Câteva probleme de teoria numerelor a căror rezolvare se bazează pe identităţi

Marian TETIVA[1]

Când vorbim despre utilizarea identităţilor în teoria numerelor, probabil că ne gândim în primul rând la ecuaţii diofantice, în special la demonstrarea existenţei soluţiilor unor asemenea ecuaţii. De exemplu, identităţile

$$(m^2-n^2)^2+(2mn)^2=(m^2+n^2)^2$$

şi

$$(m^2-2mn-n^2)^2+(m^2+2mn-n^2)^2=2(m^2+n^2)^2$$

arată că ecuaţiile $x^2+y^2=z^2$ şi, respectiv, $x^2+y^2=2z^2$ au, fiecare, o infinitate de soluţii întregi. Totuşi, în cele ce urmează, vom rezolva alte tipuri de probleme de teoria numerelor cu ajutorul identităţilor.

Avem în minte mai ales două identităţi, binecunoscute cititorilor. Este vorba de

$$(x-y)(x+y)(x^2+y^2)\cdots(x^{2^{n-1}}+y^{2^{n-1}})=x^{2^n}-y^{2^n} \tag{1}$$

şi de

$$(x^2+xy+y^2)(x^2-xy+y^2)(x^4-x^2y^2+y^4)\cdots(x^{2^n}-x^{2^{n-1}}y^{2^{n-1}}+y^{2^n})=$$
$$=x^{2^{n+1}}+x^{2^n}y^{2^n}+y^{2^{n+1}}. \tag{2}$$

Ambele sunt valabile pentru orice numere complexe x şi y (dar, desigur că pe noi ne vor interesa pentru numere întregi) şi orice număr natural $n\geq 1$. Se justifică la fel, prin aplicarea repetată a formulei $(a-b)(a+b)=a^2-b^2$.

Problema cea mai cunoscută care utilizează (1) este probabil

Problema 1. *Fie $n\geq 1$ un număr natural. Să se arate că numărul $N=11\ldots1$ scris în baza 10 cu 2^n cifre de 1 are cel puţin n divizori primi distincţi.*

Soluţie. Într-adevăr, avem

$$N=(10^{2^n}-1)/9=(10+1)(10^2+1)\cdots(10^{2^{n-1}}+1)$$

deci (1) ne permite să scriem pe N ca produsul a n numere; dacă reuşim să arătăm că acestea sunt prime între ele două câte două problema ar fi rezolvată, deoarece fiecare din aceste n numere ar aduce (cel puţin) un factor prim în descompunerea lui N ca produs de numere prime.

Avem, pentru $0\leq i<j$, că $10^{2^i}+1$ divide pe $10^{2^j}-1$ (tot pe baza identităţii (1)), deci dacă d este un divizor comun pentru $10^{2^i}+1$ şi $10^{2^j}+1$, atunci d este divizor şi al lui $2=10^{2^j}+1-(10^{2^j}-1)$. Cum d este impar, rezultă $d=1$ şi soluţia se încheie.

Problema care urmează a apărut acum ceva vreme în *Recreaţii matematice*, nr. 1/2005, pag. 42, *Problema 2*, cl. a X-a, **Lucian Tuţescu**.

Problema 2. *Există o infinitate de numere $n\in\mathbb{N}$ astfel încât n^2+n+1 divide pe $n!$.*

Soluţie. Să pornim de la un caz particular al identităţii (2):

$$m^8+m^4+1=(m^2+m+1)(m^2-m+1)(m^4-m^2+1)$$

[1] Profesor, Colegiul Naţional "Gheorghe Roşca Codreanu", Bârlad

şi să observăm că avem

$$m^2 - m + 1 < m^2 + m + 1 < m^4 - m^2 + 1 < m^4$$

pentru orice număr natural $m \geq 2$. Aceste inegalităţi arată că $(m^4)!$ se divide cu $(m^2+m+1)(m^2-m+1)(m^4-m^2+1)$, deci cu $(m^4)^2+m^4+1$ pentru orice $m \geq 2$ număr natural. Problema este aşadar rezolvată: putem alege $n = m^4$, $m \geq 2$. (De exemplu, 16! se divide cu $16^2 + 16 + 1 = 7 \cdot 3 \cdot 13$; de fapt, $n = 16$ este cel mai mic cu proprietatea din enunţ.)

O problemă asemănătoare a apărut mai demult în *American Mathematical Monthly*:

Problema 3. *Există o infinitate de numere $n \in \mathbb{N}$ astfel încât n^2+1 divide pe $n!$.*

Soluţie. De data asta ne vom folosi de identitatea

$$4m^4 + 1 = (2m^2 - 2m + 1)(2m^2 + 2m + 1),$$

unde vom încerca să mai descompunem şi cel de-al doilea factor. Pentru asta să observăm că

$$4m^2 + 4m + 2 = (2m+1)^2 + 1 = 2p^2 \Rightarrow 2m^2 + 2m + 1 = p^2,$$

dacă $2m + 1$ şi p sunt soluţii ale ecuaţiei $x^2 - 2y^2 = -1$.

Dar acest lucru este cunoscut: ecuaţia menţionată are, într-adevăr, o infinitate de soluţii. Mai precis, dacă notăm $x_k + y_k\sqrt{2} = (1+\sqrt{2})^{2k+1}$, cu x_k şi y_k numere naturale, atunci avem şi $x_k - y_k\sqrt{2} = (1-\sqrt{2})^{2k+1}$, deci

$$x_k^2 - 2y_k^2 = (x_k + y_k\sqrt{2})(x_k - y_k\sqrt{2}) = ((1+\sqrt{2})(1-\sqrt{2}))^{2k+1} = (-1)^{2k+1} = -1$$

pentru orice k; de exemplu, primele trei soluţii (care corespund lui $k = 0$, $k = 1$, respectiv $k = 2$) sunt $(1, 1)$, $(7, 5)$ şi $(41, 29)$. În plus, se arată destul de uşor că x_k este impar pentru orice k.

Atunci, este suficient să alegem perechea $(2m + 1, p)$ ca fiind una dintre soluţiile (x_k, y_k) ale ecuaţiei $x^2 - 2y^2 = -1$, pentru a avea

$$(2m^2)^2 + 1 = (2m^2 - 2m + 1)p^2.$$

În aceste condiţii,

$$4m^4 + 1 = (2m^2 - 2m + 1)p^2 > 17p^2 \geq 16p^2 + 1,$$

dacă m este suficient de mare (ceea ce se poate, deoarece şirul (x_k) tinde la ∞; de fapt, pentru $k \geq 2$, avem $m = (x_k - 1)/2 \geq 20$, ceea ce asigură valabilitatea inegalităţii care ne trebuie), de unde obţinem

$$m^2 > 2p \Rightarrow 2m^2 - 2m + 1 \geq m^2 > 2p.$$

Astfel că $2m^2 > 2m^2 - 2m + 1 > 2p > p$, deci produsul $(2m^2)!$ conţine factorii (distincţi) $2m^2 - 2m + 1$, $2p$ şi p, deci se divide cu $(2m^2 - 2m + 1)p^2 = (2m^2)^2 + 1$; prin urmare sunt soluţii toate numerele $n = 2m^2$, unde $m = (x_k - 1)/2$, $k \geq 2$.

Se poate vedea prin calcul direct că soluţia cea mai mică este $n = 18$ (18! se divide cu $18^2 + 1 = 5^2 \cdot 13$). Această soluţie face parte din şirul de mai sus; se obţine pentru $k = 1$, când $m = 3$ şi $p = 5$ (inegalitatea $2m^2 - 2m + 1 > 2p$ are loc şi în acest caz, chiar dacă nu are loc $m^2 > 2p$).

Problema 4. *Pentru un număr natural $n \geq 2$ notăm cu $h(n)$ cel mai mare divizor prim al lui n. Să se arate că există o infinitate de numere n astfel încât $h(n) < h(n+1) < h(n+2)$.*

Soluţie. De astă dată, pe lângă identitatea (2), vom folosi şi o idee ceva mai subtilă. Anume, să fixăm un număr prim impar p şi să observăm că, la fel ca la Problema 1, oricare două dintre numerele

$$p+1, p^2+1, \ldots, p^{2^k}+1, \ldots$$

au cel mai mare divizor comun 2. De aceea există unul dintre ele care are măcar un factor prim mai mare decât p. Să considerăm primul dintre aceste numere, adică fie k acel număr natural pentru care $h(p^{2^k}+1) > p$ şi $h(p^{2^j}+1) < p$ pentru $j = 1, 2, \ldots, k-1$ (clar, nu putem avea $h(p^{2^s}+1) = p$, deoarece nici unul dintre aceste numere nu poate avea factorul p). Numărul $n = p^{2^k}-1$ are atunci proprietatea din enunţ. Într-adevăr, $h(n+1) < h(n+2)$ înseamnă $p < h(p^{2^k}+1)$, deci rezultă din alegerea lui k; şi tot din alegerea lui k rezultă şi cealaltă inegalitate, deoarece

$$\begin{aligned} h(p^{2^k}-1) &= h((p-1)(p+1)(p^2+1)\cdots(p^{2^{k-1}}+1)) = \\ &= \max\{(h(p-1), h(p+1), h(p^2+1), \ldots, h(p^{2^{k-1}}+1)\} < p. \end{aligned}$$

Astfel vedem că pentru fiecare număr prim impar p există un număr întreg pozitiv k astfel încât $n = p^{2^k}-1$ să aibă proprietatea $h(n) < h(n+1) < h(n+2)$, q.e.d.

Exerciţii pentru cititor.

Problema 5. Fie a, b, c numere întregi astfel încât ab nu este pătrat perfect şi a, b sunt pozitive. Arătaţi că dacă ecuaţia $ax^2 - by^2 = c$ are o soluţie în mulţimea numerelor întregi, atunci ea are o infinitate de asemenea soluţii.

Problema 6. Să se dea o altă soluţie Problemei 3 folosind identitatea

$$(4x^2-2x+1)^2+1 = 2(4x^2+1)(2x^2-2x+1).$$

Verificaţi această identitate!

De asemenea, puteţi obţine o soluţie a problemei folosind identitatea

$$(x^2+1)((x+1)^2+1) = (x^2+x+1)^2+1.$$

Problema 7. Fie $p > 0$ un număr prim. Să se arate că din oricare $2p-1$ numere întregi $x_1, \ldots, x_{2p-1}$ se pot alege p a căror sumă se divide cu p.

Indicaţie. Aceasta nu e o problemă uşoară. De fapt ea este valabilă pentru orice număr natural n (adică din oricare $2n-1$ numere întregi $x_1, \ldots, x_{2n-1}$ se pot alege n a căror sumă se divide cu n) şi în această formă se numeşte **teorema Erdös-Ginzburg-Ziv** (a fost pentru prima dată demonstrată de cei trei matematicieni în 1961). Se poate arăta că acest enunţ are proprietatea de multiplicativitate, în sensul că dacă este adevărat pentru $n = a$ şi $n = b$, atunci este adevărat şi pentru $n = ab$ (a se vedea cartea lui **Horea Banea** de *Probleme traduse din revista Kvant*); prin urmare demonstrarea sa pentru n număr prim îi asigură valabilitatea pentru orice n. Şi ajungem acum şi la indicaţia promisă: utilizaţi identitatea

$$\sum (x_1+\cdots+x_p)^{p-1} - \sum (x_1+\cdots+x_{p-1})^{p-1} + \cdots + (-1)^{p-1}\sum x_1^{p-1} = 0$$

pentru care se poate consulta, de exemplu, **Ioan Tomescu**, *Probleme de combinatorică şi teoria grafurilor*, E. D. P., Bucureşti, 1981. Sumele se fac după toate posibilităţile de a alege din cele $2p-1$ numere câte p, $p-1$, ..., respectiv câte unul.