Numere prime şi sume de pătrate

Ştefan TUDOSE [1]

Abstract. In this Note, the Theorems 1 and 2 regarding the representation of prime numbers as sums of perfect squares, are employed for solving some problems that were proposed at mathematical contests.

Keywords: prime numbers, perfect square, Legendre′ symbol.

MSC 2010: 11A07, 11D72.

În această Notă, Q_2 va nota mulţimea numerelor ce se pot scrie ca sumă de două pătrate perfecte, iar P_3 - mulţimea numerelor prime de forma M_4+3. Vom prezenta câteva rezultate teoretice necesare în rezolvarea problemelor discutate în continuare. Utilizarea *simbolului lui Legendre* aduce simplificări demonstraţiilor obişnuite ale teoremelor de mai jos.(v. [**1**], 53-54). Pentru definirea şi proprietăţile acestui simbol, cât şi *simbolului lui Jacobi,* se poate consulta [**2**], 181-196. Instrumentul oferit de aceste simboluri este folosit şi în rezolvarea problemelor.

Avem nevoie de următoarea lemă ([**1**], 53):

Lemă (Thue). *Dacă $n \in \mathbb{N}^\star$ şi a este coprim cu n, atunci există numerele naturale x şi y, $0 < x, y < \sqrt{n}$ astfel încât $xa \equiv \pm y (\mathrm{mod}\ n)$ pentru o alegere convenabilă a semnelor $+$ şi $-$.*

Teorema 1. *Orice număr prim $p \equiv 1(\mathrm{mod}\ 4)$ aparţine lui Q_2, iar scrierea sa ca o sumă de pătrate este unică.*

Demonstraţie. Cum $p \equiv 1(\mathrm{mod}\ 4)$, rezultă că

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1,$$

deci există $n \in \mathbb{N}^\star$ astfel încât $p|n^2+1$. Evident, p şi n sunt coprime. Aplicând Lema, obţinem că există x şi y, $0 < x, y < \sqrt{p}$ cu proprietatea că $p|n^2x^2 - y^2$. Deoarece $p|n^2+1$, rezultă că $p|x^2+y^2$. Cum $x^2+y^2 < 2p$, conchidem că $p = x^2+y^2$.

Teorema 2. *Fie numărul prim $p \in P_3$ cu proprietatea că $p|a^2+b^2$. Atunci $p|(a,b)$.*

Demonstraţie. Dacă $(p,(a,b)) = 1$, rezultă că $(p,a) = (p,b) = 1$. Utilizând simbolul lui Legendre, avem:

$$1 = \left(\frac{a^2}{p}\right) = \left(\frac{-b^2}{p}\right) = \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = -1,$$

contradicţie. Presupunerea făcută este falsă, deci $p|(a,b)$.

Consecinţă. *Un număr aparţine lui Q_2 dacă şi numai dacă orice factor prim de forma M_4+3 din descompunerea sa în factori primi apare la un exponent par.*

[1] Elev, cl. a X-a, Lic. Internat. de Informatică, Bucureşti; e-mail: *tudosestefanrares@gmail.com*

Se demonstrează folosind teoremele de mai sus şi *identitatea lui Lagrange*: $(a^2+b^2)(c^2+d^2)=(ac-bd)^2+(ad+bc)^2$.

Problema 1. *Ecuaţia $y^2=x^3+7$ nu are soluţii întregi.*

Soluţie. Problema în sine nu este foarte grea, dar merită menţionată pentru idee.[1]

Să presupunem că ecuaţia are măcar o soluţie în $\mathbb{Z}^2$. Rezultă că numărul x este impar (altfel, $y^2\equiv 7(\text{mod } 8)$). Să rescriem ecuaţia în altă formă; avem:

$$x^3+8=y^2+1\Leftrightarrow (x+2)(x^2-2x+4)=y^2+1.$$

Deoarece x este impar, $x^2-2x+4=(x-1)^2+3\equiv 3(\text{mod } 4)$, deci x^2-2x+4 va avea un divizor p, cu $p\in P_3$. Observăm că $p|x^2-2x+4|y^2+1$. Conform Teoremei 2, $p|(y,1)=1$, contradicţie.

Observaţie. În aceeaşi manieră pot fi rezolvate şi alte ecuaţii de *tip Mordell*: $y^2=x^3-5,\ y^2=x^3-6,\ y^2=x^3+6$.[2]

Problema 2. *Să se demonstreze că există o infinitate de numere naturale k pentru care se pot găsi numerele naturale m şi n cu proprietatea că $3^k=m^2+n^2+1$.*

Soluţie. Utilizăm identitatea:

$$3^{2^x}-1=(3-1)(3+1)(3^2+1)...(3^{2^{x-1}}+1).$$

Cum fiecare factor din produs se scrie ca sumă a două pătrate perfecte (pentru primele două paranteze avem: $(3-1)(3+1)=2^2+2^2$), din identitatea lui Lagrange rezultă că există m,n numere naturale astfel încât $3^k-1=m^2+n^2$, pentru orice $k=2^x,\ x\in\mathbb{N}$.

Problema 3. *Să se demonstreze că există secvenţe de numere consecutive oricât de lungi astfel încât niciunul din numere să nu aparţină lui Q_2.*

Soluţie. Fie numărul $n\in\mathbb{N}^\star$ şi numerele $p_1,p_2,...,p_n\in P_3$ (mulţimea P_3 este infinită, consecinţă imediată a teoremei lui Dirichlet ([**2**], p.214)). Să observăm că un număr $n\equiv p(\text{mod } p^2)$, cu $p\in P_3$, nu poate aparţine lui Q_2, fapt ce sugerează alegerea unui număr x astfel încât

$$x\equiv p_1-1(\text{mod } p_1^2),\ x\equiv p_2-2(\text{mod } p_2^2),\ ...,\ x\equiv p_n-n(\text{mod } p_n^2).$$

Deoarece $(p_i,p_j)=1,\ \forall i\neq j$, din lema chineză a resturilor ([**2**], p.172), există un x care să satisfacă sistemul de congruenţe de mai sus. Astfel, niciunul din numerele $x+1,x+2,...,x+n$ nu aparţine lui Q_2. Cum n a fost ales arbitrar, afirmaţia este demonstrată.

[1] Cam mult spus idee; soluţia prezentată aici îi aparţine lui Lebesgue şi a fost dată de către acesta în 1869. Între timp, ideea a devenit metodă, cel mai recent exemplu fiind Problema 2 din al treilea test de selecţie pentru OBMJ, 2014.

[2] O ecuaţie de tipul $y^2=x^3+k$ se numeşte *ecuaţie Mordell*. Acesta a arătat în 1920 că, pentru $k\in\mathbb{Z}$, ecuaţia are un număr finit de soluţii.

Problema 4. *Să se demonstreze că nu există numerele naturale* m, n, p *astfel încât* $4mn - m - n = p^2,\ p \in \mathbb{N}^\star$. (Shortlist OIM, 1984)

Soluţie. Să presupunem că ecuaţia dată are măcar o soluţie. Are loc factorizarea:

$$4mn - m - n = p^2 \Leftrightarrow (4m-1)(4n-1) = 4p^2 + 1.$$

În acest moment problema este ca şi rezolvată, deoarece există un $r \in P_3,\ r|4p^2+1$, contradicţia fiind aceeaşi cu cea din Problema 1.

Observaţie. O analiză mai atentă a problemei sugerează şi o posibilă generalizare: *Să se afle soluţiile ecuaţiei* $4mnq - m - n = p^2$*, cu* q *un număr impar.*

Fără a şti enunţul problemei precedente, această ecuaţie pare destul de inabordabilă, fapt datorat în mare parte prezenţei lui q. Din nou, factorizarea este cheia:

$$4mnq - m - n = p^2 \Leftrightarrow (4mq-1)(4nq-1) = 4qp^2 + 1.$$

Utilizarea simbolul lui Legendre este inadecvată în acest caz, deoarece este relativ greu să-l calculăm fără a avea informaţii despre conexiunea dintre divizorii lui $4mq - 1,\ 4nq - 1$ şi $4qp^2 + 1$. Apare cu totul firesc ca simbolul lui Jacobi, ce îl generalizează pe cel al lui Legendre, să fie instrumentul util în scopul rezolvării acestei probleme mai generale.

Cum $4mq - 1$ şi q sunt impare, avem:

$$1 = \left(\frac{1}{4mq-1}\right) = \left(\frac{-4qp^2}{4mq-1}\right) = \left(\frac{-q}{4mq-1}\right) =$$

$$(-1)^{2mq-1} \cdot \left(\frac{4mq-1}{q}\right) \cdot (-1)^{\frac{q-1}{2}\cdot(2mq-1)} = (-1)(-1)^{\frac{q-1}{2}} \left(\frac{-1}{q}\right) = -1,$$

contradicţie. În concluzie, nici ecuaţia mai generală nu are soluţii.

Teme de gândire.

1) Există o bijecţie $f : \mathbb{N}^\star \longrightarrow \mathbb{N}^\star$ astfel încât $f(3mn + m + n) = 4f(m)f(n) + f(m) + f(n)$?

2) Să se determine toate funcţiile $f : \mathbb{Z} \to [0, \infty)$ care satisfac simultan condiţiile:

a) $f(xy) = f(x)f(y)$,

b) $2f(x^2 + y^2) - f(x) - f(y) \in \{0, 1\},\ \forall x, y \in \mathbb{Z}$.

Indicaţie. Deşi au un aspect algebric, ambele se rezolvă prin idei ,,împrumutate" din teoria numerelor: substituţii, bijecţii între diverşi monoizi, *identitatea lui Bézout* şi unele rezultate utilizate în acest material.

Bibliografie

1. **T. Andreescu, G. Dospinescu** – *Problems from the book*, XYZ Press, 2008.
2. **I. Creangă et al.** – *Introducere în teoria numerelor*, Editura didactică şi pedagogică, Bucureşti, 1965.
3. *www.artofproblemsolving.com*