I. megoldás. Ha a $p(x)$ polinom konstans, akkor $p\big(p(x)\big) = p(x) = q(x)^2$, így $r(x) = q(x)$ megfelelő választás. Megmutatjuk, hogy a kérdésre igenlő a válasz akkor is, ha a p polinom legalább elsőfokú, amit a továbbiakban felteszünk. A bizonyításhoz felhasználjuk a komplex számkört és az algebra alaptételét. Konkrétan azt, hogy ha $p(x) = a_0 + a_1x + \ldots + a_kx^k$, akkor léteznek olyan $\alpha_1, \alpha_2, \ldots, \alpha_k$ komplex számok, melyekre

$$p(x) = a_k \cdot (x - \alpha_1) \cdot (x - \alpha_2) \cdot \ldots \cdot (x - \alpha_k) \tag{1}$$

teljesül, továbbá ez az ú.n. kanonikus alak az $(x - \alpha_i)$ gyöktényezők sorrendjétől eltekintve egyértelmű. Világos, hogy a fenti α_i számok a polinom gyökei, továbbá, mivel a $p(x)$ polinom valós együtthatós, ha α_i gyöke $p(x)$-nek, akkor annak $\overline{\alpha_i}$ is gyöke lesz, ráadásul e két gyök multiplicitása megegyezik, hiszen ha α_i nem valós, akkor

$$\frac{p(x)}{(x - \alpha_i)(x - \overline{\alpha_i})} = \frac{p(x)}{\big(x^2 - 2\operatorname{Re}(\alpha_i) \cdot x + |\alpha_i|^2\big)}$$

valós együtthatós polinomok hányadosaként maga is valós együtthatós. Ezért pontosan akkor létezik olyan valós együtthatós $r(x)$ polinom, amelyre $p(x) = r(x)^2$, ha az a_k főegyüttható nemnegatív, valamint $p(x)$ fenti kanonikus alakjában minden $(x - \alpha_i)$ gyöktényező páros sokszor fordul elő.

Az algebra alaptétele szerint tehát a kompozíciópolinom előáll

$$p\big(p(x)\big) = a_k \cdot \big(p(x) - \alpha_1\big) \cdot \big(p(x) - \alpha_2\big) \cdot \ldots \cdot \big(p(x) - \alpha_k\big) \tag{2}$$

alakban. Mivel $p\big(p(x)\big) = q(x)^2$, ezért fokszámaik megegyeznek: $p\big(p(x)\big)$-é k^2, $q(x)^2$-é pedig páros. Így $deg\big(p(x)\big) = k$ is páros. Az is látszik a (2) alapján, hogy $p\big(p(x)\big)$ főegyütthatója a_k^{k+1}, és ez megegyezik $q(x)^2$ pozitív főegyütthatójával. Ezért $a_k^{k+1} > 0$. Mivel $k+1$ páratlan, innen $a_k > 0$ adódik.

Figyeljük meg továbbá, hogy $p\big(p(x)\big)$ kanonikus alakja megkapható úgy, hogy a (2) szorzatban minden nemkonstans tényezőt helyettesítünk az adott tényezőnek a k gyöktényezőt tartalmazó kanonikus alakjával, azaz $\big(p(x) - \alpha_i\big)$-t egy

$$p(x) - \alpha_i = a_k \cdot (x - \alpha_{i,1}) \cdot (x - \alpha_{i,2}) \cdot \ldots \cdot (x - \alpha_{i,k})$$

polinommal. A konstrukcióból világos, hogy $p(\alpha_{i,j}) = \alpha_i$, ezért $\alpha_i \neq \alpha_{i'}$ esetén $\alpha_{i,j} \neq \alpha_{i',j'}$ adódik. Azaz $p\big(p(x)\big)$ kanonikus alakjában egy $(x - \alpha_{i,j})$ gyöktényező előfordulásainak száma megegyezik az (1) kanonikus alakjában az $(x - \alpha_i)$ előfordulásai számának és a $p(x) - \alpha_i$ polinom kanonikus alakjában az $(x - \alpha_{i,j})$ gyöktényező előfordulásai számának szorzatával. A $p\big(p(x)\big) = q(x)^2$ azonosság miatt tehát minden ilyen $(x - \alpha_{i,j})$ gyöktényező páros sokszor fordul elő $p\big(p(x)\big)$ kanonikus alakjában.

A feladat kérdésére adott igenlő válasz igazolásához elegendő megmutatni, hogy az (1) kanonikus alakban minden $(x - \alpha_i)$ gyöktényező páros sokszor fordul elő. Ezt indirekt módon bizonyítjuk: tegyük fel, hogy valamely $(x - \alpha_i)$ gyöktényező multiplicitása páratlan. Tekintettel arra, hogy a $p\big(p(x)\big)$ polinom fokszáma k^2, és a $p\big(p(x)\big) = q(x)^2$ azonosság miatt k^2 páros, a $p(x)$ polinom k fokszámának is párosnak kell lennie. Ez viszont azt jelenti, hogy az (1) kanonikus alakban a páratlan multiplicitású gyöktényezők száma páros. Létezik tehát egy $\alpha_{i'} \neq \alpha_i$ gyök, amelyre az $(x - \alpha_{i'})$ gyöktényező is páratlan sokszor fordul elő az (1) alakban. A fenti megfigyelésünk szerint tehát mind a $p(x) - \alpha_i$, mind a $p(x) - \alpha_{i'}$ polinomok kanonikus alakja olyan, hogy azokban minden gyöktényező páros sokszor fordul elő. Más szóval, léteznek olyan $r_1(x)$ és $r_2(x)$ polinomok, melyekre

$$p(x) - \alpha_i = r_1(x)^2 \qquad \text{és} \qquad p(x) - \alpha_{i'} = r_2(x)^2. \tag{3}$$

Ezek szerint

$$\begin{aligned} \alpha_{i'} - \alpha_i &= \big(p(x) - \alpha_i\big) - \big(p(x) - \alpha_{i'}\big) = r_1(x)^2 - r_2(x)^2 = \\ &= \big(r_1(x) + r_2(x)\big) \cdot \big(r_1(x) - r_2(x)\big). \end{aligned}$$

Azt kaptuk, hogy a bal oldalon található konstans előáll két polinom szorzataként, vagyis mind $r_1(x) + r_2(x)$, mind $r_1(x) - r_2(x)$ konstans polinomok. Ekkor azonban ezek összege, $r_1(x) + r_2(x) + r_1(x) - r_2(x) = 2 \cdot r_1(x)$ is konstans polinom, tehát (3) alapján $p(x) = r_1(x)^2 - \alpha_i$ is konstans, ami ellentmond a kezdeti feltevésünknek. Ezzel pedig kétséget kizáróan igazoltuk a feladat kérdésére adott igenlő választ. □

II. megoldás. Meg fogjuk mutatni, hogy a megadott feltételek mellett mindig létezik olyan r valós együtthatós polinom, melyre $p(x) = r(x)^2$.

Ha $p\big(p(x)\big) = q(x)^2$, akkor $(\deg p)^2 = 2\deg q$, és így a p polinom foka páros. Továbbá p főegyütthatója pozitív, különben a ∞-ben $p\big(p(x)\big)$, és így $q(x)^2$ határértéke is negatív lenne. Legyen tehát $p(x) = a_{2n}x^{2n} + a_{2n-1}x^{2n-1} + \ldots + a_1x + a_0$, ahol n nemnegatív egész szám és $a_{2n} > 0$. Megmutatjuk hogy léteznek olyan r és s valós együtthatós polinomok, melyekre $p(x) = r(x)^2 + s(x)$ és $\deg s < n$. Mivel egy ilyen r polinom foka csak n lehet, keressük r-et $r(x) = b_nx^n + b_{n-1}x^{n-1} + \ldots + b_1x + b_0$ alakban. Akkor kapunk megfelelő előállítást, ha $p(x)$-ben és $r(x)^2$-ben minden $n \leq j \leq 2n$-re megegyezik x^j együtthatója. Ha b_i értékét $i = n, n-1, \ldots, 0$ sorrendben választjuk meg, akkor b_i

megfelelő választásával elérhető, hogy x^{n+i} együtthatója egyezzen. Legyen ugyanis $b_n = \sqrt{a_{2n}}$, ekkor x^{2n} együtthatója egyezik. Tegyük fel, hogy $b_n, b_{n-1}, \ldots, b_{i+1}$ értékét már rögzítettük. Mivel $r(x)^2$-ben x^{n+i} együtthatója $\sum\limits_{i \le k \le n} b_k b_{n+i-k}$, így

$$b_i = \frac{a_{n+i} - \sum_{i<k<n} b_k b_{n+i-k}}{2b_n}$$

választással x^{n+i} együtthatója éppen a_{n+i} lesz $r(x)^2$-ben is. Az így megválasztott n-edfokú $r(x)$ polinomra valóban n-nél kisebb fokú lesz az $s(x) = p(x) - r(x)^2$ polinom.

Mivel $q(x)^2 = p\big(p(x)\big) = r\big(p(x)\big)^2 + s\big(p(x)\big)$, ezért

$$s\big(p(x)\big) = q(x)^2 - r\big(p(x)\big)^2 = \big[q(x) + r\big(p(x)\big)\big] \cdot \big[q(x) - r\big(p(x)\big)\big]\,.$$

Az $s\big(p(x)\big)$ polinom foka s és p fokának szorzata, és így kisebb, mint $2n^2$. Ha $s \not\equiv 0$, akkor ebből az is következik, hogy a $q(x) + r\big(p(x)\big)$ és $q(x) - r\big(p(x)\big)$ polinomok foka is kisebb, mint $2n^2$. Ekkor viszont

$$q(x) = \frac{q(x) + r\big(p(x)\big) + q(x) - r\big(p(x)\big)}{2}$$

foka is $2n^2$-nél kisebb lenne, ami ellentmondás, hiszen $\deg q = \dfrac{(\deg p)^2}{2} = 2n^2$. Mindez azt jelenti, hogy $s \equiv 0$, és így $p(x) = r(x)^2$. $\square$

Megjegyzés. Williams Kada megjegyzése nyomán könnyen látható, hogy az I. megoldás módszerével igazolható a kitűzött feladat azon általánosítása, mely szerint ha valamely valós együtthatós $p(x)$ és $q(x)$ polinomokra, illetve $k \ge 2$ prímszámra $p\big(p(x)\big) = q(x)^k$ teljesül, akkor van olyan valós együtthatós $r(x)$ polinom, amelyre $p(x) = r(x)^k$ áll fenn.