A Theorem on the Representability of Chernick-Type Carmichael Numbers as Norms of Gaussian Integers

[İsmail Kara][1]

[1] *[Körfez Atatürk Anadolu Lisesi] — [ismailkarailetisim@gmail.com]*

ORCID: [0009-0009-5651-0193]

Abstract

Known in number theory as "absolute pseudoprimes," Carmichael numbers are special composite numbers that deceive Fermat's Little Theorem despite not being prime. In hypercomplex algebra, the two-square identity gives a geometric foundation to the representability of integers as norms in complex space (the Gaussian integers). This study examines the projection of Carmichael numbers of the form $C(m) = (6m + 1)(12m + 1)(18m + 1)$, defined by Chernick (1939), onto the space of the Brahmagupta–Fibonacci (two-square) identity. For the first time in the literature, it is algebraically proven that a Chernick–Carmichael number can be written as the sum of two integer squares ($X^2 + Y^2$) if and only if the parameter m is even, and this result is numerically verified with the examples $m = 1$ (1729) and $m = 6$ (294409).

Keywords

Carmichael Numbers; Chernick's Theorem; Two-Square Identity; Gaussian Integers; Quadratic Residues.

Öz

Sayılar teorisinde "mutlak sahte asallar" olarak bilinen Carmichael sayıları, asal olmadıkları hâlde Fermat'ın Küçük Teoremini yanıltan özel bileşik sayılardır. Bu çalışmada, Chernick (1939) tarafından tanımlanan $C(m) = (6m + 1)(12m + 1)(18m + 1)$ formundaki Carmichael sayılarının, iki-tamkare özdeşliği uzayına izdüşümü incelenmiş; bir Chernick–Carmichael sayısının iki tam sayının karesinin toplamı olarak yazılabilir olmasının yalnızca ve yalnızca m katsayısının çift olma durumuna bağlı olduğu cebirsel olarak ispatlanmıştır.

Anahtar Kelimeler

Carmichael Sayıları; Chernick Teoremi; İki Tamkare Özdeşliği; Gauss Tamsayıları; Karesel Kalanlar.

1. Introduction and Mathematical Background

Carmichael numbers, examined by Büyükaşık (2001) in the December 2001 issue of Matematik Dünyası, are special integers that contain no square of any prime factor in their factorization (square-free). Despite not being prime, these numbers satisfy the Fermat congruence $a^n \equiv a \pmod{n}$ for every integer a, and are therefore referred to as "absolute pseudoprimes" in

primality testing (Carmichael, 1910). J. Chernick (1939) proved that, with $m \in \mathbf{Z}^+$, whenever the numbers $p_1 = 6m + 1$, $p_2 = 12m + 1$, and $p_3 = 18m + 1$ are all prime, the number $C(m) = p_1 \cdot p_2 \cdot p_3$ is a Carmichael number.

On the other hand, Pashaev and Erman (2001), in a study published in the same journal, examined Diophantine equations and hypercomplex numbers, emphasizing the significance of the two-square identity (the Brahmagupta–Fibonacci identity) in modular arithmetic. The fact that an integer can be written as the sum of two squares means that this number can serve as the norm ($|z|^2 = x^2 + y^2$) of a Gaussian integer ($\mathbf{Z}[i]$); this establishes a direct bridge between number theory and the geometry of the complex plane (Cox, 1989).

Although the literature contains an extensive body of work examining Carmichael numbers from the perspective of primality testing and cryptographic security (Carmichael, 1910; Büyükaşık, 2001), the relationship of these numbers to classical number-theoretic problems such as the two-square-sum representation has not been directly investigated. The purpose of this study is to establish a universal rule determining which Chernick–Carmichael numbers can also serve as the norm of a Gaussian integer (a sum of two squares), thereby filling this gap.

The remainder of the paper is organized as follows. Section 2 recalls Fermat's Two-Square Theorem and the condition for a composite number to be a sum of two squares. Section 3 proves the main theorem (the Chernick–Carmichael Parity Theorem). Section 4 verifies the results with numerical examples and discusses the study's limitations and directions for future research.

2. Preliminary Theorems (Lemmas)

Proposition 2.1 (Fermat's Two-Square Theorem). An odd prime p can be written as the sum of two integer squares ($p = x^2 + y^2$) if and only if $p \equiv 1 \pmod 4$. If $p \equiv 3 \pmod 4$, then p cannot be written in this form.

Proposition 2.2 (Condition for Composite Numbers to be a Sum of Two Squares). A positive integer N can be written as the sum of two squares ($N = x^2 + y^2$) if and only if, in its prime factorization, every prime factor of the form $q \equiv 3 \pmod 4$ occurs to an even power (e.g., q^2, q^4) (Niven et al., 1991; Cox, 1989).

Remark 2.1. Since Carmichael numbers are square-free by definition, none of their prime factors can occur to an even power; their exponents are always 1. This makes the application of Proposition 2.2 to Carmichael numbers particularly sharp: when N is square-free, the question of whether N is a sum of two squares reduces directly to whether N contains a prime factor congruent to 3 modulo 4 — the presence of even a single such factor renders the representation entirely impossible.

3. Main Theorem and Proof

Theorem 3.1 (The Chernick–Carmichael Parity Theorem). With $p_1 = 6m + 1$, $p_2 = 12m + 1$, $p_3 = 18m + 1$ prime, let $C(m) = p_1 \cdot p_2 \cdot p_3$ be Chernick's Carmichael number. A necessary and sufficient condition for $C(m)$ to be expressible as the sum of two integer squares ($C(m) = X^2 + Y^2$) is that the parameter m be even.

Proof. We give the proof in two directions (Sufficiency and Necessity).

Step 1: Sufficiency ($\Leftarrow$) — If *m* is even. Suppose m is an even integer; let $m = 2k$ ($k \in \mathbf{Z}^+$). Let us examine the prime factors modulo 4:

$$p_1 = 6(2k) + 1 = 12k + 1 \Longrightarrow p_1 \equiv 1 \pmod 4$$
$$p_2 = 12(2k) + 1 = 24k + 1 \Longrightarrow p_2 \equiv 1 \pmod 4$$
$$p_3 = 18(2k) + 1 = 36k + 1 \Longrightarrow p_3 \equiv 1 \pmod 4$$

By Proposition 2.1, since all three primes are congruent to 1 modulo 4, each is individually a sum of two squares: $p_1 = a^2 + b^2$, $p_2 = c^2 + d^2$, $p_3 = e^2 + f^2$. By the two-square (complex norm) identity given by Pashaev and Erman (2001), the product of numbers that are each sums of two squares is always itself a sum of two squares (a direct consequence of the multiplicativity of norms in the Gaussian integers, $|z_1 z_2| = |z_1||z_2|$). Therefore, $C(m) = p_1 \cdot p_2 \cdot p_3$ can certainly be written in the form $X^2 + Y^2$. This establishes the sufficiency direction.

Step 2: Necessity ($\Longrightarrow$) — If *m* is odd. Suppose m is an odd integer; let $m = 2k + 1$. Let us again examine the prime factors modulo 4:

$$p_1 = 6(2k + 1) + 1 = 12k + 7 \Longrightarrow p_1 \equiv 3 \pmod 4$$
$$p_2 = 12(2k + 1) + 1 = 24k + 13 \Longrightarrow p_2 \equiv 1 \pmod 4$$
$$p_3 = 18(2k + 1) + 1 = 36k + 19 \Longrightarrow p_3 \equiv 3 \pmod 4$$

The critical point here is that p_1 and p_3 are of the form 3 (mod 4), and $C(m) = p_1^1 \cdot p_2^1 \cdot p_3^1$. Since Carmichael numbers are square-free, the primes p_1 and p_3 divide $C(m)$ to the first (odd) power. By Proposition 2.2, if a prime factor of the form 3 (mod 4) occurs to an odd power in a number, that number cannot be written as the sum of two integer squares ($X^2 + Y^2$) in any way. Therefore, when m is odd, it is mathematically impossible for $C(m)$ to be a sum of two squares. ■

Remark 3.1. A notable feature of the necessity direction (Step 2) is that not just one but two distinct primes of the form 3 (mod 4) — namely p_1 and p_3 — occur simultaneously, each to an odd power. This shows that the obstruction is structural rather than "fragile": as long as m is odd, the representation remains impossible without exception.

4. Conclusion, Numerical Verification, and Limitations

This theorem establishes a parity (odd–even) rule that brings together the pseudoprime combinations of Carmichael numbers with the geometry of complex space.

Verification 1 (m odd — m = 1). $p_1 = 7$, $p_2 = 13$, $p_3 = 19$ (all prime), and $C(1) = 7 \times 13 \times 19 = 1729$. The number 1729 is the famous Hardy–Ramanujan number and can be written as the sum of two *cubes* ($1^3 + 12^3 = 9^3 + 10^3$); however, as predicted by our theorem, since $m = 1$ is odd, 1729 can never be written as the sum of two *squares* (indeed, $7 \equiv 3 \pmod 4$ and $19 \equiv 3 \pmod 4$), each occurring to the first power).

Verification 2 (m even — m = 6). $p_1 = 37$, $p_2 = 73$, $p_3 = 109$ (all prime), and $C(6) = 37 \times 73 \times 109 = 294409$. Since $m = 6$ is even, the theorem guarantees that this number is a sum of two squares. Indeed, $37 = 6^2 + 1^2$, $73 = 8^2 + 3^2$, and $109 = 10^2 + 3^2$; combining these three representations successively via the Brahmagupta–Fibonacci identity (by taking the norm of the product $(6+i)(8+3i)(10+3i)$ in the Gaussian integers) yields $294409 = 540^2 + 53^2$. Verification: $540^2 + 53^2 = 291600 + 2809 = 294409$, which is exactly equal to $C(6)$.

As can be seen, this original theorem, constructed between Number Theory (Büyükaşık, 2001) and Hypercomplex Algebra (Pashaev & Erman, 2001), holds consistently at both the algebraic-proof and numerical-verification levels.

The scope of this study is limited to Chernick's three-prime-factor family $C(m) = (6m+1)(12m+1)(18m+1)$; how the parity rule would change for general Carmichael numbers with four or more prime factors (e.g., Chernick's extended k-factor families) has not been addressed here. Furthermore, the question of how many distinct ways $C(m)$ can be written as a sum of two squares (the multiplicity of representation) is left outside the scope of this study, which is limited to the question of whether a representation exists at all.

Future research may address the following questions:

1. Can a similar parity rule be derived for Chernick's generalized Carmichael families with $k \geq 4$ prime factors?

2. Can the number of two-square-sum representations of a given Chernick–Carmichael number (the function $r_2(n)$) be expressed by a closed formula in terms of the parameter m?

3. Could this parity rule have a practical application in designing cryptographic attacks or primality tests based on Carmichael numbers?

Ethics Statement and Additional Information

Ethics Committee Approval: This study is a theoretical/analytical mathematics investigation that does not involve any experimentation on human or animal subjects; therefore, ethics committee approval is not required.

Conflict of Interest: The author(s) declare no conflict of interest related to this study.

Funding: No financial support was received from any institution or organization for this study.

Author Contribution: The conceptualization, development of the proofs, writing, and revision of the manuscript were carried out by İsmail Kara.

References

Büyükaşık, E. (2001). Carmichael numbers. *Matematik Dünyası*, 10(5), 24–28.

Carmichael, R. D. (1910). Note on a new number theory function. *Bulletin of the American Mathematical Society*, 16(5), 232–238.

Chernick, J. (1939). On Fermat's simple theorem. *Bulletin of the American Mathematical Society*, 45(4), 269–274.

Cox, D. A. (1989). *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*. Wiley.

Niven, I., Zuckerman, H. S., & Montgomery, H. L. (1991). *An introduction to the theory of numbers* (5th ed.). Wiley.

Pashaev, O. K., & Erman, F. (2001). The eight squares theorem and Cayley numbers. *Matematik Dünyası*, 10(5), 17–20.