Megoldás. Tegyük fel, hogy az állítással ellentétben léteznek olyan legalább elsőfokú egész együtthatós p és q polinomok, amelyekre

$$f(x) = (x - a_1)(x - a_2) \dots (x - a_n) - 1 = p(x) \cdot q(x).$$

Ekkor minden $1 \leq i \leq n$ esetén $p(a_i) \cdot q(a_i) = f(a_i) = -1$. Mivel $p(a_i)$ és $q(a_i)$ egész számok ez azt jelenti, hogy közülük az egyik 1-gyel, a másik pedig -1-gyel egyenlő. Mindenképpen igaz tehát, hogy $p(a_i) + q(a_i) = 0$. Mivel p és q legalább elsőfokú és a szorzatuk f, ami n-edfokú, azért mindegyikük foka legfeljebb $n - 1$; így a $p + q$ olyan legfeljebb $(n - 1)$-edfokú polinom, amelynek van n darab különböző gyöke: $a_1, a_2, \dots, a_n$. Ez csak úgy lehet, hogy $p + q = 0$, vagyis $q = -p$, tehát $f = -p^2$. Ez azonban nem lehetséges, hiszen f főegyütthatója 1, a $-p^2$ polinomé pedig nyilván negatív.

Megjegyzések. 1. Eljutva a fenti gondolatmenetben odáig, hogy minden $1 \leq i \leq n$-re a $p(a_i)$ és $q(a_i)$ egyike 1, a másika pedig -1, a bizonyítás folytatására egy másik út is kínálkozik. Mivel egy $k \geq 1$-edfokú polinom semmilyen értéket sem vehet föl k-nál többször, és a p és q fokának összege n, mindketten ugyanannyiszor veszik fel az 1 és a -1 értéket, és ez a szám egyben mindkettőjük közös foka, $n/2$. Ha például a $p(x)$ polinom éppen az $a_1, a_2, \dots, a_k$ helyeken vesz fel 1-et (és az $a_{k+1}, a_{k+2}, \dots, a_{2k}$ helyeken -1-et), akkor az előbbi feltétel alapján

$$p(x) - 1 = c(x - a_1)(x - a_2) \dots (x - a_k)$$

alakú, alkalmas c egésszel. Viszont a $p(a_{j+k}) = -1$ $(1 \leq j \leq k)$ feltétel szerint

$$p(x) + 1 = d(x - a_{k+1})(x - a_{k+2}) \dots (x - a_{2k}),$$

alkalmas d egésszel. A két eredményt összevetve azt kapjuk, hogy egyrészt nyilván $c = d$ (a p polinom főegyütthatója), másrészt

$$1 + c(x - a_1)(x - a_2) \dots (x - a_k) = -1 + c(x - a_{k+1})(x - a_{k+2}) \dots (x - a_{2k}).$$

A sors fintora, hogy a kapott azonosság bizonyos esetekben nem vezet ellentmondáshoz. A feladat alábbiakban tárgyalt változatában viszont éppen ezeket a kivételes eseteket kell meghatározni.

2. A $g(x) = (x - a_1)(x - a_2) \dots (x - a_n) + 1$ polinom nem mindig felbonthatatlan. A közölt megoldáshoz hasonlóan azonban meghatározható, hogy pontosan mely esetekben bomlik föl a g két legalább elsőfokú egész együtthatós polinom szorzatára. Két ilyen eset van: 1. $n = 2$, $\{a_1, a_2\} = \{a, a + 2\}$, illetve 2. $n = 4$, $\{a_1, a_2, a_3, a_4\} = \{a, a + 1, a + 2, a + 3\}$, ahol a tetszőleges egész szám. Az első esetben

$$(x - a)(x - a - 2) + 1 = \big((x - a - 1) + 1\big)\big((x - a - 1) - 1\big) + 1 = (x - a - 1)^2,$$

a második esetben pedig

$$\begin{aligned} g(x) &= \big((x - a - 1)(x - a - 2)\big)\big((x - a)(x - a - 3)\big) + 1 = \\ &= \big((x - a - 1)(x - a - 2) - 1\big)\big((x - a)(x - a - 3) + 1\big) = \\ &= \big(x^2 - (2a + 3)x + (a^2 + 3a + 1)\big)^2. \end{aligned}$$