Jelöljük $p(x)$-szel az $(x-a)^2(x-b)^2+1$ polinomot, és tegyük fel, hogy találtunk két egész együtthatós polinomot, $q(x)$-et és $r(x)$-et, amelyekre

$$q(x)\cdot r(x)\equiv p(x). \tag{1}$$

Ha $q(x)$ főegyütthatója (legmagasabb fokú tagjának együtthatója) b, akkor $r(x)$ főegyütthatója $1/b$, hiszen a két főegyüttható szorzata adja $p(x)$ fő együtthatóját, ami 1. De b és $1/b$ is egész, ami csak úgy lehet, hogy ha $b=\dfrac{1}{b}=+1$ vagy $b=\dfrac{1}{b}=-1$. A második esetben tekinthetjük a $-q(x)$ és $-r(x)$ polinomokat. Ezek szorzata is $p(x)$, mindkettő főegyütthatója $+1$, és nyilván mindkettő egész együtthatós.

(i) Feltehető tehát, hogy (1)-ben $r(x)$ és $q(x)$ főegyütthatója is $+1$.

Világos, hogy $p(x)\geqq 1$ minden valós x-re, $p(x)$-nek tehát nincsen valós gyöke, következésképp $q(x)$-nek és $r(x)$-nek sincsen. Ezért $q(x)$ és $r(x)$ nem lehet elsőfokú, vagyis

(ii) $q(x)$ és $r(x)$ másodfokú polinomok. (i) szerint $q(x)$ és $r(x)$ főegyütthatója egyenlő, ezért

(iii) $q(x)-r(x)$ (legfeljebb) elsőfokú.

A $p(x)$ polinom az $x=a$ és az $x=b$ helyen 1 értéket vesz fel, (1) szerint tehát

$$p(a)=q(a)r(a)=p(b)=q(b)r(b)=1. \tag{1'}$$

$q(x)$ és $r(x)$ egész együtthatós, a és b egész, tehát $q(a)$, $r(a)$, $q(b)$ és $r(b)$ egész számok. Ha két egész szám szorzata 1, akkor a számok egyenlők, hisz vagy mindkettő 1, vagy pedig mindkettő -1. Ezért

$$q(a)=r(a)\quad \text{és}\quad q(b)=r(b),$$

vagyis

$$q(a)-r(a)=q(b)-r(b)=0. \tag{2}$$

(2) szerint

(iv) a $q(x)-r(x)$ legfeljebb elsőfokú polinomnak a is és b is gyöke. De a és b különbözők, és egy legfeljebb elsőfokú polinomnak csak úgy lehet két különböző gyöke, ha a polinom azonosan nulla. Azt kaptuk tehát, hogy

(v) $q(x)\equiv r(x)$, vagyis (1) alapján

$$(x-a)^2(x-b)^2+1=q^2(x). \tag{3}$$

Jelöljük most $s(x)$-szel az $(x-a)(x-b)$ polinomot! Ekkor (3) így alakul:

$$s^2(x)+1\equiv q^2(x),\quad \text{ahonnan}$$
$$(q(x)-s(x))(q(x)+s(x))=1.$$

Két polinom szorzata csak akkor lehet konstans, ha mindkettő konstans, így

(vi) $q(x)-s(x)$ és $q(x)+s(x)$ konstans polinomok.

Ebből viszont következik, hogy különbségük, a $(q(x)+s(x))-(q(x)-s(x))=2s(x)$ polinom is konstans. Ez azonban nem igaz.

Ellentmondásra jutottunk abból a feltevésből, hogy vannak (1)-nek eleget tevő, egész együtthatós $q(x)$ és $r(x)$ polinomok, s ezzel a feladat állítását beláttuk.

Megjegyzés. Általában is igaz, hogy ha a_1, a_2, …, a_n különböző egészek, akkor a $p(x)=(x-a_1)^2(x-a_2)^2\dots(x-a_n)^2+1$ polinom nem bontható két alacsonyabb fokú egész együtthatós polinom szorzatára. Ha ugyanis volna két ilyen polinom, $q(x)$ és $r(x)$, amelyekre tehát (1) teljesül, akkor a megoldásban követett okoskodás most is adja (i)-t, (ii), (iii) és (iv) pedig így alakul:

(ii') $q(x)$ és $r(x)$ is n-edfokú.

(iii') $q(x)-r(x)$ $(n-1)$-edfokú.

(iv') a $q(x)-r(x)$ polinomnak gyöke a_1, a_2, $\dots a_n$.

(v) és (vi) változatlan.

(ii')-ből ugyanúgy vezethető le (iii'), (iv'), (v) és (vi), mint a fenti megoldásban. Elég tehát (ii')-t bebizonyítani.

Ehhez megint felhasználjuk, hogy $q(x)$-nek és $r(x)$-nek nincs valós gyöke. (i) szerint főegyütthatójuk pozitív, tehát értékük nagy pozitív számokra pozitív. Ha felvennének negatív értéket is, akkor lenne gyökük is, mert $r(x)$ is, $q(x)$ is folytonos függvény. Így $q(x)$ és $r(x)$ csak pozitív értékeket vehet fel.

(1') most így írható: $1=q(a_1)r(a_1)=\ldots=q(a_j)r(a_j)=\ldots=q(a_n)r(a_n)$. Mivel $q(a_i)$, $r(a_i)$ egész szám, tehát $q(a_i)$, $r(a_i)$ csak ±1 lehet. De láttuk, hogy -1 nem lehet, vagyis $q(a_1)=q(a_2)=\ldots=q(a_n)=1=r(a_1)=r(a_2)=\ldots=r(a_n)$. A $q(x)-1$ polinomnak találtunk tehát n darab különböző gyökét, így $q(x)-1$ és $q(x)$ is legalább n-edfokú.

Ugyanúgy $r(x)$ is legalább n-ed fokú. $q(x)$ és $r(x)$ fokszámának összege (1) szerint $2n$, tehát $q(x)$ is, $r(x)$ is pontosan n-edfokú, ahogyan (ii') állítja.

(ii')-ből most már a megoldás gondolatmenetével vezethető le (vi), ahol $s(x) = (x - a_1)\dots(x - a_n)$, majd innen hogy $s(x)$ konstans, ami ellentmondás. Ez az ellentmondás bizonyítja állításunkat, hogy tehát $p(x)$ nem bontható két egész együtthatós, alacsonyabb fokú polinom szorzatára. Az itt igazolt állítás és annak egy bizonyítása megtalálható *Sklarszkij-Csencov-Jaglom:* Válogatott feladatok és tételek az elemi matematika köréből I. rész c. könyvének 211. feladatában.