O ÎNTĂRIRE A UNEI PROBLEME DE OLIMPIADĂ

Sergiu Novac[1)]

Abstract. This article represents a continuation of a contest problem, submitted at the Romanian National Olympiad. The problem asked the contestants to show that a polynomial has at least a certain number of irreducible factors; we show that the number of irreducible factors is precisely that number.

Keywords: finite field, polynomial, irreducible

MSC: 12E05

În anul 2002 a fost propusă următoarea problemă la ONM clasa a 12-a.

Fie $\mathbb{K}$ *un corp cu* $q = p^n$ *elemente, unde* p *e prim, iar* $n \in \mathbb{N}$ *cu* $n \geq 2$. *Pentru* $a \in \mathbb{K}$ *arbitrar se defineşte polinomul* $f_a = X^q - X + a$. *Să se demonstreze că*:

a) f_1 *divide polinomul* $f = (X^p - X)^q - (X^p - X)$;

b) f_a *are cel puţin* p^{n-1} *divizori ireductibili, neasociaţi doi câte doi în divizibilitate.*

Pentru completitudine, prezentăm şi soluţia „oficială”.

[1)] Student.

a) Este clar că $p = char(\mathbb{K})$ şi, deoarece $C_q^i \equiv 0 \pmod p$ pentru $i = 0, 1, \ldots, q-1$, obţinem

$$f = (X^p - X)^q - (X^p - X) = \sum_{i=0}^{q} (-1)^i C_q^i X^{p(q-i)} X^i - (X^p - X)$$
$$= X^{pq} - X^q - X^p + X$$

(se poate ridica problema că pentru q par termenul X^q ar apărea cu semnul $+$ în dezvoltare, însă, în acest caz, $p = 2$, deci $-1 = 1 \in \mathbb{K}$). În continuare, $f = X^{pq} - X^p + 1 - X^q + X - 1 = (X^q - X + 1)^p - (X^q - X + 1)$, ceea ce face clar faptul că f_1 divide f.

b) Avem

$$f_0 = X^q - X = \prod_{\alpha \in \mathbb{K}} (X - b),$$

deci f_0 este produsul a q factori de gradul I, neasociaţi doi câte doi în divizibilitate.

Pentru $a \in \mathbb{K}^*$, observăm că $f_a(aX) = af_1(X)$, deci este suficient să demonstrăm rezultatul pentru $a = 1$. Pentru aceasta, din a) avem $f_1 = (f_1, f)$ (unde, ca de obicei, notaţia (u, v) desemnează cel mai mare divizor comun al polinoamelor u, v). Mai mult, notând $g = X^p - X$ avem că $f = g^q - g = \prod_{\alpha \in \mathbb{K}} (g - \alpha)$. Astfel, $f_1 = \left(f_1, \prod_{\alpha \in \mathbb{K}} (g - \alpha) \right) = \prod_{\alpha \in \mathbb{K}} (f_1, g - \alpha)$. Deoarece $\deg(f_1, g - \alpha) \leq \deg(g - \alpha) = p$ deducem că fiecare factor ireductibil al lui f_1 are grad cel mult p, deci există cel puţin p^{n-1} asemenea factori. ($g - \alpha$ si $g - \beta$ sunt coprime, orivare ar fi $\alpha \neq \beta \in \mathbb{K}$, deci factorii sunt neasociaţi în divizibilitate). □

Ne va interesa în principal partea a doua a problemei, în sensul că vom demonstra urmatorul rezultat.

Propoziţia 1. Pentru $a \in \mathbb{K}^*$, f_a are exact p^{n-1} factori ireductibili neasociaţi în divizibilitate.

Demonstraţie. Fie $G \in \mathbb{K}[X]$ un factor ireductibil al lui f_a, de grad m, şi fie $\xi \in \overline{\mathbb{K}}$ o rădăcină a lui G. Atunci, ξ e rădăcină si pentru f_a, deci $\xi^q = \xi - a$, care implică $\xi^{q^2} = (\xi^q - a)^q = \xi^q - a$. Aceasta ne spune pe de-o parte că ξ^q e de asemenea o rădăcină a lui f_a(nu rezultă neapărat că ξ^q ar fi o rădăcină a lui G, însă tocmai asta vom demonstra!). Pe de altă parte, $\xi^{q^2} = \xi^q - a = \xi - 2a$. Iterând, vedem că ξ^{q^k} e rădăcină a lui f_a pentru orice $k \in \mathbb{N}$ şi $\xi^{q^k} = \xi - ka$. Deoarece $char(\mathbb{K}) = p$, elementele ξ^{q^k} sunt distincte două câte două pentru $k \in \{0, 1, \ldots, p-1\}$ şi $\xi^{q^p} = \xi$. Lucrând în extensia $\mathbb{K}(\xi)$, ultima relaţie ne spune că ordinul γ al lui ξ îl divide pe $q^p - 1$. Pe de altă parte, $|\mathbb{K}(\xi)| = q^m$, cu $m \in \mathbb{N}^*$, ceea ce ne spune că γ divide $q^m - 1$. Astfel, $\gamma | (q^p - 1, q^m - 1) = q^{(p,m)} - 1$.

Dacă $(p, m) = 1$ atunci $\gamma | q - 1$ care implica $\xi^q = \xi$ şi deci $f_a(\xi) = a$, ceea ce contrazice faptul că ξ e o rădăcina a lui f_a. Astfel obtinem că $p | m$.

Să observăm că ne-am putea opri aici: am obţinut $m \geq p$, deci $\deg G \geq p$, însă din prima soluţie prezentată ştim că gradul oricărui factor ireductibil al lui f_a e cel mult p, astfel că, de fapt, gradul fiecărui astfel de polinom este exact p. Considerăm, însă, că următorul argument merită prezentat datorită ingeniozităţii sale, a faptului că nu apelează deloc la prima soluţie prezentată (unirea celor 2 argumente complet diferite poate părea superficială), dar şi a faptului că pune în lumină mai multe aspecte ale obiectelor studiate.

Să construim acum polinomul $H = \prod_{k=0}^{p-1}(X - \xi^{p^k})$. Vom arăta că $H \in \mathbb{K}[X]$. Pentru aceasta, scriem H sub forma $H(X) = \sum_{i=0}^{p}(-1)^i \sigma_i X^{p-i}$, unde

$$\sigma_i = \sum_{0 \leq k_1 < k_2 < \ldots < k_i \leq p} \xi^{q^{k_1} + q^{k_2} + \ldots + q^{k_i}}.$$

Uitându-ne la σ_i^q avem

$$\sigma_i^q = \sum_{0 \leq k_1 < k_2 < \ldots < k_i < p} \xi^{q^{1+k_1} + q^{1+k_2} + \ldots + q^{1+k_i}}.$$

Datorită faptului că $\xi^{q^p} = \xi$ avem

$$\sum_{0 \leq k_1 < k_2 < \ldots < k_i < p} \xi^{q^{1+k_1} + q^{1+k_2} + \ldots + q^{1+k_i}} =$$

$$= \sum_{0 \leq k_1 < k_2 < \ldots < k_i < p} \xi^{q^{(1+k_1) \bmod p} + q^{(1+k_2) \bmod p} + \ldots + q^{(1+k_i) \bmod p}} =$$

$$= \sum_{0 \leq k_1 < k_2 < \ldots < k_i < p} \xi^{q^{k_1} + q^{k_2} + \ldots + q^{k_i}},$$

ceea ce ne arată că $\sigma_i^q = \sigma_i$, astfel că $\sigma_i \in \mathbb{K}, \forall i \in \overline{0, p}$, deci $H \in \mathbb{K}[X]$ (ultimul argument, deşi pare laborios, este doar o formalizare a faptului că ridicând σ_i la puterea q nu facem decât să translatăm exponenţii $k_1, k_2, \ldots, k_n$ cu 1, ceea ce nu afectează valoarea sumei, întrucât putem lucra cu exponenţii modulo p). În final, avem că ξ e o rădăcină a lui $H \in \mathbb{K}[X]$, dar, fiind ireductibil, G e polinomul minimal al lui ξ peste $\mathbb{K}$, deci G divide H. Avem, însă, că $m = \deg G \geq p = \deg H$, ceea ce ne arată că G e asociat în divizibilitate cu H şi $\deg G = p$. G a fost arbitrar ales, astfel că orice factor ireductibil al lui f_a are gradul p şi concluzionăm că f_a are exact p^{n-1} factori ireductibili. (Pentru a ne convinge că nu exista doi factori asociaţi în divizibilitate putem observa că $f_a' = -1$, deci f_a e liber de pătrate). □

Încheiem cu un rezultat asupra ireductibilităţii unor polinoame în $\mathbb{K}[X]$. Legătura dintre cele două abordări, destul de diferite, este dată de ireductubilitatea unor polinoame de forma $X^p - X + \alpha \in \mathbb{K}[X]$. Într-adevăr, dacă $g_\alpha =: X^p - X + \alpha$ divide f_1 atunci g_α e ireductibil. Ne propunem atunci să vedem pentru ce α, este g_α ireductibil.

Pentru aceasta introducem polinomul $\phi = X + X^p + X^{p^2} + \ldots + X^{p^{n-1}}$.

Propoziţia 2. Singurele elemente α pentru care g_α nu e ireductibil sunt rădăcinile lui ϕ.

Demonstraţie. Similar cu cea de-a doua abordare prezentată, fie G un factor ireductibil al lui g_α şi $\xi \in \overline{\mathbb{K}}$ o rădăcină a lui G. Deoarece ξ este rădăcină a lui g_α, la fel este şi ξ^q, şi, în general ξ^{q^k} pentru $k \in \mathbb{N}$. Avem, însă, că $\xi^{p^2} = \xi^p - \alpha^p = \xi - \alpha - \alpha^p$ şi, iterând, $\xi^{p^k} = \xi - \alpha - \alpha^p - \ldots - \alpha^{p^{k-1}}$. Astfel, e clar că, dacă α e o rădăcină a lui ϕ, atunci $\xi^q = \xi - \phi(\alpha) = \xi$, deci $\xi \in \mathbb{K}$ şi, de fapt, nu doar că g_α nu e iredictibil, ci are toate rădăcinile în $\mathbb{K}$. Să ne uităm acum la $\xi^{q^i} - \xi^{q^j}$, cu $i < j$. Avem, $\xi^{q^j} - \xi^{q^i} = \alpha^{p^{ni}} + \alpha^{p^{n(i+1)}} + \ldots + \alpha^{p^{nj-1}} = (j-i)\phi(\alpha)$. Aceasta ne spune pe de-o parte că, dacă α nu e rădăcină a lui ϕ, atunci $\xi, \xi^q, \ldots \xi^{q^{p-1}}$ sunt distincte, şi deci acestea sunt toate rădăcinile lui g_α, dar, pe de altă parte că $\xi^{q^p} = \xi$. Ca mai înainte, ne uităm la ordinul lui ξ în $\mathbb{K}(\xi)$ şi deducem că $p | \deg G$, dar $\deg G \leq \deg(g_\alpha) = p$ de unde $G = g_\alpha$ şi g_α este astfel ireductibil.

Am demonstrat astfel că singurele $\alpha \in \mathbb{K}$ pentru care g_α nu e ireductibil se află printre rădăcinile lui ϕ. Întrebarea care se ridică natural este: care (sau câte) dintre rădăcinile lui ϕ se află, însă, în $\mathbb{K}$? Deşi nu cunoaştem o caracterizare a lor, putem demonstra că toate rădăcinile lui ϕ sunt în $\mathbb{K}$. Să observăm că, din nou, deoarece $char(\mathbb{K} = p)$ avem $\phi(x+y) = \phi(x) + \phi(y)$ (am notat tot cu ϕ şi funcţia polinomială asociată), astfel că ϕ e un endomorfism al grupului $(\mathbb{K}, +)$. Pe de-o parte, aceasta înseamnă că $\phi(\mathbb{K})$ e un subgrup al lui $\mathbb{K}$, şi, mai mult, cum $\phi(x)^p = \phi(x)$, $\forall x \in \mathbb{K}$, avem $|\phi(\mathbb{K})| \leq p$ (elementele aflându-se printre rădăcinile polinomului $X^p - X$). Evident, $\phi(\mathbb{K})$ nu e grupul trivial, deci acesta are exact p elemente, întrucât ordinul său îl divide pe cel al lui $\mathbb{K}$. Pe de altă parte, din prima teoremă de izomorfism, $\mathbb{K}/\ker(\phi) \cong Im(\phi)$, care ne arată acum că $|\ker(\phi)| = p^{n-1} = \deg \phi$, ceea ce încheie demonstraţia.

BIBLIOGRAFIE

[1] M. Andronache, *Problema* 4, Olimpiada Naţională de Matematică 2002, Etapa finală, GM-B nr 3/2002