Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
2023, Volume 29, Number 1, 24–29
DOI: 10.7546/nntdm.2023.29.1.24-29

A note on the number $a^n + b^n - dc^n$

Nguyen Viet Dung[1] **and Luu Ba Thang**[2]

[1] Department of Mathematics and Informatics, Hanoi National University of Education
36 Xuan Thuy, Cau Giay, Hanoi, Vietnam
e-mail: vietdung10122000@gmail.com

[2] Department of Mathematics and Informatics, Hanoi National University of Education
36 Xuan Thuy, Cau Giay, Hanoi, Vietnam
e-mail: thanglb@hnue.edu.vn

Received: 24 May 2022 **Revised:** 28 January 2023
Accepted: 6 February 2023 **Online First:** 8 February 2023

Abstract: We say that a positive integer d is special number of degree n if for every integer m, there exist nonzero integers a, b, c such that $m = a^n + b^n - dc^n$. In this paper, we investigate some necessary conditions on n for existing a special number of degree n.
Keywords: Representation of integers.
2020 Mathematics Subject Classification: 11E25.

1 Introduction

A positive integer d is called a *special number of degree* n if for every integer m there exist nonzero integers a, b, c such that $m = a^n + b^n - dc^n$. Specially, every special number of degree 2 will be called *special number* for short.

In 2015, Nowicki [3] 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 $4k + 1$. In 2021, Dung and Thang [1] proved that every positive integers that is the form q or $2q$, where either $q = 1$ or q is a product of prime numbers of the form $4k + 1$ is a special number.

In this article, when $n > 2$, we present some necessary conditions of n if there exists a special number of degree n and an approach to check the existence of special number of degree n.

2 The existence of the special number of degree n

First, we recall the definition of a special number of degree n.

Definition 2.1. Let $n \geq 2$ be a positive integer. A positive integer d is called a *special number of degree* n if for every integer m, there exist nonzero integers a, b, c such that $m = a^n + b^n - dc^n$.

Let n, m be two positive integers such that $m|n$. Since $a^n = \left(a^{\frac{n}{m}}\right)^m$ for all integers a, we have:

Lemma 2.1. *If there exists a special numbers of degree n and $m|n$, then there exists a special number of degree m.*

By this lemma, if we have proved that there does not exist a special number of degree n, then we also have the non-existence of the special number of degree nk, for all positive integer k. In the case $n = 4$, we have the following result:

Theorem 2.1. *There does not exist any special number of degree* 4.

Proof. Suppose that there exists a special number d of degree 4. For each $x \in \mathbb{Z}$, then

$$x^4 \equiv 0 \text{ or } 1 \pmod{16}.$$

Hence,

$$a^4 + b^4 - dc^4 \equiv \{0, 1, 2, -d, 1-d, 2-d\} \pmod{16} \tag{1}$$

for all $a, b, c \in \mathbb{Z}$.

Let $m_0 \in \mathbb{Z}$ such that m_0 is not congruent to $0, 1, 2, -d, 1-d, 2-d$ modulo 16. Then by (1), the equation $a^4 + b^4 - dc^4 = m_0$ does not have any integer solutions. This obviously contradicts to the supposition. Therefore, there does not exist any special number of degree 4. □

Definition 2.2. Let $n > 1$ be a positive integer, p be a prime divisor of n, and let $v_p(n)$ denote the largest positive integer k such that $p^k \mid n$. If p is not a divisor of n, then we set $v_p(n) := 0$.

Clearly, if n has a prime factorization

$$n = \prod_{j=1}^{k} p_j^{a_j},$$

then $v_{p_j}(n) = a_j$, for $j = 1, 2, \ldots, k$.

Now, we recall an important lemma which relates directly to the function v_p, namely the Lifting The Exponent (LTE).

Lemma 2.2. [2, p. 392] *Let p be an odd prime and a, b be two integers such that* $\gcd(a,p) = \gcd(b,p) = 1$. *If p is a divisor of $a - b$, then we have*

$$v_p(a^n - b^n) = v_p(a-b) + v_p(n), \text{ for all } n \in \mathbb{N}.$$

Using this Lemma, we obtain the following two results.

Lemma 2.3. *Let p be an odd prime. Then for every $x \in \mathbb{Z}$, there exists $r \in \{0, 1, 2, \ldots, p-1\}$ such that $x^{p^2} \equiv r^{p^2} \pmod{p^3}$.*

Proof. Let r be the remainder when we divide x by p. Then $r \in \{0, 1, 2, \ldots, p-1\}$ and $p \mid x - r$.

If $p \mid x$, then $p^3 \mid x^{p^2} - r^{p^2}$. If $\gcd(p, x) = 1$, then by Lemma 2.2, we have

$$v_p(x^{p^2} - r^{p^2}) = v_p(x - r) + v_p(p^2) \geq 3.$$

This implies $x^{p^2} \equiv r^{p^2} \pmod{p^3}$. □

Lemma 2.4. *Let $S \subset \mathbb{R}$ be a finite set and set $S + S := \{a + b \mid a, b \in S\}$. Then we have*

$$|S + S| \leq |S| + \binom{|S|}{2}.$$

Proof. Set $A := \{(a, b) \mid a \geq b \text{ and } a, b \in S\}$. Then $|A| = |S| + \binom{|S|}{2}$.

Consider the function

$$\begin{aligned} f : A &\to S + S \\ (a, b) &\mapsto a + b. \end{aligned}$$

Then f is a surjection, and hence $|S + S| \leq |A| = |S| + \binom{|S|}{2}$. □

Theorem 2.2. *Let p be an odd prime. Then there does not exist any special number of degree p^2.*

Proof. Suppose that there exists a special number d of degree p^2. Then for every integer m, there exist nonzero integers a, b, c such that

$$m = a^{p^2} + b^{p^2} - dc^{p^2}.$$

For a positive integer $n > 1$, we let $\mathbb{Z}_n$ denote the ring of residue classes modulo n. We have

$$\mathbb{Z}_{p^3} = \{a^{p^2} + b^{p^2} - dc^{p^2} \mid a, b, c \in \mathbb{Z}_{p^3}\}.$$

Hence,

$$p^3 = |\mathbb{Z}_{p^3}| = \left|\{a^{p^2} + b^{p^2} - dc^{p^2} \mid a, b, c \in \mathbb{Z}_{p^3}\}\right|. \tag{2}$$

We see that

$$\left|\{a^{p^2} + b^{p^2} - dc^{p^2} \mid a, b, c \in \mathbb{Z}_{p^3}\}\right| \leq \left|\{a^{p^2} + b^{p^2} \mid a, b \in \mathbb{Z}_{p^3}\}\right| \cdot \left|\{-dc^{p^2} \mid c \in \mathbb{Z}_{p^3}\}\right|. \tag{3}$$

By Lemma 2.3, we have $|\{-dc^{p^2} \mid c \in \mathbb{Z}_{p^3}\}| \leq p$.

Also, using Lemma 2.3 and Lemma 2.4, we have

$$\begin{aligned} \left|\{a^{p^2} + b^{p^2} \mid a, b \in \mathbb{Z}_{p^3}\}\right| &= \left|\{a^{p^2} + b^{p^2} \mid a, b \in \{[0], [1], \ldots, [p-1]\} \subset \mathbb{Z}_{p^3}\}\right| \\ &\leq \left|\{a^{p^2} + b^{p^2} \mid a, b \in \{0, 1, \ldots, p-1\}\}\right| \\ &\leq p + \binom{p}{2}, \end{aligned}$$

where we call $[m]$ the residue class of m modulo p^3. Combining with (3), we have the following inequality

$$\left|\{a^{p^2}+b^{p^2}-dc^{p^2}\mid a,b,c\in\mathbb{Z}_{p^3}\}\right|\le p\Big(p+\binom{p}{2}\Big)=\frac{p^2(p+1)}{2}.$$

Combine with (2), we have

$$p^3\le\frac{p^2(p+1)}{2}.$$

Deduce that $p\le 1$, this is impossible. Therefore, there does not exist any special number of degree p^2. □

From Theorem 2.2, we obtain immediately the following result:

Theorem 2.3. *If there exists a special number of degree n, then n must be a square-free number.*

We now give an criterion for n to check the non-existence of the special of degree n.

Lemma 2.5. [6, p. 273] *Let p be a prime and $k\mid p-1$. Then*

(i) *The equation $x^{\frac{p-1}{k}}\equiv a\pmod p$ has a solution if and only if $a^k\equiv 1\pmod p$ or $p\mid a$.*

(ii) *The equation $x^k\equiv 1\pmod p$ has k distinct solutions modulo p.*

Theorem 2.4. *Let p be a prime number and k be a positive number such that $k\mid p-1$. Assume that there exists a special number of the degree $\frac{p-1}{k}$. Then we have*

$$p\le\frac{(k+1)^2(k+2)}{2}.$$

Moreover, if k is even, then we have a better bound

$$p\le\frac{(k+1)(k^2+2k+2)}{2}.$$

Proof. Let p be a prime such that $k\mid p-1$ and there exists a special number d of degree $\frac{p-1}{k}$. Then we have

$$\mathbb{Z}_p=\{a^{\frac{p-1}{k}}+b^{\frac{p-1}{k}}-dc^{\frac{p-1}{k}}|a,b,c\in\mathbb{Z}_p\}.\tag{4}$$

Let $[x_1],[x_2],\ldots,[x_k]$ be k distinct solutions of the polynomial x^k-1 in the field $\mathbb{Z}_p$. Then

$$\{a^{\frac{p-1}{k}}|a\in\mathbb{Z}_p\}=\{[0],[x_1],[x_2],\ldots,[x_k]\}.\tag{5}$$

We have

$$\left|\{a^{\frac{p-1}{k}}+b^{\frac{p-1}{k}}-dc^{\frac{p-1}{k}}\mid a,b,c\in\mathbb{Z}_p\}\right|\le\left|\{a^{\frac{p-1}{k}}+b^{\frac{p-1}{k}}\mid a,b\in\mathbb{Z}_p\}\right|.\left|\{dc^{\frac{p-1}{k}}\mid c\in\mathbb{Z}_p\}\right|.\tag{6}$$

By (5), we have

$$\left|\{dc^{\frac{p-1}{k}}|c\in\mathbb{Z}_p\}\right|\le k+1.$$

Using Lemma 2.4 and (5), we have

$$\begin{aligned}\left|\{a^{\frac{p-1}{k}}+b^{\frac{p-1}{k}}\mid a,b\in\mathbb{Z}_p\}\right|&=|\{x+y\mid x,y\in\{[0],[x_1],[x_2],\ldots,[x_k]\}|\\&\le|\{x+y\mid x,y\in\{0,x_1,x_2,\ldots,x_k\}\}|\\&\le\frac{(k+1)(k+2)}{2}.\end{aligned}$$

Combine with (6) we have

$$\left|\{a^{\frac{p-1}{k}} + b^{\frac{p-1}{k}} - dc^{\frac{p-1}{k}} | a, b, c \in \mathbb{Z}_p\}\right| \leq \frac{(k+1)^2(k+2)}{2}.$$

Combine with (4), we have

$$p \leq \frac{(k+1)^2(k+2)}{2}.$$

If k is even, $[-x_j]$ is also a solution of the polynomial $x^k - 1$ in $\mathbb{Z}_p$, for every $j = 1, 2, \ldots, k$. Therefore, for each $j \in \{1, 2, \ldots, k\}$, it has the unique index $h(j) \neq j, h(j) \in \{1, 2, \ldots, k\}$ such that $[x_{h(j)}] + [x_j] = [0]$.

Set $A := \{x+y \mid x+y \neq [0], x, y \in \{[x_1], [x_2], \ldots, [x_k]\}$, and $B := \{(l, j) \mid l \geq j, l \neq h(j)\}$. Then

$$|B| = k + \binom{k}{2} - \frac{k}{2} = \frac{k^2}{2}.$$

Consider the function

$$f : B \to A$$
$$(l, j) \mapsto [x_j] + [x_l].$$

Then f is a surjection and hence $|A| \leq |B| = \frac{k^2}{2}$. From this, we deduce that

$$\begin{aligned} |\{x + y | x, y \in \{[0], [x_1], \ldots, [x_k]\}\}| &\leq |\{[0]\}| + |A| + |\{[x_1], [x_2], \ldots, [x_k]\}| \\ &\leq 1 + \frac{k^2}{2} + k = \frac{k^2 + 2k + 2}{2}. \end{aligned}$$

Moreover,

$$\left|\{a^{\frac{p-1}{k}} + b^{\frac{p-1}{k}} | a, b \in \mathbb{Z}_p\}\right| = |\{x + y | x, y \in \{[0], [x_1], \ldots, [x_k]\}\}|.$$

So, we obtain

$$\left|\{a^{\frac{p-1}{k}} + b^{\frac{p-1}{k}} | a, b \in \mathbb{Z}_p\}\right| \leq \frac{k^2 + 2k + 2}{2}.$$

□

From Theorem 2.4, we have the following corollary:

Corollary 2.1. (i) *There does not exist any special number of degree $p - 1$ with $p \geq 5$.*

(ii) *Let k be a given positive integer. Then there are only finitely many primes p such that $k \mid p - 1$ and there exists a special number of degree $\frac{p-1}{k}$.*

Let x be a positive real number and a, b be positive integers such that $\gcd(a, b) = 1$. We let $\pi(x, a, b)$ denote the number of primes p such that $p \leq x$ and $p \equiv a \pmod{b}$. Then we have the following corollary.

Corollary 2.2. *Let t be a positive integer such that $\pi(t(\sqrt{2t-1} - 3) + 1, 1, t) > 0$. Then there does not exist any special numbers of degree t.*

Proof. Suppose that there exists a special number d of degree t.

Since $\pi(t(\sqrt{2t-1}-3)+1,1,t)>0$, there exists a prime $p\equiv 1 \pmod t$ such that $p\le t(\sqrt{2t-1}-3)+1$. We write $p=kt+1, k\in\mathbb{N}$, then $t=\frac{p-1}{k}$ and because $p\le t(\sqrt{2t-1}-3)+1$, we have

$$k\le\sqrt{2k-1}-3. \tag{7}$$

By Theorem 2.4, we deduce that

$$p\le\frac{(k+1)^2(k+2)}{2}.$$

This implies $t\le\frac{k^2+4k+5}{2}$ and therefore, $k\ge\sqrt{2t-1}-2$. This contradicts to (7). Thus, there does not exist any special number of degree t. $\square$

From Corollary 2.1, Corollary 2.2 and Theorem 2.3, we see that for each positive integer n, to check the existence of the special number of degree n, we need to determine if n is a square-free satisfies that $\pi(n(\sqrt{2n-1}-3)+1,1,n)$ vanishes and $n+1$ is not a prime. By computer, we have proved that if $n\le 10000$ and

$$n\notin\{1,2,3,5,7,11,13,17,19,31,59,85,159,197,227,317,415,457,521\},$$

then there does not exist any special number of degree n.

3 Conclusion

In this article, we prove that if there exists a special number of degree n, then n must be a square-free number and present many square-free numbers n such that there does not exist any special number of degree n. In the future, we will consider the special number of degree 3.

References

[1] Dung, N. V., & Thang, L. B. (2021). The number $a^2+b^2-dc^2$ revisited. *Journal of Integer Sequences*, 24, Article 21.9.3.

[2] Nathason, M. B. (2021). *Combinatorial and Additive Number Theory IV:CANT*. Springer, New York, USA.

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

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

[5] Prugsapitak S., & Thongngam, N. (2022). Representation of integers of the form $x^2+ky^2-lz^2$. *Journal of Integer Sequences*, 25, Article 22.8.5.

[6] Sierpiński, W. (1988). *Elementary Theory of Numbers*. North-Holland.