Podróże po Imperium Liczb

Część 03. Liczby Kwadratowe

Rozdział 8

8. Równanie $ax^2 + by^2 = cz^2$

Andrzej Nowicki 27 kwietnia 2013, http://www.mat.uni.torun.pl/~anow

Spis treści

Wszystkie książki z serii "Podróże po Imperium Liczb" napisano w edytorze LaTeX. Spisy treści tych książek oraz pewne wybrane rozdziały moża znaleźć na internetowej stronie autora: http://www-users.mat.uni.torun.pl/~anow.

8 Równanie $ax^2 + by^2 = cz^2$

8.1 Informacje wstępne

W tym podrozdziale zajmować się będziemy rozwiązaniami całkowitymi (czyli rozwiązaniami w zbiorze liczb całkowitych) równania postaci

$$ax^2 + by^2 = cz^2,$$

w którym a, b, c są danymi liczbami naturalnymi. Jednym z takich równań zajmowaliśmy się już w rozdziale o trójkach Pitagorasa. Tam badaliśmy rozwiązania równania $x^2 + y^2 = z^2$, czyli takiego równania jak powyżej dla $a = b = c = 1$.

Jednym z rozwiązań całkowitych równania $ax^2 + by^2 = cz^2$ jest *rozwiązanie zerowe*, czyli trójka $(x, y, z) = (0, 0, 0)$. Interesować nas będą jednak niezerowe rozwiązania całkowite. Mówić będziemy, że rozwiązanie (x, y, z) jest niezerowe, jeśli $(x, y, z) \neq (0, 0, 0)$. Mówić będziemy ponadto, że rozwiązanie (x, y, z) jest *pierwotne*, jeśli jest niezerowym rozwiązaniem całkowitym oraz $\mathrm{nwd}(x, y, z) = 1$.

8.1.1. *Jeśli równanie $ax^2+by^2 = cz^2$ ma niezerowe rozwiązanie całkowite, to ma co najmniej jedno rozwiązanie pierwotne.*

D. Niech (x, y, z) będzie niezerowym rozwiązaniem całkowitym rozważanego równania. Niech $d = \mathrm{nwd}(x, y, z)$, $x = dx_1$, $y = dy_1$, $z = dz_1$, $x_1, y_1, z_1 \in \mathbb{Z}$. Wtedy $\mathrm{nwd}(x_1, y_1, z_1) = 1$ oraz $a(dx_1)^2 + b(dy_1)^2 = c(dz_1)^2$. Dzielimy przez d^2 i mamy: $a(x_1)^2 + b(y_1)^2 = c(z_1)^2$. Trójka (x_1, y_1, z_1) jest więc rozwiązaniem pierwotnym. ⊠

W powyższym oczywistym stwierdzeniu założyliśmy, że dane równanie ma niezerowe rozwiązanie całkowite. Istnieją tego typu równania, które takich rozwiązań nie mają.

8.1.2. *Jedynym rozwiązaniem całkowitym równania $2x^2 + 3y^2 = z^2$ jest rozwiązanie zerowe.* ([S59] 64).

D. (Sposób I). Przypuśćmy, że równanie $2x^2 + 3y^2 = z^2$ ma niezerowe rozwiązanie całkowite. Istnieje wtedy (na mocy 8.1.1) niezerowe rozwiązanie całkowite (x, y, z), spełniające dodatkowy warunek $\mathrm{nwd}(x, y, z) = 1$.

Z równości $2x^2 + 3y^2 = z^2$ otrzymujemy kongruencję $2x^2 \equiv z^2 \pmod 3$, z której w oczywisty sposób wynika, że liczby x oraz z są podzielne przez 3. To dalej implikuje, że liczba $3y^2$ (która jest równa $z^2 - 2x^2$) jest podzielna przez 9 i stąd wynika, że liczba y również jest podzielna przez 3. Zatem $3 \mid x$, $3 \mid y$ oraz $3 \mid z$, wbrew temu, że $\mathrm{nwd}(x, y, z) = 1$.

(Sposób II). Ten dowód podamy po stwierdzeniu 8.2.2. ⊠

★ R. Alter, *The congruent number problem*, [Mon] 87(1)(1980) 43-45.

8.2 Warunki konieczne

W dalszym ciągu zakładać będziemy, że dane liczby naturalne a, b, c są bezkwadratowe i parami względnie pierwsze.

Udowodnimy najpierw następujące znane stwierdzenie.

8.2.1. *Niech a, b, c będą bezkwadratowymi liczbami naturalnymi i parami względnie pierwszymi. Jeśli równanie $ax^2 + by^2 = cz^2$ ma niezerowe rozwiązanie całkowite, to każda z następujących kongruencji*

$$X^2 \equiv bc \pmod{a},\ X^2 \equiv ac \pmod{b},\ X^2 \equiv -ab \pmod{c}$$

ma rozwiązanie.

D. Niech (x, y, z) będzie takim niezerowym rozwiązaniem całkowitym, że $\mathrm{nwd}(x, y, z) = 1$. Takie rozwiązanie istnieje na mocy 8.1.1.

Zauważmy, że $\mathrm{nwd}(x, b) = 1$. Istotnie, przypuśćmy, że istnieje taka liczba pierwsza p, że $p \mid x$ oraz $p \mid b$. Wtedy $p \mid cz^2 = ax^2 + by^2$. Ale $p \nmid c$ (gdyż $\mathrm{nwd}(b, c) = 1$), więc $p \mid z$. Zatem $p^2 \mid x^2$ oraz $p^2 \mid z^2$, a zatem $p^2 \mid by^2 = cz^2 - ax^2$ i stąd $p \mid y$ (ponieważ liczba b jest bezkwadratowa). Liczba pierwsza p dzieli więc wszystkie liczby x, y, z. Jest to sprzeczne z tym, że $\mathrm{nwd}(x, y, z) = 1$. Zatem $\mathrm{nwd}(x, b) = 1$.

Istnieje więc taka liczba całkowita u, że $xu \equiv 1 \pmod{b}$. Mamy teraz:

$$ac = ac \cdot 1^2 \equiv ac(xu)^2 = cu^2(ax^2) = cu^2(cz^2 - by^2) \equiv cu^2 \cdot cz^2 = (cuz)^2 \pmod{b}$$

i stąd wynika, że kongruencja $X^2 \equiv ac \pmod{b}$ ma rozwiązanie. W ten sam sposób wykazujemy, że kongruencja $X^2 \equiv bc \pmod{a}$ również ma rozwiązanie.

Zauważmy jeszcze, że $\mathrm{nwd}(x, c) = 1$. Istnieje zatem taka liczba całkowita v, że $xv \equiv 1 \pmod{c}$. Mamy teraz:

$$-ab = -ab \cdot 1^2 \equiv -ab(xv)^2 = -bv^2(ax^2) = -bv^2(cz^2 - by^2) \equiv -bv^2 \cdot (-by^2) = (bvy)^2 \pmod{c}$$

i stąd wynika, że kongruencja $X^2 \equiv -ab \pmod{c}$ ma rozwiązanie. ☒

W przypadku, gdy $c = 1$, powyższe stwierdzenie ma następującą postać.

8.2.2. *Niech a, b będą bezkwadratowymi i względnie pierwszymi liczbami naturalnymi. Jeśli równanie $ax^2 + by^2 = z^2$ ma niezerowe rozwiązanie całkowite, to kongruencje*

$$X^2 \equiv b \pmod{a} \quad \textit{oraz} \quad X^2 \equiv a \pmod{b}$$

mają rozwiązania.

Z tego stwierdzenia wynika natychmiast, że równanie $2x^2 + 3y^2 = z^2$ nie ma niezerowych rozwiązań całkowitych (patrz 8.1.2). Jest bowiem oczywiste, że kongruencja

$$X^2 \equiv 2 \pmod{3}$$

nie ma rozwiązań.

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

8.3 Pomocnicze fakty i lematy

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

Wykażemy, że stwierdzenie odwrotne do stwierdzenia 8.2.2 jest również prawdziwe. W tym celu udowodnimy najpierw dwa lematy. W pierwszym z tych lematów przez $\mathbb{Z}[X]$ oznaczamy pierścień $\mathbb{Z}[x_1, \ldots, x_n]$, wielomianów zmiennych $x_1, \ldots, x_n$ o współczynnikach całkowitych.

8.3.1. *Niech m_1, m_2 będą względnie pierwszymi liczbami naturalnymi i niech F będzie wielomianem należącym do $\mathbb{Z}[X]$. Załóżmy, że A, B, C, D są wielomianami postaci*

$$A = a_1x_1 + \cdots + a_nx_n, \qquad B = b_1x_1 + \cdots + b_nx_n,$$
$$C = c_1x_1 + \cdots + a_nc_n, \qquad D = d_1x_1 + \cdots + d_nx_n,$$

należącymi do $\mathbb{Z}[X]$. Jeżeli wszystkie współczynniki wielomianu $F - AB$ są podzielne przez m_1 oraz wszystkie współczynniki wielomianu $F - CD$ są podzielne przez m_2, to istnieją takie wielomiany

$$U = u_1x_1 + \cdots + u_nx_n \quad \textit{oraz} \quad V = v_1x_1 + \cdots + v_nx_n$$

należące do $\mathbb{Z}[X]$, że wszystkie współczynniki wielomianu $F - UV$ są podzielne przez m_1m_2.

D. Oznaczmy przez M_1 i M_2 ideały w $\mathbb{Z}[X]$ generowane odpowiednio przez liczby m_1 i m_2. Ideał M_1 jest zbiorem tych wszystkich wielomianów należących do $\mathbb{Z}[X]$, których wszystkie współczynniki są podzielne przez m_1. Natomiast ideał M_2 jest zbiorem tych wszystkich wielomianów należących do $\mathbb{Z}[X]$, których wszystkie współczynniki są podzielne przez m_2. Z założeń wynika, że $F - AB \in M_1$ oraz $F - CD \in M_2$.

Na mocy twierdzenia chińskiego o resztach, dla każdego $i \in \{1, 2, \ldots, n\}$ istnieją takie liczby całkowite u_i oraz v_i, że

$$\left.\begin{array}{l} u_i \equiv a_i \pmod{m_1}, \\ u_i \equiv c_i \pmod{m_2} \end{array}\right\} \quad \text{oraz} \quad \left\{\begin{array}{l} v_i \equiv b_i \pmod{m_1}, \\ v_i \equiv d_i \pmod{m_2}. \end{array}\right.$$

Niech $U = u_1x_1 + \cdots + u_nx_n$ oraz $V = v_1x_1 + \cdots + v_nx_n$. Wtedy $U - A \in M_1$, $V - B \in M_1$, $U - C \in M_2$ oraz $V - D \in M_2$.

Ponieważ $F - UV = (F - AB) - (U - A)V - A(V - B)$ oraz wielomiany $F - AB$, $U - A$ i $V - B$ należą do ideału M_1, więc wielomian $F - UV$ należy do M_1. Mamy również: $F - UV = (F - CD) - (U - C)V - C(V - D)$ oraz wielomiany $F - CD$, $U - C$ i $V - D$ należą do ideału M_2. Stąd wynika, że wielomian $F - UV$ należy również do M_2. Zatem wielomian $F - UV$ należy do ideału $M_1 \cap M_2$. Ale liczby m_1, m_2 są względnie pierwsze, więc przekrój $M_1 \cap M_2$ jest ideałem w $\mathbb{Z}[X]$ generowanym przez iloczyn m_1m_2. Zatem wszystkie współczynniki wielomianu $F - UV$ są podzielne przez iloczyn m_1m_2. ⊠

W dowodzie tego lematu wykorzystaliśmy twierdzenie chińskie o resztach. W dowodzie następnego lematu wykorzystamy zasadę szufladkową Dirichleta.

8.3.2. *Niech a, b, c będą niezerowymi liczbami całkowitymi i niech u, v, w będą liczbami całkowitymi. Wtedy kongruencja*

$$ux + vy + wz \equiv 0 \pmod{|abc|}$$

ma niezerowe rozwiązanie (x, y, z) takie, że $|x| \leqslant \sqrt{|bc|}$, $|y| \leqslant \sqrt{|ac|}$, $|z| \leqslant \sqrt{|ab|}$. ([Mol2] 275).

D. ([Mol2] 275). Rozważmy zbiór

$$S = \left\{(x, y, z) \in \mathbb{Z}^3;\ 0 \leqslant x \leqslant \left[\sqrt{|bc|}\right],\ 0 \leqslant y \leqslant \left[\sqrt{|ac|}\right],\ 0 \leqslant z \leqslant \left[\sqrt{|ab|}\right]\right\}.$$

Jest to skończony zbiór posiadający dokładnie n elementów, gdzie

$$n = \left(1 + \left[\sqrt{|bc|}\right]\right)\left(1 + \left[\sqrt{|ac|}\right]\right)\left(1 + \left[\sqrt{|ab|}\right]\right).$$

Zauważmy, że $n > \sqrt{|bc|} \cdot \sqrt{|ac|} \cdot \sqrt{|ab|} = |abc|$. Zbiór S posiada więc więcej niż $|abc|$ elementów. Na mocy zasady szufladkowej Dirichleta istnieją zatem dwa różne elementy zbioru S, powiedzmy (x_1, y_1, z_1) i (x_2, y_2, z_2) takie, że

$$ux_1 + vy_1 + wz_1 \equiv ux_2 + vy_2 + wz_2 \pmod{|abc|}.$$

Niech $x = x_1 - x_2$, $y = y_1 - y_2$ oraz $z = z_1 - z_2$. Wtedy $|x| \leqslant \sqrt{|bc|}$, $|y| \leqslant \sqrt{|ac|}$, $|z| \leqslant \sqrt{|ab|}$, $(x, y, z) \neq (0, 0, 0)$ oraz $ux + vy + wz \equiv 0 \pmod{|abc|}$. ⊠

W przypadku, gdy $c = 1$ oraz $a, b \in \mathbb{N}$, powyższy lemat przyjmuje następującą postać.

8.3.3. *Jeśli a, b są liczbami naturalnymi oraz u, v, w liczbami całkowitymi, to kongruencja*

$$ux + vy + wz \equiv 0 \pmod{ab}$$

ma niezerowe rozwiązanie (x, y, z) takie, że $|x| \leqslant \sqrt{b}$, $|y| \leqslant \sqrt{a}$, $|z| \leqslant \sqrt{ab}$.

8.4 Twierdzenie Legendre'a

W stwierdzeniu 8.2.1 podaliśmy pewne warunki konieczne, które muszą być spełnione by dane równanie $ax^2 + by^2 = cz^2$ posiadało niezerowe rozwiązanie całkowite. Teraz możemy już udowodnić, że są to również warunki wystarczające. Z tym faktem spotykamy się w różnych książkach z elementarnej teorii liczb (patrz na przykład: ([Dave] 154-159, [Mol2] 274-276, [Nagl] 218-226). Jest to tzw. twierdzenie Legendre'a. Udowodnimy najpierw to twierdzenie dla równania $ax^2 + by^2 = z^2$.

8.4.1 (Twierdzenie Legendre'a)**.** *Niech a, b będą bezkwadratowymi i względnie pierwszymi liczbami naturalnymi. Równanie $ax^2 + by^2 = z^2$ ma niezerowe rozwiązanie całkowite, wtedy i tylko wtedy, gdy każda z dwóch kongruencji*

$$X^2 \equiv b \pmod{a} \quad \textit{oraz} \quad X^2 \equiv a \pmod{b}$$

ma rozwiązanie.

D. (Na podstawie dowodu podanego w [Mol2] 274-276). Już wiemy (patrz 8.2.2), że rozwiązalność podanych kongruencji jest warunkiem koniecznym. Załóżmy teraz, że te kongruencje mają rozwiązania. Istnieją wtedy takie liczby całkowite d, e, że $a \equiv d^2 \pmod{b}$ oraz $b \equiv e^2 \pmod{a}$. Rozpatrzmy wielomian $zx^2 + by^2 - z^2$. Modulo b mamy:

$$ax^2 + by^2 - z^2 \equiv ax^2 - z^2 \equiv d^2x^2 - z^2 = (dx - z)(dx + z) \pmod{b}$$

i podobnie: $ax^2 + by^2 - z^2 \equiv by^2 - z^2 \equiv e^2y^2 - z^2 = (ey - z)(ey + z) \pmod{a}$. Ponieważ liczby a, b są względnie pierwsze, więc (patrz lemat 8.3.1) istnieją takie liczby całkowite m, n, r, u, v, w, że

$$ax^2 + by^2 - z^2 \equiv (mx + ny + rz)(ux + vy + wz) \pmod{ab}.$$

Z lematu 8.3.3 wiemy, że kongruencja $ux + vy + wz \equiv 0 \pmod{ab}$ ma niezerowe rozwiązanie (x, y, z) takie, że $|x| \leqslant \sqrt{b}$, $|y| \leqslant \sqrt{a}$, $|z| \leqslant \sqrt{ab}$. Mamy zatem trójkę liczb całkowitych (x, y, z) taką, że:

$$ax^2 + by^2 - z^2 \equiv 0 \pmod{ab}$$

oraz: $(x, y, z) \neq (0, 0, 0)$, $x^2 \leqslant b$, $y^2 \leqslant a$, $z^2 \leqslant ab$.

Ponieważ liczby a, b są względnie pierwsze i bezkwadratowe, równość $x^2 = b$ zachodzi jedynie dla $b = 1$, równość $y^2 = a$ zachodzi jedynie dla $a = 1$ i podobnie równość $z^2 = ab$ jest możliwa tylko dla $a = b = 1$. W przypadku, gdy $a = b = 1$ rozważane równanie jest równaniem Pitagorasa i nie ma czego dowodzić. Załóżmy więc dalej, że $a \neq 1$ lub $b \neq 1$. Mamy wtedy:

$$ax^2 + by^2 - z^2 \leqslant ax^2 + by^2 < ab + ab = 2ab \quad \text{oraz} \quad ax^2 + by^2 - z^2 \geqslant -z^2 > -ab.$$

Zatem, $-ab < ax^2 + by^2 - z^2 < 2ab$ i liczba całkowita $ax^2 + by^2 - z^2$ jest podzielna przez ab. Stąd wynika, że $ax^2 + by^2 - z^2 = 0$ lub $ax^2 + by^2 - z^2 = ab$. W pierwszym przypadku trójka (x, y, z) jest niezerowym rozwiązaniem całkowitym równania $ax^2 + by^2 = z^2$. W drugim przypadku, gdy $ax^2 + by^2 - z^2 = ab$, zachodzi równość

$$a(-by + xz)^2 + b(ax + yz)^2 = (z^2 + ab)^2,$$

którą łatwo sprawdzić. Z równości tej wynika, że w tym drugim przypadku trójka

$$\Big(x_1, y_1, z_1\Big) = \Big(- by + xz,\ ax + yz,\ z^2 + ab\Big)$$

jest niezerowym rozwiązaniem całkowitym równania $ax^2 + by^2 = z^2$ i to kończy dowód. ☒

Teraz udowodnimy twierdzenie Legendre'a dla równania $ax^2 + by^2 = cz^2$.

8.4.2 (Twierdzenie Legendre'a)**.** *Niech a, b, c będą bezkwadratowymi liczbami naturalnymi i parami względnie pierwszymi. Równanie $ax^2 + by^2 = cz^2$ ma niezerowe rozwiązanie całkowite wtedy i tylko wtedy, gdy każda z następujących kongruencji*

$$X^2 \equiv bc \pmod{a},\ X^2 \equiv ac \pmod{b},\ X^2 \equiv -ab \pmod{c}$$

ma rozwiązanie.

D. (Drobna modyfikacja dowodu podanego w [Mol2] 274-276). Już wiemy (patrz 8.2.1), że rozwiązalność podanych kongruencji jest warunkiem koniecznym. Załóżmy teraz, że te kongruencje posiadają rozwiązania. Istnieją wtedy takie liczby całkowite d, h, że $ab \equiv -d^2 \pmod{c}$ oraz $ah \equiv 1 \pmod{c}$ (takie h istnieje ponieważ liczby a i c są względnie pierwsze). Rozpatrzmy wielomian $zx^2 + by^2 - cz^2$. Modulo c mamy:

$$\begin{aligned} ax^2 + by^2 - cz^2 &\equiv ax^2 + by^2 = 1 \cdot (ax^2 + by^2) \\ &\equiv (ah)(ax^2 + by^2) = ha^2x^2 + abhy^2 \equiv ha^2x^2 - d^2hy^2 \\ &\equiv (hax - dhy)(ax + dy) \pmod{c}. \end{aligned}$$

Istnieją również takie liczby całkowite e, h_1, że $ac \equiv e^2 \pmod{b}$ oraz $ah_1 \equiv 1 \pmod{b}$. Modulo b mamy zatem:

$$\begin{aligned} ax^2 + by^2 - cz^2 &\equiv ax^2 - cz^2 = 1 \cdot (ax^2 - cz^2) \\ &\equiv (ah_1)(ax^2 - cz^2) = h_1a^2x^2 - ach_1z^2 \equiv h_1(a^2x^2 - e^2z^2) \\ &\equiv (h_1ax - h_1ez)(ax + ez) \pmod{b}. \end{aligned}$$

Istnieją również takie liczby całkowite f, h_2, że $bc \equiv f^2 \pmod{a}$ oraz $bh_2 \equiv 1 \pmod{a}$. Modulo a mamy zatem:

$$\begin{aligned} ax^2 + by^2 - cz^2 &\equiv by^2 - cz^2 = 1 \cdot (by^2 - cz^2) \\ &\equiv (bh_2)(by^2 - cz^2) = h_2b^2y^2 - bch_2z^2 \equiv h_2(b^2y^2 - f^2z^2) \\ &\equiv (h_2by - h_2fz)(by + fz) \pmod{a}. \end{aligned}$$

Ponieważ liczby a, b, c są parami względnie pierwsze, więc (patrz lemat 8.3.1) istnieją takie liczby całkowite m, n, r, u, v, w, że

$$ax^2 + by^2 - cz^2 \equiv (mx + ny + rz)(ux + vy + wz) \pmod{abc}.$$

Z lematu 8.3.2 wiemy, że kongruencja $ux + vy + wz \equiv 0 \pmod{abc}$ ma niezerowe rozwiązanie (x, y, z) takie, że $|x| \leqslant \sqrt{bc}$, $|y| \leqslant \sqrt{ac}$, $|z| \leqslant \sqrt{ab}$. Mamy zatem trójkę liczb całkowitych (x, y, z) taką, że:

$$ax^2 + by^2 - cz^2 \equiv 0 \pmod{abc}$$

oraz: $(x, y, z) \neq (0, 0, 0)$, $x^2 \leqslant bc$, $y^2 \leqslant ac$, $z^2 \leqslant ab$.

Ponieważ liczby a, b są parami względnie pierwsze i bezkwadratowe, równość $x^2 = bc$ zachodzi jedynie dla $b = c = 1$, równość $y^2 = ac$ zachodzi jedynie dla $a = c = 1$ i podobnie równość $z^2 = ab$ jest możliwa tylko dla $a = b = 1$.

Załóżmy, że $a \neq 1$ lub $b \neq 1$. Mamy wtedy:

$$ax^2 + by^2 - cz^2 \leqslant ax^2 + by^2 < abc + abc = 2abc \quad \text{oraz} \quad ax^2 + by^2 - cz^2 \geqslant -z^2 > -abc.$$

Zatem, $-abc < ax^2 + by^2 - cz^2 < 2abc$ i liczba całkowita $ax^2 + by^2 - cz^2$ jest podzielna przez abc. Stąd wynika, że $ax^2 + by^2 - cz^2 = 0$ lub $ax^2 + by^2 - cz^2 = abc$. W pierwszym przypadku trójka (x, y, z) jest niezerowym rozwiązaniem całkowitym równania $ax^2 + by^2 = cz^2$. W drugim przypadku, gdy $ax^2 + by^2 - cz^2 = abc$, zachodzi równość

$$a(-by + xz)^2 + b(ax + yz)^2 = c(z^2 + ab)^2,$$

którą łatwo sprawdzić. Z równości tej wynika, że w tym drugim przypadku trójka

$$\Big(x_1, y_1, z_1\Big) = \Big(-by + xz,\ ax + yz,\ z^2 + ab\Big)$$

jest niezerowym rozwiązaniem całkowitym równania $ax^2 + by^2 = cz^2$.

Jeśli więc $a \neq 1$ lub $b \neq 1$, to dowód jest zakończony. Należy jeszcze rozpatrzyć przypadek $a = b = 1$. W tym przypadku rozważane równanie jest postaci $x^2 + y^2 = cz^2$ i wiemy, że kongruencja $X^2 \equiv -1 \pmod{c}$ ma rozwiązanie. Niech p będzie nieparzystą liczbą pierwszą dzielącą c. Wtedy kongruencja $X^2 \equiv -1 \pmod{p}$ ma rozwiązanie, a więc (patrz podstawowe własności symbolu Legendre'a) p jest postaci $4k + 1$. Liczba c nie ma więc żadnego dzielnika pierwszego postaci $4k + 3$. To implikuje, że c jest sumą dwóch kwadratów liczb całkowitych; powiedzmy u i v, Trójka $(u, v, 1)$ jest więc niezerowym rozwiązaniem całkowitym równania $x^2 + y^2 = cz^2$ i to kończy dowód. ⊠

★ H. Davenport, *The equation $ax^2 + by^2 = z^2$*, [Dave] 154-159.
L. E. Dickson, *The equation $ax^2 + by^2 + cz^2 = 0$*, [Dic2] 419-428.
R. A. Mollin, *The equation $ax^2 + by^2 + cz^2 = 0$*, [Mol2] 274-276.
L. J. Mordell, *Homogeneous equation of the second degree*, [Morl], 42-52.
T. Nagell, *The diophantine equation $ax^2 + by^2 + cz^2 = 0$*, [Nagl] 218-226.

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

8.5 Równanie $x^2 + ny^2 = z^2$

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

W tym podrozdziale zajmować się będziemy rozwiązaniami równania $x^2 + by^2 = z^2$, gdzie b jest niezerową liczbą całkowitą. Jeśli $b = -n < 0$, to równanie takie sprowadza się do równania $z^2 + ny^2 = z^2$. W dalszym ciągu zakładać więc będziemy, że $b = n$ jest liczbą naturalną. W przypadku $n = 1$ mamy równanie Pitagorasa $x^2 + y^2 = z^2$, którym już się zajmowaliśmy. Przypomnijmy, że równanie Pitagorasa (patrz 7.1.1) ma nieskończenie wiele rozwiązań pierwotnych, czyli takich rozwiązań naturalnych (x, y, z), że $\operatorname{nwd}(x, y, z) = 1$. Tę samą własność posiadają wszystkie równania $x^2 + ny^2 = z^2$.

8.5.1. *Każde równanie postaci $x^2 + ny^2 = z^2$, gdzie $n \in \mathbb{N}$, ma nieskończenie wiele rozwiązań pierwotnych.*

D. Załóżmy najpierw, że n jest liczbą niekwadratową. Przyjmując $x = 1$, otrzymujemy równanie Pella $z^2 - ny^2 = 1$, o którym wiemy (patrz [N14]), że ma nieskończenie wiele rozwiązań naturalnych. Jeśli para (u, v) jest rozwiązaniem naturalnym tego równania Pella, to trójka $(1, v, u)$ jest rozwiązaniem pierwotnym równania $x^2 + ny^2 = z^2$. Rozwiązań pierwotnych jest więc nieskończenie wiele.

Załóżmy teraz, że $n = k^2$ jest liczbą kwadratową. Niech $a = kr + 1$, $b = kr$, gdzie $r \in \mathbb{N}$. Wtedy trójka $(a^2 - b^2, 2ab, a^2 + b^2)$ jest rozwiązaniem pierwotnym równania Pitagorasa (patrz 7.1.1). Trójka $(x, y, z) = (a^2 - b^2, 2ar, a^2 + b^2)$ jest więc rozwiązaniem pierwotnym. równania $x^2 + k^2y^2 = z^2$. W tym przypadku rozpatrywane równanie również ma nieskończenie wiele rozwiązań pierwotnych. ⊠

Jeśli (u, v, w) jest niezerową trójką liczb całkowitych, to przez $\gamma(u, v, w)$ oznaczać będziemy trójkę $(\frac{u}{d}, \frac{v}{d}, \frac{w}{d})$, gdzie $d = \text{nwd}(u, v, w)$. Mamy na przykład: $\gamma(8, 4, 6) = (4, 2, 3)$ oraz $\gamma(15, 9, 18) = (5, 3, 6)$. Dla każdej niezerowej trójki liczb całkowitych (u, v, w) zachodzą równości

$$\gamma(mu, mv, mw) = \gamma(u, v, w) \quad \text{dla} \quad m \in \mathbb{N}.$$

Zanotujmy następujący lemat.

8.5.2. *Jeśli x, y, z, x_1, y_1, z_1 są takimi liczbami naturalnymi, że $\frac{x}{z} = \frac{x_1}{z_1}$ oraz $\frac{y}{z} = \frac{y_1}{z_1}$, to $\gamma(x, y, z) = \gamma(x_1, y_1, z_1)$.*

D. Z podanych równości wynika, że $xz_1 = zx_1$ oraz $yz_1 = zy_1$. Zatem:

$$\gamma(x, y, z) = \gamma(xz_1, yz_1, zz_1) = \gamma(zx_1, zy_1, zz_1) = \gamma(x_1, y_1, z_1)$$

i to kończy dowód. ⊠

Jest oczywiste, że jeśli trójka (x, y, z) jest rozwiązaniem naturalnym pewnego równania postaci $ax^2 + by^2 = cz^2$, to $\gamma(x, y, z)$ jest rozwiązaniem pierwotnym tego równania.

8.5.3. *Niech $n \in \mathbb{N}$. Każde rozwiązanie pierwotne równania $x^2 + ny^2 = z^2$ jest postaci*

$$(x, y, z) = \gamma(a^2 - nb^2, 2ab, a^2 + nb^2),$$

gdzie a, b są względnie pierwszymi liczbami naturalnymi takimi, że $a > \sqrt{n}b$.

D. Niech (x, y, z) będzie rozwiązaniem pierwotnym i niech $u = \frac{x}{z}$, $v = \frac{y}{z}$. Wtedy u, v są dodatnimi liczbami wymiernymi spełniającymi równość $u^2 + nv^2 = 1$. Jest jasne, że $u < 1$ oraz $v < \frac{1}{\sqrt{n}}$. Mamy: $v^2 = \frac{1-u^2}{n} = \frac{(1-u)(1+u)}{n}$ i stąd $t^2 = \frac{1-u}{n(1+u)}$, gdzie $t = \frac{v}{1+u}$ jest dodatnią liczbą wymierną. Z tych zależności otrzymujemy równości

$$u = \frac{1 - nt^2}{1 + nt^2} \quad \text{oraz} \quad v = \frac{2t}{1 + nt^2},$$

z których wynika w szczególności, że $t < \frac{1}{\sqrt{n}}$ (gdyż $u > 0$, $t > 0$). Ponieważ t jest dodatnią liczbą wymierną, więc istnieją liczby naturalne a, b takie, że $t = \frac{b}{a}$ oraz $\text{nwd}(a, b) = 1$. Ponadto $a > \sqrt{n}b$, gdyż $t < \frac{1}{\sqrt{n}}$. Mamy zatem

$$\frac{x}{z} = u = \frac{a^2 - nb^2}{a^2 + nb^2} \quad \text{oraz} \quad \frac{y}{z} = v = \frac{2ab}{a^2 + nb^2}$$

i teza wynika z lematu 8.5.2. ⊠

Podamy teraz pewne rozwiązania równań postaci $x^2 + ny^2 = z^2$ dla małych liczb naturalnych n. Rozpoczynamy od przypadku $n = 2$.

8.5.4. *Jeśli (x, y, z) jest pierwotnym rozwiązaniem równania $x^2+2y^2 = z^2$, to x, z są liczbami nieparzystymi oraz y jest liczbą parzystą.*

8.5.5. (1) *Wszystkie rozwiązania naturalne równania $x^2 + 2y^2 = z^2$ są postaci*

$$x = r|m^2 - 2n^2|, \quad y = 2rmn, \quad z = r(m^2 + 2n^2),$$

gdzie $r, m, n \in \mathbb{N}$. ([S56] 39, [S59] 67, [Br83] s.59).

(2) *Wszystkie względnie pierwsze rozwiązania całkowite równania $x^2+2y^2 = z^2$ są postaci*

$$x = |m^2 - 2n^2|, \quad y = 2mn, \quad z = m^2 + 2n^2,$$

gdzie $m, n \in \mathbb{N}$, $\text{nwd}(m, n) = 1$ oraz m nieparzyste. ([Gelf] 23).

8.5.6. *Przykłady rozwiązań pierwotnych równania $x^2 + 2y^2 = z^2$.*

$(1,2,3)$, $(1,12,17)$, $(1,70,99)$, $(1,408,577)$,
$(7,4,9)$, $(7,6,11)$, $(7,30,43)$, $(7,40,57)$, $(7,176,249)$, $(7,234,331)$,
$(17,6,19)$, $(17,20,33)$, $(17,56,81)$, $(17,126,179)$, $(17,330,467)$,
$(23,10,27)$, $(23,24,41)$, $(23,84,121)$, $(23,154,219)$, $(23,494,699)$,
$(31,8,33)$, $(31,42,67)$, $(31,90,131)$, $(31,260,369)$, $(31,532,753)$,
$(41,28,57)$, $(41,30,59)$, $(41,198,283)$, $(41,208,297)$,
$(47,14,51)$, $(47,60,97)$, $(47,144,209)$, $(47,374,531)$,
$(49,10,51)$, $(49,72,113)$, $(49,132,193)$, $(49,442,627)$,
$(71,12,73)$, $(71,110,171)$, $(71,182,267)$,
$(73,36,89)$, $(73,70,123)$, $(73,286,411)$, $(73,456,649)$,
$(79,18,83)$, $(79,112,177)$, $(79,220,321)$,
$(89,42,107)$, $(89,88,153)$, $(89,340,489)$, $(89,570,811)$,
$(97,14,99)$, $(97,156,241)$, $(97,240,353)$. (Maple).

8.5.7. *Wszystkie rozwiązania naturalne równania $x^2 + 3y^2 = z^2$ są postaci*

$$x = r|m^2 - 3n^2|, \quad y = 2rmn, \quad z = r(m^2 + 3n^2),$$

gdzie $r, m, n \in \mathbb{N}$.

8.5.8. *Przykłady rozwiązań pierwotnych równania $x^2 + 3y^2 = z^2$.*

$(1,1,2)$, $(1,4,7)$, $(1,15,26)$, $(1,56,97)$, $(1,209,362)$,
$(11,4,13)$, $(11,5,14)$, $(11,21,38)$, $(11,24,43)$, $(11,80,139)$, $(11,91,158)$, $(11,340,589)$,
$(13,3,14)$, $(13,8,19)$, $(13,20,37)$, $(13,35,62)$, $(13,77,134)$, $(13,132,229)$, $(13,288,499)$,
$(23,7,26)$, $(23,12,31)$, $(23,40,73)$, $(23,55,98)$, $(23,153,266)$, $(23,208,361)$,
$(37,5,38)$, $(37,28,61)$, $(37,48,91)$, $(37,117,206)$, $(37,187,326)$, $(37,440,763)$,
$(47,8,49)$, $(47,33,74)$, $(47,65,122)$, $(47,140,247)$, $(47,252,439)$,
$(59,11,62)$, $(59,40,91)$, $(59,84,157)$, $(59,171,302)$,
$(61,16,67)$, $(61,35,86)$, $(61,99,182)$, $(61,156,277)$, $(61,380,661)$,
$(71,20,79)$, $(71,39,98)$, $(71,119,218)$, $(71,176,313)$, $(71,456,793)$,
$(73,7,74)$, $(73,60,127)$, $(73,88,169)$, $(73,247,434)$,
$(83,13,86)$, $(83,60,133)$, $(83,112,211)$,
$(97,20,103)$, $(97,63,146)$, $(97,143,266)$, $(97,272,481)$. (Maple).

8.5.9. *Przykłady rozwiązań pierwotnych równania $x^2 + 4y^2 = z^2$.*

$(3,2,5)$, $(5,6,13)$, $(7,12,25)$, $(8,3,10)$, $(9,20,41)$, $(11,30,61)$,
$(13,42,85)$, $(15,4,17)$, $(15,56,113)$, $(16,15,34)$, $(17,72,145)$, $(19,90,181)$,
$(21,10,29)$, $(24,5,26)$, $(24,35,74)$. (Maple).

8.5.10. *Przykłady rozwiązań pierwotnych równania $x^2 + 5y^2 = z^2$.*

$(1,4,9)$, $(1,72,161)$,
$(2,1,3)$, $(2,3,7)$, $(2,21,47)$, $(2,55,123)$,
$(11,8,21)$, $(11,12,29)$, $(11,156,349)$, $(11,224,501)$,
$(19,4,21)$, $(19,48,109)$, $(19,120,269)$,
$(22,3,23)$, $(22,7,27)$, $(22,45,103)$, $(22,65,147)$, $(22,119,267)$, $(22,171,383)$,
$(29,24,61)$, $(29,28,69)$,
$(31,12,41)$, $(31,56,129)$, $(31,272,609)$,
$(38,9,43)$, $(38,33,83)$, $(38,35,87)$, $(38,91,207)$,
$(41,12,49)$, $(41,88,201)$, $(41,304,681)$,
$(58,11,63)$, $(58,15,67)$, $(58,133,303)$, $(58,153,347)$,
$(59,16,69)$, $(59,132,301)$,
$(61,36,101)$, $(61,80,189)$. (Maple).

8.5.11. *Przykłady rozwiązań pierwotnych równania $x^2 + 6y^2 = z^2$.*

$(1, 2, 5)$, $(1, 20, 49)$,
$(5, 2, 7)$, $(5, 4, 11)$, $(5, 24, 59)$, $(5, 42, 103)$, $(5, 238, 583)$,
$(19, 10, 31)$, $(19, 12, 35)$, $(19, 112, 275)$, $(19, 130, 319)$,
$(23, 4, 25)$, $(23, 30, 77)$, $(23, 70, 173)$, $(23, 304, 745)$,
$(25, 6, 29)$, $(25, 28, 73)$, $(25, 88, 217)$,
$(29, 8, 35)$, $(29, 30, 79)$, $(29, 110, 271)$,
$(43, 14, 55)$, $(43, 40, 107)$, $(43, 180, 443)$,
$(47, 10, 53)$, $(47, 56, 145)$, $(47, 156, 385)$,
$(53, 6, 55)$, $(53, 80, 203)$, $(53, 140, 347)$. (Maple).

8.5.12. *Przykłady rozwiązań pierwotnych równania $x^2 + 7y^2 = z^2$.*

$(1, 3, 8)$, $(1, 48, 127)$,
$(3, 1, 4)$, $(3, 4, 11)$, $(3, 20, 53)$, $(3, 65, 172)$,
$(9, 5, 16)$, $(9, 8, 23)$, $(9, 88, 233)$, $(9, 133, 352)$,
$(19, 12, 37)$, $(19, 15, 44)$, $(19, 252, 667)$,
$(27, 4, 29)$, $(27, 55, 148)$, $(27, 119, 316)$,
$(29, 12, 43)$, $(29, 33, 92)$,
$(31, 3, 32)$, $(31, 72, 193)$, $(31, 120, 319)$,
$(37, 9, 44)$, $(37, 60, 163)$, $(37, 204, 541)$,
$(47, 24, 79)$, $(47, 45, 128)$,
$(53, 36, 109)$, $(53, 39, 116)$. (Maple).

8.5.13. *Przykłady rozwiązań pierwotnych równania $x^2 + 8y^2 = z^2$.*

$(1, 1, 3)$, $(1, 6, 17)$, $(1, 35, 99)$, $(1, 204, 577)$,
$(7, 2, 9)$, $(7, 3, 11)$, $(7, 15, 43)$, $(7, 20, 57)$, $(7, 88, 249)$,
$(17, 3, 19)$, $(17, 10, 33)$, $(17, 28, 81)$, $(17, 63, 179)$,
$(23, 5, 27)$, $(23, 12, 41)$, $(23, 42, 121)$,
$(31, 4, 33)$, $(31, 21, 67)$, $(31, 45, 131)$, $(31, 130, 369)$, $(31, 266, 753)$,
$(41, 14, 57)$, $(41, 15, 59)$, $(41, 104, 297)$,
$(47, 7, 51)$, $(47, 30, 97)$, $(47, 72, 209)$,
$(49, 5, 51)$, $(49, 36, 113)$, $(49, 66, 193)$. (Maple).

8.5.14. *Przykłady rozwiązań pierwotnych równania $x^2 + 9y^2 = z^2$.*

$(4, 1, 5), (5, 4, 13), (7, 8, 25), (8, 5, 17), (9, 4, 15), (11, 20, 61)$,
$(13, 28, 85), (16, 21, 65), (17, 48, 145), (19, 60, 181), (20, 7, 29)$, $(20, 33, 101)$. (Maple).

★ J. Cel, *O teorii równania $z^2 - By^2 = x^2$*, [Mat] 1/1987 39-44.

Różne informacje o rozwiązaniach równania $x^2 + by^2 = z^2$ znajdziemy w: [S50] 242, [S56] 40, [S59] 109, 159, [S64] 127, [Mat] 5/1972 303.

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

8.6 Równanie $x^2 + y^2 = nz^2$

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

Z twierdzenia Legendre'a 8.4.2 wynika natychmiast następujący wniosek.

8.6.1. *Jeśli n jest bezkadratową liczbą naturalną, to równanie $x^2 + y^2 = nz^2$ ma niezerowe rozwiązanie całkowite wtedy i tylko wtedy, gdy kongruencja $X^2 \equiv -1 \pmod{n}$ ma rozwiązanie.*

Jest jasne, że kongruencja $X^2 \equiv -1 \pmod 3$ nie ma rozwiązań. Zatem, na mocy powyższego wniosku, równanie $x^2+y^2 = 3z^2$ nie ma niezerowych rozwiązań całkowitych. Podobnie jest z równaniami $x^2+y^2 = 7z^2$ oraz $x^2+y^2 = 11z^2$. Istnieją więc równania postaci $x^2+y^2 = nz^2$, które nie mają niezerowych rozwiązań całkowitych.

8.6.2. *Niech n będzie liczbą naturalną. Równanie $x^2 + y^2 = nz^2$ ma niezerowe rozwiązanie całkowite wtedy i tylko wtedy, gdy n jest sumą kwadratów dwóch liczb całkowitych.*

D. Jeśli $n = a^2 + b^2$, gdzie $a, b \in \mathbb{Z}$, to trójka $(a, b, 1)$ jest niezerowym rozwiązaniem rozważanego równania. Załóżmy, że (x, y, z) jest niezerowym rozwiązaniem równania $x^2 + y^2 = nz^2$. Wtedy $z \neq 0$ i wtedy $n = u^2 + v^2$, gdzie u, v są liczbami wymiernymi równymi odpowiednio x/z i y/z. Z twierdzenia 3.14.1 wynika zatem, że n jest sumą kwadratów dwóch liczb całkowitych. ⊠

Przypomnijmy, że jeśli (x, y, z) jest niezerową trójką liczb całkowitych, to przez $\gamma(x, y, z)$ oznaczamy trójkę $(x/d, y/d, z/d)$, gdzie $d = \mathrm{nwd}(x, y, z)$.

8.6.3. *Każde rozwiązanie pierwotne równania $x^2 + y^2 = 2z^2$ jest postaci*

$$\gamma\Big(|a^2 + 2ab - b^2|,\ |-a^2 + 2ab + b^2|,\ a^2 + b^2\Big),$$

gdzie a, b są względnie pierwszymi liczbami całkowitymi i $b > 0$.

D. Niech (x, y, z) będzie rozwiązaniem pierwotnym równania $x^2 + y^2 = 2z^2$. Niech $u = \frac{x}{z}$, $v = \frac{y}{z}$. Wtedy u, v są dodatnimi liczbami wymiernymi spełniającymi równość $u^2 + v^2 = 2$, a zatem (u, v) jest punktem wymiernym leżącym na okręgu $X^2 + Y^2 = 2$. Na tym okręgu leży również punkt wymierny $(-1, -1)$, który jest różny od punktu (u, v) (ponieważ $u > 0$, $v > 0$). Prosta przechodząca przez te dwa punkty ma równanie postaci $Y + 1 = t(X + 1)$, gdzie t jest pewną liczbą wymierną. Mamy zatem układ równań

$$\begin{cases} u^2 + v^2 = 2, \\ v = t(u + 1) - 1. \end{cases}$$

Podstawiając równanie drugie do równania pierwszego, otrzymujemy równość

$$(1 + t^2)u^2 + (2t^2 - 2t)u + (t^2 - 2t - 1) = 0,$$

która jest w oczywisty sposób spełniona dla $u = -1$. Z wzorów Viete'a wynika, że

$$u + (-1) = \frac{2t - 2t^2}{1 + t^2}.$$

Zatem $u = \frac{-t^2+2t+1}{1+t^2}$ oraz $v = tu + t - 1 = \frac{t^2+2t-1}{1+t^2}$. Liczba t jest wymierna. Istnieją zatem względnie pierwsze liczby całkowite a, b takie, że $t = \frac{a}{b}$ oraz $b > 0$. Mamy zatem

$$\frac{x}{z} = u = \frac{a^2 + 2ab - b^2}{a^2 + b^2} = \frac{\big|a^2 + 2ab - b^2\big|}{a^2 + b^2} \quad \text{oraz} \quad \frac{y}{z} = v = \frac{-a^2 + 2ab + b^2}{a^2 + b^2} = \frac{\big|-a^2 + 2ab + b^2\big|}{a^2 + b^2}$$

i teza wynika z lematu 8.5.2. ⊠

8.6.4. *Przykłady rozwiązań pierwotnych równania $x^2 + y^2 = 2z^2$.*

$(1, 1, 1)$, $(1, 7, 5)$, $(1, 41, 29)$, $(1, 239, 169)$,
$(7, 1, 5)$, $(7, 17, 13)$, $(7, 23, 17)$, $(7, 103, 73)$, $(7, 137, 97)$, $(7, 601, 425)$,
$(17, 7, 13)$, $(17, 31, 25)$, $(17, 73, 53)$, $(17, 193, 137)$, $(17, 431, 305)$,
$(23, 7, 17)$, $(23, 47, 37)$, $(23, 89, 65)$, $(23, 289, 205)$, $(23, 527, 373)$,
$(31, 17, 25)$, $(31, 49, 41)$, $(31, 151, 109)$, $(31, 311, 221)$,
$(41, 1, 29)$, $(41, 113, 85)$, $(41, 119, 89)$, $(41, 679, 481)$,
$(47, 23, 37)$, $(47, 79, 65)$, $(47, 217, 157)$, $(47, 497, 353)$,
$(49, 31, 41)$, $(49, 71, 61)$, $(49, 257, 185)$, $(49, 457, 325)$,
$(71, 49, 61)$, $(71, 97, 85)$, $(71, 391, 281)$, $(71, 631, 449)$. (Maple).

8.6.5. *Każde rozwiązanie pierwotne równania $x^2 + y^2 = 4z^2$ jest postaci*

$$\gamma\Big(2(a^2 - b^2),\ 4ab,\ a^2 + b^2\Big),$$

gdzie $a > b$ są względnie pierwszymi liczbami naturalnymi. Przykłady rozwiązań pierwotnych:

$(6, 8, 5), (8, 6, 5), (10, 24, 13), (14, 48, 25), (16, 30, 17), (18, 80, 41), (22, 120, 61),$
$(24, 10, 13),\ (24, 70, 37), (26, 168, 85), (30, 16, 17),\ (30, 224, 113),$
$(32, 126, 65), (34, 288, 145), (38, 360, 181), (40, 42, 29),\ (40, 198, 101),$
$(42, 40, 29), (48, 14, 25),\ (48, 286, 145).$ (Maple).

8.6.6. *Każde rozwiązanie pierwotne równania $x^2 + y^2 = 5z^2$ jest postaci*

$$\gamma\Big(\Big|a^2 + 4ab - b^2\Big|,\ 2\Big|a^2 - ab - b^2\Big|,\ a^2 + b^2\Big),$$

gdzie a, b są względnie pierwszymi liczbami całkowitymi i $b > 0$. (Dowodzimy tak samo jak 8.6.3).

8.6.7. *Przykłady rozwiązań pierwotnych równania $x^2 + y^2 = 5z^2$.*

$(1, 2, 1),\ (1, 38, 17),\ (1, 682, 305),$
$(2, 1, 1),\ (2, 11, 5),\ (2, 29, 13),\ (2, 199, 89),$
$(11, 2, 5),\ (11, 82, 37),\ (11, 118, 53),$
$(19, 22, 13),\ (19, 62, 29),\ (19, 458, 205),$
$(22, 19, 13),\ (22, 31, 17),\ (22, 61, 29),\ (22, 89, 41),\ (22, 431, 193),$
$(29, 2, 13),\ (29, 242, 109),\ (29, 278, 125),$
$(31, 22, 17),\ (31, 142, 65),\ (31, 538, 241),$
$(38, 1, 17),\ (38, 41, 25),\ (38, 131, 61),\ (38, 331, 149),\ (38, 349, 157),$
$(41, 38, 25),\ (41, 158, 73),\ (41, 842, 377),$
$(58, 59, 37),\ (58, 71, 41),\ (58, 181, 85),\ (58, 209, 97),$
$(59, 58, 37),\ (59, 218, 101),$
$(61, 22, 29),\ (61, 382, 173),\ (61, 778, 349),$
$(62, 19, 29),\ (62, 101, 53),\ (62, 151, 73),\ (62, 409, 185).$ (Maple).

8.6.8. *Przykłady rozwiązań pierwotnych równania $x^2 + y^2 = 8z^2$.*

$(2, 2, 1),\ (2, 14, 5),\ (2, 82, 29),\ (2, 478, 169),$
$(14, 2, 5),\ (14, 34, 13),\ (14, 46, 17),\ (14, 206, 73),\ (14, 274, 97),\ (14, 1202, 425),$
$(34, 14, 13),\ (34, 62, 25),\ (34, 146, 53),\ (34, 386, 137),\ (34, 862, 305),$
$(46, 14, 17),\ (46, 94, 37),\ (46, 178, 65),\ (46, 578, 205),\ (46, 1054, 373),$
$(62, 34, 25),\ (62, 98, 41),\ (62, 302, 109),\ (62, 622, 221).$ (Maple).

8.6.9. *Przykłady rozwiązań pierwotnych równania $x^2 + y^2 = 9z^2$.*

$(9, 12, 5), (12, 9, 5), (15, 36, 13), (21, 72, 25), (24, 45, 17), (27, 120, 41),$
$(33, 180, 61), (36, 15, 13),\ (36, 105, 37), (39, 252, 85), (45, 24, 17),\ (45, 336, 113),$
$(48, 189, 65), (51, 432, 145), (57, 540, 181), (60, 63, 29),\ (60, 297, 101).$ (Maple).

★ K. Szymiczek, *Zasada lokalno-globalna*, (O równaniach diofantycznych postaci $x^2 + y^2 = nz^2$), [Dlt] 2/1980 14-16.

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

8.7 Rozwiązania pewnych równań postaci $ax^2 + by^2 = cz^2$

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

8.7.1. *Równania $x^2 + vy^2 = wz^2$ ($dla\ v, w \in \{1, 2, 3, 4, 5\}$) i ich wszystkie rozwiązania całkowite. Liczby a, b, r są całkowite.* (Maple).

(1) $x^2 + y^2 = 2z^2$; $x = (-a^2 - 2ab + b^2)r$, $y = (-a^2 + 2ab + b^2)r$, $z = (a^2 + b^2)r$.

(2) $x^2 + y^2 = 4z^2$; $x = 4rab$, $y = 2(-a^2 + b^2)r$, $z = (a^2 + b^2)r$.

(3) $x^2 + y^2 = 5z^2$; $x = 2(-a^2 - ab + b^2)r$, $y = (-a^2 + 4ab + b^2)r$, $z = (a^2 + b^2)r$.

(4) $x^2 + 2y^2 = 2z^2$; $x = 4rab$, $y = (-a^2 + 2b^2)r$, $z = (a^2 + 2b^2)r$.

(5) $x^2 + 2y^2 = 3z^2$; $x = (a^2 + 4ab - 2b^2)r$, $y = (-a^2 + 2ab + 2b^2)r$, $z = (a^2 + 2b^2)r$.

(6) $x^2 + 2y^2 = 4z^2$; $x = 2(-a^2 + 2b^2)r$, $y = 4rab$, $z = (a^2 + 2b^2)r$. ([Br83] 41).

(7) $x^2 + 3y^2 = z^2$; $x = (-a^2 + 3b^2)r$, $y = 2rab$, $z = (a^2 + 3b^2)r$.

(8) $x^2 + 3y^2 = 3z^2$; $x = 6rab$, $y = (-a^2 + 3b^2)r$, $z = (a^2 + 3b^2)r$.

(9) $x^2 + 3y^2 = 4z^2$; $x = 2(-a^2 + 3b^2)r$, $y = 4rab$, $z = (a^2 + 3b^2)r$.

(10) $x^2 + 4y^2 = z^2$; $x = 8rab$, $y = (-a^2 + 4b^2)r$, $z = 2(a^2 + 4b^2)r$.

(11) $x^2 + 4y^2 = 2z^2$; $x = 2(a^2 + 4ab - 4b^2)r$, $y = (a^2 - 4ab - 4b^2)r$, $z = 2(a^2 + 4b^2)r$.

(12) $x^2 + 4y^2 = 4z^2$; $x = 8rab$, $y = (-a^2 + 4b^2)r$, $z = (a^2 + 4b^2)r$.

(13) $x^2 + 4y^2 = 5z^2$; $x = 4(a^2 + 2ab - 4b^2)r$, $y = (a^2 - 8ab - 4b^2)r$, $z = 2(a^2 + 4b^2)r$.

(14) $x^2 + 5y^2 = z^2$; $x = (-a^2 + 5b^2)r$, $y = 2rab$, $z = (a^2 + 5b^2)r$.

(15) $x^2 + 5y^2 = 4z^2$; $x = 2(-a^2 + 5b^2)r$, $y = 4rab$, $z = (a^2 + 5b^2)r$.

(16) $x^2 + 5y^2 = 5z^2$; $x = 10rab$, $y = (-a^2 + 5b^2)r$, $z = (a^2 + 5b^2)r$.

8.7.2. *Równania $2x^2 + vy^2 = wz^2$ ($dla\ v, w \in \{1, 2, 3, 4, 5\}$, $2 \leqslant v$, $\mathrm{nwd}(2, v, w) = 1$) i ich wszystkie rozwiązania całkowite. Liczby a, b, r są całkowite.* (Maple).

(1) $2x^2 + 2y^2 = z^2$; $x = (-a^2 - 2ab + b^2)r$, $y = (-a^2 + 2ab + b^2)r$, $z = 2(a^2 + b^2)r$.

(2) $2x^2 + 2y^2 = 5z^2$; $x = (-3a^2 - 2ab + 3b^2)r$, $y = (-a^2 + 6ab + b^2)r$, $z = 2(a^2 + b^2)r$.

(3) $2x^2 + 3y^2 = 2z^2$; $x = (-2a^2 + 3b^2)r$, $y = 4rab$, $z = (2a^2 + 3b^2)r$.

(4) $2x^2 + 3y^2 = 3z^2$; $x = 6rab$, $y = (-2a^2 + 3b^2)r$, $z = (2a^2 + 3b^2)r$.

(5) $2x^2 + 3y^2 = 5z^2$; $x = (2a^2 + 6ab - 3b^2)r$, $y = (2a^2 - 4ab - 3b^2)r$, $z = (2a^2 + 3b^2)r$.

(6) $2x^2 + 4y^2 = z^2$; $x = 4rab$, $y = (-a^2 + 2b^2)r$, $z = 2(a^2 + 2b^2)r$.

(7) $2x^2 + 4y^2 = 3z^2$; $x = 2(a^2 + 2ab - 2b^2)r$, $y = (-a^2 + 4ab + 2b^2)r$, $z = 2(a^2 + 2b^2)r$.

(8) $2x^2 + 5y^2 = 2z^2$; $x = (-2a^2 + 5b^2)r$, $y = 4rab$, $z = (2a^2 + 5b^2)r$.

(9) $2x^2 + 5y^2 = 5z^2$; $x = 10rab$, $y = (-2a^2 + 5b^2)r$, $z = (2a^2 + 5b^2)r$.

8.7.3. *Równania $3x^2 + vy^2 = wz^2$ ($dla\ v, w \in \{1, 2, 3, 4, 5\}$, $3 \leqslant v$, $\mathrm{nwd}(3, v, w) = 1$) i ich wszystkie rozwiązania całkowite. Liczby a, b, r są całkowite.* (Maple).

(1) $3x^2 + 4y^2 = z^2$; $x = 8rab$, $y = (-3a^2 + 4b^2)r$, $z = 2(3a^2 + 4b^2)r$.

(2) $3x^2 + 4y^2 = 3z^2$; $x = (-3a^2 + 4b^2)r$, $y = 6rab$, $z = (3a^2 + 4b^2)r$.

(3) $3x^2 + 4y^2 = 4z^2$; $x = 8rab$, $y = (-3a^2 + 4b^2)r$, $z = (3a^2 + 4b^2)r$.

(4) $3x^2 + 5y^2 = 2z^2$; $x = (3a^2 + 10ab - 5b^2)r$, $y = (3a^2 - 6ab - 5b^2)r$, $z = 2(3a^2 + 5b^2)r$.

(5) $3x^2 + 5y^2 = 3z^2$; $x = (-3a^2 + 5b^2)r$, $y = 6rab$, $z = (3a^2 + 5b^2)r$.

(6) $3x^2 + 5y^2 = 5z^2$; $x = 10rab$, $y = (-3a^2 + 5b^2)r$, $z = (3a^2 + 5b^2)r$.

8.7.4. *Równania* $4x^2 + vy^2 = wz^2$ *(dla* $v, w \in \{1,2,3,4,5\}$, $4 \leqslant v$, $\mathrm{nwd}(4,v,w) = 1$*) i ich wszystkie rozwiązania całkowite. Liczby* a, b, r *są całkowite.* (Maple).

(1) $4x^2 + 4y^2 = z^2$; $x = 2rab$, $y = (-a^2 + b^2)r$, $z = 2(a^2 + b^2)r$.

(2) $4x^2 + 4y^2 = 5z^2$; $x = 2(-a^2 - ab + b^2)r$, $y = (-a^2 + 4ab + b^2)r$, $z = 2(a^2 + b^2)r$.

(3) $4x^2 + 5y^2 = z^2$; $x = (-4a^2 + 5b^2)r$, $y = 8rab$, $z = 2(4a^2 + 5b^2)r$.

(4) $4x^2 + 5y^2 = 4z^2$; $x = (-4a^2 + 5b^2)r$, $y = 8rab$, $z = (4a^2 + 5b^2)r$.

(5) $4x^2 + 5y^2 = 5z^2$; $x = 10rab$, $y = (-4a^2 + 5b^2)r$, $z = (4a^2 + 5b^2)r$.

8.7.5. *Równania* $5x^2 + 5y^2 = wz^2$ *(dla* $w \in \{1,2,3,4,5\}$, $\mathrm{nwd}(5,w) = 1$*) i ich wszystkie rozwiązania całkowite. Liczby* a, b, r *są całkowite.* (Maple).

(1) $5x^2 + 5y^2 = z^2$; $x = 2(-a^2 - ab + b^2)r$, $y = (-a^2 + 4ab + b^2)r$, $z = 5(a^2 + b^2)r$.

(2) $5x^2 + 5y^2 = 2z^2$; $x = (3a^2 + 2ab - 3b^2)r$, $y = (-a^2 + 6ab + b^2)r$, $z = 5(a^2 + b^2)r$.

(3) $5x^2 + 5y^2 = 4z^2$; $x = 4(-a^2 - ab + b^2)r$, $y = 2(-a^2 + 4ab + b^2)r$, $z = 5(a^2 + b^2)r$.

8.7.6. *Wszystkie trójki* (a,b,c)*, gdzie* $a, b, c \in \{1,2,3,4,5\}$, $\mathrm{nwd}(a,b,c) = 1$, $a \leqslant b$*, dla których równanie* $ax^2 + by^2 = cz^2$ *nie ma naturalnych rozwiązań:* (Maple).

$(1,1,3), (1,3,2), (1,3,5), (1,4,3), (1,5,2), (1,5,3),$
$(2,2,3), (2,3,1), (2,3,4), (2,4,5), (2,5,1), (2,5,3), (2,5,4),$
$(3,3,1), (3,3,2), (3,3,4), (3,3,5), (3,5,1), (3,5,4),$
$(4,4,3), (4,4,7), (4,5,2), (4,5,3),$
$(5,5,3).$

Literatura

[Br83] J. Browkin, *Zbiór Zadań z Olimpiad Matematycznych*, tom 6, 26-30, 74/75 - 78/79, WSiP, Warszawa, 1983.

[Dave] H. Davenport, *The Higher Arithmetic*, Seventh edition, Cambirdge University Press, 1999.

[Dic2] L. E. Dickson, *History of the Theory of Numbers*, Vol. II. *Diophantine analysis*, Carnegie Institute of Washington, 1919. Reprinted by AMS Chelsea Publishing, New York, 1992.

[Dlt] Delta, popularny polski miesięcznik matematyczno-fizyczno-astronomiczny.

[Gelf] A. O. Gelfond, *Rozwiązywanie równań w liczbach całkowitych* (po rosyjsku), Popularne lekcje z matematyki 8, Moskwa, Leningrad 1952.

[Mat] Matematyka, polskie czasopismo dla nauczycieli.

[Mol2] R. A. Mollin, *Fundamental Number Theory with Applications*, Second Edition, CRC Press, Boca Raton, London, New York, 2008.

[Mon] The American Mathematical Monthly, Mathematical Association of America.

[Morl] L. J. Mordell, *Diophantine Equations*, Academic Press, London and New York, 1969.

[N14] A. Nowicki, *Równanie Pella*, Podróże po Imperium Liczb, cz.14, Wydawnictwo OWSIiZ, Toruń, Olsztyn, 2011.

[Nagl] T. Nagell, *Introduction to Number Theory*, Chelsea Publishing Company, New York, 1964.

[S50] W. Sierpiński, *Teoria Liczb*, Warszawa - Wrocław, 1950.

[S56] W. Sierpiński, *O Rozwiązywaniu Równań w Liczbach Całkowitych*, PWN, Warszawa, 1956.

[S59] W. Sierpiński, *Teoria Liczb* II, PWN, Warszawa, 1959.

[S64] W. Sierpiński, *200 Zadań z Elementarnej Teorii Liczb*, Biblioteczka Matematyczna 17, PZWS, Warszawa, 1964.