ECUAŢIA DIOFANTICĂ $7^x = 3^y + 100$

Marcel Ţena[1)]

Abstract. This article contains four approaches of the diophantine equation $7^x = 3^y + 100$ and some considerations for the more general Pillai's diophantine equation $a^x - b^y = c$.

Keywords: Congruences, diophantine equations, Pillai's equation.
MSC : 11D61

Problema **26907** din G.M.-B nr. 4/2004, propusă de profesorul *Ovidiu Ţâţan* din Rm. Sărat, cere rezolvarea în numere întregi a ecuaţiei

$$7^x = 3^y + 100. \tag{1}$$

Este uşor de văzut că x şi y trebuie să fie pozitive, deci vom rezolva ecuaţia (1) în numere naturale.

Prezentăm patru rezolvări ale acestei probleme, după care vom face câteva consideraţii pe marginea unor ecuaţii diofantice mai generale.

Reamintim că pentru un număr natural $n \geq 2$ şi un număr întreg a cu $(a, n) = 1$, ordinul clasei $\widehat{a}$ în grupul $U(\mathbb{Z}_n)$ al elementelor inversabile din inelul $\mathbb{Z}_n$ se numeşte *gaussianul* (*ordinul*) *lui a modulo n* şi se notează $\gamma_n(a)$. Pentru $q, q_1, q_2 \in \mathbb{N}$ avem echivalenţele:

$$a^q \equiv 1 \pmod n \Leftrightarrow q \equiv 0 \pmod{\gamma_n(a)};$$
$$a^{q_1} \equiv a^{q_2} \pmod n \Leftrightarrow q_1 \equiv q_2 \pmod{\gamma_n(a)}.$$

În cazul $n = p =$număr prim, grupul $U(\mathbb{Z}_p) = \mathbb{Z}_p^*$ este ciclic, iar când clasa $\widehat{a}$ este un generator al acestui grup, adică $\gamma_p(a) = p - 1$, se spune că a este *rădăcină primitivă modulo p*.

Următorul rezultat îl vom folosi în toate soluţiile.

Propoziţie. *Dacă $(x, y) \in \mathbb{N} \times \mathbb{N}$ este o soluţie a ecuaţiei* (1), *atunci x şi y sunt numere impare.*

Demonstraţie. Reducem ecuaţia modulo 4 şi avem

$$(-1)^x \equiv (-1)^y \pmod 4,$$

deci x şi y au aceeaşi paritate. Dacă x şi y ar fi pare, scriind $x = 2a$, $y = 2b$ cu $a, b \in \mathbb{N}$, ecuaţia devine $49^a = 9^b + 100$. Dacă reducem această ecuaţie modulo 8, avem $1 \equiv 1 + 4 \pmod 8$, absurd. Aşadar, x şi y sunt impare. □

Soluţia 1 (*J. L. Brenner, L. L. Foster* [2]). Evident $(x = 3, y = 5)$ este soluţie a ecuaţiei (1) şi vom arăta că este unică. Se constată uşor că nu există soluţii cu $x < 3$, $y < 5$. Presupunem prin absurd că există o soluţie cu $x > 3$, $y > 5$. Reducând ecuaţia modulo 729, avem $7^x \equiv 100 \pmod{729} \Leftrightarrow 7^x \equiv 7^{84} \pmod{729}$ şi, deoarece $\gamma_{729}(7) = 243$, rezultă $x \equiv 84 \pmod{243}$. Aşadar $x = 243a + 84$, cu $a \in \mathbb{N}$, dar x este impar şi atunci $a = 2b + 1$, cu $b \in \mathbb{N}$,

[1)] Prof.dr., Colegiul Naţional „Sf. Sava", Bucureşti deci $x = 243(2b+1) + 84 = 486b + 327$. Deoarece 3 este rădăcină primitivă modulo numărul prim 487, adică $\gamma_{487}(3) = 486$, iar $\gamma_{487}(7) = 162$, reducând ecuaţia modulo 487, avem:

$$7^{486b+327} \equiv 3^y + 100 \pmod{487} \Leftrightarrow 7^{162(3b+2)+3} \equiv 3^y + 100 \pmod{487} \Leftrightarrow$$
$$\Leftrightarrow \left(7^{162}\right)^{3b+2} \cdot 343 \equiv 3^y + 100 \pmod{487} \Leftrightarrow$$
$$\Leftrightarrow 3^y \equiv 3^5 \pmod{487} \Leftrightarrow y \equiv 5 \pmod{486},$$

deci $y = 486c + 5$, cu $c \in \mathbb{N}$. Reducem acum ecuaţia modulo numărul prim 1459. Deoarece 3 este rădăcină primitivă modulo 1459, adică $\gamma_{1459}(3) = 1458$, iar $\gamma_{1459}(7) = 243$, scriind $c = 3k + r$, cu $k \in \mathbb{N}$, $r \in \{0, 1, 2\}$, rezultă $y = 1458k + 486r + 5$ şi ecuaţia redusă este:

$$7^{486b+327} \equiv 3^{1458k+486r+5} + 100 \pmod{1459} \Leftrightarrow$$
$$\Leftrightarrow \left(7^{243}\right)^{2b+1} \cdot 7^{84} \equiv \left(3^{1458}\right)^k \cdot \left(3^{486}\right)^r \cdot 243 + 100 \pmod{1459} \Leftrightarrow$$
$$\Leftrightarrow 7^{84} \equiv 243 \left(3^{486}\right)^r + 100 \pmod{1459},$$

unde $r \in \{0, 1, 2\}$. Dar $7^{84} \equiv 1016 \pmod{1459}$, $3^{486} \equiv 339 \pmod{1459}$ şi atunci ultima congruenţă obţinută este o contradicţie în fiecare din cele trei cazuri corespunzătoare lui $r \in \{0, 1, 2\}$. $\square$

Soluţia 2 (conf. univ. dr. *Alexandru Gica*). Să observăm că avem congruenţele $7^3 \equiv 1 - 9 \pmod{27}$, $7^9 \equiv 1 - 27 \pmod{81}$ şi prin inducţie

$$7^{3^k} \equiv 1 - 3^{k+1} \pmod{3^{k+2}}. \tag{2}$$

Să presupunem prin absurd că există o soluţie (x, y) cu $y \geq 7$. Scriind ecuaţia sub forma

$$7^x = 3^y + 7^3 - 3^5 \Leftrightarrow 7^x - 7^3 = 3^y - 3^5 \Leftrightarrow 7^3\left(7^{x-3} - 1\right) = 3^5\left(3^{y-5} - 1\right),$$

rezultă $7^{x-3} \equiv 1 \pmod{243}$.

Dar $\gamma_{243}(7) = 81$, prin urmare $x - 3 \equiv 0 \pmod{81}$, adică $x = 81a + 3$, cu $a \in \mathbb{N}$. Reducem ecuaţia modulo 3^6.

Folosind (2) şi congruenţa $(1 - 243)^a \equiv 1 - 243a \pmod{3^6}$, rezultată din formula binomului, avem

$$7^x \equiv 100 \pmod{3^6} \Leftrightarrow 7^{81a+3} \equiv 100 \pmod{3^6} \Leftrightarrow$$
$$\Leftrightarrow (1 - 243)^a \cdot 343 \equiv 100 \pmod{3^6} \Leftrightarrow 343 - 243a \cdot 343 \equiv 100 \pmod{3^6} \Leftrightarrow$$
$$\Leftrightarrow 243 - 243 \cdot 343a \equiv 0 \pmod{3^6},$$

de unde $1 - 343a \equiv 0 \pmod{3} \Leftrightarrow a \equiv 1 \pmod{3}$, deci $a = 3b + 1$, cu $b \in \mathbb{N}$.

Rezultă $x = 81(3b+1) + 3 = 243b + 84$. Reducem acum ecuaţia modulo 3^7, deci

$$7^x \equiv 100 \pmod{3^7} \Leftrightarrow 7^{243b+84} \equiv 100 \pmod{3^7} \Leftrightarrow$$
$$\Leftrightarrow 7^{84}\left(1 - 3^6\right)^b \equiv 100 \pmod{3^7}. \tag{3}$$

Dar $7^3 \equiv 1 + 2 \cdot 9 \pmod{81}$, $7^9 \equiv 1 + 2 \cdot 27 \pmod{243}$,

$$7^{27} \equiv 1 + 2 \cdot 81 \,(\mathrm{mod}\ 3^6),\ 7^{81} \equiv 1 + 2 \cdot 243 \,(\mathrm{mod}\ 3^7), \text{ adică}$$
$$7^{81} \equiv 1 + 486 (\mathrm{mod}\ 3^7), \text{ deci } 7^{84} \equiv 343(1 + 486)(\mathrm{mod}\ 3^7).$$

Atunci, congruenţa (3) se continuă astfel:

$$343(1+486)\left(1-3^6 b\right) \equiv 100 \pmod{3^7} \Leftrightarrow$$
$$\Leftrightarrow 343\left(1-3^6 b+486\right) \equiv 100 \pmod{3^7} \Leftrightarrow$$
$$\Leftrightarrow 243 - 343 \cdot 3^6 b + 343 \cdot 2 \cdot 3^5 \equiv 0 \pmod{3^7} \Leftrightarrow$$
$$\Leftrightarrow 243 - \left(38 \cdot 3^2 + 1\right) \cdot 3^6 b + \left(38 \cdot 3^2 + 1\right) \cdot 2 \cdot 3^5 \equiv 0 \pmod{3^7} \Leftrightarrow$$
$$\Leftrightarrow 243 - 3^6 b + 2 \cdot 3^5 \equiv 0 \pmod{3^7} \Leftrightarrow 3^6 - 3^6 b \equiv 0 \pmod{3^7},$$

deci $1 - b \equiv 0 (\mathrm{mod}\ 3)$, adică $b = 3c + 1$, cu $c \in \mathbb{N}$. Obţinem

$$x = 243(3c+1) + 84 = 729c + 327.$$

Deoarece x este impar, trebuie să avem $c = 2d$, cu $d \in \mathbb{N}$, prin urmare $x = 1458d + 327$.

Vom folosi acum congruenţe modulo 1459, numărul 1459 fiind prim. Prin calcul: $7^{324} \equiv 339 \,(\mathrm{mod}\ 1459)$. Atunci, reducând ecuaţia modulo 1459, avem:

$$3^y = 7^x - 100 \equiv \left(7^{1458}\right)^d \cdot 7^{327} - 100 \equiv 7^3 \cdot 7^{324} - 100 \equiv$$
$$\equiv 343 \cdot 339 - 100 \equiv 916 \pmod{1459}.$$

Folosind proprietăţile simbolului lui *Legendre* şi legea reciprocităţii pătratice, calculăm în două moduri simbolul lui *Legendre* $\left(\frac{916}{1459}\right)$. Pe de o parte, avem:

$$\left(\frac{916}{1459}\right) = \left(\frac{2^2 \cdot 229}{1459}\right) = \left(\frac{2}{1459}\right)^2 \cdot \left(\frac{229}{1459}\right) =$$
$$= \left(\frac{229}{1459}\right) = (-1)^{\frac{229-1}{2} \cdot \frac{1459-1}{2}} \cdot \left(\frac{1459}{229}\right) = \left(\frac{1459}{229}\right) =$$
$$= \left(\frac{6 \cdot 229 + 85}{229}\right) = \left(\frac{85}{229}\right) = \left(\frac{17 \cdot 5}{229}\right) = \left(\frac{17}{229}\right)\left(\frac{5}{229}\right) =$$
$$= (-1)^{\frac{17-1}{2} \cdot \frac{229-1}{2}} \left(\frac{229}{17}\right) \cdot (-1)^{\frac{5-1}{2} \cdot \frac{229-1}{2}} \cdot \left(\frac{229}{5}\right) = \left(\frac{229}{17}\right)\left(\frac{229}{5}\right) =$$
$$= \left(\frac{13 \cdot 17 + 8}{17}\right)\left(\frac{45 \cdot 5 + 4}{5}\right) = \left(\frac{8}{17}\right) \cdot \left(\frac{2}{5}\right)^2 = \left(\frac{8}{17}\right) = 1.$$

Reţinem:

$$\left(\frac{916}{1459}\right) = 1. \tag{4}$$

Pe de altă parte, deoarece $916 \equiv 3^y \,(\mathrm{mod}\ 1459)$, avem

$$\left(\frac{916}{1459}\right) = \left(\frac{3^y}{1459}\right).$$

Dar:

$$\left(\frac{3}{1459}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{1459-1}{2}} \cdot \left(\frac{1459}{3}\right) = -\left(\frac{486\cdot 3+1}{3}\right) = -\left(\frac{1}{3}\right) = -1$$

şi cum y este impar, vom avea $\left(\frac{3^y}{1459}\right) = \left(\frac{3}{1459}\right)^y = -1$, deci

$$\left(\frac{916}{1459}\right) = -1. \tag{5}$$

Egalităţile (4) şi (5) se contrazic. Aşadar, nu există soluţii cu $y \geq 7$, iar pentru $y \leq 5$ unica soluţie este $(x = 3,\ y = 5)$. $\square$

Soluţia 3 (elev *Ovidiu Avădanei*, Iaşi). Gândim ecuaţia (1) în inelul $\mathbb{Z}\left[\frac{1+\mathrm{i}\sqrt{3}}{2}\right] = \left\{p + q\cdot\frac{1+\mathrm{i}\sqrt{3}}{2} \,\middle|\, p,q\in\mathbb{Z}\right\}$ al întregilor pătratici asociat corpului pătratic $\mathbb{Q}\left(\mathrm{i}\sqrt{3}\right) = \left\{p + q\mathrm{i}\sqrt{3} \,\middle|\, p,q\in\mathbb{Q}\right\}$. Acest inel este euclidian în raport cu norma $N : \mathbb{Z}\left[\frac{1+\mathrm{i}\sqrt{3}}{2}\right] \to \mathbb{N}$, unde $N(z) = z\cdot\overline{z} = |z|^2$, pentru orice $z \in \mathbb{Z}\left[\frac{1+\mathrm{i}\sqrt{3}}{2}\right]$. Atunci el este un inel factorial, adică orice element (nenul, neinversabil) se descompune în mod unic într-un produs de factori ireductibili (primi). Elementele inversabile (unităţile) inelului sunt rădăcinile unităţii de ordin 6, adică elementele grupului $U_6 = \left\{\pm 1, \pm\frac{1}{2} \pm \mathrm{i}\frac{\sqrt{3}}{2}\right\}$.

În acest inel elementele $2 + \mathrm{i}\sqrt{3}$ şi $2 - \mathrm{i}\sqrt{3}$ sunt ireductibile, întrucât au ca normă numărul prim întreg 7. Pentru că x şi y sunt impare, deci $x = 2a+1$, $y = 2b+1$, cu $a, b \in \mathbb{N}$,iar $7 = \left(2+\mathrm{i}\sqrt{3}\right)\left(2-\mathrm{i}\sqrt{3}\right)$, ecuaţia (1) se scrie

$$7^{2a+1} = 100 + 3^{2b+1} \Leftrightarrow$$

$$\Leftrightarrow \left(2+\mathrm{i}\sqrt{3}\right)^{2a+1}\cdot\left(2-\mathrm{i}\sqrt{3}\right)^{2a+1} = \left(10+3^b\mathrm{i}\sqrt{3}\right)\left(10-3^b\mathrm{i}\sqrt{3}\right). \tag{6}$$

Elementele $10 + 3^b\mathrm{i}\sqrt{3}$ şi $10 - 3^b\mathrm{i}\sqrt{3}$ sunt relativ prime în inelul considerat. Într-adevăr, dacă $d = \left(10+3^b\mathrm{i}\sqrt{3}, 10-3^b\mathrm{i}\sqrt{3}\right)$, rezultă $d \mid 2\cdot 3^b\mathrm{i}\sqrt{3}$, deci $N(d) \mid N\left(2\cdot 3^b\mathrm{i}\sqrt{3}\right)$, adică $N(d) \mid 4\cdot 3^{2b+1}$.

De asemenea, din $d \mid 10 + 3^b\mathrm{i}\sqrt{3}$, rezultă $N(d) \mid N\left(10+3^b\mathrm{i}\sqrt{3}\right)$, adică $N(d) \mid 100 + 3^{2b+1}$ sau $N(d) \mid 7^{2a+1}$. Prin urmare $N(d) \mid \left(4\cdot 3^{2b+1}, 7^{2a+1}\right)$, adică $N(d) = 1$, deci d este asociat în divizibilitate cu 1 (este o unitate) în inelul $\mathbb{Z}\left[\frac{1+\mathrm{i}\sqrt{3}}{2}\right]$ şi aceasta arată că elementele $10 + 3^b\mathrm{i}\sqrt{3}$ şi $10 - 3^b\mathrm{i}\sqrt{3}$ sunt relativ prime. Elementul $10 + 3^b\mathrm{i}\sqrt{3}$ este un divizor propriu al lui 7^{2a+1}, căci norma sa este diferită de 1 şi $N\left(7^{2a+1}\right) = 7^{4a+2}$. Atunci din (6) rezultă că $10 + 3^b\mathrm{i}\sqrt{3} = u\left(2+\mathrm{i}\sqrt{3}\right)^{2a+1}$ sau $10 + 3^b\mathrm{i}\sqrt{3} = u\left(2-\mathrm{i}\sqrt{3}\right)^{2a+1}$, unde $u \in U_6$.

Analizăm toate posibilităţile după valorile lui u şi alegerea semnelor $\pm$.

1) $u = 1$, $10 + 3^b\mathrm{i}\sqrt{3} = \left(2+\mathrm{i}\sqrt{3}\right)^{2a+1}$. Să observăm că:

$$\begin{aligned}\left(2\pm\mathrm{i}\sqrt{3}\right)^{2a+1} &= \left(2^{2a+1} - 3\cdot 2^{2a+1}\cdot C_{2a+1}^{2} + \ldots + (-3)^a\cdot 2\cdot C_{2a+1}^{2a}\right)\pm\\ &\pm \mathrm{i}\sqrt{3}\left(2^{2a}\cdot C_{2a+1}^{1} - 2^{2a-2}\cdot 3\cdot C_{2a+1}^{3} + \ldots + (-3)^a\right).\end{aligned} \tag{7}$$

Din ipoteză şi (7), varianta cu $+$, identificând părţile reale şi reducând modulo 3 obţinem $1 \equiv 2 (\mathrm{mod}\ 3)$, contradicţie.

2) $u = 1$, $10 + 3^b\mathrm{i}\sqrt{3} = \left(2-\mathrm{i}\sqrt{3}\right)^{2a+1}$. Analog.

3) $u = -1$, $10 + 3^b\mathrm{i}\sqrt{3} = -\left(2+\mathrm{i}\sqrt{3}\right)^{2a+1}$. Arătăm mai întâi că $a \equiv 1 (\mathrm{mod}\ 9)$. Într-adevăr, în soluţia precedentă am văzut că

$$x \equiv 3 \ (\mathrm{mod}\ 81) \Leftrightarrow 2a+1 \equiv 3 \ (\mathrm{mod}\ 81) \Leftrightarrow$$
$$\Leftrightarrow 2(a-1) \equiv 0 \ (\mathrm{mod}\ 81) \Leftrightarrow a \equiv 1 \ (\mathrm{mod}\ 81)$$

şi, cu atât mai mult, $a \equiv 1 (\mathrm{mod}\ 9)$. Să presupunem prin absurd că $y \geq 7$, adică $b \geq 3$. În ipoteza $10 + 3^b\mathrm{i}\sqrt{3} = -\left(2+\mathrm{i}\sqrt{3}\right)^{2a+1}$ identificăm părţile imaginare, împărţim prin $\mathrm{i}\sqrt{3}$ şi reducem modulo 27. Obţinem:

$$0 \equiv -2^{2a}\cdot C_{2a+1}^{1} + 2^{2a-2}\cdot 3\cdot C_{2a+1}^{3} - 3^2\cdot 2^{2a-4}\cdot C_{2a+1}^{5} \ \ (\mathrm{mod}\ 27)$$

şi, după o împăţire cu 2^{2a-4}, avem:

$$\begin{aligned} 0 \equiv -16(2a+1) + 4\cdot 3\cdot \frac{(2a+1)2a(2a-1)}{6} - \\ -9\cdot\frac{(2a+1)2a(2a-1)(2a-2)(2a-3)}{5!} \ \ (\mathrm{mod}\ 27).\end{aligned}$$

Deoarece $2a+1 = x \equiv 3 (\mathrm{mod}\ 81)$, dând la o parte acest factor, care îl conţine pe 3 la puterea 1, obţinem:

$$0 \equiv -16 + 4a(2a-1) - \frac{3a(a-1)(2a-1)(2a-3)}{10} \ \ (\mathrm{mod}\ 9)$$

şi înmulţind cu 10, după calcule, avem:

$$0 \equiv -160 - a(2a-1)\left(6a^2 - 15a - 31\right). \tag{8}$$

Cum $a \equiv 1 (\mathrm{mod}\ 9)$, membrul drept din (8) este congruent modulo 9 cu $-160 - 1\cdot 1\cdot(6-15-31) = -120 \equiv 6 (\mathrm{mod}\ 9)$ şi astfel (8) este o contradicţie. Cazurile $b = 1$, $b = 2$ duc de asemenea la o contradicţie în ipoteza 3).

4) $u = -1$, $10 + 3^b\mathrm{i}\sqrt{3} = -\left(2-\mathrm{i}\sqrt{3}\right)^{2a+1}$. Pentru $b = 1$ avem o imposibilitate, dar pentru $b = 2$ egalitatea are loc pentru $a = 1$ şi obţinem astfel soluţia $x = 2a+1 = 3$, $y = 2b+1 = 5$. Pentru $b \geq 3$ se procedează ca la 3) şi obţinem o contradicţie.

5) $u \in \left\{\pm\frac{1}{2} \pm \frac{\mathrm{i}\sqrt{3}}{2}\right\}$. Putem scrie unitar $u = \frac{2m+1}{2} + \frac{2n+1}{2}\mathrm{i}\sqrt{3}$, cu $m, n \in \{-1, 0\}$.

Din (7) rezultă $\left(2 \pm \mathrm{i}\sqrt{3}\right)^{2a+1} = (4p+2) \pm \mathrm{i}\sqrt{3}(2q+1)$, cu $p, q \in \mathbb{Z}$. Atunci, ipoteza $10 + 3^b\mathrm{i}\sqrt{3} = u\left(2 \pm \mathrm{i}\sqrt{3}\right)^{2a+1}$ se scrie:

$$10 + 3^b\mathrm{i}\sqrt{3} = \left(\frac{2m+1}{2} + \frac{2n+1}{2}\mathrm{i}\sqrt{3}\right)\left((4p+2) \pm \mathrm{i}\sqrt{3}(2q+1)\right).$$

Egalând părţile reale obţinem:

$$10 = (2m+1)(2p+1) \pm \frac{3(2n+1)(2q+1)}{2},$$

care este o contradicţie, căci membrul drept nu este întreg.

Epuizarea tuturor posibilităţilor arată că unica soluţie a ecuaţiei (1) este ($x = 3$, $y = 5$). □

Soluţia 4 (*Marcel Ţena*). Folosim următorul rezultat, care poate fi consultat în [5]:

Teoremă. *Ecuaţia*[1)] *diofantică* $u^2 + 3v^2 = t^3$ *are soluţia* $(u, v, t) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$, *cu* t *impar şi* $(u, v) = 1$ *dacă şi numai dacă există* $a, b \in \mathbb{Z}$, *de parităţi diferite, cu* $(a, 3b) = 1$, *astfel încât*:

$$\begin{cases} u = a\left(a^2 - 9b^2\right) \\ v = 3b\left(a^2 - b^2\right) \\ t = a^2 + 3b^2. \end{cases}$$

Deoarece y este impar, scriem $y = 2k + 1$, cu $k \in \mathbb{N}^*$.

Reducem ecuaţia (1) modulo 9 şi avem $7^x \equiv 1 (\bmod 9)$. Dar $\gamma_9(7) = 3$, prin urmare $x \equiv 0 (\bmod 3)$, adică $x = 3p$, cu $p \in \mathbb{N}^*$. Ecuaţia (1) se scrie $10^2 + 3 \cdot \left(3^k\right)^2 = (7^p)^3$ şi arată că $(u, v, t) = \left(10, 3^k, 7^p\right)$ este o soluţie a ecuaţiei din teoremă. Prin urmare

$$\begin{cases} 10 = a\left(a^2 - 9b^2\right) & (9) \\ 3^k = 3b\left(a^2 - b^2\right) & (10) \\ 7^p = a^2 + 3b^2, & (11) \end{cases}$$

cu $a, b \in \mathbb{Z}$.

Din (9) rezultă că a divide 10, deci $a \in \{\pm 1, \pm 2, \pm 5, \pm 10\}$.

Dacă $a = \pm 1$, (9) devine $\pm 10 = 1 - 9b^2$, deci $b^2 \in \left\{-1, \frac{11}{9}\right\}$, absurd.

Dacă $a = \pm 2$, (9) devine $\pm 5 = 4 - 9b^2$, deci $b^2 \in \left\{-\frac{1}{9}, 1\right\}$.

Pentru $a = -2$, avem $b^2 = 1$, iar (10) dă $3^k = 9b$, deci $b > 0$, de unde $b = 1$. Atunci $k = 2$, iar din (11) $p = 1$, prin urmare $x = 3p = 3$, $y = 2k + 1 = 5$.

[1)] Ecuaţiile diofantice de tipul $ax^2 + by^2 = cz^n$ au fost studiate pentru prima oară de *Euler* şi *Lagrange*.

Dacă $a = \pm 5$, (9) devine $\pm 2 = 25 - 9b^2$, deci $b^2 \in \left\{\frac{23}{9}, 3\right\}$, absurd.

Dacă $a = \pm 10$, (9) devine $\pm 1 = 100 - 9b^2$, deci $b^2 \in \left\{11, \frac{101}{9}\right\}$, absurd.

Rezultă că unica soluţie a ecuaţiei (1) este ($x = 3$, $y = 5$). $\square$

Ne ocupăm acum de ecuaţia exponenţială diofantică mai generală

$$a^x - b^y = c, \tag{12}$$

unde $a > 1$, $b > 1$, $c \geq 1$ sunt numere întregi date, iar $x \geq 1$, $y \geq 1$ sunt necunoscutele. Ecuaţia (12) se numeşte *ecuaţia lui Pillai* şi a fost abordată în [6]. Un rezultat pe care îl vom stabili relativ la această ecuaţie este că mulţimea soluţiilor sale este finită. Demonstraţia dată aici este una proprie, diferită de cea din [6]. Folosim următorul rezultat auxiliar, care poate fi consultat în [3].

Lemă (*A.O. Ghelfond*, [3]). *Fie $a > 1$, $b > 1$ numere întregi şi $\varepsilon > 0$ date. Există un rang $n_\varepsilon \in \mathbb{N}$ cu proprietatea că pentru orice $m, n \in \mathbb{N}$, $m, n \geq n_\varepsilon$, $(m, n) = 1$, cu $a^n > b^m$, există inegalitatea*:

$$a^n - b^m > a^n \cdot \mathrm{e}^{-(\ln n)^{3+\varepsilon}}. \qquad \square$$

Semnificaţia acestei leme este aceea că pentru n, m mari, puterile a^n şi b^m nu pot fi apropiate. Avem următoarea:

Teoremă. *Ecuaţia exponenţială diofantică* (12) *are cel mult un număr finit de soluţii* (*eventual, niciuna*).

Demonstraţie. Observăm că, dacă (x, y) este soluţie a ecuaţiei (12) şi $x = dx'$, $y = dy'$, $d, x', y' \in \mathbb{N}$, $(x', y') = 1$, atunci

$$c = (a^{x'})^d - (b^{y'})^d = (a^{x'} - b^{y'})((a^{x'})^{d-1} + (a^{x'})^{d-2}(b^{y'}) + \ldots + (b^{y'})^{d-1}),$$

deci (x', y') este soluţie a unei ecuaţii de forma $a^x - b^y = c'$, cu $c' \mid c$. Cum numărul divizorilor lui c este finit şi $d \leq c$, demonstraţia teoremei este terminată dacă arătăm că ecuaţia (12) are un număr finit de soluţii cu x, y prime între ele.

Fixăm acum un $\varepsilon > 0$. Presupunem prin absurd că ecuaţia are o infinitate de soluţii. Conform lemei, există $n_\varepsilon \in \mathbb{N}$ astfel încât pentru orice soluţie (x, y) cu $x, y \geq n_\varepsilon$ avem:

$$c = a^x - b^y > a^x \cdot \mathrm{e}^{-(\ln x)^{3+\varepsilon}} \Leftrightarrow c \cdot \mathrm{e}^{(\ln x)^{3+\varepsilon}} > a^x \Leftrightarrow$$

$$\Leftrightarrow \ln c + (\ln x)^{3+\varepsilon} > x \ln a \Leftrightarrow \frac{\ln c}{x} + \frac{(\ln x)^{3+\varepsilon}}{x} > \ln a. \tag{13}$$

Când $x \to \infty$, inegalitatea (13) devine $0 \geq \ln a$, contradicţie. Teorema este demonstrată. $\square$

Comentariu. Putem da şi o altă demonstraţie teoremei precedente, în cazul particular când a şi b sunt numere prime, $a \equiv 3(\text{mod } 4)$, $b \equiv 3(\text{mod } 4)$, iar $c \equiv 0(\text{mod } 4)$, $c \not\equiv 0(\text{mod } 8)$. Folosim următorul rezultat din [9]:

Teoremă (*A. Thue*, [9]). *Dacă*

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0 \in \mathbb{Z}[X]$$

este un polinom ireductibil de grad $n \geq 3$, *iar* $F(X, Y)$ *este forma binară asociată, definită prin*

$$F(X, Y) = a_n X^n + a_{n-1} X^{n-1} Y + \ldots + a_1 X Y^{n-1} + a_0 Y^n,$$

atunci pentru $\lambda \in \mathbb{Z}^*$, *ecuaţia* $F(u, v) = \lambda$ *are cel mult un număr finit de soluţii* $(u, v) \in \mathbb{Z} \times \mathbb{Z}$.

Mai întâi, ca în propoziţia de la începutul articolului, se arată că x şi y sunt impare, deci $x = 4k + i$, $y = 4p + j$, unde $k, p \in \mathbb{N}$, $i, j \in \{1, 3\}$. Ecuaţia (12) se scrie:

$$a^x - b^y = c \Leftrightarrow a^i \cdot \left(a^k\right)^4 - b^j \cdot (b^p)^4 = c \Leftrightarrow a^i \cdot u^4 - b^j \cdot v^4 = c,$$

unde am notat $u = a^k$, $v = b^p$. Polinomul $f(X) = a^i X^4 - b^j$ este ireductibil în $\mathbb{Q}[X]$, conform criteriului lui *Capelli* (vezi de exemplu [11]) şi, fiind primitiv (c.m.m.d.c al coeficienţilor= 1), este ireductibil în $\mathbb{Z}[X]$. Forma binară asociată este $F(X, Y) = a^i X^4 - b^j Y^4$ şi, conform teoremei lui *Thue*, ecuaţia $F(u, v) = c$ adică $a^i \cdot u^4 - b^j \cdot v^4 = c$ are un număr finit de soluţii $(u, v) \in \mathbb{Z} \times \mathbb{Z}$. Atunci ecuaţia (12) are un număr finit de soluţii $(x, y) \in \mathbb{N}^* \times \mathbb{N}^*$.

Să remarcăm că ecuaţia iniţială (1) se situează în acest caz particular. □

Recent s-au obţinut rezultate mult mai precise referitoare la ecuaţia lui *Pillai*. Cu titlu informativ, prezentăm trei dintre ele.

Teoremă (*M. Bennett*, [1]). Ecuaţia (12) are cel mult 2 soluţii, iar cazurile când are două soluţii sunt următoarele 11:
$3 - 2 = 3^2 - 2^3 = 1$; $2^3 - 3 = 2^5 - 3^3 = 5$; $2^4 - 3 = 2^8 - 3^5 = 13$; $2^3 - 5 = 2^7 - 5^3 = 9$; $13 - 3 = 13^3 - 3^7 = 10$; $91 - 2 = 91^2 - 2^{13} = 89$; $6 - 2 = 6^2 - 2^5 = 4$; $15 - 6 = 15^2 - 6^3 = 9$; $280 - 5 = 280^2 - 5^7 = 275$; $4930 - 30 = 4930^2 - 30^5 = 4900$; $6^4 - 3^4 = 6^5 - 3^8 = 1215$. □

Observaţie. *Din această teoremă rezultă că ecuaţia* (1) *are cel mult o soluţie, deci* $(x = 3,\ y = 5)$ *este soluţie unică.* □

Teoremă (*R. Scott*, *R. Styer*, [7]). *Considerăm ecuaţia diofantică*

$$p^x - q^y = c, \tag{14}$$

cu $p > 1$, $q > 1$ *numere prime şi* $c > 0$ *număr întreg.*

Atunci, dacă $q \not\equiv 1(\text{mod } 12)$, *ecuaţia* (14) *are cel mult o soluţie, în afară de cazurile când* $(p, q, c) \in \{(3, 2, 1), (2, 3, 5), (2, 3, 13), (2, 5, 3), (13, 3, 10)\}$ *sau când* $p^2 \mid q^{\gamma_p(q)} - 1$ *şi* $\gamma_p(q) = \textit{impar} > 1$. □

Observaţie. *Unicitatea soluţiei ecuaţiei* (1) *rezultă din teorema precedentă, luând* $p = 7$, $q = 3$, $c = 100$, $\gamma_7(3) = 6$.

Pentru cel de al treilea rezultat, definim mai întâi câteva noţiuni.

Un număr prim p se numeşte *număr prim Wieferich* dacă

$$2^{p-1} \equiv 1 \pmod{p^2}.$$

Un număr prim p se numeşte *bază largă 2- Wieferich* dacă este un număr prim *Wieferich* şi $p > 1,25 \cdot 10^{15}$.

Un număr prim p se numeşte *bază largă 3- Wieferich* dacă este un număr prim *Wieferich* şi $p > 2^{32}$.

Reamintim că un număr prim p se numeşte *număr prim Fermat* dacă $p = 2^v + 1$, unde $v \in \mathbb{N}^*$.

Teoremă (*R. Scott*, *R. Styer*, [8]). *Fie $b \in \{2,3\}$, iar a un număr prim mai mare ca b şi care nu este bază largă $b-$Wieferich. Egalitatea*

$$|a^{x_1} - b^{y_1}| = |a^{x_2} - b^{y_2}|,$$

cu $1 \le x_1 \le x_2$, $1 \le y_1 \le y_2$, $(x_1, y_1) \ne (x_2, y_2)$ are loc doar în următoarele 11 cazuri:

$3 - 2 = 3^2 - 2^3$; $2^3 - 3 = 2^5 - 3^3$; $2^4 - 3 = 2^8 - 3^5$; $2^3 - 5 = 2^7 - 5^3$; $13 - 3 = 13^3 - 3^7$; $2^2 - 3 = 3^2 - 2^3$; $3^2 - 2^2 = 2^5 - 3^3$; $5 - 2 = 2^7 - 5^3$; $11 - 2^2 = 2^7 - 11^2$; $5 - 3 = 3^3 - 5^2$; $F - 2 = 2^{v+1} - F$, unde $F = 2^v + 1$ este un număr prim *Fermat* sau $F = 9$. □

Observaţie. *Scriind ecuaţia* (1) *sub forma* $7^x - 3^y = 7^3 - 3^5$ *şi observând că pentru $a = 7$, $b = 3$ nu ne aflăm în niciunul din cazurile de excepţie date de teorema precedentă, rezultă $x = 3$, $y = 5$.* □

În fine, o categorie şi mai generală de ecuaţii, o constituie cele de tipul (12) în care doar c este dat, iar a, b, x, y sunt necunoscute.

Cazul $c = 1$ este cel al celebrei *conjecturi a lui Catalan*, rezolvată acum 10 ani de matematicianul român *Preda Mihăilescu*.

Este vorba de următorul rezultat:

Teoremă (*P. Mihăilescu*, [4]). *Ecuaţia diofantică*

$$a^x - b^y = 1,$$

cu necunoscutele $a > 1$, $b > 1$, $x > 1$, $y > 1$, are soluţia unică $(a,b,x,y) = (3,2,2,3)$, corespunzătoare egalităţii $3^2 - 2^3 = 1$. □

BIBLIOGRAFIE

[1] M. Bennett, *On some exponential equations of S.S.Pillai*, Canadian J. Math., 53 (2001),897-922.

[2] J. L. Brenner, L. L. Foster, *Exponential Diophantine Equations*, Pacific J. Math., vol. 101, nr.2 (1982), 263-391.

[3] A. O. Ghelfond, *Sur la divisibilité de la difference des puissances de deux nombres entiers par une puissance d'un idéal premier*, Mat. Sbornik, 1940, 7-25.

[4] P. Mihăilescu, *Primary Cyclotomic Units and a Proof of Catalan's Conjecture*, J. Reine Angew. Math., 572 (2004), 167-195.

[5] L. Panaitopol, A. Gica, *O introducere în aritmetică şi teoria numerelor*, Ed. Univ. Bucureşti, 2001.

[6] S. S. Pillai, *On the inequality* $0 < a^x - b^y \leq n$, J. Indian Math. Soc., 19 (1931), 1-11.
[7] R. Scott, R. Steyer, *On* $p^x - q^y = c$ *and related three term exponential Diophantine equations with prime bases*, J. Number Theory, 105 (2004), 212-234.
[8] R. Scott, R. Steyer, *On the generalized Pillai equation* $\pm a^x \pm b^y = c$, J. Number Theory, 118 (2) (2006), 236-265.
[9] A. Thue, *Über Annäherungswerte algebraischer Zahlen*, J. Reine Angew. Math., 135 (1909), 284-305.
[10] O. Ţâţan, *Problema 26907*, G. M.-B. vol. CXIX, 2014, nr. 4, 212.
[11] M. Ţena, *Cinci teme de aritmetică superioară*, S.S.M.R., Bucureşti, 1991.