

Megjegyzés. Tegyük föl, hogy létezik ilyen $2 \leq n$ -edfokú f polinom. Elsőként azt igazoljuk, hogy a polinom minden együtt-hatója racionális szám (az f feltételezett tulajdonságából itt csupán arra lesz szükség, hogy a polinom minden racionális helyen racionális értéket vesz föl). Ehhez egyrészt megmutatjuk, hogy egy legfeljebb n -edfokú polinomot egyértelműen meghatároz $n + 1$ különböző helyen fölvetett értéke. Valóban, ha f_1 és f_2 foka legfeljebb n , és például $f_1(1) = f_2(1)$, $f_1(2) = f_2(2)$, $\dots$, $f_1(n+1) = f_2(n+1)$, akkor az ugyancsak legfeljebb n -edfokú $f_1 - f_2$ polinomnak létezik legalább $n + 1$ különböző gyöke: $1, 2, \dots, n+1$. Ez csak úgy lehetséges, hogy $f_1 - f_2$ a nullapolinom, vagyis $f_1 = f_2$.

Tekintsük másrészt (minden $1 \leq j \leq n+1$ -re) az n -edfokú

$$\ell_j = \frac{(x-1)(x-2)\dots(x-(j-1))(x-(j+1))\dots(x-(n+1))}{(j-1)(j-2)\dots(j-(j-1))(j-(j+1))\dots(j-(n+1))}$$

polinomokat. Ezek együtt-hatói racionális számok, és minden $1 \leq k \leq n+1$ -re

$$\ell_j(k) = \begin{cases} 1, & \text{ha } k = j, \\ 0, & \text{ha } k \neq j. \end{cases}$$

Ebből könnyen látható, hogy az ugyancsak racionális együtt-hatós és legfeljebb n -edfokú $f^* = f(1)\ell_1 + f(2)\ell_2 + \dots + f(n+1)\ell_{n+1}$ polinom az $1, 2, \dots, n+1$ helyeken rendre ugyanazokat az értékeket veszi föl, mint f , ezért a fentiek értelmében $f^* = f$.

Másodjára azt mutatjuk meg, hogy ha létezik a feladat követelményeit kielégítő polinom, akkor olyan polinom is található erre a célra, amelynek együtt-hatói egész számok. Jelölje ugyanis t az előbbi f polinom együtt-hatóiban a nevezők legkisebb közös többszörösét, ekkor f helyett tf ugyanúgy megfelelő, és egészek az együtt-hatói.

I. megoldás. Ha f egy megfelelő, egész együtt-hatós polinom, akkor $f+c$ is megfelelő, bármilyen c racionális szám választása mellett. Ennek alapján feltehetjük, hogy

$$f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x$$

olyan, a feladat feltételeit kielégítő, egész együtt-hatós polinom, amelynek a konstans tagja nulla. Mivel a racionális helyeken f minden racionális értéket felvesz, speciálisan minden p prímhez létezik olyan $\frac{s_p}{t_p}$ – egyszerűsített törtként felírt – racionális szám, amelyre $f\left(\frac{s_p}{t_p}\right) = p$. Itt mindkét oldalt t_p^n -nel megszorozva, majd rendezve:

$$a_n s_p^n + a_{n-1} s_p^{n-1} t_p + \dots + a_1 s_p t_p^{n-1} = p t_p^n.$$

A bal oldalon minden tag osztható s_p -vel, ezért s_p osztója $p t_p^n$ -nek is; azonban (a tört egyszerűsített alakja miatt) s_p relatív prím t_p -hez, így t_p^n -hez is, következésképpen s_p osztója p -nek.

Hasonlóan kapjuk, az iménti egyenlőség

$$-a_n s_p^n = a_{n-1} s_p^{n-1} t_p + \dots + a_1 s_p t_p^{n-1} - p t_p^n$$

alakba történő átrendezésével, hogy $a_n s_p^n$ osztható t_p -vel, ezért a_n is osztható t_p -vel. Mindez azt jelenti, hogy

$$\frac{s_p}{t_p} = \frac{p}{v_p} \quad \text{vagy} \quad \frac{s_p}{t_p} = \frac{1}{v_p},$$

ahol v_p az a_n főegyüttható valamelyik (pozitív vagy negatív) osztója. Az ilyen $\frac{1}{v_p}$ számok csak véges sokan vannak, a

p prímek száma viszont végtelen, ezért végtelen sok p prímre az első eset következik be: $f\left(\frac{p}{v_p}\right) = p$, azaz (felhasználva, hogy $f = x \cdot g$, alkalmas g polinommal)

$$\frac{p}{v_p} \cdot g\left(\frac{p}{v_p}\right) = p.$$

Innen $g\left(\frac{p}{v_p}\right) = v_p$, végtelen sok p prímre. Mint láttuk, itt $\frac{p}{v_p}$ végtelen sok, v_p pedig véges sok számot jelent, így van olyan racionális (v_p) érték, amelyet g végtelen sokszor felvesz. Ebből következik, hogy g konstans polinom, akkor viszont $f = x \cdot g$ elsőfokú, ami ellentmondás. Tehát nem létezik a feladat követelményeit kielégítő polinom.

II. megoldás. A feladat feltétele és az előljáróban bizonyítottak szerint van olyan legalább másodfokú, egész együtt-hatós f polinom, hogy az $f(x) = a$ egyenletnek minden a racionális számra van racionális megoldása – vagyis a $h = f - a$ polinomnak minden a racionális számra van racionális gyöke. Legyen $a = 1/p$, ahol p olyan prímszám, amivel az f polinom a_n főegyütthatója nem osztható. Tekintsük a $ph = pf - 1$ egész együtt-hatós polinomot, ennek tehát létezik racionális gyöke. Ugyanakkor itt a konstans tag nem osztható p -vel, a többi együtt-ható viszont osztható vele, a pa_n főegyüttható pedig nem osztható p^2 -tel (hiszen a_n nem osztható p -vel); vagyis erre a polinomra teljesül a *Schönemann–Eisenstein-kritérium* „fordított” változata. Az erről szóló nevezetes tétel szerint ph (és ezzel ekvivalens módon h) nem bontható fel két racionális együtt-hatós, nem konstans polinom szorzatára. Ez viszont ellentmond annak, hogy a polinomnak van racionális gyöke – $h(r) = 0$ ugyanis éppen azt jelenti, hogy $x - r$ kiemelhető h -ból. Mivel pedig

f , és így h is legalább másodfokú, a $h = (x - r) \cdot g$ felbontásban egyik tényező sem konstans. A kapott ellentmondás szerint nem létezik a keresett polinom.

III. megoldás. Legyen ismét $f = a_n x^n + \dots + a_1 x + a_0$ egy keresett, egész együtthatós polinom; nyilván feltehető, hogy a főegyütthatója, a_n pozitív. Ekkor f végtelenben vett határértéke $+\infty$, a $-\infty$ -ben pedig $-\infty$, hiszen egyébként alulról korlátos lenne, és úgy nem vehetne föl minden racionális értéket. Így létezik olyan (pozitív) c korlát, hogy $(c, +\infty)$ -en az f függvény szigorúan monoton nő, és minden $a < c$ -re $f(c) > f(a)$. Ezekből következik, hogy ha $c < m < k$, akkor $f(m)$ és $f(k)$ közötti értékeket csak m és k között vehet fel az f . Így, mivel $k > c$,

$$\begin{aligned} f(k+1) - f(k) &= \\ &= a_n((k+1)^n - k^n) + a_{n-1}((k+1)^{n-1} - k^{n-1}) + \dots + a_1((k+1) - k) = \\ &= a_n \left(nk^{n-1} + \binom{n}{2} k^{n-2} + \dots + 1 \right) + \\ &\quad + a_{n-1} \left((n-1)k^{n-2} + \binom{n-1}{2} k^{n-3} + \dots + 1 \right) + \dots + a_1 = \\ &= na_n k^{n-1} + c_{n-2} k^{n-2} + \dots + c_1 k + c_0, \end{aligned}$$

alkalmas, csak az a_i együtthatóktól és n -től függő c_j konstansokkal. Ezért

$$f(k+1) - f(k) = k^{n-1} \left(na_n + \frac{c_{n-2}}{k} + \dots + \frac{c_1}{k^{n-2}} + \frac{c_0}{k^{n-1}} \right).$$

Az első tényező $+\infty$ -ben vett határértéke $+\infty$, a másodiké na_n , így $f(k+1) - f(k)$ a $+\infty$ -hez tart. Ebből következik, hogy tetszőlegesen sok egész szám esik $f(k+1)$ és $f(k)$ közé, ha k elég nagy, és ezeket az egész értékeket az f -nek $k+1$ és k közé eső racionális helyeken kell felvennie.

Utóbbiak általános alakja $k + \frac{s}{t} = \frac{kt+s}{t}$, ahol $0 < s < t$, és az s, t egészek egymáshoz relatív prímek.

Ha $f(k) < q < f(k+1)$, q egész, és $f\left(\frac{kt+s}{t}\right) = q$, akkor

$$\begin{aligned} a_n \left(\frac{kt+s}{t} \right)^n + a_{n-1} \left(\frac{kt+s}{t} \right)^{n-1} + \dots + a_1 \left(\frac{kt+s}{t} \right) + a_0 &= q, \\ a_n (kt+s)^n + a_{n-1} (kt+s)^{n-1} t + \dots + a_1 (kt+s) t^{n-1} + a_0 t^n &= q t^n, \\ -a_n (kt+s)^n &= a_{n-1} (kt+s)^{n-1} t + \dots + a_1 (kt+s) t^{n-1} + a_0 t^n - q t^n, \end{aligned}$$

így $a_n (kt+s)^n$ osztható t -vel. Mivel s és t egymáshoz relatív prímek, azért $kt+s$ és t is relatív prímek egymáshoz, tehát az a_n is osztható t -vel. Ez véges sok (legfeljebb a_n darab) értéket enged meg t -nek, akkor viszont ($0 < s < t$ miatt) s , és így a szóba jövő $k + \frac{s}{t} = \frac{kt+s}{t}$ helyek száma is korlátozott – mondjuk, legfeljebb M . Ha k olyan nagy, hogy M -nél több egész szám esik $f(k+1)$ és $f(k)$ közé, akkor ellentmondást kapunk, tehát a kívánt polinom nem létezik.

Megjegyzés. Mind a három ismertett megoldás a feltételezett polinomról csupán azt használja ki, hogy minden racionális értéket fölvesz racionális helyen; már ilyen polinom sem létezik tehát.