Megmutatjuk, hogy ha $r(x)$ nem nulla, egész együtthatós polinom és $q(x) = r(x)p(x) + x$, akkor $p(q(x))$-ből $p(x)$ kiemelhető, sőt a két polinom hányadosa is egész együtthatós.

Legyen

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0,$$

ahol $a_0, \ldots, a_n$ egész számok.

A binomiális tétel alapján tetszőleges k pozitív egészre

$$\begin{aligned} q^k(x) = (r(x)p(x) + x)^k = \\ = \binom{k}{0} r^k(x)p^k(x) + \binom{k}{1} r^{k-1}(x)p^{k-1}(x)x + \binom{k}{2} r^{k-2}(x)p^{k-2}(x)x^2 + \ldots \\ \ldots + \binom{k}{k-1} r(x)p(x)x^{k-1} + \binom{k}{k} x^k = \\ = \left(\binom{k}{0} r^k(x)p^{k-1}(x) + \binom{k}{1} r^{k-1}(x)p^{k-2}(x)x + \binom{k}{2} r^{k-2}(x)p^{k-3}(x)x^2 + \ldots \right. \\ \left. \ldots + \binom{k}{k-1} r(x)x^{k-1} \right) p(x) + x^k. \end{aligned}$$

Az első tényezőt az egyszerűség kedvéért jelöljük $m_k(x)$-szel:

$$q^k(x) = m_k(x)p(x) + x^k,$$

ahol m_k egész együtthatós polinom.

Ezeket az azonosságokat behelyettesítve $p(q(x))$-be:

$$\begin{aligned} p(q(x)) = \\ = a_n \left(m_n(x)p(x) + x^n\right) + a_{n-1}\left(m_{n-1}(x)p(x) + x^{n-1}\right) + \ldots + a_1\left(m_1(x)p(x) + x\right) + a_0 = \\ = \left(a_n m_n(x) + a_{n-1}m_{n-1}(x) + \ldots + a_1 m_1(x)\right)p(x) + \left(a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0\right) = \\ = \left(a_n m_n(x) + a_{n-1}m_{n-1}(x) + \ldots + a_1 m_1(x) + 1\right)p(x). \end{aligned}$$

Az első tényező most is egész együtthatós.

Ezután már csak az $r(x)$ polinomot kell megválasztanunk, vigyázva arra, hogy $p(q(x))$ szorzat alakjában mindkét tényező legalább elsőfokú legyen. Ez a $p(x)$ tényezőre biztosan teljesül. A másik tényező pedig pontosan akkor legalább elsőfokú, ha $p(q(x))$ foka nagyobb, mint $p(x)$ foka. Mivel $(p(q(x))$ foka $p(x)$ és $q(x)$ fokszámainak szorzata, ez akkor igaz, ha $q(x)$ legalább másodfokú. Ha $p(x)$ legalább másodfokú, akkor $q(x)$ is legalább másodfokú. Ha $p(x)$ elsőfokú, akkor szükséges és elégséges az, ha $r(x)$ legalább elsőfokú.

Tehát, ha $p(x)$ elsőfokú, akkor legyen $r(x) = x$, azaz $q(x) = xp(x) + x$. Ha pedig $p(x)$ legalább másodfokú, akkor legyen $r(x) = 1$ és $q(x) = p(x) + x$.

Tóth Gábor Zsolt (Budapest, Árpád Gimn., III. o.t.) dolgozata alapján