The Collapse of Fermat's Little Theorem in the Algebra of Octonions: A Modular Approach

[İsmail Kara][1]
[1] *[Körfez Atatürk Anadolu Lisesi] - [ismailkarailetisim@gmail.com]*
ORCID: [0009-0009-5651-0193]

Abstract

Fermat's Little Theorem ($a^p \equiv a \pmod{p}$) underlies numerical cryptography and primality testing in commutative rings and the integers. However, the validity of this theorem in hypercomplex spaces, where associativity and commutativity are abandoned as the algebraic structure is extended, has rarely been examined in the literature. This study builds a bridge between number theory and eight-dimensional abstract algebra (Cayley numbers / octonions) by testing the general validity of Fermat's Little Theorem over integer-coefficient octonions. Because the anti-commutative multiplication rule disrupts the binomial expansion, it is algebraically proven that the theorem collapses specifically for primes of the form $p \equiv 5 \pmod 8$ and $p \equiv 7 \pmod 8$, and this collapse is tied to a modular boundary condition via the Legendre symbol. The findings are verified with numerical examples (p = 7, 13, 17).

Keywords

Fermat's Little Theorem; Octonions; Cayley Numbers; Legendre Symbol; Anti-Commutative Algebra; Modular Arithmetic.

Öz

Fermat'ın Küçük Teoremi ($a^p \equiv a \pmod{p}$), değişmeli halkalarda ve tam sayılar cisminde sayısal kriptografinin ve asal sayı testlerinin temelini oluşturur. Bu çalışmada, tam katsayılı oktonyonlar üzerinde bu teoremin genel geçerliliği test edilmiş; anti-komütatif çarpım kuralının binom açılımını bozması sebebiyle, özellikle $p \equiv 5 \pmod 8$ ve $p \equiv 7 \pmod 8$ formundaki asal sayılar için teoremin çöktüğü cebirsel olarak ispatlanmış ve Legendre Sembolü yardımıyla modüler bir sınır koşuluna bağlanmıştır.

Anahtar Kelimeler

Fermat'ın Küçük Teoremi; Oktonyonlar; Cayley Sayıları; Legendre Sembolü; Anti-Komütatif Cebir; Modüler Aritmetik.

1. Introduction and Motivation

Fermat's Little Theorem, one of the most fundamental building blocks of number theory, states that $a^p \equiv a \pmod{p}$ for a prime p and an integer a (Büyükaşık, 2001). Classical proofs of this theorem generally rely on the binomial expansion of the form $(A + B)^p$, and for the binomial

theorem to hold, it is a mathematical necessity that the elements involved commute ($A \cdot B = B \cdot A$).

In the literature on hypercomplex number systems, it is well known that as one moves from the real numbers to the complex numbers, then to the quaternions (4-dimensional, non-commutative but associative), and finally to the octonions (8-dimensional, neither commutative nor associative), the underlying algebraic structure progressively weakens (Baez, 2002; Conway & Smith, 2003). Within this hierarchy, the question of which algebraic assumptions (commutativity, associativity) classical number-theoretic results actually require has not been directly tested in the literature; existing studies generally focus on the geometric and algebraic properties of octonions (Baez, 2002) or on representation problems in number theory (Pashaev & Erman, 2001), without offering a modular analysis that directly connects the two fields.

The motivation for this study is to test whether this well-known prime-number rule holds in the algebra of octonions (Cayley numbers) (Pashaev & Erman, 2001), an 8-dimensional hypercomplex number system that possesses neither associativity nor commutativity. Although octonions are not associative, since they form a "power-associative" algebra, the expression X^p can still be uniquely (well-)defined (Baez, 2002). This fact legitimizes the study of modular exponentiation over octonions.

The remainder of the paper is organized as follows. Section 2 defines integer-coefficient octonions, modular congruence, and Euler's Criterion / the Legendre symbol. Section 3 proves the main theorem and verifies it with numerical examples. Section 4 discusses the findings and addresses the study's limitations and directions for future research.

2. Basic Concepts and Preliminaries

Definition 2.1 (Integer-Coefficient Octonions). With $x_k \in \mathbf{Z}$, a Cayley number (octonion) X is expressed as:

$$X = x_0 + x_1 i_1 + x_2 i_2 + \cdots + x_7 i_7$$

Here, i_k ($k = 1, \ldots, 7$) represent the imaginary units. According to the multiplication table given by Pashaev and Erman (2001), these units obey the following rules:

$$i_m^2 = -1 \quad and \quad i_m i_n = -i_n i_m \ (m \neq n)$$

Definition 2.2 (Congruence Modulo p). For two octonions $X = \Sigma\, x_k i_k$ and $Y = \Sigma\, y_k i_k$, the expression $X \equiv Y \pmod{p}$ means that $x_k \equiv y_k \pmod{p}$ for every $k = 0, \ldots, 7$; that is, congruence is defined component-wise.

Proposition 2.1 (Euler's Criterion and the Legendre Symbol). Let $p > 2$ be an odd prime and $a \in \mathbf{Z}$. The Legendre symbol (a/p), which determines whether a is a quadratic residue modulo p, is defined via Euler's criterion as:

$$a^{(p-1)/2} \equiv (a/p) \pmod{p}$$

In particular, for $a = -2$, the quadratic residue status is given by the following (Ireland & Rosen, 1990):

$$(-2/p) = 1, \quad \text{if } p \equiv 1 \text{ or } 3 \pmod 8$$
$$(-2/p) = -1, \quad \text{if } p \equiv 5 \text{ or } 7 \pmod 8$$

3. Main Theorem and Proof

Theorem 3.1 (Collapse of Fermat's Theorem over Octonions). Fermat's Little Theorem does not hold in general in the ring of integer-coefficient octonions. For a prime p satisfying $p \equiv 5 \pmod 8$ or $p \equiv 7 \pmod 8$, there exist octonions X for which $X^p \not\equiv X \pmod p$.

Proof.

1. To prove the claim, let us define the elementary integer-coefficient octonion $X = i_1 + i_2$.

2. Let us compute the square of X according to the Cayley multiplication rules (Definition 2.1):

$$X^2 = (i_1 + i_2)(i_1 + i_2) = i_1^2 + i_1 i_2 + i_2 i_1 + i_2^2$$

By the anti-commutativity rule, $i_1 i_2 = -i_2 i_1$, so the cross terms cancel. Also, $i_1^2 = i_2^2 = -1$. Hence:

$$X^2 = -1 + (i_1 i_2 - i_1 i_2) - 1 = -2$$

Remark 3.1. Owing to the anti-commutative property, the square of this octonion is stripped entirely of its imaginary parts and reduces to a negative real integer. This result is not specific to i_1, i_2: the same reasoning applies to the sum $Y = i_m + i_n$ of any two distinct imaginary units ($m \neq n$), since the identity $i_m i_n + i_n i_m = 0$ holds for every pair $m \neq n$. Hence the proof below applies verbatim to any pair chosen from $\{i_1, \ldots, i_7\}$.

3. Since $p > 2$ is an odd prime, it has the form $p = 2k + 1$ ($k = (p - 1)/2$). Because octonions are power-associative, the expression X^p is well-defined independently of parenthesization; therefore:

$$X^p = X^{2k+1} = (X^2)^k \cdot X$$

Substituting $X^2 = -2$:

$$X^p = (-2)^{(p-1)/2} \cdot X$$

4. Let us examine this expression modulo p. By Euler's Criterion (Proposition 2.1), $(-2)^{(p-1)/2} \equiv (-2/p) \pmod{p}$, so:

$$X^p \equiv (-2/p) \cdot X \pmod{p}$$

5. From the properties of the Legendre symbol (Proposition 2.1), if $p \equiv 5 \pmod 8$ or $p \equiv 7 \pmod 8$, then $(-2/p) = -1$. In this case, the equation becomes:

$$X^p \equiv -X \pmod{p}$$

6. The components of $X = i_1 + i_2$ are (1, 1), and since p is odd ($p \nmid 1$), by Definition 2.2 we have $X \not\equiv 0 \pmod p$. Moreover, since p is odd ($p \neq 2$), the equality $X \equiv -X \pmod p$ would require $2X \equiv 0 \pmod p$, i.e., $p \mid 2$, which is impossible since $p > 2$. Therefore, X and $-X$ cannot be congruent modulo p:

$$X \not\equiv -X \pmod{p} \implies X^p = -X \not\equiv X \pmod{p}$$

This establishes that Fermat's Little Theorem collapses whenever $p \equiv 5, 7 \pmod 8$. ■

Numerical Verification ($p = 13$). Since $13 \equiv 5 \pmod 8$, the theorem predicts collapse. Here $k = 6$, so $X^{13} = (-2)^6 \cdot X = 64X$. Since $64 \equiv -1 \pmod{13}$, $X^{13} \equiv -X \pmod{13}$; since $X = i_1 + i_2 \not\equiv 0 \pmod{13}$, this confirms $X^{13} \not\equiv X \pmod{13}$.

Numerical Verification ($p = 7$). Since $7 \equiv 7 \pmod 8$, collapse is again expected. Here $k = 3$, $X^7 = (-2)^3 \cdot X = -8X \equiv -X \pmod 7$ (since $-8 \equiv -1 \pmod 7$); this confirms $X^7 \not\equiv X \pmod 7$.

Boundary-Case Verification ($p = 17$). Since $17 \equiv 1 \pmod 8$, Proposition 2.1 predicts $(-2/17) = 1$, so the theorem should not collapse. Indeed, with $k = 8$, $X^{17} = (-2)^8 \cdot X = 256X$, and since $256 \equiv 1 \pmod{17}$, we obtain $X^{17} \equiv X \pmod{17}$; this numerically confirms that the theorem remains valid for $p \equiv 1, 3 \pmod 8$, and that the collapse is indeed confined to the modular classes identified above.

4. Conclusion, Discussion, and Limitations

The theorem proven in this study reveals the inseparable links between the characteristic properties of algebraic spaces (commutativity/associativity) and the fundamental building blocks of number theory. The classical Fermat theorem relies, at its core, on the divisibility of binomial coefficients by p. However, in anti-commutative spaces such as the octonions, the expansion of $(A + B)^p$ does not produce the standard binomial coefficients; the terms AB and BA cancel each other out, creating an algebraic "short circuit" (the collapse $X^2 = -2$ seen in the proof).

This algebraic short circuit instantly transforms the problem into a "quadratic residues" problem from number theory. Consequently, it has been shown mathematically that, when designing primality tests and cryptographic algorithms in higher-dimensional hypercomplex spaces, classical theorems such as Fermat's Little Theorem can only be relied upon within the boundary conditions set by the Legendre symbol ($p \equiv 1, 3 \pmod 8$). This finding indicates that an octonion-based Fermat primality test cannot be reliable for all primes indiscriminately.

The scope of this study is limited to a specific family of octonions of the form $X = i_m + i_n$ (consisting of exactly two imaginary units, with zero real part); the behaviour of X^2 for general octonions with a nonzero real component or more than two nonzero imaginary components has not been examined here. Furthermore, the result concerns only prime moduli; no generalization to prime-power (p^k) moduli has been made.

Future research may address the following questions:

1. How can the conditions for Fermat collapse be characterized for a general octonion $X = x_0 + \Sigma x_k i_k$ with nonzero real part?

2. Is a similar modular collapse observed in the lower-dimensional algebra of quaternions (associative but non-commutative)?

3. Could this collapse property have a practical application in the security analysis of cryptographic protocols designed over hypercomplex spaces?

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

Baez, J. C. (2002). The octonions. *Bulletin of the American Mathematical Society*, 39(2), 145–205.

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

Conway, J. H., & Smith, D. A. (2003). *On quaternions and octonions: Their geometry, arithmetic, and symmetry*. A K Peters.

Ireland, K., & Rosen, M. (1990). *A classical introduction to modern number theory* (2nd ed.). Springer-Verlag.

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