\text{rad}(2017) = 2017$ és $\text{rad}(2018) = 2018$.) Az abc-sejtésből számos nehéz tétel és sejtés következik. Levezethető belőle például a nagy Fermat-tételt általánosító Beal-sejtés gyengítése, miszerint

az $a^n + b^m = c^k$ egyenletnek csak véges sok olyan megoldása van a pozitív egészek körében, amelyre a, b, c relatív prímek és n, m, k mindegyike legalább 3. Az abc-sejtésre jelenleg nem ismert általánosan elfogadott bizonyítás. Ígéretes fejlemény azonban Mocsizuki Sinicsi japán matematikus 2012-ben publikált 500 oldalas munkája, amelyben egy egészen új elméletet dolgoz ki és bizonyít számos számelméletet érintő sejtést, többek között az abc-sejtést. Mocsizuki elmélete azonban annyira újszerű, hogy még jelenleg is tart annak ellenőrzése. Tekintettel arra, hogy az intenzív munka ellenére még nem találtak benne lényeges hibát, könnyen elképzelhető, hogy a közeli jövőben bejelentik a sejtés megoldását. Ha pedig ez megtörténik, valószínűleg semmi sem mentheti meg a szerzőt egy igen tekintélyes matematikai díjtól, ami persze nem lehet a Fields-érem, hiszen azt 40 év felettiek nem kaphatják.

Ismert és bizonyított azonban az abc-sejtésnek egy polinomos megfelelője, az ún. Mason-tétel. Jelölje $\text{rad}(f)$ az f komplex együtthatós polinom különböző irreducibilis faktorainak szorzatát. (Tehát $\text{rad}(f)$ foka az f különböző komplex gyökeinek száma.) Legyenek f, g és h olyan komplex együtthatós relatív prím polinomok, amelyek nem mindegyike konstans és $f + g = h$. Ekkor a Mason-tétel szerint

$$\max(\deg(f), \deg(g), \deg(h)) \leq \deg(\text{rad}(fgh)) - 1.$$

A Mason-tétel segítségével a kitűzött feladat könnyen megoldható. Tegyük fel tehát, hogy (5) teljesül. A II. megoldásban láttuk, hogy f, g relatív prímek, tehát f^3, g^2 és r is azok. Nyilván $\deg(f) = 2k, \deg(g) = 3k$ alkalmas k pozitív egészre. A Mason-tétel szerint ekkor

$$\begin{aligned} 6k = \max(6k, 6k, 1) &\leq \deg(\text{rad}(f^3 g^2 r)) - 1 = \deg(\text{rad}(fgr)) - 1 \leq \\ &\leq \deg(fgr) - 1 = \deg(f) + \deg(g) + \deg(r) - 1 = 5k, \end{aligned}$$

ami ellentmondás, így (5) nem teljesülhet.