PENTRU CERCURILE DE ELEVI

CÂTEVA APLICAŢII ALE LEMEI LUI HENSEL

LIA IOANA[1)]

În această lecţie vom prezenta o relaţie utilă în rezolvarea unor probleme de teoria numerelor. Lecţia a fost prezentată la tabăra Gazeta Matematică şi Viitori Olimpici de la Câmpulung Muscel, 2015.

Formula lui Taylor pentru polinoame

Fie $P \in \mathbb{R}[X]$ un polinom de grad n si $x_0 \in \mathbb{R}$ un punct fixat. Atunci are loc egalitatea:

$$P(x) = P(x_0) + \frac{P'(x_0)}{1!}(x - x_0) + \frac{P''(x_0)}{2!}(x - x_0)^2 + \ldots + \frac{P^{(n)}(x_0)}{n!}(x - x_0)^n.$$

Demonstraţie. Fie $P(x) = b_0 + b_1 x + \ldots + b_n x^n$. Considerând $x = (x - x_0) + x_0$, avem $P(x) = \sum_{k=0}^{n} b_k[(x - x_0) + x_0]^k$, unde ridicând la puterea k paranteza dreaptă şi reducând termenii asemenea ai aceloraşi puteri ale lui $(x - x_0)$, obţinem pentru $P(x)$ expresia

$$P(x) = a_0 + a_1(x - x_0) + \ldots + a_n(x - x_0)^n.$$

Valorile lui a_i, $i = \overline{0, n}$, depind de b_i şi x_0.

Calculând valorile derivatelor succesive ale lui $P(x)$, avem

$P'(x) = a_1 + 2a_2(x - x_0) + \ldots + na_n(x - x_0)^{n-1}$,

$P''(x) = 2a_2 + 2 \cdot 3a_3(x - x_0) + \ldots + n(n-1)a_n(x - x_0)^{n-2}$,

. . . . . ,

$P^{(n)}(x) = 2 \cdot 3 \cdot \ldots \cdot na_n$.

Derivatele de ordin mai mare decât n ale lui P sunt 0. Considerând $x = x_0$ în relaţiile de mai sus obţinem $P(x_0) = a_0$, $P'(x_0) = a_1$, ..., $P^{(n)}(x_0) = n!a_n$. Astfel, $a_k = P^{(k)}(x_0)/k!$ pentru $k = \overline{0, n}$, ceea ce finalizează demonstraţia.

Lema lui Hensel. *Fie $f(X)$ un polinom monic, de o singură variabilă, cu coeficienţi întregi şi p un număr prim. Fie $k \geq 1$ şi $a \in \mathbb{Z}$ astfel încât $f(a) \equiv 0 \pmod{p^k}$, iar $f'(a) \not\equiv 0 \pmod{p}$. Atunci există $t \in \mathbb{Z}$ (unic modulo p) astfel încât $f(a + tp^k) \equiv 0 \pmod{p^{k+1}}$.*

Demonstraţie. Căutăm t astfel încât $f(a + tp^k) \equiv 0 \pmod{p^{k+1}}$. Considerăm $b = a + tp^k$. Folosind scrierea în serie Taylor a polinomului f pentru $x = a + tp^k$ şi $x_0 = a$, obţinem

$$f(a + tp^k) = f(a) + f'(a)tp^k + \frac{f''(a)}{2!}(tp^k)^2 + \ldots.$$

[1)]Elevă, Liceul Internaţional de Informatică Bucureşti

Este uşor de observat că $\frac{f^{(r)}(a)}{r!} \in \mathbb{Z}$, oricare ar fi r astfel încât $1 \leq r \leq \deg(f)$ şi, cum $2k \geq k+1$,

$$f(a+tp^k) \equiv f(a) + tp^k f'(a) \pmod{p^{k+1}}. \tag{1}$$

Dacă $f(a) \equiv 0 \pmod{p^{k+1}}$, atunci, cum $f'(a) \not\equiv 0 \pmod{p}$, unicul $t \pmod{p}$ care satisface concluzia este 0.

Dacă $f(a) \not\equiv 0 \pmod{p^{k+1}}$, atunci există $c \in \mathbb{Z}$, $(c,p)=1$ astfel încât $f(a) = cp^k$. În acest caz, conform (1), congruenţa din concluzie este echivalentă cu

$$c + tf'(a) \equiv 0 \pmod{p}. \tag{2}$$

Din $f'(a) \not\equiv 0 \pmod{p}$ reiese că $f'(a)$ este inversabil in $\mathbb{Z}_p$. Astfel, (2) este echivalentă cu $t \equiv -c(f'(a))^{-1} \pmod{p}$, ceea ce arată existenţa şi unicitatea lui t şi demonstraţia este încheiată. □

Observaţii.

1. Demonstraţia precedentă arată că dacă $f(a) = cp^k$, $c \in \mathbb{Z}$, iar $f'(a) \not\equiv 0 \pmod{p}$, atunci soluţia ecuaţiei $f(x) \equiv 0 \pmod{p^{k+1}}$ este $a - cp^k(f'(a))^{-1}$, adică $a - f(a)(f'(a))^{-1}$, unde $(f'(a))^{-1}$ este inversul lui $f'(a)$ în $\mathbb{Z}_p$.

2. Dacă $f(a) \equiv 0 \pmod{p^k}$, atunci $f'(a+tp^k) \equiv f'(a) \pmod{p}$, oricare ar fi $k \in \mathbb{N}^*$ şi $t \in \mathbb{Z}$. Astfel, dacă avem o soluţie a_k a congruenţei $f(a) \equiv 0 \pmod{p^k}$ şi $f'(a_k) \not\equiv 0 \pmod{p}$, atunci $a_{k+1} = a_k - f(a_k)(f'(a_k))^{-1}$ este o soluţie a congruenţei $f(a) \equiv 0 \pmod{p^{k+1}}$ şi $f'(a_{k+1}) \equiv f'(a_k) \pmod{p}$.

Problema 1. *Găsiţi toate soluţiile ecuaţiei* $x^2 + x + 47 \equiv 0 \pmod{7^3}$.

Soluţie. Fie $f(x) = x^2 + x + 47$. Atunci $f'(x) = 2x+1$, $f(x) \equiv 0 \pmod{7}$ are soluţiile $x \equiv 1 \pmod{7}$ şi $x \equiv 5 \pmod{7}$, $f'(1) \equiv 3 \pmod{7}$; $f'(5) \equiv \equiv 4 \pmod{7}$, deci putem aplica lema lui *Hensel*. Notăm inversul lui $f'(x)$ în $\mathbb{Z}_p$ cu $f'(x)^{-1}$.

Deoarece $f'(1)^{-1} = 5$, pentru $a=1$, $a_2 = 1 - 49 \cdot 5$ este soluţie modulo 7^2; reducând modulo 7^2, se poate considera $a_2 = 1$.

Atunci $a_3 = 1 - 49 \cdot 5 \equiv 99 \pmod{7^3}$.

Deoarece $f'(5)^{-1} = 2$, pentru $a=5$, $a_2 = 5 - 77 \cdot 2 \equiv 47 \pmod{7^2}$, $a_3 = 47 - f(47) \cdot 2 \equiv 243 \pmod{7^3}$, deci 99 si 243 sunt singurele soluţii modulo 7^3.

Problema 2. *Demonstraţi că oricare ar fi* $n \in \mathbb{N}$, *există* $a \in \mathbb{Z}$ *astfel încât* $a^3 - a + 1 \equiv 0 \pmod{5^n}$.

Soluţie. Problema este una evidentă utilizând lema lui *Hensel*, dar destul de complicată folosind alte metode standard.

Fie $f(a) = a^3 - a + 1$; $f'(a) = 3a^2 - 1$. Se observă că $f(a) \equiv 0 \pmod{5}$ numai pentru $a \equiv 3 \pmod{5}$. Cum $f'(3) \equiv 1 \pmod{5}$, putem aplica inductiv observaţia 2 pentru polinomul f şi numărul prim 5, deci oricare ar fi n natural, există a întreg astfel încât concluzia să fie îndeplinită.

Problema 3 (România TST 2014). *Arătaţi că, oricare ar fi numărul întreg $n \geq 2$, există $n+1$ numere $x_1, x_2, \ldots, x_n, x_{n+1}$ în $\mathbb{Q} \setminus \mathbb{Z}$ astfel încât*

$$\{x_1^3\} + \{x_2^3\} + \{x_3^3\} + \ldots + \{x_n^3\} = \{x_{n+1}^3\}.$$

Soluţie. În această rezolvare vom folosi şi teorema lui *Schur*:

Teoremă. *Fie $p(X)$ un polinom nenul cu coeficienţi întregi. Fie S mulţimea tuturor valorilor nenule ale lui p, în punctele întregi:*

$$S = \{p(n) \neq 0 \mid n \in \mathbb{N}\}.$$

Atunci, mulţimea tuturor numerelor prime care divid cel puţin un element al lui S este infinită.

Considerăm polinomul $f(X) = X^3 - 2$. Din teorema lui *Schur* reiese că există numere prime p oricât de mari, care să dividă anumite valori nenule $f(x)$, $x \in \mathbb{Z}$. Fie $p \geq 2^{3n}$ şi y astfel încât $f(y) \equiv 0 \pmod{p}$. Cum $y^3 \equiv 2 \pmod{p}$ şi $f'(y) = 3y^2 \not\equiv 0 \pmod{p}$, se poate aplica lema lui *Hensel*: există $z \in \mathbb{Z}$ cu proprietatea ca $f(z) \equiv 0 \pmod{p^2}$.

Analog vom obţine că există $a \in \mathbb{Z}$ astfel încât $f(a) \equiv 0 \pmod{p^3}$, deci există a cu proprietatea că $a^3 \equiv 2 \pmod{p^3}$. Deducem $\left\{\frac{a^3}{p^3}\right\} = \left\{\frac{2}{p^3}\right\} = \frac{2}{p^3}$. Notăm $x_3 = \frac{a}{p}$. Din $a^3 \equiv 2 \pmod{p^3}$ reiese $(a^3)^2 \equiv 2^2 \pmod{p^3}$ şi considerăm $x_4 = \frac{a^2}{p}$. Obţinem $\left\{\frac{a^{2\cdot 3}}{p^3}\right\} = \left\{\frac{2^2}{p^3}\right\} = \frac{2^2}{p^3} = \{x_4^3\}$. Procedând asemănător, notăm cu $x_k = \frac{a^{k-2}}{p}$, cu $(a^3)^{k-2} \equiv 2^{k-2} \pmod{p^3}$, iar $\{x_k^3\} = \frac{2^{k-2}}{p^3}$, pentru $k = \overline{1, n+1}$.

Alegem s_1 si s_2 congruente cu 1 modulo p^3, deci $s_1^3 \equiv s_2^3 \equiv 1 \pmod{p^3}$, de unde $\left\{\frac{s_1^3}{p^3}\right\} = \left\{\frac{s_2^3}{p^3}\right\} = \left\{\frac{1}{p^3}\right\} = \frac{1}{p^3}$ şi notăm $x_1 = \frac{s_1}{p}$ şi $x_2 = \frac{s_2}{p}$. Urmează să demonstrăm că numerele x_k alese, $k = \overline{1, n+1}$, corespund cerinţei.

Cum p este prim, $p \geq 2^{3n}$, nu vor exista numere egale între ele sau întregi.

Mai trebuie arătat că $\{x_1^3\} + \{x_2^3\} + \{x_3^3\} + \ldots + \{x_n^3\} = \{x_{n+1}^3\}$. Avem

$$\{x_1^3\} + \{x_2^3\} + \ldots + \{x_n^3\} = \frac{1}{p^3} + \frac{1}{p^3} + \frac{2}{p^3} + \frac{2^2}{p^3} + \ldots + \frac{2^{n-2}}{p^3} = \frac{2^{n-1}}{p^3} = \{x_{n+1}^3\}.$$

Deci, oricare ar fi numărul întreg $n \geq 2$, există $n+1$ numere care să satisfacă condiţia din enunţ.

Propunem încă două aplicaţii ca temă:

1. Găsiţi toate soluţiile congruenţei $5x^3 + x^2 - 1 \equiv 0 \pmod{125}$.

2. (Iranian TST). Găsiţi toate polinoamele f cu coeficienţi întregi astfel încât $n \mid m$ dacă $f(n) \mid f(m)$.

Bibliografie

[1] Titu Andreescu, Gabriel Dospinescu, *Problems from the book*, XYZ Press, 2008.
[2] Mircea Ganga, *Elemente de analiză matematică*, MATHPRESS, 2007.
[3] `www.artofproblemsolving.com`