

a) A 7-tel való oszthatósághoz legalább 7-ed fokúnak kell lennie a polinomnak. Feltehetjük, hogy a polinomban egyáltalán nem fordul elő 7-tel osztható együttható, mert az ilyen tagokat mint fentebb is tettük, elhagyhatjuk. Feltétel szerint marad tagja a polinomnak. Elég megmutatni, hogy 6-od fokú nem felelhet meg a feltételeknek, mert ha mondjuk egy negyedfokú polinom osztható volna minden egész x értékre 7-tel anélkül, hogy volna benne 7-tel osztható együttható, akkor a polinom x^2 -szerese is kielégítené ezt a feltételt és az már 6-od fokú volna. Így ha 6-od fokú nem lehet, akkor alacsonyabb fokú sem.

Legyen $ax^6 + bx^5 + cx^4 + dx^3 + ex^2 + fx + g$ olyan hatodfokú polinom, melyben a tényleg szereplő együtthatók nem oszthatók 7-tel és a polinom értéke minden egész x értékre osztható 7-tel. Ekkor a minden esetre 7-tel nem osztható egész szám, különben a polinom nem volna valójában 6-od fokú. Megmutatjuk, hogy ez lehetetlen. Ez esetben ugyanis az $x = -3, -2, -1, 0, 1, 2, 3$ helyeken is 7-tel osztható volna a polinom értéke, vagyis a

$$\begin{aligned} 729a - 243b + 81c - 27d + 9e - 3f + g, \\ 64a - 32b + 16c - 8d + 4e - 2f + g, \\ a - b + c - d + e - f + g, \\ g, \\ a + b + c + d + e + f + g, \\ 64a + 32b + 16c + 8d + 4e + 2f + g, \\ \text{és } 729a + 243b + 81c + 27d + 9e + 3f + g. \end{aligned}$$

számok mindegyike is és így az összegük: $1588a + 196c + 28e + 7g = 7 \cdot (227a + 28c + 4e + g) - a$ is 7-tel osztható kell hogy legyen, tehát külön a is. Ez azonban lehetetlen a mondottak szerint, tehát nincs hetediknél alacsonyabb fokú polinom, mely eleget tenne a feltételeknek.

b) 12-vel való oszthatósághoz legalább 4-ed fokú polinom szükséges. Ha volna alacsonyabb fokú, azt írhatjuk 3-ad fokúnak, 0 együtthatókat is megengedve. Legyen $ax^3 + bx^2 + cx + d$ minden egész x -re 12-vel osztható, akkor $x = 0$ -t téve d 12-vel osztható s így elhagyható. Marad $x(ax^2 + bx + c)$. $x = 1, -1$ helyettesítésekkel $a + b + c$ és $-a + b - c$ is osztható kell, hogy legyen 12-vel, tehát összegük is különbségük is, vagyis b és $a + c$ 6-tal osztható. Tegyük x helyett 2-t, akkor a második tényező $4a + 2b + c$ 6-tal osztható kell, hogy legyen, tehát c s így a is páros, minden együttható 2-vel osztható, amit éppen kizártunk.

Elég jól oldotta meg: Gacsányi S., Kővári T.

Megjegyzés: A megoldás első részében nyertük, hogy ha x egész, akkor $7|x^7 - x = x(x^6 - 1)$. (Függőleges vonallal az oszthatóságot szokás jelölni, tehát $7|49$ olvasd: 49 osztható 7-tel. Az ellentétét a vonal áthúzásával jelöljük: $7 \nmid 36$ olvasd: 36 nem osztható 7-tel.) Ez azonban csak úgy lehet, ha vagy x osztható 7-tel, vagy $x^6 - 1$, mivel 7 törzsszám. Így szétszedve persze csak az állítás második fele érdekes: *ha x 7-tel nem osztható egész szám, akkor $x^6 - 1$ mindig osztható 7-tel.*

Fermat¹⁾ vette észre, hogy ilyen összefüggés minden törzsszámra érvényes. *Ha p egy tetszőleges törzsszámot jelent, a pedig p -vel nem osztható szám, akkor mindig $p|a^{p-1} - 1$.* Ennek a tételnek sok egyszerű bizonyítása van. Azok számára, akik ismerik a kéttagúak hatványozására vonatkozó binomiális tételt, ajánlunk is egyet. A tétel minden p -vel nem osztható a -ra vonatkozik. Ezt a kivételt sem kell tennünk, ha a -val megszorozzuk a jobboldali kifejezést: $p|a^p - a$ minden p primszámra és minden a egész számra igaz. Miután most már minden egész a -ra érvényes tételt nyertünk, megpróbálhatjátok teljes indukcióval bizonyítani a tételt. Sikerülni is fog, csak a fellépő együtthatók oszthatóságáról kell még egy egyszerű tényt bebizonyítani.

¹⁾PIERRE DE FERMAT (1601–1665) francia ügyvéd volt, a toulousi legfőbb bíróság tagja. Szabadidejét legszívesebben matematikával töltötte. Vizsgálatai, melyeket csak fia kezdett kiadni, FERMAT halála után 14 évvel, igen sok fontos eredményt tartalmaznak.