(Megjegyzés a 2508. feladathoz)[1]

A 2508. feladatban olyan ötödfokú f polinomot kellett megadni, amelyre teljesül, hogy $[f(x)-1]$-ből $(x+1)^3$, $[f(x)+1]$-ből pedig $(x-1)^3$ kiemelhető. Azt, hogy ilyen polinom létezik, a feladat feltételezte.

De vajon akkor is létezik-e megoldás, ha a konstansokat megváltoztatjuk, azaz: megadható-e olyan n-edfokú f polinom, amelyre teljesül, hogy $[f(x)-\alpha_i]$-ből $(x-\beta_i)^{\gamma_i}$ kiemelhető, ahol $\alpha_1, \alpha_2, \ldots, \alpha_k, \beta_1, \beta_2, \ldots, \beta_k$ adott valós számok, $\gamma_1, \gamma_2, \ldots, \gamma_k$ adott pozitív egészek?

Ez a kérdés emlékeztet egy számelméleti problémára:

Legyenek $m_1, m_2, \ldots, m_k$; $a_1, a_2, \ldots, a_k$ egész számok. Létezik-e olyan M egész szám, amelyre teljesül, hogy $M-a_i$ osztható m_i-vel?

A probléma így egy bizonyára sokak által ismert feladattípus általános megfogalmazása. Például a következő formában találkozhattunk vele: ha néhány gyereket párosával állítunk sorba, akkor egy gyerek marad a sor végén, ha hármasával, akkor pedig kettő. Hányan maradnak, ha hatosával állítjuk őket sorba?

A kérdés megválaszolásához olyan M számokat kell keresnünk, amelyek 2-vel osztva 1, 3-mal osztva pedig 2 maradékot adnak, azaz $M-1$ osztható 2-vel, $M-2$ pedig osztható 3-mal. Egyszerűen belátható, hogy éppen a 6-tal osztva 5 maradékot adó számok rendelkeznek a fenti tulajdonsággal.

Ami az általános számelméleti problémát illeti, a szóban forgó M szám nem feltétlenül létezik. Legyen például $m_1=4$, $m_2=6$, $a_1=1$ és a $a_2=2$. Ha most $M-1$ osztható 4-gyel, akkor M páratlan és így $M-2$ nem lehet 6-tal osztható. Ebben a példában m_1 és m_2 is páros volt, és hasonló ellenpéldák készíthetők általában is, ha az adott m_i-k között vannak páronként nem relatív prímek. A 2508. feladatban szereplő $m_1(x)=(x+1)^3$ és $m_2(x)=(x-1)^3$ polinomok azonban számelméleti szempontból nem ilyenek. Nincs közös tényezőjük, a legnagyobb közös osztójuk 1. Nos, ha az adott m_i számok páronként relatív prímek, akkor már igennel válaszolhatunk a feltett kérdésre, ahogy ezt az alábbi tétel állítja:

(I) *Kínai maradéktétel*

Ha $m_1, m_2, \ldots, m_k$ páronként relatív prím egész számok és $a_1, a_2, \ldots, a_k$ tetszőleges egész számok, akkor az $M \equiv a_i \pmod{m_i}$ kongruenciáknak van közös M megoldása, és a megoldások kongruensek modulo $m_1 \cdot m_2 \cdot \ldots \cdot m_k$.

A tételt megfogalmazhatjuk a polinomok nyelvén is:

(II) *Ha az $m_1, m_2, \ldots, m_k$ polinomok páronként relatív prímek (azaz nem emelhető ki belőlük ugyanaz a legalább elsőfokú polinom), $a_1, a_2, \ldots, a_k$ pedig tetszőleges polinomok, akkor van olyan M polinom, amelyre teljesül, hogy $[M(x)-a_i(x)]$-ből $m_i(x)$ kiemelhető; bármely két ilyen M polinom különbségéből $m_1(x)\cdot m_2(x)\cdot \ldots \cdot m_k(x)$ kiemelhető.*

Ez az átfogalmazás annyira szerencsés, hogy még a bizonyítása is szinte szóról szóra megegyezik (I) bizonyításával.

(III) *A maradéktétel bizonyítása*

a) Mivel $m_1, m_2, \ldots, m_k$ páronként relatív prímek, m_i és $m_1 \cdot m_2 \cdot \ldots \cdot m_{i-1} \cdot m_{i+1} \cdot \ldots \cdot m_k = \dfrac{m_1 \cdot m_2 \ldots \cdot m_k}{m_i}$ is relatív prímek. Ekkor viszont létezik olyan b_i egész szám, amelyre $b_i \cdot \dfrac{m_1 m_2 \ldots m_k}{m_i} \equiv 1 \pmod{m_i}$. Ekkor pedig

$$M = \sum_{j=1}^{k} a_j b_j \cdot \frac{m_1 m_2 \ldots m_k}{m_j}$$

megoldás, hiszen $j \neq i$ esetén $a_j b_j \cdot \dfrac{m_1 m_2 \ldots m_k}{m_j}$ osztható m_i-vel és így

$$M = \sum_{j=1}^{k} a_j b_j \cdot \frac{m_1 m_2 \ldots m_k}{m_j} \equiv a_i b_i \cdot \frac{m_1 m_2 \ldots m_k}{m_i} \equiv a_i \cdot 1 = a_i \pmod{m_i}$$

minden $1 \leqq i \leqq k$-ra.

b) Ha M_1 és M_2 két megoldás, akkor $M_1 - M_2$ osztható $m_1, m_2, \ldots, m_k$ mindegyikével, így $[m_1, m_2, \ldots, m_k] = m_1 m_2 \ldots m_k$-val is, tehát

$$M_1 \equiv M_2 \pmod{m_1 m_2 \ldots m_k}.$$

Megfordítva, ha M_1 megoldás és $M_2 \equiv M_1 \pmod{m_1 m_2 \ldots m_k}$, akkor M_2 is megoldás. A megoldások tehát egy modulo $m_1 m_2 \ldots m_k$ maradékosztály elemei.

(A kínai maradéktétel legalább 2000 éves – természetesen nem ebben az általános formában. Történetéről Davis–Hersh: A matematika élménye c. műben olvashatunk, Műszaki Könyvkiadó, 1984. Az utóbbi időben a tételt nagy számokkal végzett számításokra kidolgozott algoritmusokban alkalmazták eredményesen. Erről bővebben: Lovász–Gács: Algoritmusok, Műszaki Könyvkiadó, 1978 c. mű „Moduláris algoritmusok" c. fejezetében olvashatunk. *A szerk.*)

Ahhoz, hogy ugyanezt a bizonyítást elmondhassuk (II)-re is, csupán egy felhasznált tételt kell bebizonyítanunk.

(IV) *Ha p és q relatív prím polinomok, akkor van olyan r polinom, hogy $r(x)\cdot p(x) \equiv 1 \pmod{q(x)}$, azaz vannak olyan r és s polinomok, amelyekre teljesül, hogy $r(x)\cdot p(x) - s(x)\cdot q(x) = 1$.*

[1] A 2508. feladat megoldása az 1985. évi 10. szám 442–444.oldalán olvasható.

A bizonyításhoz az euklideszi algoritmus módszerét alkalmazzuk. Legyen p fokszáma α, q-é β. Ha $\alpha \geqq \beta$, akkor legyen

$$P(x) = p(x) - h \cdot x^{\alpha-\beta} \cdot q(x) \quad \text{és} \quad Q(x) = q(x),$$

ellenkező esetben

$$P(x) = p(x) \quad \text{és} \quad Q(x) = q(x) - \frac{1}{h} \cdot x^{\beta-\alpha} \cdot p(x),$$

ahol h a p és q polinomok főegyüttható inak hányadosa. P vagy Q fokszáma ezzel kisebb lett, mint p, illetve q fokszáma, másfelől P és Q továbbra is relatív prímek, hiszen ha egy nem konstans $f(x)$ polinom kiemelhető lenne belőlük, akkor ugyanez kiemelhető lenne

$$p(x) = P(x) + hx^{\alpha-\beta}Q(x) \quad \text{és} \quad q(x) = Q(x)\text{-ből, illetve}$$
$$p(x) = P(x) \quad \text{és} \quad q(x) = Q(x) + \frac{1}{h}x^{\beta-\alpha}P(x)\text{-ből is.}$$

A fenti fokszámcsökkentés éppen az euklideszi algoritmus maradékos osztásának első fázisa és (IV) bizonyításán túl az állításban szereplő $r(x)$ és $s(x)$ polinomok kiszámolására is alkalmas algoritmus egy lépése.

Lássuk tehát a bizonyítást a p és a q fokszámának összege szerinti teljes indukcióval!

Ha p és q fokszámának összege 0, akkor mindkét polinom konstans, és $r(x) = \frac{1}{p}$ és $s(x) = 0$ megfelelő. Tegyük fel, hogy a bizonyítást elvégeztük azokra az esetekre, amikor a fokszámok összege kisebb, mint n.

Bebizonyítjuk az állítást akkor is, amikor ez az összeg éppen n. Definiáljuk a P és Q polinomokat az előbbiek szerint! Ezek relatív prímek, és fokszámaik összege kisebb, mint p és q fokszámának összege, n. Ezért az indukciós feltevés szerint léteznek olyan R és S polinomok, hogy $R(x) \cdot P(x) - S(x) \cdot Q(x) = 1$.

Most írjunk $P(x)$, $Q(x)$ helyére $p(x) - hx^{\alpha-\beta}q(x)$, $q(x)$-et, illetve $p(x)$, $q(x) - \frac{1}{h}x^{\beta-\alpha}p(x)$-et:

$$R(x) \cdot [p(x) - hx^{\alpha-\beta}q(x)] - S(x)q(x) = R(x)p(x) - [hx^{\alpha-\beta} + S(x)] \cdot q(x) = 1,$$

illetve

$$R(x)p(x) - S(x) \cdot \left[q(x) - \frac{1}{h}x^{\beta-\alpha}p(x)\right] =$$
$$= \left[\frac{1}{h}x^{\beta-\alpha} + R(x)\right] p(x) - S(x)q(x) = 1.$$

Azt kaptuk tehát, hogy $r(x) = R(x)$ és $s(x) = S(x) + hx^{\alpha-\beta}$, illetve $r(x) = R(x) + \frac{1}{h}x^{\beta-\alpha}$ és $s(x) = S(x)$ megfelelő.

Most már bebizonyíthatjuk a (II) állítást:

(V) *a)* Mivel az m_1, m_2, …, m_k polinomok közül semelyik kettőnek nincs közös (komplex) gyöke, m_i-nek és $m_1 \cdot m_2 \cdot \ldots \cdot m_{i-1} \cdot m_{i+1} \cdot \ldots \cdot m_k = \frac{m_1 m_2 \ldots m_k}{m_i}$-nek sincs, tehát m_i és $\frac{m_1 m_2 \ldots m_k}{m_i}$ relatív prímek.

(IV) alapján tehát létezik olyan b_i polinom, hogy $\left[b_i(x)\frac{m_1(x)m_2(x)\ldots m_k(x)}{m_i(x)} - 1\right]$-ből $m_i(x)$ kiemelhető.

Ebből pedig következik, hogy

$$M(x) = a_1(x)b_1(x)\frac{m_1(x)m_2(x)\ldots m_k(x)}{m_1(x)} +$$
$$+a_2(x)b_2(x)\frac{m_1(x)m_2(x)\ldots m_k(x)}{m_2(x)} + \ldots + a_k(x)b_k(x)\frac{m_1(x)m_2(x)\ldots m_k(x)}{m_k(x)}$$

megoldás, hiszen minden $1 \leqq i \leqq k$-ra

$$M(x) - a_i(x) = a_1(x)b_1(x)\frac{m_1(x)\ldots m_k(x)}{m_1(x)} + \ldots + a_{i-1}(x)b_{i-1}(x)\frac{m_1(x)\ldots m_k(x)}{m_{i-1}(x)} +$$
$$+a_i(x)\left[b_i(x)\frac{m_1(x)\ldots m_k(x)}{m_i(x)} - 1\right] +$$
$$+a_{i+1}(x)b_{i+1}(x)\frac{m_1(x)\ldots m_k(x)}{m_{i+1}(x)} + \ldots + a_k(x)b_k(x)\frac{m_1(x)\ldots m_k(x)}{m_k(x)}$$

minden tagjából kiemelhető $m_i(x)$.

b) Ha M_1 és M_2 két különböző megoldás, akkor $M_1 - M_2$-ből m_1, m_2, …, m_k mindegyike kiemelhető. Ekkor viszont összes (komplex) gyöktényezőjük kiemelhető, így $m_1 m_2 \ldots m_k$ is, ami ezek szorzatának egy konstansszorosa.

A megfordítás ugyanúgy bizonyítható, mint a kínai maradéktétel:

Ha M_1 megoldás és $M_1 - M_2$-ből $m_1 m_2 \dots m_k$ kiemelhető, akkor M_2 is megoldás, mert minden $1 \leqq i \leqq k$-ra

$$M_2(x) - a_i(x) = [M_1(x) - a_i(x)] - [M_1(x) - M_2(x)]\text{-ből}$$

$m_i(x)$ kiemelhető.

Ezzel (II)-t bebizonyítottuk.

A 2508. feladatban szereplő polinomok együtthatói egész számok voltak, így joggal vetődik fel a kérdés, vajon várható-e, hogy a kapott M polinom is ilyen. A kulcsfontosságú (IV) állítás bizonyításának indukciós lépésében a $P(x)$ és a $Q(x)$ együtthatóinak számolásakor a $p(x)$ és a $q(x)$ főegyütthatóinak h hányadosát használjuk, ami nem szükségképpen egész, így a végül kapott $r(x)$ és $s(x)$ polinomok együtthatóiról csak annyit állíthatunk, hogy racionálisak, és így a felhasználásukkal nyert M polinom is ilyen.

A (II) tételben ugyanakkor a komplex számtestbe ágyazva fogalmaztuk meg az m_i polinomok relatív prím voltát. Az oszthatóság ténye a polinomok között függ attól, hogy milyen számkörből valók az együtthatók. Az egész együtthatós polinomok körében például a $2x+2$ polinom nem osztója a $3x^2+3x$ polinomnak, a racionális együtthatós polinomok körében már igen $\left[3x^2+3x = \frac{3}{2}x(2x+2)\right]$.

(A legnagyobb közös osztó – és így a polinomok relatív prím volta – viszont nem függ attól, hogy az egész, a racionális, a valós vagy pedig a komplex számkörből indulunk-e ki. Az algebra alaptételének felhasználásával megmutatható, hogy ha két egész együtthatós polinomnak 1 a legnagyobb közös osztója, akkor nem lehet közös komplex gyökük sem; a feltételben tehát jogosan használtuk az ilyen polinomok relatív prím voltának e legáltalánosabb jellemzését. *A szerk.*)

(II) egyszerű következménye az alábbi tétel.

(VI) *Legyenek m_1, m_2, …, m_k páronként relatív prím polinomok, m_i fokszáma φ_i; a_1, a_2, …, a_k pedig tetszőleges polinomok. Ekkor pontosan egy olyan M polinom létezik, amelynek fokszáma kisebb, mint $\varphi_1 + \varphi_2 + \ldots + \varphi_k$, és $[M - a_i(x)]$-ből $m_i(x)$ kiemelhető* $(i = 1, 2, \ldots, k)$.

Ilyen megoldást előállíthatunk az ismert osztási algoritmus segítségével: egy tetszőleges M^* polinomot, amely eleget tesz az $M^*(x) = a_i(x) \pmod{m_i(x)}$ kongruenciáknak, elosztjuk az $m_1(x) \cdot m_2(x) \cdot \ldots \cdot m_k(x)$ polinommal, és az osztási maradék megfelelő lesz.

Az is könnyen látható, hogy legfeljebb egy ilyen polinom létezik; ha M_1 és M_2 is eleget tenne a feltételeknek, $M_1 - M_2$ osztható lenne $m_1 m_2 \dots m_k$-val. Mivel viszont $M_1 - M_2$ fokszáma kisebb, mint $m_1 m_2 \dots m_k$ fokszáma, $\varphi_1 + \varphi_2 + \ldots + \varphi_k$, azért $M_1 - M_2$ csak azonosan 0 lehet, ami ellentmond annak a feltételezésünknek, hogy M_1 és M_2 különböző.

Befejezésül nézzük meg a 2508. feladat egy némiképp számolásigényes megoldását a fenti eredmények felhasználásával. Az adatok:

$$m_1(x) = x^3 + 3x^2 + 3x + 1, \quad m_2(x) = x^3 - 3x^2 + 3x - 1,$$
$$a_1(x) = 1, \quad a_2(x) = -1.$$

Először írjuk fel azokat az $r(x)$ és $s(x)$ polinomokat, amelyekre a (IV) állítás szerint $r(x) \cdot m_1(x) - s(x) \cdot m_2(x) = 1$.

Az $m_1(x)$ és $m_2(x)$ polinomok között az euklideszi algoritmust elvégezve és a maradékokat kifejezve:

$$m_1(x) = m_2(x) + (6x^2+2), \quad \text{ebből} \quad 6x^2 + 2 = m_1(x) - m_2(x), \tag{1}$$

$$m_2(x) = \left(\frac{1}{6}x - \frac{1}{2}\right)(6x^2+2) + \frac{8}{3}x, \quad \text{ebből} \quad \frac{8}{3}x = m_2(x) - (6x^2+2)\left(\frac{1}{6}x - \frac{1}{2}\right), \tag{2}$$

$$6x^2 + 2 = \frac{9}{4}x \cdot \frac{8}{3}x + 2, \quad \text{ebből} \quad 2 = (6x^2+2) - \frac{8}{3}x \cdot \frac{9}{4}x. \tag{3}$$

(2)-ből (1) alapján

$$\frac{8}{3}x = m_2(x) - [m_1(x) - m_2(x)] \cdot \left[\frac{1}{6}x - \frac{1}{2}\right] = \tag{4}$$
$$= m_2(x) \cdot \left[\frac{1}{6}x - \frac{1}{2}\right] - m_1(x) \cdot \left[\frac{1}{6}x - \frac{1}{2}\right],$$

és (3)-ból hasonlóan kapjuk (4) és (l) felhasználásával, hogy

$$2 = m_1(x) \cdot \left(\frac{3}{8}x^2 - \frac{9}{8}x + 1\right) - m_2(x) \cdot \left(\frac{3}{8}x^2 + \frac{9}{8}x + 1\right)$$

Ha mindkét oldalt osztjuk 2-vel, akkor épp a kívánt felbontást kapjuk, innen tehát

$$r(x) = \frac{3}{16}x^2 - \frac{9}{16}x + \frac{1}{2} \text{ és } s(x) = \frac{3}{16}x^2 - \frac{9}{16}x + \frac{1}{2}.$$

A (II) tétel bizonyítása, (V) alapján most már felírhatjuk az M polinomot.

$$M(x) = 1 \cdot [-s(x)] \cdot \frac{m_1(x)m_2(x)}{m_1(x)} + (-1) \cdot r(x) \cdot \frac{m_1(x)m_2(x)}{m_2(x)} =$$
$$= -s(x) \cdot m_2(x) - r(x) \cdot m_1(x) = -\frac{3}{8}x^5 + \frac{5}{4}x^3 - \frac{15}{8}x.$$