Podróże po Imperium Liczb

Część 03. Liczby Kwadratowe

Rozdział 3

3. Sumy dwóch kwadratów

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`.

⊡⊡

3 Sumy dwóch kwadratów

⊡⊡

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

3.1 Warunki rozkładalności na sumę dwóch kwadratów

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

3.1.1. *Każda liczba naturalna postaci* $4k+3$ *nie jest sumą dwóch kwadratów liczb całkowitych.*

3.1.2. *Każda liczba naturalna postaci* $9k+3$ *nie jest sumą dwóch kwadratów liczb całkowitych.*

3.1.3. *Liczba naturalna jest sumą dwóch kwadratów liczb całkowitych wtedy i tylko wtedy, gdy w jej rozkładzie na czynniki pierwsze nie ma żadnej liczby pierwszej postaci* $4k+3$ *w potędze nieparzystej.* ([S50] 80).

3.1.4. *Liczba naturalna jest sumą dwóch kwadratów względnie pierwszych liczb całkowitych wtedy i tylko wtedy, gdy nie jest podzielna przez* 4 *i nie ma żadnego czynnika pierwszego postaci* $4k+3$*.* ([Dave] 139).

3.1.5. *Liczba naturalna jest sumą dwóch kwadratów liczb całkowitych wtedy i tylko wtedy, gdy jest postaci* $2^s(4m+1)$*, gdzie* $s \geqslant 0$ *oraz* m *jest sumą dwóch liczb trójkątnych.*
([MG] 41(338)(1957) 288-289).

★ R. A. Mollin, *Sums of two squares*, [Mol2] 243-251.
A. Sutcliffe, *On sums of two squares*, [MG] 41(338)(1957) 288-289.

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

3.2 Własności sum dwóch kwadratów

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

3.2.1. *Z równości*

$$(a^2+b^2)(c^2+d^2) = (ad-bc)^2 + (ac+bd)^2$$

wynika, że jeśli liczby n *i* m *są sumami dwóch kwadratów liczb całkowitych, to liczba* nm *również jest sumą dwóch kwadratów liczb całkowitych.*

3.2.2. *Jeśli* $2n$ *jest sumą kwadratów dwóch liczb całkowitych, to* n *również.* ([Str67] s.29).

3.2.3. *Dla każdej liczby naturalnej* n *równania* $x^2+y^2=n$ *oraz* $x^2+y^2=2n$ *mają jednakowe liczby rozwiązań całkowitych.* ([S-kg] 78).

D. Niech $A = \{(a,b) \in \mathbb{Z}^2;\ a^2+b^2=n\}$, $B = \{(c,d) \in \mathbb{Z}^2;\ c^2+d^2=2n\}$. Zauważmy, że jeśli $(c,d) \in B$, to liczby c i d są tej samej parzystości. Funkcje $(a,b) \mapsto (a+b, a-b)$ oraz $(c,d) \mapsto ((c+d)/2, (c-d)/2)$ są wzajemnie odwrotnymi bijekcjami. ⊠

3.2.4. *Niech* $m,n \in \mathbb{N}$*. Jeżeli* $5m = n^2+49$*, to* m *jest sumą dwóch kwadratów liczb całkowitych.*

3.2.5. *Niech $a, n \in \mathbb{N}$. Jeśli $a^2 + 2n$ jest kwadratem liczby całkowitej, to $a^2 + n$ jest sumą dwóch kwadratów liczb całkowitych.* ([Str67] 5).

3.2.6. *Jeżeli liczby a, b, m są całkowite i $a^2 + 2mb^2$ jest kwadratem liczby całkowitej, to $a^2 + mb^2$ jest sumą dwóch kwadratów liczb całkowitych.* ([OM] Słowenia 1993, [Pa97]).

3.2.7. *Dla każdej liczby naturalnej n istnieją liczby naturalne a, b, c takie że $n + a^2 = b^2 + c^2$.*

3.2.8. *Równanie $x^2 + y^2 = z^2 + 3$ ma nieskończenie wiele rozwiązań całkowitych.*
([OM] Włochy 1996, [Pa97]).

★ L. E. Dickson, *Sum of two squares*, [Dic2] 225-257.

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

3.3 Liczba rozkładów na sumy dwóch kwadratów

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

Dla danej liczby naturalnej n przez $\gamma(n)$ oznaczać będziemy (tylko w tym podrozdziale) liczbę wszystkich par (x, y) liczb całkowitych takich, że $x^2 + y^2 = n$. Na przykład $\gamma(5) = 8$ gdyż jest dokładnie 8 par (x, y) liczb całkowitych spełniających równość $5 = x^2 + y^2$; są to pary: $(1, 2)$, $(1, -2)$, $(-1, 2)$, $(-1, -2)$, $(2, 1)$, $(2, -1)$, $(-2, 1)$, $(-2, -1)$.

3.3.1. *Niech $n \in \mathbb{N}$. Zapiszmy n w postaci $n = 2^s n_1 n_3$, gdzie $s \geqslant 0$, n_1 jest iloczynem liczb pierwszych postaci $4k + 1$, n_3 jest iloczynem liczb pierwszych postaci $4k + 3$. Wtedy*

$$\gamma(n) = \begin{cases} 4\tau(n_1), & \text{jeśli } n_3 \text{ jest liczbą kwadratową,} \\ 0, & \text{jeśli } n_3 \text{ nie jest liczbą kwadratową,} \end{cases}$$

gdzie $\tau(n_1)$ jest liczbą podzielników naturalnych liczby n_1. ([S50], [Gio] 90).

3.3.2 (Jacobi 1828). *Liczba $\gamma(n)$, przedstawień liczby naturalnej n w postaci sumy dwóch kwadratów, jest równa $4(d_1(n) - d_3(n))$, gdzie $d_r(n)$ jest liczbą dzielników naturalnych d liczby n takich, $d \equiv r \pmod 4$.*

3.3.3. *Niech n będzie nieparzystą liczbą naturalną. Niech $\delta(n)$ oznacza liczbę przedstawień liczby n w postaci sumy dwóch kwadratów względnie pierwszych liczb całkowitych.*

(1) *Jeśli n dzieli się przez co najmniej jedną liczbę pierwszą postaci $4k + 3$, to $\delta(n) = 0$.*

(2) *Jeśli n nie dzieli się przez żadną liczbę pierwszą postaci $4k+3$, to $\delta(n) = 2^{s+2}$, gdzie s jest liczbą podzielników pierwszych liczby n postaci $4k + 1$.*

(3) *Jeśli $n > 1$ i n nie dzieli się przez żadną liczbę pierwszą postaci $4k + 3$, to istnieje dokładnie 2^{s-1} par $(a, b) \in \mathbb{N} \times \mathbb{N}$ takich, że $n = a^2 + b^2$, $a < b$ i $\mathrm{nwd}(a, b) = 1$, gdzie s jest liczbą podzielników pierwszych liczby n postaci $4k + 1$.* ([Dave] 147, [Mol2] 247).

3.3.4. *Liczba $2 \cdot 5^{2n-1}$, gdzie $n \in \mathbb{N}$, ma dokładnie n różnych rozkładów na sumę dwóch kwadratów liczb naturalnych.* ([Mat] 4/1966 188, [OM] Polska 1990).

★ H. Gupta, A. M. Vaidya, *The number of representations of a number as a sum of two squares*, [Mon] 70(10)(1963) 1081-1082.

M. D. Hirschorn, *A simple proof of Jacobi's two-square theorem*, [Mon] 3/1985 579-580.

M. D. Hirschorn, *Partial fractions and four classical theorems of number theory*, [Mon] 3/2000 260-264.

---

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

3.4 Najmniejsze liczby o danej liczbie rozkładów

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

3.4.1. $25 = 5^2 + 0^2 = 3^2 + 4^2$. *Liczba* 25 *jest najmniejszą liczbą naturalną mającą dwa istotnie różne rozkłady na sumę dwóch kwadratów liczb całkowitych.*

3.4.2. $50 = 5^2 + 5^2 = 7^2 + 1^2$. *Liczba* 50 *jest najmniejszą liczbą naturalną mającą dwa istotnie różne rozkłady na sumę dwóch kwadratów liczb naturalnych.*

3.4.3. *Najmniejszą liczbą naturalną mającą dokładnie trzy istotnie różne rozkłady na sumę dwóch kwadratów liczb całkowitych jest* $325 = 1^2 + 18^2 = 6^2 + 17^2 = 10^2 + 15^2$.

3.4.4. *Najmniejszą liczbą naturalną mającą dokładnie cztery istotnie różne rozkłady na sumę dwóch kwadratów liczb całkowitych jest* $1105 = 4^2 + 33^2 = 9^2 + 32^2 = 12^2 + 31^2 = 23^2 + 24^2$.

3.4.5. *Najmniejszą liczbą naturalną mającą dokładnie pięć istotnie różnych rozkładów na sumę dwóch kwadratów liczb całkowitych jest* $8125 = 5^2 + 90^2 = 27^2 + 86^2 = 30^2 + 85^2 = 50^2 + 75^2 = 58^2 + 69^2$. (Maple).

Poniższe przykłady otrzymano przy pomocy komputera.

3.4.6. *Liczby naturalne mające dokładnie k istotnie różnych rozkładów na sumę dwóch kwadratów liczb całkowitych, dla pewnych k:*

$k = 2:$	25,	50,	65,	85,	100;
$k = 3:$	325,	425,	625,	650,	725;
$k = 4:$	1105,	1625,	1885,	2125,	2210;
$k = 5:$	4225,	7225,	8125,	8450,	10625;
$k = 6:$	5525,	9425,	11050,	12025,	12325;
$k = 8:$	27625,	32045,	40885,	45305,	47125;
$k = 9:$	71825,	93925,	122525,	143650,	156325;
$k = 10:$	138125;				
$k = 12:$	160225.				

3.4.7. *Liczby naturalne mające dokładnie k istotnie różnych rozkładów na sumę dwóch kwadratów liczb naturalnych, dla $k = 2, 3, 4, 5, 6$:*

$k = 2:$	50,	65,	85,	125,	130;
$k = 3:$	325,	425,	650,	725,	845;
$k = 4:$	1105,	1625,	1885,	2125,	2210;
$k = 5:$	8125,	8450,	10625,	14450,	16250;
$k = 6:$	5525,	9425,	11050,	12025,	12325.

3.4.8. *Liczby naturalne mające k istotnie różnych rozkładów na sumę dwóch kwadratów liczb naturalnych dla $k = 7, 8, \dots, 18$ i $k = 20$ (brak danych dla $k = 19$):*

$k = 7$:	105625,	180625,	203125,	265625,	406250;
$k = 8$:	27625,	32045,	40885,	45305,	47125;
$k = 9$;	71825,	93925,	122525,	143650,	156325;
$k = 10$;	138125,	235625,	276250,	300625,	308125;
$k = 11$:	5281250,	9031250,	21125000,	26281250,	36125000;
$k = 12$:	160225,	204425,	226525,	292825,	320450;
$k = 13$:	1221025,	3553225,	4884100,	5784025,	6076225;
$k = 14$:	2442050,	3453125,	5890625,	6906250,	7106450;
$k = 15$:	1795625,	2348125,	3063125,	3591250,	3908125;
$k = 16$:	801125,	1022125,	1132625,	1185665,	1313845;
$k = 17$:	446265625,	1305015625,	1785062500;		
$k = 18$:	2082925,	2657525,	2723825,	2944825,	3475225;
$k = 20$:	4005625,	5110625,	5663125,	7320625,	8011250.

3.4.9. *Liczby naturalne mające dokładnie k istotnie różnych rozkładów na sumę dwóch kwadratów liczb naturalnych dla pewnych $k > 20$:*

$k = 21$:	44890625,	58703125,	76578125,	89781250,	97703125;
$k = 22$:	30525625,	88830625,	122102500,	144600625,	151905625;
$k = 23$:	61051250,	177661250,	244205000,	289201250,	303811250;
$k = 24$:	5928325,	6569225,	8381425,	8491925,	9773725;
$k = 25$:	303460625,	517668125,	606921250,	660473125,	678608125;
$k = 27$:	35409725,	45177925,	50062025,	60404825,	64714325;
$k = 28$:	100140625,	127765625,	141578125,	183015625,	200281250;
$k = 30$:	52073125,	66438125,	68095625,	73620625,	86880625;
$k = 31$:	763140625;				
$k = 32$:	29641625,	32846125,	41907125,	42459625,	48612265;
$k = 36$:	77068225,	85399925,	100781525,	108958525,	110395025;
$k = 40$:	148208125,	164230625,	209535625,	212298125,	244343125;
$k = 41$:	2053764050;				
$k = 42$:	1301828125,	1660953125,	1702390625,	1840515625;	
$k = 45$:	885243125,	1129448125,	1251550625,	1510120625,	1617858125;
$k = 48$:	243061325,	314201225,	348168925,	361627825,	385341125;
$k = 54$:	1310159825,	1451798725,	1852294925,	1876715425;	
$k = 60$:	1926705625,	2134998125;			
$k = 64$:	1215306625,	1571006125,	1740844625,	1808139125,	2003613625.

★ L. Kurlandczyk, A. Nowicki, *Różne rozkłady na sumy kwadratów*, [Dlt] 3/1998 12-13.
L. Kurlandczyk, A. Nowicki, *Sumy dwóch kwadratów i kolejne liczby nat.*, [Dlt] 7/1999 10-11.

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

3.5 Rozkłady dla kolejnych liczb naturalnych

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

3.5.1. *Istnieje nieskończenie wiele liczb naturalnych n takich, że liczby n, $n+1$, $n+2$ są sumami dwóch kwadratów liczb całkowitych.* ([Mon] 74(2)(1967) E1814, [Kw] 10/1983 47, [Putn] 2000).

D. Sposób 1. Niech $n = 8m^2$, gdzie $m = \frac{1}{2}k(k+1)$. Wtedy $n = (2m)^2 + (2m)^2$, $n + 1 = (k^2-1)^2 + (k^2+2k)^2$, $n+2 = (2m-1)^2 + (2m+1)^2$.

Sposób 2. Niech $n = 4k^4 + 4k^2$. Wtedy $n = (2k^2)^2 + (2k)^2$, $n + 1 = (2k^2+1)^2 + 0^2$, $n + 2 = (2k^2+1)^2 + 1^2$. ⊠

3.5.2. *Niech $n \in \mathbb{N}$ i niech $a, b, c, d, e, f \in \mathbb{Z}$ takie, że $n = a^2 + b^2$, $n+1 = c^2 + d^2$, $n+2 = e^2 + f^2$. Wówczas dla $m = n^2 + 2n$ zachodzą równości:*

$$\begin{array}{lcl} m & = & (af - be)^2 + (ae + bf)^2, \\ m+1 & = & (c^2 - d^2)^2 + (2cd)^2, \\ m+2 & = & (n+1)^2 + 1^2. \end{array}$$

Stąd otrzymujemy również inny dowód faktu 3.5.1. ([Mon] 74(2)(1967) E1814).

3.5.3. *Jeśli każda z liczb n, $n+1$ i $n+2$ jest sumą dwóch kwadratów liczb całkowitych, to własność tę mają również liczby m, $m+1$ i $m+2$, dla $m = n(n+2)$.* ([Putn] 2000).

D. Skoro liczby n i $n+2$ są sumami dwóch kwadratów, to liczba $m = n(n+2)$ również jest sumą dwóch kwadratów, gdyż zbiór wszystkich sum dwóch kwadratów jest zamknięty na mnożenie. Mamy ponadto: $m + 1 = n^2 + 2n + 1 = (n+1)^2 + 0^2$, $m + 2 = n^2 + 2n + 2 = (n+1)^2 + 1^2$. ⊠

3.5.4. *Każda z liczb $3^{2^k} - 1$, 3^{2^k}, $3^{2^k} + 1$, jest sumą dwóch kwadratów liczb całkowitych.* ([Putn] 2000).

D. Jeśli $x^2 - 1$ jest sumą dwóch kwadratów, to $x^4 - 1$ również jest sumą dwóch kwadratów. Startując od równości $3^2 - 1 = 2^2 + 2^2$ i powtarzając ten fakt stwierdzamy, że każda liczba postaci $3^{2^k} - 1$ jest sumą dwóch kwadratów. Jest oczywiste, że pozostałe dwie liczby, mianowicie 3^{2^k} i $3^{2^k} + 1$, są sumami dwóch kwadratów. ⊠

3.5.5. *Każda z liczb $73^{2^k} - 1$, 73^{2^k}, $73^{2^k} + 1$, jest sumą dwóch kwadratów liczb całkowitych.* ([Kw] 10/1983 47).

3.5.6. *Istnieje nieskończenie wiele liczb naturalnych n takich, że liczba n jest sumą dwóch kwadratów liczb naturalnych, a liczby $n - 1$ oraz $n + 1$ nie są sumami dwóch kwadratów liczb naturalnych.* ([OM] Moskwa 1996, [Kw] 1/1997 M1556).

D. Taką własność posiadają wszystkie liczby n postaci $2 \cdot 100^m$ ([Kw]). Inne przykłady: $n = (36k+2)^2 + 4^2$, $n = 9^k + 1$ ([FieK] 186-187). ⊠

3.5.7. *Para* (169, 170) *składa się z kolejnych liczb naturalnych, z których każda ma dokładnie dwa różne rozkłady na sumę dwóch kwadratów liczb całkowitych. Są to najmniejsze liczby o tej własności. Tę samą własność mają pary:* (289, 290), (900, 901), (985, 986), (1156, 1157). *Czy takich par jest nieskończenie wiele?* (Maple).

3.5.8. *Trójka* $(11024, 11025, 11026)$ *składa się z kolejnych liczb naturalnych, z których każda ma dokładnie dwa różne rozkłady na sumę dwóch kwadratów liczb całkowitych. Są to najmniejsze liczby o tej własności. Tę samą własność mają trójki:*

$(22048, 22049, 22050)$	$(26280, 26281, 26282)$	$(26440, 26441, 26442)$
$(29520, 29521, 29522)$	$(34280, 34281, 34282)$	$(47888, 47889, 47890)$
$(51208, 51209, 51210)$	$(72592, 72593, 72594)$	$(84240, 84241, 84242)$
$(92240, 92241, 92242)$	$(96840, 96841, 96842)$	$(98568, 98569, 98570)$

Czy takich trójek jest nieskończenie wiele? (Maple).

3.5.9. *Para* $(33524, 33525)$ *składa się z kolejnych liczb naturalnych, z których każda ma dokładnie trzy różne rozkłady na sumę dwóch kwadratów liczb całkowitych. Są to najmniejsze liczby o tej własności. Tę samą własność ma para* $(39700, 39701)$. *Czy takich par jest nieskończenie wiele?* (Maple).

3.5.10. *Para* $(19720, 19721)$ *składa się z kolejnych liczb naturalnych, z których każda ma dokładnie cztery różne rozkłady na sumę dwóch kwadratów liczb całkowitych. Są to najmniejsze liczby o tej własności. Tę samą własność mają pary:*

$$(28249, 28250), (32929, 32930), (76465, 76466).$$

Czy takich par jest nieskończenie wiele? (Maple).

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

3.6 Sumy dwóch kwadratów i podzielność

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

3.6.1. *Niech* $a, b \in \mathbb{Z}$. *Jeżeli* $3 \mid a^2 + b^2$, *to* $3 \mid a$ *i* $3 \mid b$.

3.6.2. *Niech* $a, b \in \mathbb{Z}$. *Jeżeli* $7 \mid a^2 + b^2$, *to* $7 \mid a$ *i* $7 \mid b$. ([S87] 3).

3.6.3. *Niech* $a, b \in \mathbb{N}$. *Jeżeli* $21 \mid a^2 + b^2$, *to* $441 \mid a^2 + b^2$. ([BoL] 173 s.67,[G-if] 33).

3.6.4. *Jeśli* $31^{1995} \mid a^2 + b^2$, *to* $31^{1996} \mid ab$. ([Crux] 1997 s.67).

3.6.5. *Niech* $a, b \in \mathbb{N}$. *Jeśli* $ab \mid a^2 + b^2$, *to* $a = b$. ([TT] 1997).

3.6.6. *Mówimy, że liczba naturalna* m *spełnia warunek* $(*)$ *jeśli*

$$\underset{a,b\in\mathbb{Z}}{\forall}\ m \mid a^2 + b^2 \Longrightarrow m^2 \mid a^2 + b^2.$$

Liczba naturalna m *spełnia warunek* $(*)$ *wtedy i tylko wtedy, gdy jest iloczynem parami różnych liczb pierwszych postaci* $4k + 3$. ([Mat] 3/1999 s.133).

3.6.7. *Każda liczba postaci* a^2+b^2, *gdzie* $a, b \in \mathbb{N}$, *ma dzielnik pierwszy tej postaci.* ([S59] 442).

3.6.8. *Dla każdej liczby naturalnej* $n > 1$ *istnieją różne liczby naturalne* a, b, c, *leżące pomiędzy* n^2 *i* $(n + 1)^2$ *taki, że* $c \mid a^2 + b^2$. ([OM] St Petersburg 1998, [OM] Mołdawia 2001, [Zw] 2004).

D. Niech $c = n^2 + 1$, $a = n^2 + 2$, $b = n^2 + n + 1$. Liczby te są parami różne oraz leżą pomiędzy n^2 i $(n + 1)^2$. Ponadto, $a \equiv 1 \pmod{c}$, $b \equiv n \pmod{c}$, więc $a^2 + b^2 \equiv c \equiv 0 \pmod{c}$. ⊠

3.6.9. *Niech* $a, b, x, y \in \mathbb{N}$. *Jeśli* $a^2 + b^2 \mid ax + by$, *to* $\operatorname{nwd}(a^2 + b^2, x^2 + y^2) > 1$.
([OM] St Petersburg 1994).

D. Z równości $(ax + by)(ay + bx) = (a^2 + b^2)xy + ab(x^2 + y^2)$ wynika, że $a^2 + b^2 \mid ab(x^2 + y^2)$ i stąd już łatwo otrzymujemy tezę. ⊠

3.6.10. *Niech* $x, y, z \in \mathbb{Z}$ *i niech* $, m \in \mathbb{N}$, $m > 1$. *Niech* $x^2 + y^2 = z^{2m}$, $(x, y) = 1$. *Jeśli* $4m - 1$ *jest liczbą pierwszą, to* $p \mid xy$. ([Mon] 6(1978) E2642).

3.6.11. *Niech* $n = x^2 + y^2$, $n > 1$, $x, y, \in \mathbb{Z}$. *Istnieje wówczas nieujemna liczba całkowita* k *taka, że* $n \equiv 2^k \pmod{2^{k+2}}$. ([FQ] B-440).

3.6.12. *Dla każdej liczby naturalnej* $n \geqslant 2$ *istnieje zbiór* A *składający się z* n *parami różnych liczb naturalnych taki, że dla wszystkich różnych liczb* $a, b \in A$, *liczba* $|a - b|$ *dzieli* $a^2 + b^2$.
([OM] Ukraina 2005).

---

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

3.7 Sumy dwóch kwadratów i liczby pierwsze

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

3.7.1. *Liczby pierwsze* < 100 *będące sumami dwóch kwadratów:*

$$\begin{array}{rcrcrcrcrcrcr} 2 &=& 1^2 &+& 1^2, &\quad& 41 &=& 4^2 &+& 5^2, \\ 5 &=& 1^2 &+& 2^2, && 53 &=& 2^2 &+& 7^2, \\ 13 &=& 2^2 &+& 3^2, && 61 &=& 5^2 &+& 6^2, \\ 17 &=& 1^2 &+& 4^2, && 73 &=& 3^2 &+& 8^2, \\ 29 &=& 2^2 &+& 5^2, && 89 &=& 5^2 &+& 8^2, \\ 37 &=& 1^2 &+& 6^2, && 97 &=& 4^2 &+& 9^2. \end{array}$$

3.7.2 (Fermat, Gauss)**.** *Jeżeli* p *jest liczbą pierwszą postaci* $4k+1$*, to* $p = a^2 + b^2$*, gdzie* a *i* b *są takimi liczbami naturalnymi, że* $a \equiv (2k)!/2 \cdot (k!)^2 \pmod{p}$, $\quad b \equiv (2k)! \cdot a \pmod{p}$*, przy czym* $|a| < \frac{1}{2}p$ *i* $|b| < \frac{1}{2}p$*.*

3.7.3. *Liczba postaci* $4k+1$ *jest pierwsza wtedy i tylko wtedy, gdy ma jednoznaczny rozkład na sumę dwóch względnie pierwszych kwadratów.* ([Trost] 37).

3.7.4. *Niech* p *będzie liczbą pierwszą postaci* $4k+1$ *i nich* $p = a^2 + b^2$ *będzie jedynym jej rozkładem na sumę dwóch kwadratów liczb naturalnych* (*taki rozkład istnieje na mocy twierdzenia* 3.7.2)*. Wtedy:*

(1) *Liczba* p^2 *ma dokładnie jeden rozkład na sumę dwóch kwadratów liczb naturalnych, mianowicie:* $p^2 = (2ab)^2 + (a^2 - b^2)^2$*.*

(2) *Liczba* p^3 *ma dokładnie dwa rozkłady:* $p^3 = (pa)^2 + (pb)^2 = (a^3 - 3ab^2)^2 + (3a^2b - b^3)^2$*.*

(3) *Liczba* p^4 *ma dokładnie dwa rozkłady:* $p^4 = (pa^2 - pb^2)^2 + (2pab)^2 = (a^4 - 6a^2b^2 + b^4)^2 + (4ab(a^2 - b^2))^2$*.* ([S59] 441).

3.7.5 (Friedlander-Iwaniec 1998)**.** *Istnieje nieskończenie wiele liczb pierwszych postaci* $a^2 + b^4$*, gdzie* $a, b \in \mathbb{N}$*.* ([Gy04] 8).

3.7.6. *Równanie* $p^2 + 1 = q^2 + r^2$ *ma rozwiązanie w zbiorze liczb pierwszych, na przykład* $(p, q, r) = (13, 7, 11),\ (17, 11, 13),\ (23, 13, 19),\ (31, 11, 29)$*.* ([S64] 70).

3.7.7. *Równanie* $p^2 + q^2 = a^2 + b^2 + c^2$ *nie ma rozwiązań w zbiorze liczb pierwszych.* ([S64] 71).

★ F. W. Clarke, W. N. Everitt, L. L. Littlejohn, S. J. R. Vorster, *H.J.S.Smith and the Fermat two squares theorem*, [Mon] 106(7)(1999) 652-665.

J. A. Ewell, *A simple proof of Fermat's two-square theorem*, [Mon] 90(9)(1983) 635-637.

V. V. Prasolov, *Representing numbers as the sum of two squares*, [Pras] 9-10.

W. Tichomirow, *Twierdzenie Fermata - Eulera o dwóch kwadratach*, [Kw] 10/1991 9-12.

D. Zagier, *A one-sentence proof that every prime* $p \equiv 1 \pmod{4}$ *is a sum of two squares*, [Mon] 97(1990) 114.

---

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

3.8 Przykłady rozkładów z liczbami pierwszymi

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

Przedstawione tu przykłady otrzymano przy pomocy komputera.

3.8.1. *Trzy różne rozkłady z liczbami pierwszymi:*

$$\begin{array}{rcrcrcrcrcrcr}
2210 & = & 19^2 & + & 43^2 & = & 23^2 & + & 41^2 & = & 29^2 & + & 37^2 \\
3770 & = & 7^2 & + & 61^2 & = & 17^2 & + & 59^2 & = & 31^2 & + & 53^2, \\
5330 & = & 17^2 & + & 71^2 & = & 29^2 & + & 67^2 & = & 43^2 & + & 59^2, \\
6290 & = & 7^2 & + & 79^2 & = & 31^2 & + & 73^2 & = & 53^2 & + & 59^2 \\
12818 & = & 7^2 & + & 113^2 & = & 37^2 & + & 107^2 & = & 47^2 & + & 103^2.
\end{array}$$

3.8.2. *Cztery różne rozkłady z liczbami pierwszymi:*

$$\begin{array}{rcrcrlrcrcr}
10370 & = & 13^2 & + & 101^2, & \qquad & 10730 & = & 11^2 & + & 103^2, \\
10370 & = & 31^2 & + & 97^2, & & 10730 & = & 23^2 & + & 101^2, \\
10370 & = & 59^2 & + & 83^2, & & 10730 & = & 53^2 & + & 89^2, \\
10370 & = & 71^2 & + & 73^2, & & 10730 & = & 67^2 & + & 79^2,
\end{array}$$

$$\begin{array}{rcrcr}
11570 & = & 11^2 & + & 107^2, \\
11570 & = & 31^2 & + & 103^2, \\
11570 & = & 37^2 & + & 101^2, \\
11570 & = & 73^2 & + & 79^2.
\end{array}$$

3.8.3. *Pięć różnych rozkładów z liczbami pierwszymi:*

$$\begin{array}{rcrcrlrcrcr}
202130 & = & 23^2 & + & 449^2, & \qquad & 240890 & = & 61^2 & + & 487^2, \\
202130 & = & 97^2 & + & 439^2, & & 240890 & = & 107^2 & + & 479^2, \\
202130 & = & 163^2 & + & 419^2, & & 240890 & = & 151^2 & + & 467^2, \\
202130 & = & 211^2 & + & 397^2, & & 240890 & = & 179^2 & + & 457^2, \\
202130 & = & 251^2 & + & 373^2, & & 240890 & = & 283^2 & + & 401^2.
\end{array}$$

3.8.4. *Każda z następujących liczb ma* 5 *różnych rozkładów na sumę dwóch kwadratów liczb pierwszych:* 202130, 3314090, 4226690, 4687850, 6950450, 7227890, 7296770, 8508890.

3.8.5. *Sześć różnych rozkładów z liczbami pierwszymi:*

$$\begin{array}{rcrcrlrcrcr}
229970 & = & 23^2 & + & 479^2, & \qquad & 229970 & = & 263^2 & + & 401^2, \\
229970 & = & 109^2 & + & 467^2, & & 229970 & = & 269^2 & + & 397^2, \\
229970 & = & 193^2 & + & 439^2, & & 229970 & = & 331^2 & + & 347^2.
\end{array}$$

3.8.6. *Każda z następujących liczb ma* 6 *różnych rozkładów na sumę dwóch kwadratów liczb pierwszych:* 229970, 383690, 420290, 453050, 3146258, 4165850, 4482530, 5667290. (Maple).

3.8.7. *Siedem różnych rozkładów z liczbami pierwszymi:*

$$\begin{array}{rcrcrlrcrcr}
197210 & = & 31^2 & + & 443^2, & \qquad & 197210 & = & 199^2 & + & 397^2, \\
197210 & = & 67^2 & + & 439^2, & & 197210 & = & 241^2 & + & 373^2, \\
197210 & = & 107^2 & + & 431^2, & & 197210 & = & 311^2 & + & 317^2. \\
197210 & = & 173^2 & + & 409^2, & & & & & &
\end{array}$$

3.8.8. *Każda z następujących liczb ma* 7 *różnych rozkładów na sumę dwóch kwadratów liczb pierwszych:* 197210, 781898, 983450, 999050, 1752530, 2199650, 2627690, 13668170. (Maple).

3.8.9. *Osiem różnych rozkładów z liczbami pierwszymi:*

$$\begin{array}{lllll} 81770 = 41^2 + 283^2, & & 81770 = 137^2 + 251^2, \\ 81770 = 53^2 + 281^2, & & 81770 = 157^2 + 239^2, \\ 81770 = 71^2 + 277^2, & & 81770 = 179^2 + 223^2, \\ 81770 = 97^2 + 269^2, & & 81770 = 193^2 + 211^2. \end{array}$$

81770 *jest najmniejszą liczbą o takiej własności. Nie ma ona żadnych innych rozkładów na sumę dwóch kwadratów liczb naturalnych.* (Maple).

3.8.10. *Osiem różnych rozkładów z liczbami pierwszymi:*

$$\begin{array}{lllll} 369410 = 31^2 + 607^2, & & 369410 = 277^2 + 541^2, \\ 369410 = 103^2 + 599^2, & & 369410 = 313^2 + 521^2, \\ 369410 = 191^2 + 577^2, & & 369410 = 347^2 + 499^2, \\ 369410 = 229^2 + 563^2, & & 369410 = 389^2 + 467^2. \end{array}$$

Liczba 369410 *nie ma żadnych innych rozkładów na sumę dwóch kwadratów liczb naturalnych.* (Maple).

3.8.11. *Każda z następujących liczb ma* 8 *różnych rozkładów na sumę dwóch kwadratów liczb pierwszych:* 81770, 369410, 1540370, 2044250, 3396770, 8192210, 12329930, 44158010, 310673810, 322683290. (Maple).

3.8.12. *Dziewięć różnych rozkładów z liczbami pierwszymi:*

$$\begin{array}{lllll} 36964850 = 103^2 + 6079^2, & & 34159970 = 139^2 + 5843^2, \\ 36964850 = 571^2 + 6053^2, & & 34159970 = 257^2 + 5839^2, \\ 36964850 = 1801^2 + 5807^2, & & 34159970 = 1811^2 + 5557^2, \\ 36964850 = 2069^2 + 5717^2, & & 34159970 = 2521^2 + 5273^2, \\ 36964850 = 2243^2 + 5651^2, & & 34159970 = 3221^2 + 4877^2, \\ 36964850 = 2273^2 + 5639^2, & & 34159970 = 3359^2 + 4783^2, \\ 36964850 = 2713^2 + 5441^2, & & 34159970 = 3617^2 + 4591^2, \\ 36964850 = 2963^2 + 5309^2, & & 34159970 = 3709^2 + 4517^2, \\ 36964850 = 3299^2 + 5107^2, & & 34159970 = 3929^2 + 4327^2. \end{array}$$

3.8.13. *Każda z następujących liczb ma* 9 *różnych rozkładów na sumę dwóch kwadratów liczb pierwszych:* 34159970, 36964850, 47143850, 160289090, 304266170, 635698850, 1295451170, 1321812050. (Maple).

3.8.14. *Dziesięć różnych rozkładów z liczbami pierwszymi:*

$$\begin{array}{lllll} 68768570 = 167^2 + 8291^2, & & 78656450 = 181^2 + 8867^2, \\ 68768570 = 571^2 + 8273^2, & & 78656450 = 373^2 + 8861^2, \\ 68768570 = 701^2 + 8263^2, & & 78656450 = 593^2 + 8849^2, \\ 68768570 = 1103^2 + 8219^2, & & 78656450 = 727^2 + 8839^2, \\ 68768570 = 2143^2 + 8011^2, & & 78656450 = 1231^2 + 8783^2, \\ 68768570 = 3343^2 + 7589^2, & & 78656450 = 1777^2 + 8689^2, \\ 68768570 = 3709^2 + 7417^2, & & 78656450 = 2179^2 + 8597^2, \\ 68768570 = 4049^2 + 7237^2, & & 78656450 = 2309^2 + 8563^2, \\ 68768570 = 4507^2 + 6961^2, & & 78656450 = 4801^2 + 7457^2, \\ 68768570 = 4799^2 + 6763^2, & & 78656450 = 6067^2 + 6469^2. \end{array}$$

3.8.15. *Każda z następujących liczb ma* 10 *różnych rozkładów na sumę dwóch kwadratów liczb pierwszych:* 68768570, 78656450, 97224530, 125680490, 154136450, 1422293690. (Maple).

3.8.16. *Jedenaście różnych rozkładów z liczbami pierwszymi:*

$$\begin{array}{rcrcl}
19547450 &=& 47^2 &+& 4421^2, \\
19547450 &=& 751^2 &+& 4357^2, \\
19547450 &=& 859^2 &+& 4337^2, \\
19547450 &=& 1283^2 &+& 4231^2, \\
19547450 &=& 1627^2 &+& 4111^2, \\
19547450 &=& 1657^2 &+& 4099^2, \\
19547450 &=& 2039^2 &+& 3923^2, \\
19547450 &=& 2179^2 &+& 3847^2, \\
19547450 &=& 2713^2 &+& 3491^2, \\
19547450 &=& 2837^2 &+& 3391^2, \\
19547450 &=& 3083^2 &+& 3169^2,
\end{array}
\qquad
\begin{array}{rcrcl}
62430290 &=& 67^2 &+& 7901^2, \\
62430290 &=& 593^2 &+& 7879^2, \\
62430290 &=& 619^2 &+& 7877^2, \\
62430290 &=& 1151^2 &+& 7817^2, \\
62430290 &=& 1669^2 &+& 7723^2, \\
62430290 &=& 1759^2 &+& 7703^2, \\
62430290 &=& 2333^2 &+& 7549^2, \\
62430290 &=& 3407^2 &+& 7129^2, \\
62430290 &=& 4231^2 &+& 6673^2, \\
62430290 &=& 4253^2 &+& 6659^2, \\
62430290 &=& 5107^2 &+& 6029^2.
\end{array}$$

3.8.17. *Każda z następujących liczb ma* 11 *różnych rozkładów na sumę dwóch kwadratów liczb pierwszych:* $19547450, 62430290, 137455370, 292942130, 589731530, 696337850$. (Maple).

3.8.18. *Piętnaście różnych rozkładów z liczbami pierwszymi:*

$$\begin{array}{rcrcl}
723255650 &=& 149^2 &+& 26893^2, \\
723255650 &=& 3467^2 &+& 26669^2, \\
723255650 &=& 4139^2 &+& 26573^2, \\
723255650 &=& 4703^2 &+& 26479^2, \\
723255650 &=& 5651^2 &+& 26293^2, \\
723255650 &=& 5843^2 &+& 26251^2, \\
723255650 &=& 7057^2 &+& 25951^2, \\
723255650 &=& 8311^2 &+& 25577^2, \\
723255650 &=& 8863^2 &+& 25391^2,
\end{array}
\qquad
\begin{array}{rcrcl}
723255650 &=& 9227^2 &+& 25261^2, \\
723255650 &=& 9491^2 &+& 25163^2, \\
723255650 &=& 11093^2 &+& 24499^2, \\
723255650 &=& 13873^2 &+& 23039^2, \\
723255650 &=& 16921^2 &+& 20903^2, \\
723255650 &=& 18439^2 &+& 19577^2.
\end{array}$$

3.8.19. *Szesnaście różnych rozkładów z liczbami pierwszymi:*

$$\begin{array}{rcrcl}
1030580018 &=& 1123^2 &+& 32083^2, \\
1030580018 &=& 1283^2 &+& 32077^2, \\
1030580018 &=& 3833^2 &+& 31873^2, \\
1030580018 &=& 4273^2 &+& 31817^2, \\
1030580018 &=& 5413^2 &+& 31643^2, \\
1030580018 &=& 8293^2 &+& 31013^2, \\
1030580018 &=& 9343^2 &+& 30713^2, \\
1030580018 &=& 11617^2 &+& 29927^2,
\end{array}
\qquad
\begin{array}{rcrcl}
1030580018 &=& 12227^2 &+& 29683^2, \\
1030580018 &=& 14107^2 &+& 28837^2, \\
1030580018 &=& 15797^2 &+& 27947^2, \\
1030580018 &=& 17167^2 &+& 27127^2, \\
1030580018 &=& 17623^2 &+& 26833^2, \\
1030580018 &=& 17903^2 &+& 26647^2, \\
1030580018 &=& 21193^2 &+& 24113^2, \\
1030580018 &=& 21313^2 &+& 24007^2.
\end{array}$$

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

3.9 Równanie $x^2 + y^2 = z^n$

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

3.9.1. *Liczba* n^3 *jest sumą kwadratów dwóch liczb całkowitych wtedy i tylko wtedy, gdy* n *jest sumą kwadratów dwóch liczb całkowitych.* ([S59] 443).

3.9.2. *Istnieje nieskończenie wiele trójek* (x, y, z)*, liczb naturalnych takich, że*

$$x^2 + y^2 = z^3$$

oraz $\mathrm{nwd}(x, y, z) = 1$*. Każda taka tójka jest postaci*

$$(x, y, z) = \Big(a(a^2 - 3b^2),\ b(3a^2 - b^2),\ a^2 + b^2\Big),$$

gdzie a, b *są względnie pierwszymi liczbami naturalnymi i dokładnie jedna z nich jest liczbą parzystą.* ([Coh2] 466).

3.9.3. $7^2 + 24^2 = 5^4$, $119^2 + 120^2 = 13^4$, $161^2 + 240^2 = 17^4$.

3.9.4. *Istnieje nieskończenie wiele trójek* (x, y, z), *liczb naturalnych takich, że*

$$x^2 + y^2 = z^4$$

oraz $\mathrm{nwd}(x, y, z) = 1$. *Każda taka tójka jest postaci*

$$(x, y, z) = \Big((a^2 - b^2)^2 - (2ab)^2,\ 4ab(a^2 - b^2),\ a^2 + b^2\Big),$$

gdzie a, b *są względnie pierwszymi liczbami naturalnymi i dokładnie jedna z nich jest liczbą parzystą.* ([Mon] 21(6)(1914) 199-200, [Coh2] 466).

3.9.5. *Równanie* $x^2 + y^2 = z^{1998}$ *ma nieskończenie wiele rozwiązań naturalnych.*
([Crux] 1998 s.236 z.2347).

3.9.6. *Dla każdej liczby naturalnej* n *równanie* $x^2 + y^2 = z^n$ *ma rozwiązanie naturalne.*
([Mon] 68(1)(1961) E1416).

★ I. Reiner, *The diophantine equation* $x^2 + b^2 = y^5$, [Mon] 69(4)(1962) 280-282.

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

3.10 Liczby postaci $(\mathrm{a}^2 + \mathrm{b}^2)/(\mathrm{ab} \pm 1)$ i ich uogólnienia

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

3.10.1. *Jeśli* a *i* b *są takimi liczbami naturalnymi, że liczba* $ab+1$ *dzieli liczbę* a^2+b^2, *to iloraz* $(a^2 + b^2)/(ab + 1)$ *jest liczbą kwadratową.* ([IMO] 1988, [Kw] 4/1989 M 1135, [Br], [Kucz] 1.18, [San2] 3).

3.10.2. *Jeśli* a *i* b *są takimi liczbami całkowitymi, że liczba* $(a^2 + b^2)/(ab + 1)$ *jest naturalna, to* $(a^2 + b^2)/(ab + 1)$ *jest liczbą kwadratową.* ([Br]).

3.10.3. *Jeśli* a *i* b *są takimi liczbami całkowitymi, że* $(a^2 + b^2)/(ab + 1)$ *jest całkowitą liczbą ujemną, to* $(a^2 + b^2)/(ab + 1) = -5$. ([Br]).

3.10.4. *Niech* (x_n) *i* (y_n) *będą ciągami zdefiniowanymi następująco:*

$$\begin{cases} x_1 &= 1, \\ x_2 &= 2, \\ x_{n+1} &= 5x_{n+1} - 5x_n; \end{cases} \qquad \begin{cases} y_1 &= 1, \\ y_2 &= 3, \\ y_{n+1} &= 5y_{n+1} - 5y_n. \end{cases}$$

(1) *Przykłady:* $(x_n) = (1, 2, 9, 43, 206, 987, \dots)$, $(y_n) = (1, 3, 14, 67, 321, 1538, \dots)$.

(2) *Niech* $(a, b) = (x_n, -x_{n+1})$ *lub* $(a, b) = (y_n, -y_{n+1})$, *gdzie* $n \in \mathbb{N}$. *Wtedy*

$$(a^2 + b^2)/(1 + ab) = -5.$$

(3) *Jeśli* $a, b \in \mathbb{Z}$ *i* $(a^2+b^2)/(1+ab)$ *jest całkowitą liczbą ujemną, to para* (a, b) *jest jedną z par opisanych w punkcie* (2). ([Br]).

3.10.5. *Niech* $a, b \in \mathbb{N}$ *i niech* $r = (a^2 + b^2)/(ab - 1)$. *Jeśli* $r \in \mathbb{N}$, *to* $r = 5$.
([Kw] 10/1990 25, [Zw] 2004).

3.10.6. *Jeśli a, n są liczbami naturalnymi takimi, że $a^2 + 4 = n(2a - 1)$, to $n = 5$.*

3.10.7. *Jeśli a, n są liczbami naturalnymi takimi, że $a^2 + 9 = n(3a - 1)$, to $n = 5$.*

3.10.8. *Jeśli a, n są liczbami naturalnymi takimi, że $a^2 + 81 = n(9a - 1)$, to $n = 5$.*

3.10.9. *Niech n będzie liczbą naturalną postaci $4^s(8k + 7)$, gdzie $k, s \geqslant 0$.*

(1) *Istnieje nieskończenie wiele piątek (a, b, c, d, e) liczb naturalnych takich, że*

$$n = \frac{a^2 + b^2 + c^2 + d^2 + e^2}{abcde + 1}.$$

(2) *Nie ma żadnej czwórki $(a, b, c, d) \in \mathbb{N}^4$ takiej, że $n = \frac{a^2+b^2+c^2+d^2}{abcd+1}$.*

(3) *Jeśli $a_1, \dots a_m$ są nieujemnymi liczbami całkowitymi i $u = \frac{a_1^2+a_2^2+\cdots+a_m^2}{1+a_1a_2\cdots a_m}$, jest liczbą liczbą całkowitą, to u jest sumą m kwadratów liczb całkowitych.* ([Mon] 98(7)(1991) 665-666 z.6619).

★ K. Brown, $N = (x^2 + y^2)/(1 + xy)$ *is a square*, [Br].

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

3.11 Liczby, które nie są sumami dwóch kwadratów

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

3.11.1. *Liczby postaci $4k + 3$ nie są sumami dwóch kwadratów liczb całkowitych.*

3.11.2. *Jeśli a i b są względnie pierwszymi liczbami naturalnymi, z których co najmniej jedna jest postaci $4k + 3$, to liczba ab nie jest sumą kwadratów dwóch liczb całkowitych.*

D. Załóżmy, że liczba b jest postaci $4k+3$. Ponieważ iloczyn liczb postaci $4k+1$ jest liczbą postaci $4k+1$ oraz iloczyn dwóch liczb postaci $4k+3$ jest postaci $4k+1$, więc w rozkładzie na czynniki pierwsze liczby b występuje liczba pierwsza p postaci $4k + 3$ w nieparzystej potędze. Ta liczba pierwsza p nie może występować w rozkładzie na iloczyn liczb pierwszych liczby a, gdyż $\operatorname{nwd}(a, b) = 1$. W rozkładzie na iloczyn liczb pierwszych liczby ab występuje więc liczba pierwsza postaci $4k + 3$ w nieparzystej potędze. Teza wynika zatem z twierdzenia 3.1.3. ⊠

3.11.3. *Liczby 6 i 7, to kolejne liczby naturalne i żadna z nich nie jest sumą dwóch kwdratów liczb całkowitych. Liczby 42, 43, 44, to trzy kolejne liczby o tej własności. Liczby 21, 22, 23, 24, to cztery kolejne liczby o tej własności.*

3.11.4. *Tabelka przedstawia ciągi k kolejnych liczb naturalnych, z których każda nie jest sumą dwóch kwadratów liczb całkowitych. Podano długość ciągu, liczbę początkową i liczbę końcową. Występujące tu liczby są najmniejsze z możliwych.* (Maple).

$k = 5$	75	79
$k = 6$	91	96
$k = 7$	186	192
$k = 8$	378	385
$k = 9$	3051	3059
$k = 10$	987	996
$k = 11$	1670	1680
$k = 12$	4182	4193

$k = 13$	6531	6543
$k = 14$	1494	1507
$k = 15$	8435	8449
$k = 16$	9705	9720
$k = 17$	22161	22177
$k = 18$	5166	5183
$k = 19$	16110	16128
$k = 20$	16869	16888
$k = 21$	154709	154729

$k = 22$	57099	57120
$k = 23$	31658	31680
$k = 24$	52394	52417
$k = 26$	176811	176836
$k = 27$	101350	101376
$k = 28$	105573	105600
$k = 30$	241883	241912
$k = 33$	284003	284035

3.11.5. *Dla każdej liczby naturalnej n istnieje n kolejnych liczb naturalnych, z których każda nie jest sumą dwóch kwadratów liczb całkowitych.*
([Crux] 1984 s.19, [Cmj] 20(2)(1989) s.168 z.345, [Cmj] 29(5)(1998) s.438 z.614).

D. Spsób I ([Cmj] 29(5)(1998) s.438). Niech $s \geqslant 4n$ i niech $a = s! - n - 1$. Wtedy liczby $a+1, a+2, \dots, a+n$, czyli liczby

$$s! - n,\ s! - (n-1),\ \dots,\ s! - 2,\ s! - 1$$

spełniają żądaną właność. Niech bowiem $m \in \{1, \dots n\}$. Wtedy m^2 dzieli $s!$, liczba $s!/m - 1$ jest postaci $4k+3$ oraz $s! - m = m(s!/m - 1)$. Z faktu 3.11.2 wynika zatem, że $s! - m$ nie jest sumą dwóch kwadratów liczb całkowitych.

Sposób II ([Cmj] 20(2)(1989) s.168, [Cmj] 29(5)(1998) s.439). Niech $p_1, \dots, p_n$ będą parami różnymi liczbami pierwszymi postaci $4k+3$. Istnienie takich liczb pierwszych wynika z twierdzenia Dirichleta o liczbach pierwszych w postępie arytmetycznym. Na mocy twierdzenia chińskiego o resztach, istnieje liczba naturalna x taka, że

$$\begin{cases} x \equiv p_1 - 1 \pmod{p_1^2}, \\ x \equiv p_2 - 2 \pmod{p_2^2}, \\ x \equiv p_3 - 3 \pmod{p_3^2}, \\ \vdots \\ x \equiv p_n - n \pmod{p_n^2}. \end{cases}$$

Kolejne liczby naturalne $x+1, x+1, \dots, x+n$ posiadają omawianą własność. Niech bowiem $k \in \{0, 1, \dots, n\}$. Wtedy $x \equiv p_k - k \pmod{p_k^2}$, więc $x + k = p_k + a_k p_k^2 = p_k(1 + a_k p_k)$ (dla pewnego całkowitego a_k) i na mocy 3.11.2 liczba $x+k$ nie jest sumą kwadratów dwóch liczb całkowitych. ⊠

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

3.12 Liczby postaci $\mathbf{a^2 + 1}$

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

3.12.1.

(1) $(2n^2)^2 + 1^2 = (2n^2-1)^2 + (2n)^2$. ([Mat] 5/1949 47).

(2) $(5n+13)^2 + 1^2 = (3n+7)^2 + (4n+11)^2$. ([S64] s.59)

(3) $(n^2+n+1)^2 + 1^2 = (n^2-n-1)^2 + (2n+1)^2$. ([S56] 41).

(4) $(16n^3+2n)^2 + 1^2 = (2n(4n+1))^2 + (16n^2-1)^2$. ([S56] 41).

3.12.2. *Równanie $(x-1)^2 + (x+1)^2 = y^2 + 1$ ma nieskończenie wiele rozwiązań naturalnych. Para $(2,3)$ jest rozwiązaniem. Jeśli para (a,b) jest rozwiązaniem naturalnym, to para $(3a+2b, 4a+3b)$ również jest rozwiązaniem naturalnym.* ([S64] 123).

3.12.3. *Niech $m, n \in \mathbb{N}$. Jeżeli $2m = n^2 + 1$, to m jest sumą kwadratów dwóch liczb całkowitych.*

3.12.4. *Niech $x, y, z \in \mathbb{N}$. Jeśli $xy = z^2 + 1$, to istnieją liczby całkowite a, b, c, d takie, że $x = a^2 + b^2$, $y = x^2 + d^2$ oraz $z = ac + bd$.* ([OM] Iran 2000/2001).

3.12.5. *Nie ma takiego nieskończonego i rosnącego ciągu geometrycznego, którego każdy wyraz należy do zbioru $\{a^2 + 1;\ a \in \mathbb{Z}\}$.* ([OM] St Petersburg 1995).

3.12.6. $(a^2+1)\left((a+1)^2+1\right) = (a^2+a+1)^2+1, \ \ (a^2+1)((2a^2)^2+1) = (2a^3+a)^2+1.$ ([Mon] 68(9)(1961) 930-931).

3.12.7. *Równanie* $(x^2+1)(y^2+1) = (z^2+1)$ *ma nieskończenie wiele rozwiązań naturalnych.* ([OM] St Petersburg 1997, [Barb] s.19).

3.12.8. *Istnieją liczby naturalne* $x, y, z > 1997\,1997$ *takie, że* $(x^2+1)(y^2+1) = (z^2+1)$. ([OM] St Petersburg 1997).

3.12.9. *Istnieje nieskończenie wiele liczb naturalnych n takich, że liczba*

$$(0^2+1)(1^2+1)(2^2+1)\cdots((n-1)^2+1)$$

jest podzielna przez n^2+1. ([OM] Mongolia).

3.12.10. *Dla każdej liczby naturalnej m istnieje liczba naturalna n taka, że każdy dzielnik pierwszy liczby n^2+1 jest większy od m.* ([Mat] 4/1960 242).

3.12.11. *W ciągu (n^2+1) istnieją dowolnie długie ciągi kolejnych wyrazów, będących liczbami złożonymi.* ([Mat] 5/1976 316).

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

3.13 Trójki liczb kwadratowych postaci $a^2 + b^2$, $b^2 + c^2$, $c^2 + a^2$

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

3.13.1. *Niech (x, y, z) będzie trójką Pitagorasa i niech*

$$a = x(4y^2 - z^2), \quad b = y(4x^2 - z^2), \quad c = 4xyz.$$

Wtedy wszystkie trzy liczby a^2+b^2, b^2+c^2 oraz c^2+a^2 są kwadratowe. Dokładniej,

$$a^2+b^2 = (z^3)^2, \quad b^2+c^2 = \Big(y(4x^2+z^2)\Big)^2, \quad c^2+a^2 = \Big(x(4y^2+z^2)\Big)^2.$$

([S88] 60).

Startując od trójki Pitagorasa $(x, y, z) = (3, 4, 5)$ otrzymujemy: $a = 177$, $b = 44$, $c = 240$ i stąd mamy:

3.13.2. $44^2+117^2 = 125^2, \ 44^2+240^2 = 244^2, \ 117^2+240^2 = 267^2.$ (P. Halcke 1719, [Dic2] 497).

Istnieją tego typu przykłady, które nie powstają przy pomocy trójek Pitagorasa. Taką trójką jest $(a, b, c) = (252, 240, 275)$:

3.13.3. $252^2+240^2 = 348^2, \ 240^2+275^2 = 244^2, \ 275^2+252^2 = 373^2.$ ([S88] 60).

Następne przykłady:

3.13.4. $85^2+132^2 = 157^2, \ 85^2+720^2 = 725^2, \ 132^2+720^2 = 732^2.$

3.13.5. *Jeśli* (a, b, c) *jest jedną z trójek*

$$(44, 117, 240),\quad (240, 252, 275),\quad (85, 132, 720),\quad (160, 231, 729),$$
$$(140, 480, 693),\quad (195, 748, 6336),\quad (429, 880, 2340),$$

to liczby $a^2 + b^2$, $b^2 + c^2$, $c^2 + a^2$ *są kwadratowe.* ([S59] 81).

3.13.6. *Jeśli* (a, b, c) *jest trójką liczb naturalnych takich, że liczby* $a^2 + b^2$, $b^2 + c^2$, $c^2 + a^2$ *są kwadratowe, to trójka* (ab, bc, ca) *również ma tę własność.* ([S88] 61).

D. Niech $a^2+b^2 = x^2$, $b^2+c^2 = y^2$, $c^2+a^2 = z^2$. Wtedy $(ab)^2+(bc)^2 = (bz)^2$, $(bc)^2+(ca)^2 = (cx)^2$, $(ca)^2 + (ab)^2 = (ay)^2$. ⊠

3.13.7. *Jeśli liczby* $a^2 + b^2$, $b^2 + c^2$, $c^2 + a^2$, *gdzie* $a, b, c \in \mathbb{N}$ *są kwadratowe, to co najmniej jedna z liczb* a, b, c *jest podzielna przez* 11. ([Krai] 317, [S59] 80).

3.13.8. *Jeśli liczby* $a^2 + b^2$, $b^2 + c^2$, $c^2 + a^2$, *gdzie* $a, b, c \in \mathbb{N}$ *są kwadratowe, to co najmniej jedna z liczb* a, b, c *jest podzielna przez* 5. ([Kr47] 76, [S59] 81).

3.13.9. *Jeśli liczby* $a^2 + b^2$, $b^2 + c^2$, $c^2 + a^2$, *gdzie* $a, b, c \in \mathbb{N}$ *są kwadratowe, to liczby* a, b, c *nie są parami względnie pierwsze.* ([S59] 82).

3.13.10 (H. Olson 1918). *Jeśli* $a^2+b^2 = x^2$, $b^2+c^2 = y^2$, $c^2+a^2 = z^2$, *gdzie* $a, b, c, x, y, z \in \mathbb{N}$, *to liczba* $abcxyz$ *jest podzielna przez* $3^4 4^4 5^2$. ([Dic2] 501).

3.13.11. $(x^2 + y^2)(y^2 + z^2)(z^2 + x^2) = (x^2y + y^2z + z^2x - xyz)^2 + (x^2z + y^2x + z^2y - xyz)^2$.

3.13.12 (Otwarty problem). *Czy istnieją trzy liczby naturalne* a, b, c *takie, że wszystkie cztery liczby*

$$a^2 + b^2,\quad b^2 + c^2,\quad c^2 + a^2,\quad a^2 + b^2 + c^2$$

są kwadratowe ? ([Gy04] 275-283, [S88] 61).

U. W pierwszym wydaniu tej książki podałem informację, że takich liczb a, b, c nie ma i odesłałem do czasopisma [Mon] z 1917 roku (24(8)(1917) strona 393), do rowiązania zadania 254 podanego przez V. M. Spunar'a. Przedstawione tam krótkie rozwiązanie zawiera jednak błąd. Zwrócił mi na to uwagę Pan Piotr Kumor z Olsztyna; podając odpowiedni kontrprzykład wyjaśnił mi na czym ten błąd polega. Nie wiedziałem wcześniej, że to jest taki stary otwarty problem. Dziękuję Panu Piotrowi za te cenne uwagi. ⊠

3.13.13 (M. Skałba). *Następujące dwa zdania są równoważne.*

(1) *Istnieją liczby naturalne* a, b, c, d, e, f, g *takie, że*

$$a^2 + b^2 = e^2,\ b^2 + c^2 = f^2,\ c^2 + a^2 = h^2,\ a^2 + b^2 + c^2 = d^2.$$

(2) *Istnieją liczby wymierne* x, y, z *większe od* 1 *takie, że*

$$\left(\frac{x}{1+x^2}\right)^2 + \left(\frac{y}{1+y^2}\right)^2 = \left(\frac{z}{1+z^2}\right)^2.$$

([S88] 72-73).

★ L. E. Dickson, $x^2 + y^2, y^2 + z^2, z^2 + x^2$ *all squares*, [Dic2] 497-502.

R. K. Guy, *Is there a perfect cuboid? Four squares whose sums in pairs are squares. Four squares whose differences are squares*, [Gy04] 275-283.

W. Sierpiński, *On three squares for which the sum of any two are squares*, [S88] 60-62.

---

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

3.14 Sumy dwóch kwadratów liczb wymiernych

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

3.14.1. *Jeśli liczba naturalna nie jest sumą kwadratów dwóch liczb całkowitych, to nie jest sumą kwadratów dwóch liczb wymiernych.* ([S50] 82, [S59] 442).

3.14.2. *Liczba wymierna $\frac{a}{b}$, gdzie $(a,b)=1$, jest sumą kwadratów dwóch liczb wymiernych wtedy i tylko wtedy, gdy liczby a, b są sumami kwadratów dwóch liczb całkowitych.* ([S50] 83).

3.14.3. *Jeśli liczba naturalna jest sumą dwóch kwadratów liczb wymiernych dodatnich, to jest nią na nieskończenie wiele sposobów.* ([S59] 442).

D. Niech $n = a^2 + b^2$, gdzie $a, b \in \mathbb{Q}$, $a \geqslant b$. Wtedy dla $k \in \mathbb{N}$ mamy:

$$n = \left(\frac{(k^2-1)a - 2kb}{k^2+1}\right)^2 + \left(\frac{(k^2-1)b + 2ka}{k^2+1}\right)^2. \boxtimes$$

3.14.4. *Jeśli liczba naturalna jest sumą dwóch kwadratów dodatnich liczb wymiernych, to jest nią na nieskończenie wiele sposobów.* ([S59] 448).

3.14.5. *Nie ma dwóch niezerowych liczb wymiernych, których suma kwadratów i różnica kwadratów byłyby kwadratami liczb wymiernych.* ([S59] 60).

3.14.6. *Kwadrat dodatniej liczby wymiernej można na nieskończenie wiele sposobób przedstawić jako sumę kwadratów dwóch dodatnich liczb wymiernych.* ([S59] 64).

R. $w^2 = \left(w\frac{4n^2-1}{4n^2+1}\right)^2 + \left(w\frac{4n}{4n^2+1}\right)^2$. ⊠

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

3.15 Dodatkowe informacje o sumach dwóch kwadratów

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

3.15.1. *Jeśli ciąg (a_n), liczb naturalnych, spełnia równość $2a_n^2 = a_{n-1}^2 + a_{n+1}^2$, dla $n \in \mathbb{N}$, to jest ciągiem stałym.* ([OM] Austria 1985).

3.15.2. *Czy istnieje nieskończony ciąg liczb kwadratowych, w którym każdy wyraz, począwszy od trzeciego, jest sumą dwóch wyrazów poprzednich?* ([Kw] 5/1995 M1488a).

R. Nie istnieje. Przypuśćmy, że taki ciąg istnieje. Nie zmniejszając ogólności możemy założyć, że każde dwa sąsiednie wyrazy są względnie pierwsze. Jeśli $a^2 + b^2 = c^2$, gdzie a, b, c są względnie pierwszymi liczbami naturalnymi, to c jest liczbą nieparzystą i jedna z liczb a i b jest parzysta. Stąd wynika, że każdy wyraz, począwszy od trzeciego, powinien być liczbą nieparzystą, a z drugiej strony powinny występować liczby parzyste. ⊠

3.15.3. *Czy istnieje nieskończony ciąg rosnący liczb kwadratowych, w którym suma każdych dwóch sąsiednich wyrazów jest liczbą kwadratową?* ([Kw] 5/1995 M1488b).

R. Istnieje. Wystarczy znaleźć taką liczbę naturalną a, dla której istnieją liczby naturalne b, c, m, n spełniające następujące warunki:

(1) $a = mn = bc$,
(2) liczby m, n są różnej parzystości,
(3) liczby b, c są różnej parzystości,
(4) $0 < b^2 - c^2 < 2a < m^2 - n^2$,
(5) $m^2 - n^2 = k(b^2 - c^2)$, dla pewnego $k \in \mathbb{N}$.

Szukanym ciągiem jest wtedy ciąg otrzymany z kwadratów liczb:

$$x = b^2 - c^2,\ y = 2a,\ kx,\ ky,\ k^2x,\ k^2y,\ k^3x,\ k^3y,\ \ldots$$

Najmniejszą liczbą naturalną a, spełniającą powyższe warunki, jest $a = 6 = 3 \cdot 2 = 6 \cdot 1$. W tym przypadku $3^2 - 2^2 = 5 < 12 < 35 = 6^2 - 1^2$ oraz $k = 7$. Szukanym ciągiem jest więc na przykład ciąg:

$$5^2,\ 12^2,\ 7^2 5^2,\ 7^2 12^2,\ 7^4 5^2,\ 7^4 12^2,\ 7^6 5^2,\ 7^6 12^2, \ldots \quad \boxtimes$$

Literatura

[Barb] E. J. Barbeau, *Pell's Equation*, Problem Books in Mathematics, Springer, 2003.

[BoL] W. G. Bołtiański, W. G. Leman, *Zbiór Zadań Moskiewskich Olimpiad Matematycznych* (po rosyjsku), Moskwa, 1965.

[Br] K. Brown, *Algebra and number theory*, `http://mathpages.com/`, 2000.

[Cmj] The College Mathematics Journal, The Mathematical Association of America.

[Coh2] H. Cohen, *Number Theory. Volume II: Analytic and Modern Tools*, Graduate Texts in Mathematics 240, Springer, 2007.

[Crux] Crux Mathematicorum, Canadian Mathematical Society, popolarne matematyczne czasopismo kanadyjskie.

[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.

[FieK] R. M. Fedorov, A. J. Kanel-Belov, A. K. Kovaldzhi, I. W. Yashchenko, *Moskiewskie Olimpiady Matematyczne* 1993 – 2005 (po rosyjsku), MCNMO Moskwa, 2006.

[FQ] The Fibonacci Quarterly, czasopismo matematyczne.

[G-if] S. A. Genkin, I. W. Itenberg, D. V. Fomin, *Leningradzkie Kółka Matematyczne* (po rosyjsku), Kirow, ASA, 1994.

[Gio] A. A. Gioia, *The Theory of Numbers, an introduction*, Dover Publications, INC, 2001.

[Gy04] R. K. Guy, *Unsolved Problems in Number Theory*, Third edition, Springer-Verlag, New York, 2004.

[IMO] Międzynarodowa Olimpiada Matematyczna.

[Kr47] M. Kraitchik, *Théorie des Nombres III*, Paris, 1947.

[Krai] M. Kraitchik, Scripta Mathemathica, 11(1945).

[Kucz] M. Kuczma, *Olimpiady matematyczne*, tom 8, WSiP, 2000.

[Kw] Kwant, popularne czasopismo rosyjskie.

[Mat] Matematyka, polskie czasopismo dla nauczycieli.

[MG] The Mathematical Gazette, angielskie popularne czasopismo matematyczne.

[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.

[OM] Olimpiada Matematyczna.

[Pa97] H. Pawłowski, *Zadania z Olimpiad Matematycznych z Całego Świata*, Tutor, Toruń, 1997.

[Pras] V. V. Prasolov, *Essays on numbers and figures*, American Mathematical Society, 2000.

[Putn] Putnam (William Lowell) Mathematical Competition.

[S-kg] W. A. Sadowniczij, A. A. Grigorjan, S. W. Konjagin, *Zadania Studenckich Olimpiad Matematycznych* (po rosyjsku), Moskwa, 1987.

[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.

[S87] W. Sierpiński, *250 Zadań z Elementarnej Teorii Liczb*, (wydanie 2), Biblioteczka Matematyczna 17, PZWS, Warszawa, 1987.

[S88] W. Sierpiński, *Elementary Theory of Numbers*, Editor: A. Schinzel, North-Holland Mathematical Library, Vol. 31, 1988.

[San2] D. A. Santos, *Elementary Number Theory Notes*, Preprint, Internet 2002.

[Str67] S. Straszewicz, *Zadania z Olimpiad Matematycznych*, tom III, 11-15, 59/60 - 63/64, PZWS, Warszawa, 1967.

[Trost] E. Trost, *Primzahlen*, Verlag Birkhauser, Basel - Stuttgard. Tłumaczenie rosyjskie, Moskwa 1959.

[TT] Tournament of the Towns.

[Zw] Zwardoń, Obóz Naukowy Olimpiady Matematycznej.