Journal of Integer Sequences, Vol. 24 (2021),
Article 21.9.3

The Number $a^2 + b^2 - dc^2$ Revisited

Nguyen Viet Dung and Luu Ba Thang
Department of Mathematics and Informatics
Hanoi National University of Education
136 Xuan Thuy
Cau Giay, Hanoi
Vietnam
thanglb@hnue.edu.vn
vietdung10122000@gmail.com

Abstract

In 2015, Nowicki posed the following question: let $d = q$ or $d = 2q$, where q is a product of prime numbers of the form $4k + 1$. Is it true that d is a special number? We answer this open question.

1 Introduction

A positive integer d is called a *special* number if for every integer m there exist nonzero integers a, b, c such that $m = a^2 + b^2 - dc^2$. Nowicki [1] proved that there are infinitely many special numbers and every special number is of the form q or $2q$, where either $q = 1$ or q is a product of prime numbers of the form $4k + 1$. Then he posed the following open question: let $d = q$ or $d = 2q$, where q is a product of prime numbers of the form $4k + 1$. Is it true that d is a special number? In this article, we confirm that the answer is yes.

Theorem 1. *Let $d = q$ or $d = 2q$, where q is a product of prime numbers of the form $4k+1$. Then d is a special number.*

2 Proof of the main result

First, we recall some lemmas that we need to prove our results.

Lemma 2. *[3, p. 378] If an odd prime p divides the sum of the squares of two relatively prime positive integers, then it must be of the form $4k+1$.*

Lemma 3. *[3, p. 227] If p is a prime of the form $4k+1$ then for $s = 1, 2, \ldots$, the number p^s admits precisely one representation as the sum of the squares of two relatively prime natural numbers.*

Lemma 4. *[3, p. 228] If m, n are two odd numbers that are relatively prime, and such that each of them is representable as the sum of the squares of two relatively prime positive integers, then the product mn admits at least two representations as the sum of the squares of two relatively prime positive integers that differ not only in the order of the summand.*

Using the lemmas above, we can obtain the following theorem.

Theorem 5. *A positive integer $d > 2$ can be written in form of $a^2 + b^2$, where a, b are two relatively prime positive integers if and only if $d = q$ or $d = 2q$, where q is a product of prime numbers of the form $4k+1$.*

Proof. Assume that $d = a^2 + b^2$, where a, b are two relatively prime positive integers. Let p be an odd prime factor of d, we have $p|a^2 + b^2$. By Lemma 2, we see that p is a prime of the form $4k+1$.

If d is divisible by 4 then $4|a^2+b^2$. This only happens when both a and b are even, which contradicts the fact that a, b are relatively prime. Therefore, $4 \nmid d$. So $d = q$ or $d = 2q$, where q is a positive integer that all of whose prime factors are of the form $4k+1$.

If $d = q$ or $d = 2q$, where q is a product of prime numbers of the form $4k+1$. We have two cases:

(i) $d = q$: We write $d = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_t^{\alpha_t}$, where $q_1, q_2, \ldots, q_t$ are distinct primes of form $4k+1$ and α_j are positive integers for all $j = 1, 2, \ldots, t$. By Lemma 3, $q_j^{\alpha_j}$ can be written as the sum of the squares of two relatively prime positive integers for all $j = 1, 2, \ldots, t$. By Lemma 4 we have $d = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_t^{\alpha_t}$ can be written as the sum of the squares of two relatively prime positive integers for all $j = 1, 2, \ldots, t$.

(ii) $d = 2q$. By (i), we have $q = A^2 + B^2$, where A, B are positive integers and $\gcd(A, B) = 1$. So

$$d = 2q = 2(A^2 + B^2) = (A + B)^2 + (A - B)^2.$$

Since q is odd, we see that $A+B$ and $A-B$ are also odd. Combined with $\gcd(A, B) = 1$, we deduce that $\gcd(A + B, A - B) = 1$.

□

Now we answer the open question that we mentioned in introduction.

Proof of Theorem 1. We consider two cases:

(i) $d = q$, where q is a product of prime numbers of the form $4k + 1$.

By Theorem 5, we have $d = A^2 + B^2$, where A, B are positive integers and $\gcd(A, B) = 1$. Since d is odd, we deduce that $A + B$ is odd. Without loss of generality, we can consider that A is even and B is odd.

Because $\gcd(A, B) = 1$, there exist integers e, f such that $Ae + Bf = 1$. Then for all integers k we have

$$A(e + Bk) + B(f - Ak) = 1. \tag{1}$$

Now let n be an arbitrary integer. We consider two cases:

(a) n is even.

Because B is odd, we can choose $k_0 \in \mathbb{Z}$ such that $e + Bk_0$ is odd. Therefore $e + B(k_0 + 2t)$ is odd for all $t \in \mathbb{Z}$. Now we can easily see that

$$\lim_{t\to+\infty} \left|n - (e + B(k_0 + 2t))^2 - (f - A(k_0 + 2t))^2\right| = +\infty;$$

$$\lim_{t\to+\infty} \left|A \cdot \frac{n - (e + B(k_0 + 2t))^2 - (f - A(k_0 + 2t))^2}{2} + e + B(k_0 + 2t)\right| = +\infty;$$

$$\lim_{t\to+\infty} \left|B \cdot \frac{n - (e + B(k_0 + 2t))^2 - (f - A(k_0 + 2t))^2}{2} + f - A(k_0 + 2t)\right| = +\infty.$$

So we can choose a large enough positive integer t_0 such that

$$n - (e + B(k_0 + 2t_0))^2 - (f - A(k_0 + 2t_0))^2 \neq 0;$$

$$A \cdot \frac{n - (e + B(k_0 + 2t_0))^2 - (f - A(k_0 + 2t_0))^2}{2} + e + B(k_0 + 2t_0) \neq 0;$$

$$B \cdot \frac{n - (e + B(k_0 + 2t_0))^2 - (f - A(k_0 + 2t_0))^2}{2} + f - A(k_0 + 2t_0) \neq 0.$$

Set $e_1 = e + B(k_0 + 2t_0), f_1 = f - A(k_0 + 2t_0)$ and $l = \dfrac{n - e_1^2 - f_1^2}{2}$; then

$$l \neq 0, Al + e_1 \neq 0, Bl + f_1 \neq 0$$

and e_1 is odd. Combined with (1), we get $Ae_1 + Bf_1 = 1$. Because A is even, Ae_1 is even and so that, Bf_1 is odd. Hence, f_1 is odd. Since e_1 and f_1 are odd, it follows that $e_1^2 + f_1^2$ is even. This deduces that

$$l = \frac{n - e_1^2 - f_1^2}{2} \in \mathbb{Z}.$$

Set

$$a = Al + e_1, b = Bl + f_1, c = l;$$

then we have

$$\begin{aligned} a^2 + b^2 - dc^2 &= (Al + e_1)^2 + (Bl + f_1)^2 - dl^2 \\ &= 2(Ae_1 + Bf_1)l + e_1^2 + f_1^2 \\ &= 2l + e_1^2 + f_1^2 = n, \end{aligned}$$

where $a = Al + e_1 \neq 0, b = Bl + f_1 \neq 0, l \neq 0$.

(b) n is odd.

Because B is odd, we can choose $k_1 \in \mathbb{Z}$ such that $e + Bk_1$ is even. Then $e + B(k_1 + 2t)$ is even for all $t \in \mathbb{Z}$. Now we see that

$$\lim_{t \to +\infty} \left| n - (e + B(k_1 + 2t))^2 - (f - A(k_1 + 2t))^2 \right| = +\infty;$$

$$\lim_{t \to +\infty} \left| A \cdot \frac{n - (e + B(k_1 + 2t))^2 - (f - A(k_1 + 2t))^2}{2} + e + B(k_1 + 2t) \right| = +\infty;$$

$$\lim_{t \to +\infty} \left| B \cdot \frac{n - (e + B(k_1 + 2t))^2 - (f - A(k_1 + 2t))^2}{2} + f - A(k_1 + 2t) \right| = +\infty.$$

Therefore, we can choose a large enough positive integer t_1 such that

$$n - (e + B(k_1 + 2t_1))^2 - (f - A(k_1 + 2t_1))^2 \neq 0;$$

$$A \cdot \frac{n - (e + B(k_1 + 2t_1))^2 - (f - A(k_1 + 2t_1))^2}{2} + e + B(k_1 + 2t_1) \neq 0;$$

$$B. \frac{n - (e + B(k_1 + 2t_1))^2 - (f - A(k_1 + 2t_1))^2}{2} + f - A(k_1 + 2t_1) \neq 0.$$

Set

$$e_2 = e + B(k_1 + 2t_1), f_2 = f - A(k_1 + 2t_1) \text{ and } l_1 = \frac{n - e_2^2 - f_2^2}{2};$$

then

$$l_1 \neq 0, Al_1 + e_2 \neq 0, Bl_1 + f_2 \neq 0$$

and e_2 is even. Combined with (1), we obtain $Ae_2 + Bf_2 = 1$. Because A is even, Ae_2 is even and Bf_2 is odd. Therefore, f_2 is odd. This implies that $e_2^2 + f_2^2$ is odd. So

$$l_1 = \frac{n - e_2^2 - f_2^2}{2} \in \mathbb{Z}.$$

Set

$$a = Al_1 + e_2, b = Bl_1 + f_2, c = l_1;$$

then we obtain

$$\begin{aligned} a^2+b^2-dc^2 &= (Al_1+e_2)^2+(Bl_1+f_2)^2-dl_1^2 \\ &= 2(Ae_2+Bf_2)l_1+e_2^2+f_2^2 \\ &= 2l_1+e_2^2+f_2^2 = n, \end{aligned}$$

where $a = Al_1+e_2 \neq 0, b = Bl_1+f_2 \neq 0, l_1 \neq 0$.

(ii) $d = 2q$, where q a product of prime numbers of the form $4k+1$.

By Theorem 5 we have $d = C^2+D^2$, where C, D are odd and relatively prime. Now let n be an arbitrary integer. Then we consider two cases:

(c) n is odd.

Because $\gcd(C, D) = 1$, there exist integers g, h such that

$$Cg+Dh = 1.$$

Then for every integer k we have

$$C(g+Dk)+D(h-Ck) = 1 \tag{2}$$

Because both C, D are odd, we have $(g+Dk)+(h-Ck)$ is odd.
Hence, $(g+Dk)^2+(h-Ck)^2$ is odd. We see that

$$\lim_{k\to+\infty} \left|n-(g+Dk)^2-(h-Ck)^2\right| = +\infty;$$

$$\lim_{k\to+\infty} \left|C\cdot\frac{n-(g+Dk)^2-(h-Ck)^2}{2}+(g+Dk)\right| = +\infty;$$

$$\lim_{k\to+\infty} \left|D\cdot\frac{n-(g+Dk)^2-(h-Ck)^2}{2}+(h-Ck)\right| = +\infty.$$

Therefore, we can choose a large enough positive integer k_2 such that

$$n-(g+Dk_2)^2-(h-Ck_2)^2 \neq 0;$$

$$C\cdot\frac{n-(g+Dk_2)^2-(h-Ck_2)^2}{2}+(g+Dk_2) \neq 0;$$

$$D\cdot\frac{n-(g+Dk_2)^2-(h-Ck_2)^2}{2}+(h-Ck_2) \neq 0.$$

Set

$$g_1 = g+Dk_2, h_1 = h-Ck_2 \text{ and } j = \frac{n-g_1^2-h_1^2}{2};$$

then $j \neq 0, Cj + g_1 \neq 0, Dj + h_1 \neq 0$ and $g_1^2 + h_1^2$ is odd. Because n and $g_1^2 + h_1^2$ are odd, it follows that $j = \dfrac{n - g_1^2 - h_1^2}{2}$ is an integer. Set $c = j, a = Cj + g_1, b = Dj + h_1$; then

$$\begin{aligned} a^2 + b^2 - dc^2 &= (Cj + g_1)^2 + (Dj + h_1)^2 - dj^2 \\ &= 2(Cg_1 + Dh_1)j + g_1^2 + h_1^2 = n. \end{aligned}$$

Notice that $a = Cj + g_1 \neq 0, b = Dj + h_1 \neq 0, c = j \neq 0$.

(d) n is even.

Because $\gcd(C, D) = 1$, there exist integers g', h' such that

$$Cg' + Dh' = 2.$$

Then for every integer k we have

$$C(g' + Dk) + D(h' - Ck) = 2 \tag{3}$$

Now we consider two small cases of n:

First case: $n \equiv 2 \pmod 4$.

Because C, D are odd, we can choose $k_4 \in \mathbb{Z}$ such that $g' + Dk_4$ is odd. From (3), we have

$$C(g' + Dk_4) + D(h' - Ck_4) = 2.$$

Therefore, $h' - Ck_4$ is also odd. Now we see that

$$\lim_{t \to +\infty} \left| n - (g' + D(k_4 + 2t))^2 - (h' - C(k_4 + 2t))^2 \right| = +\infty;$$

$$\lim_{t \to +\infty} \left| C \cdot \frac{n - (g' + D(k_4 + 2t))^2 - (h' - C(k_4 + 2t))^2}{2} + (g' + D(k_4 + 2t)) \right| = +\infty;$$

$$\lim_{t \to +\infty} \left| D \cdot \frac{n - (g' + D(k_4 + 2t))^2 - (h' - C(k_4 + 2t))^2}{2} + (h' - C(k_4 + 2t)) \right| = +\infty.$$

Therefore, we can choose a large enough positive integer t_4 such that

$$n - (g' + D(k_4 + 2t_4))^2 - (h' - C(k_4 + 2t_4))^2 \neq 0;$$

$$C \cdot \frac{n - (g' + D(k_4 + 2t_4))^2 - (h' - C(k_4 + 2t_4))^2}{2} + (g' + D(k_4 + 2t_4)) \neq 0;$$

$$D \cdot \frac{n - (g' + D(k_4 + 2t_4))^2 - (h' - C(k_4 + 2t_4))^2}{2} + (h' - C(k_4 + 2t_4)) \neq 0.$$

Set $g_2 = g' + D(k_4 + 2t_4), h_2 = h' - C(k_4 + 2t_4), y = \dfrac{n - g_2^2 - h_2^2}{4}$; then

$$y \neq 0, Cy + g_2 \neq 0, Dy + h_2 \neq 0$$

and g_2, h_2 are odd. Because g_2, h_2 are odd, we have $g_2^2 + h_2^2 \equiv n \pmod 4$ and so that $y = \dfrac{n - g_2^2 - h_2^2}{4}$ is an integer.
From (3), we have $Cg_2 + Dh_2 = 2$. Set $a = Cy + g_2, b = Dy + h_2, c = y$; then we have

$$\begin{aligned} a^2 + b^2 - dc^2 &= (Cy + g_2)^2 + (Dy + h_2)^2 - dy^2 \\ &= 2(Cg_2 + Dh_2)y + g_2^2 + h_2^2 = n, \end{aligned}$$

where $a = Cy + g_2 \neq 0, b = Dy + h_2 \neq 0, c = y \neq 0$.

Second case: $n \equiv 0 \pmod 4$.
Since D, C are odd, we can choose $k' \in \mathbb{Z}$ such that $g' + Dk'$ is even.
From (3), we have

$$C(g' + Dk') + D(h' - Ck') = 2.$$

Because $g' + Dk'$ is even, $h' - Ck'$ is even.
We see that

$$\lim_{t \to +\infty} \left| n - (g' + D(k' + 2t))^2 - (h' - C(k' + 2t))^2 \right| = +\infty;$$

$$\lim_{t \to +\infty} \left| C \cdot \frac{n - (g' + D(k' + 2t))^2 - (h' - C(k' + 2t))^2}{2} + (g' + D(k' + 2t)) \right| = +\infty;$$

$$\lim_{t \to +\infty} \left| D \cdot \frac{n - (g' + D(k' + 2t))^2 - (h' - C(k' + 2t))^2}{2} + (h' - C(k' + 2t)) \right| = +\infty.$$

So we can choose a large enough positive integer t' such that

$$n - (g' + D(k' + 2t'))^2 - (h' - C(k' + 2t'))^2 \neq 0;$$

$$C \cdot \frac{n - (g' + D(k' + 2t'))^2 - (h' - C(k' + 2t'))^2}{2} + (g' + D(k' + 2t')) \neq 0;$$

$$D \cdot \frac{n - (g' + D(k' + 2t'))^2 - (h' - C(k' + 2t'))^2}{2} + (h' - C(k' + 2t')) \neq 0.$$

Set $g_3 = g' + D(k' + 2t'), h_3 = h' - C(k' + 2t'), y_1 = \dfrac{n - g_3^2 - h_3^2}{4}$. Then $y_1 \neq 0, Cy_1 + g_3 \neq 0, Dy_1 + h_3 \neq 0$ and both g_3, h_3 are even. Because g_3, h_3 are even, we have $g_3^2 + h_3^2 \equiv n \pmod 4$ and so that $y_1 = \dfrac{n - g_3^2 - h_3^2}{4}$ is an integer.

From (3) we have $Cg_3 + Dh_3 = 2$. Set

$$a = Cy_1 + g_3, b = Dy_1 + h_3, c = y_1;$$

then we have

$$\begin{aligned} a^2 + b^2 - dc^2 &= (Cy_1 + g_3)^2 + (Dy_1 + h_3)^2 - dy_1^2 \\ &= 2(Cg_3 + Dh_3)y_1 + g_3^2 + h_3^2 = n, \end{aligned}$$

where $a = Cy_1 + g_3 \neq 0, b = Dy_1 + h_3 \neq 0, c = y_1 \neq 0$.

Combining (i) and (ii), we have the desired proof. □

3 Acknowledgments

The authors would like to thank the referee and the editor-in-chief for useful comments and suggestions. The second author thanks Hanoi National University of Education for the support during his work on this paper.

References

[1] A. Nowicki, The number $a^2 + b^2 - dc^2$, *J. Integer Sequences* **18** (2015), Article 15.2.3.

[2] S. Prugsapitak and N. Thongngam, Representation of integers of the form $x^2 + my^2 - z^2$, *J. Integer Sequences* **24** (2021), Article 24.7.7.

[3] W. Sierpiński, *Elementary Theory of Numbers*, North-Holland, 1988.

2010 *Mathematics Subject Classification*: Primary 11E25.
Keywords: sum of squares.

Received April 27 2021; revised version received September 27 2021. Published in *Journal of Integer Sequences*, October 1 2021.

Return to Journal of Integer Sequences home page.