Research Article

On Some Novel Results about Split-Complex Numbers, the Diagonalization Problem, and Applications to Public Key Asymmetric Cryptography

Mehmet Merkepci and Mohammad Abobala

1Gaziantep University, Department of Computer Engineering, Gaziantep, Turkey
2Tishreen University, Department of Mathematics, Latakia, Syria

Correspondence should be addressed to Mohammad Abobala; mohammadabobala777@gmail.com

Received 1 February 2023; Revised 7 June 2023; Accepted 27 June 2023; Published 4 July 2023

1. Introduction and Preliminaries

The field of real numbers plays an important role in the history of mathematics and computer science. The field of real numbers was extended by the field of complex numbers $\mathbb{C} = \{a + bi; \ i^2 = -1\}$ [1].

In [2, 3], we find other extensions of real numbers for algebraic or geometric purposes such as dual numbers $\mathbb{D} = \{a + bj; \ J^2 = 0\}$, neutrosophic numbers $\mathbb{N} = \{a + bj; \ J^2 = J\}$, and split-complex numbers $\mathbb{S} = \{a + bj; \ J^2 = 1\}$. For the definitions and properties of split-complex numbers, see [1]. Split-complex numbers have been studied widely, especially their applications in physics, where this class of numbers is useful in representing Dirac brackets [4], and they have been used in defining generalized version of vector spaces, see [5]. We assert that split-complex numbers represent an expansion of the real numbers in two dimensions and possess many interesting geometric properties similar to the complex numbers.

The main goal behind mathematical cryptography is to keep messages and multimedia messages secret at a time when modern means of communication have spread and become very diverse, where we find some applications of Catalan numbers and other algebraic numbers in cryptology in [6–8]. In addition, several kinds of attacks on some cryptosystems were discussed widely [9, 10]. Computer scientists have used number theory to protect messages and multimedia from attackers by providing concepts such as symmetric and asymmetric cryptoalgorithms, where some powerful algorithms such as El-Gamal algorithm and RSA algorithm were built over the algebraic properties of integers especially congruencies and relatively prime numbers [11–13]. The usage of split-complex numbers in cryptography has been suggested recently in [14].

This motivates us to introduce a novel version of RSA cryptoalgorithm depending on the algebraic properties of split-complex numbers, where we provide a brief discussion for the foundations of split-complex number theory, and we
use these algebraic properties to present the algorithm in a similar way of the classical one which has more complexity compared to the classical version of RSA cryptosystem. In addition, we illustrate some examples to clarify the validity of our results.

In addition, we study square matrices with split-complex entries where the diagonalization problem [15] of split-complex square matrices will be handled in details. The main result is to present a novel algorithm to represent any diagonalizable split-complex square matrix by a diagonal matrix, which means the possibility of writing the split-complex matrix \( X \) by the formula \( X = A^{-1}DA \) with \( A \) as an invertible split-complex matrix and \( D \) is a diagonal split-complex matrix, and in connection with this subtraction, we have determined the necessary and sufficient condition for the diagonalization of a matrix of the mentioned type.

The fundamental advance that this study makes is to close a research gap related to the diagonalization of any square matrix of the type of split-complex square matrices. Also, on the other hand, for the first time, an efficient algorithm was presented that is useful for calculating the exponent of a matrix of this type in addition to calculating the eigenvalues and related eigenvectors.

This paper consists of three main sections. Section 2 discusses the foundations of split-complex number theory such as division, relatively primes, and split-complex congruencies; Section 3 concerns with the applications of split-complex number theory in generalizing RSA cryptosystem. Section 4 discusses the conditions of diagonalizing a square split-complex matrix, as well as, it introduces an easy algorithm to solve this problem.

\[ \begin{align*}
  c &= an + bm \\
  d &= an + bm
\end{align*} \]

\[ c - d = am + bn - an - bm = (a - b)(m - n), \]

\[ c + d = an + bm + bn + bm = (a + b)(m + n). \]

Thus, \( a - b \mid c - d \) and \( a + b \mid c + d \).

The converse holds by a similar argument. \( \Box \)

**Theorem 5.** Let \( X = a + bf, Y = c + df; Z = m + nf \) be three split-complex integers, then \( X \equiv Y \pmod{Z} \) if and only if \( a - b \equiv c - d \pmod{m - n} \) and \( a + b \equiv c + d \pmod{m + n} \).

\[ \begin{align*}
  m - n &\mid (a - b) - (c - d) \\
  m + n &\mid (a + b) - (c + d)
\end{align*} \]

**Example 1.** Take \( X = 5 + 7I, Y = 3 + 2I, Z = 2 - I \), we can see that \( X - Y = 2 + 5I \) and \( Z \mid X - Y \) that is because

\[ 3 + 2 - \frac{(b - 1)}{2} - 5 = 2 - 1 - \frac{1}{2} + 5 = 7. \]

**Definition 6.** Let \( X = a + bf, Y = c + df \) be two split-complex integers, then we define \( \gcd(X, Y) = 1/2[\gcd(a-b, c-d) + \gcd(a+b, c+d)] \) as the greatest common divisor of \( a-b, c-d \) and \( a+b, c+d \).

**2. Split-Complex Number Theory and Integers**

**Definition 1.** Let \( X = p + qJ, Y = s + hJ, Z = m + nJ \) be two split-complex integers, then \( X \mid Y \) if there exists \( Z = m + nJ \) such that \( Y = XZ \).

**Definition 2.** Let \( X = p + qJ, Y = s + hJ, Z = m + nJ \) be three split-complex integers, then

(a) \( X \equiv Y \pmod{Z} \) if and only if \( Z \mid X - Y \)

(b) \( X \leq Y \) if and only if \( p - q \leq s - h \) and \( p + q \leq s + h \)

**Theorem 3.** \( \leq \) is a partial order relation.

**Proof.** Take \( X = p + qJ, Y = s + hJ, Z = m + nJ \), we have \( X \leq X \) that is because \( p - q \leq p - q, p + q \leq p + q \). If \( X \leq Y \) and \( Y \leq X \), then \( p - q \leq s - h, s - h \leq p - q, p + q \leq s + h, \) and \( s + h \leq p + q \), thus \( p - q \leq s - h, p + q \leq s + h \), this implies that \( p = s \) and \( q = h \), hence \( X = Y \). If \( X \leq Y \) and \( Y \leq Z \), then \( p - q \leq s - h \leq m - n \) and \( p + q \leq s + h \leq m + n \), hence \( X \leq Z \).

**Theorem 4.** Let \( X, Y \) be two split-complex integers with \( X = a + bf, Y = c + df, Z = m + nf \), then \( X \mid Y \) if and only if \( a - b \mid c - d \) and \( a + b \mid c + d \).

**Proof.** Assume that \( X \mid Y \), then there exists \( Z = m + nf \) such that \( XZ = Y \), so that

\[ a - b \equiv c - d \pmod{m - n} \]

and

\[ a + b \equiv c + d \pmod{m + n}. \]

**Definition 5.** Let \( X = a + bf, Y = c + df \) be two split-complex integers, then we define \( \gcd(X, Y) = 1/2[\gcd(a-b, c-d) + \gcd(a+b, c+d)] \) as the greatest common divisor of \( a-b, c-d \) and \( a+b, c+d \).

**Example 2.** Take \( X = 4 + 3I, Y = 8 + 3I \). We have the following expression:

\[ \gcd(4 - 3, 8 - 3) = 1, \gcd(4 + 3, 8 + 3) = 1, \]

thus

\[ b, c - d \mid \gcd(a + b, c + d) + 1/2[\gcd(a, b, c + d) + \gcd(a - b, c - d)]. \]
\[ \gcd(X, Y) = \frac{1}{2} [1 + 1] + \frac{1}{2} J [1 - 1] = 1. \] 

**Theorem 7.** Let \( X = a + bf, Y = c + df \) be two split-complex integers, then

- (a) If \( X \mid Y \), then \( X \leq Y \)
- (b) \( \gcd(X, Y) \) is a split-complex integer
- (c) \( \gcd(X, Y) \) is a split-complex integer
- (d) \( X \) and \( Y \) are relatively prime if and only if \( \gcd(a - b, c - d) = \gcd(a + b, c + d) = 1 \)

**Proof**

(a) Assume that \( X \mid Y \), then \( a - b \mid c - d \) and \( a + b \mid c + d \), hence \( a - b \leq c - d \) and \( a + b \leq c + d \) so that \( X \leq Y \).

(b) If \( a - b, c - d \) are even integers, then \( a + b, c + d \) are even too. This means that:
\[ \gcd(a - b, c - d), \gcd(a + b, c + d) \]
are even integers, hence \( \gcd(X, Y) \) is a split-complex integer.
If \( a - b, c - d \) are odd integers, then \( a + b, c + d \) are odd too.

This means that \( \gcd(a - b, c - d) + \gcd(a + b, c + d) \) and \( \gcd(a + b, c + d) - \gcd(a - b, c - d) \) are even integers, thus \( \gcd(X, Y) \) is a split-complex integer.
If \( a - b \) is even and \( c - d \) is odd, then \( a + b \) is even and \( c + d \) is odd, so that \( \gcd(a - b, c - d) + \gcd(a + b, c + d) \) and \( \gcd(a + b, c + d) - \gcd(a - b, c - d) \) are even integers, thus \( \gcd(X, Y) \) is a split-complex integer.

If \( a - b \) is odd and \( c - d \) is even, it holds by a similar argument.

(c) Suppose that \( Z = mn + nl \) is a divisor of \( X \) and \( Y \), then
\[ \begin{cases} m - n & | a - b, m - n | c - d, \\ m + n & | a + b, m + n | c + d. \end{cases} \]

Thus,
\[ \begin{cases} m - n & | \gcd(a - b, c - d) \\ m + n & | \gcd(a + b, c + d) \end{cases} \]
and we get \( Z \mid \gcd(X, Y) \).

(d) It holds directly from the definition.

**Definition 8.** Let \( X = a + bf \) be a positive split-complex number, i.e., \( a - b > 0, a + b > 0 \), we define the split-complex Euler’s function as follows.
\[ \varphi_S : S(J) \rightarrow S(J) \] such that \( \varphi_S(a + bf) = 1/2[\varphi(a + b) + \varphi(a - b)] + 1/2 J [\varphi(a + b) - \varphi(a - b)] \), where \( S(J) \) is the ring of split-complex integers.

**Example 4.** Take \( X = 6 + J \), \( \varphi_S(X) = 1/2[\varphi(7) + \varphi(5)] + 1/2 J [\varphi(7) - \varphi(5)] = 1/2[6 + 4] + 1/2 J [6 - 4] = 5 + J \).

**Theorem 9.** Let \( X = a + bf \) be a positive split-complex integer, then

- (a) \( \varphi_S(X) \in S(J) \)
- (b) If \( \gcd(X, Y) = 1 \), then \( Y^{\varphi_S(X)} \equiv 1 \pmod{X} \)

(which is the split-complex version of Euler's theorem).

**Proof**

(a) Since \( \varphi(a + b), \varphi(a - b) \) must be even integers, then \( \varphi_S(X) \in S(J) \).

(b) Assume that \( \gcd(X, Y) = 1 \), then \( \gcd(a - b, c - d) = \gcd(a + b, c + d) = 1 \)

According to the classical Euler's theorem, we can write
\[ (c - d)^{(a - b)} \equiv 1 \pmod{a - b}, (c + d)^{(a + b)} \]
\[ 1 \pmod{a + b} \]
on the other hand, we have the following equation:

\[ Y^{\varphi_S(X)} = (c + df)^{\varphi_S(X)}; \varphi_S(X) = 1/2[\varphi(a + b) + \varphi(a - b)] + 1/2 J [\varphi(a + b) - \varphi(a - b)] = l_1 + l_2 J \]

\[ l_2 + l_1 = \varphi(a + b), l_1 - l_2 = \varphi(a - b) \), so that:
\[ Y^{\varphi_S(X)} = 1/2 [(c - d)^{l_1 - l_2} + (c + d)^{l_1 + l_2}] + 1/2 J [(c + d)^{l_1 + l_2} - (c - d)^{l_1 - l_2}] = t_1 + t_2 J, \]

\[ t_1 + t_2 = (c + d)^{l_1 + l_2} = (c + d)^{\varphi(a + b)} = 1 \pmod{a + b}, \]

\[ t_1 - t_2 = (c - d)^{l_1 - l_2} = (c - d)^{\varphi(a - b)} = 1 \pmod{a - b}. \]
Thus, \( Y_n(X) = t_1 + t_2J \equiv 1 \pmod{X} \).

**Remark 10.** We define the raising of a split-complex integer to a split-complex integer power as follows:

\[
(c + dJ)^{(a+b)} = \frac{1}{2} [(c - d)^{a+b} + (c + d)^{a+b}]
\]

\[
+ \frac{1}{2} J [(c + d)^{a+b} - (c - d)^{a+b}].
\]

(10)

\[
gcd(X, Y) = \frac{1}{2} [gcd(3, 1) + gcd(23, 3)] + \frac{1}{2} J [gcd(23, 3) - gcd(3, 1) = 1,
\]

\[
\phi_5(X) = \frac{1}{2} [\phi(23) + \phi(3)] + \frac{1}{2} J [\phi(23) - \phi(3)] = \frac{1}{2} [22 + 2] + \frac{1}{2} J = 12 + 10J,
\]

\[
Y^{\phi_5(X)} = (2 + J)^{(12+10J)} = \frac{1}{2} \left[ (1)^2 + (3)^{22} \right] + \frac{1}{2} J \left[ (3)^{22} - (1)^2 \right] = t_1 + t_2J,
\]

\[
t_1 + t_2 = (3)^{22} \equiv 1 \pmod{23}, t_1 - t_2 = 1 \equiv 1 \pmod{3}.
\]

Thus, \( Y_n(X) \equiv 1 \pmod{13 + 10J} \).

### 3. Applications to Cryptography

Now, we are suggesting the split-complex version of RSA cryptovalgorithm by using the foundational concepts of split-complex number theory we have established.

#### 3.1. RSA Algorithm

Assume that we have two sides \( X, Y \); the first side \( X \) is a sender, the second \( Y \) is a receiver.

Consider that \( X \) has decided to send the text \( M = m_1 \), \( X \) and \( Y \) should follow these steps:

1. \( Y \) should pick two large positive prime integers \( P, Q \), then \( Y \) computes

\[
N = P \times Q.
\]

(12)

2. \( Y \) should compute:

\[
\phi(N) = (P - 1)(Q - 1).
\]

(13)

3. \( Y \) should pick \( 1 < E < \phi(N) \) such that

\[
gcd(E, \phi(N)) = 1.
\]

The public key is \((N, E)\).

\( Y \) computes the secret key \( E^{-1} \) as follows:

\[
EE^{-1} \equiv 1 \pmod{\phi(N)}.
\]

(14)

#### Step 4.

\( X \) gets the cipher text as follows:

\[
C \equiv M^E \pmod{N}.
\]

(15)

For the second side \( Y \), it decrypts the message as follows:

\[
M \equiv C^{E^{-1}} \pmod{N}.
\]

(16)

#### 3.2. Split-Complex RSA

Assume that we have two sides \( X, Y \); the first side \( X \) is a sender, the second \( Y \) is a receiver.

Consider that \( X \) has decided to send the text \( M = m_1 + m_2J \) (denoted as a split-complex integer), \( X \) and \( Y \) should follow these steps:

1. \( Y \) should pick two large positive split-complex integers \( P = p_1 + p_2J, Q = q_1 + q_2J \) (it is preferred to take \( p_1 - p_2, p_1 + p_2, q_1 - q_2, q_1 + q_2 \) as large prime numbers), then \( Y \) computes

\[
N = P \times Q = p_1q_1 + p_2q_2 + J(p_1q_2 + p_2q_1) = n_1 + n_2J.
\]

(17)

#### Step 2.

\( Y \) should compute:
\[ \varphi_5(N) = \frac{1}{2} [\varphi((p_1 + p_2)(q_1 + q_2)) + \varphi((p_1 - p_2)(q_1 - q_2))] + \frac{1}{2} J[\varphi((p_1 + p_2)(q_1 + q_2)) - \varphi((p_1 - p_2)(q_1 - q_2))] \]

\[ = \frac{1}{2} [(p_1 + p_2 - 1)(q_1 + q_2 - 1) + (p_1 - p_2 - 1)(q_1 - q_2 - 1)] + \frac{1}{2} J[(p_1 + p_2 - 1)(q_1 + q_2 - 1) - (p_1 - p_2 - 1)(q_1 - q_2 - 1)] \]

\[ = \frac{1}{2} [p_1q_1 + p_1q_2 - p_1 + p_2q_1 + p_2q_2 - p_2 - q_1 - q_2 + 1 + p_1q_1 - p_1q_2 - p_1 - p_2q_1 + p_2q_2 + p_2 - q_1 + q_2 + 1] \]

\[ + \frac{1}{2} J[p_1q_1 + p_1q_2 - p_1 + p_2q_1 + p_2q_2 - p_2 - q_1 - q_2 + 1 - p_1q_1 + p_1q_2 + p_1 + p_2q_1 - p_2q_2 - p_2 + q_1 - q_2 - 1] \]

\[ = \frac{1}{2} [2p_1q_1 - 2p_1 + 2p_2q_1 - 2q_1 + 2] + \frac{1}{2} J[2p_1q_1 + 2p_2q_1 - 2p_2 - 2q_2] \]

\[ = [p_1q_1 - p_1 + p_2q_1 - q_1 + 2] + J[p_1q_1 + p_2q_1 - p_2 - q_2] = l_1 + l_2J. \]  

(18)

\[ EE^{-1} \equiv 1 \pmod{\varphi_5(N)}, \text{ in other words if } E = e_1 + e_2J, \]

\[ E^{-1} = \frac{1}{2} [(e_1 + e_2)^{-1} + (e_1 - e_2)^{-1}] + \frac{1}{2} J[(e_1 + e_2)^{-1} - (e_1 - e_2)^{-1}] \pmod{\varphi_5(N)} \]

\[ = \frac{1}{2} [(e_1 + e_2)^{-1} \pmod{l_1 + l_2} + (e_1 - e_2)^{-1} \pmod{l_1 - l_2}] + \frac{1}{2} J[(e_1 + e_2)^{-1} \pmod{l_1 + l_2} -(e_1 - e_2)^{-1} \pmod{l_1 - l_2}]. \]

(19)

\[ C \equiv M^E \pmod{N} = (8 + 3J)^{3+2J} \pmod{N} = 21 + 16J, \]

(23)

which is the cipher text.

(Y) decrypts the message as follows:

\[ M \equiv C^{E^{-1}} \pmod{N} \equiv (21 + 16J)^{9+8J} \pmod{N} = 8 + 3J, \]

(24)

which is the plain text.

3.3. Split-Complex Matrices and Their Diagonalizations

Definition 11. Let \( A = (a_{ij}) \) be an \( n \)-square matrix with split-complex entries \( a_{ij} = x_{ij} + y_{ij}J; x_{ij}, y_{ij} \in R, J^2 = 1 \). We call \( A \) a split-complex square matrix.

Remark 12. The split-complex matrix can be written as follows: \( A = A_1 + A_2J \) and \( A_1, A_2 \) are two square matrices over \( R \).
Example 7. Consider the following $3 \times 3$ split-complex matrix:

\[
A = \begin{pmatrix} 1 + J & 2 - 2J & J \\ 1 & 3 - J & 1 + J \\ 2J & -3J & 1 + 2J \end{pmatrix}
\]

Thus, proof is complete.


Theorem 13. Let $A = A_1 + A_2J, B = B_1 + B_2J$ be two split-complex matrices, then $A \times B = A_1 \times B_1 + A_2 \times B_2 + J(A_1 \times B_2 + A_2 \times B_1)$.

A \times B = \begin{pmatrix} (1 + J)(1) + (2 - J)(2) + J & (1 + J)(1) + (2 - J)(2) - 3J \\ (3 + J)(1) + (1 + 4J)(2 + J) & (3 + J)(1) + (1 + 4J)(2 - 3J) \end{pmatrix} = \begin{pmatrix} 4 + J & 8 - 7J \\ 7 + 12J & -7 + 6J \end{pmatrix},

A_1 \times B_1 = \begin{pmatrix} 1 & 2 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 4 & 5 \\ 2 & 5 \end{pmatrix},

A_2 \times B_2 = \begin{pmatrix} 1 & -1 \\ 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & -3 \end{pmatrix} = \begin{pmatrix} 0 & 3 \\ 5 & -12 \end{pmatrix},

A_1 \times B_2 = \begin{pmatrix} 1 & 2 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & -3 \end{pmatrix} = \begin{pmatrix} 3 & -6 \\ 4 & -3 \end{pmatrix},

A_2 \times B_1 = \begin{pmatrix} 1 & -1 \\ 1 & 4 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} -2 & -1 \\ 8 & 9 \end{pmatrix}.

Thus, $A_1 \times B_1 + A_2 \times B_2 + J(A_1 \times B_2 + A_2 \times B_1) = 4 + J \begin{pmatrix} 4 & 8 - 7J \\ 7 + 12J & -7 + 6J \end{pmatrix} = A \times B$.

Theorem 14. Let $X = A + BJ$ be an $n$-square split-complex matrix, then $X$ is invertible if and only if $A - B, A + B$ are invertible matrices.
Also, \( X^{-1} = 1/2[(A + B)^{-1} + (A - B)^{-1}] + 1/2J[(A + B)^{-1} - (A - B)^{-1}] \).

\[ Y = \frac{1}{2} [(A + B)^{-1} + (A - B)^{-1}] + \frac{1}{2}J[(A + B)^{-1} - (A - B)^{-1}], \]
\[ X.Y = \frac{1}{2} [A.(A + B)^{-1} + A.(A - B)^{-1} + B.(A + B)^{-1} - B.(A - B)^{-1}] \]
\[ + \frac{1}{2}J[A.(A + B)^{-1} - A.(A - B)^{-1} + B.(A + B)^{-1} + B.(A - B)^{-1}] \]
\[ = \frac{1}{2} [(A + B)(A + B)^{-1} + (A - B)(A - B)^{-1}] \]
\[ + \frac{1}{2}J[(A + B)(A + B)^{-1} - (A - B)(A - B)^{-1}] \]
\[ = \frac{1}{2} [U_{n\times n} + U_{n\times n}] + \frac{1}{2}J[U_{n\times n} - U_{n\times n}] = U_{n\times n}, \]

where \( U_{n\times n} \) is the \( n \)-unit matrix, so that \( X \) is invertible.

For the converse, we assume that \( X = A + BJ \) is an invertible \( n \)-square split-complex matrix, then there exists \( Y = C + DJ \) such that \( X.Y = U_{n\times n} \),
\[ X.Y = AC + BD + J(AD + BC) = U_{n\times n}, \]

\[ AC + BD = U_{n\times n}, \] \hspace{1cm} (29)
\[ AD + BC = O_{n\times n}, \] \hspace{1cm} (30)

By adding (29) to (30), we obtain \( AC + BD + AD + BC = U_{n\times n} \), thus \( (A + B)(C + D) = U_{n\times n} \), which implies that \( A + B \) is invertible matrix.

\[ X^{k+1} = X.X^k = (A + BJ)\left[ \frac{1}{2} [(A + B)^k + (A - B)^k] + \frac{1}{2}J[(A + B)^k - (A - B)^k] \right] \]
\[ = \frac{1}{2} [A.(A + B)^k + A.(A - B)^k + B.(A + B)^k - B.(A - B)^k] \]
\[ + \frac{1}{2}J[A.(A + B)^k - A.(A - B)^k + B.(A + B)^k + B.(A - B)^k] \]
\[ = \frac{1}{2} [(A + B)(A + B)^k + (A - B)(A - B)^k] \]
\[ + \frac{1}{2}J[(A + B)(A + B)^k - (A - B)(A - B)^k] \]
\[ = \frac{1}{2} [(A + B)^{k+1} + (A - B)^{k+1}] \]
\[ + \frac{1}{2}J[(A + B)^{k+1} - (A - B)^{k+1}]. \]

**Proof.** Suppose that \( A + B, A - B \) are invertible matrices, we define

\[ e^X = 1/2[e^{A+B} + e^{A-B}] + 1/2J[e^{A+B} - e^{A-B}]. \]

**Theorem 15.** Let \( X = A + BJ \) be an \( n \)-square split-complex matrix, then \( e^X = 1/2[(A + B)^n + (A - B)^n] + 1/2J[(A + B)^n - (A - B)^n] \).

**Proof.** Firstly, we prove that \( X^n = 1/2[(A + B)^n + (A - B)^n] + 1/2J[(A + B)^n - (A - B)^n] \).

For \( n = 1 \), it is clear. We assume that it is true for \( n = k \). We must prove it for \( n = k + 1 \).
By induction, we obtain the desired formula.

\[ e^X = \sum_{n=0}^{\infty} \frac{X^n}{n!} = I + \frac{X}{1!} + \frac{X^2}{2!} + \ldots \]

\[ = \sum_{n=0}^{\infty} \frac{1}{n!} \left[ \frac{1}{2} (A + B)^n + \frac{1}{2} (A - B)^n + J \left( \frac{1}{2} (A + B)^n - \frac{1}{2} (A - B)^n \right) \right] \]

\[ = \frac{1}{2} \sum_{n=0}^{\infty} \frac{(A + B)^n}{n!} + \frac{1}{2} \sum_{n=0}^{\infty} \frac{(A - B)^n}{n!} + \frac{1}{2} \sum_{n=0}^{\infty} \frac{(A + B)^n}{n!} - \frac{1}{2} \sum_{n=0}^{\infty} \frac{(A - B)^n}{n!} \]

\[ = \frac{1}{2} \left[ e^{A+B} + e^{A-B} \right] + \frac{1}{2} J \left[ e^{A+B} - e^{A-B} \right]. \]  

(32)

The diagonalization problem is as follows.

An n-square matrix \( A \) is diagonalizable if and only if there exists an invertible matrix \( S \) and a diagonal matrix \( D \) such that \( A = S^{-1}DS \).

In the literature, we do not have an algorithm to diagonalize a split-complex matrix \( X = A + BJ \).

In the following, we present an easy algorithm to check if a split-complex matrix is diagonalizable, as to find its formula of diagonalization.

**Theorem 16.** Let \( X = A + BJ \) be an n-square split-complex matrix, then \( X \) is diagonalizable if and only if \( A + B, A - B \) are diagonalizable.

On the other hand, we have the following expression.

\[ (P_1 + P_2) (D_1 + D_2) P^{-1} = [(P_1 D_1 + P_2 D_2) + J (P_1 D_2 + P_2 D_1)] P^{-1} \]

\[ = \frac{1}{2} [P_1 D_1 + P_2 D_2 + J (P_1 D_2 + P_2 D_1)] \left[ (P_1 + P_2)^{-1} + (P_1 - P_2)^{-1} \right] + J \left[ (P_1 + P_2)^{-1} + (P_1 - P_2)^{-1} \right] \]

\[ = \frac{1}{2} \left[ P_1 D_1 (P_1 - P_2)^{-1} - P_1 D_1 (P_1 + P_2)^{-1} + P_2 D_2 (P_1 - P_2)^{-1} + P_2 D_2 (P_1 + P_2)^{-1} + P_1 D_2 (P_1 + P_2)^{-1} - P_1 D_2 (P_1 - P_2)^{-1} \right. \]

\[ + P_1 D_1 (P_1 + P_2)^{-1} - P_1 D_1 (P_1 - P_2)^{-1} \]

\[ + \frac{1}{2} J \left[ P_1 D_1 (P_1 + P_2)^{-1} - P_1 D_1 (P_1 - P_2)^{-1} + P_2 D_2 (P_1 + P_2)^{-1} - P_2 D_2 (P_1 - P_2)^{-1} + P_1 D_2 (P_1 + P_2)^{-1} - P_1 D_2 (P_1 - P_2)^{-1} \right] \]

\[ + P_1 D_2 (P_1 - P_2)^{-1} + P_1 D_1 (P_1 - P_2)^{-1} + P_2 D_1 (P_1 + P_2)^{-1} \]

\[ = \frac{1}{2} \left[ (P_1 + P_2) (D_1 + D_2) (P_1 + P_2)^{-1} + (P_1 - P_2) (D_1 - D_2) (P_1 - P_2)^{-1} \right] \]

\[ + \frac{1}{2} J \left[ (P_1 + P_2) (D_1 + D_2) (P_1 + P_2)^{-1} - (P_1 - P_2) (D_1 - D_2) (P_1 - P_2)^{-1} \right] = X = A + BJ. \]

(34)

So that

**Proof.** Assume that \( X \) is diagonalizable, then there exists to a diagonal split-complex matrix \( D \) and an invertible split-complex matrix \( P \) such that \( PDP^{-1} = X \), where

\[ D = D_1 + D_2 J, \]

\[ P = P_1 + P_2 J, \]

\[ P^{-1} = \frac{1}{2} \left[ (P_1 + P_2)^{-1} + (P_1 - P_2)^{-1} \right] \]

\[ + \frac{1}{2} J \left[ (P_1 + P_2)^{-1} + (P_1 - P_2)^{-1} \right]. \]

The equation \( PDP^{-1} = X \), we obtain the following expression.
\[ A = \frac{1}{2} (P_1 + P_2)(D_1 + D_2)(P_1 + P_2)^{-1} + \frac{1}{2} (P_1 - P_2)(D_1 - D_2)(P_1 - P_2)^{-1}, \]
\[ B = \frac{1}{2} (P_1 + P_2)(D_1 + D_2)(P_1 + P_2)^{-1} - \frac{1}{2} (P_1 - P_2)(D_1 - D_2)(P_1 - P_2)^{-1}. \]

Thus, \( A + B = (P_1 + P_2)(D_1 + D_2)(P_1 + P_2)^{-1} \cdot (P_1 - P_2)^{-1} \).
\[ A - B = (P_1 - P_2)(D_1 - D_2)(P_1 - P_2)^{-1}. \]

Hence, \( A + B, A - B \) are diagonalizable.

For the converse, we assume that \( A + B, A - B \) are diagonalizable, so there exists two invertible matrices \( P_1, P_2 \) and two diagonal matrices \( D_1, D_2 \) such that:

\[ P \times T = \frac{1}{4} (U_{\text{non}} + P_1 P_2^{-1} + P_2 P_1^{-1} + U_{\text{non}} + P_1 P_2^{-1} - P_2 P_1^{-1}) + \frac{1}{4} (P_1 P_2^{-1} - U_{\text{non}} + P_1 P_2^{-1} + P_2 P_1^{-1} - U_{\text{non}} + P_1 P_2^{-1}) = \frac{1}{4} (4U_{\text{non}}) + \frac{1}{4} J(O_{\text{non}}) \]
\[ = U_{\text{non}}, \text{ thus } T = P^{-1}. \]

Now, let us check the matrices product \( PDP^{-1} \).

\[ P \times D = \frac{1}{4} (P_1 + P_2)(D_1 + D_2) + \frac{1}{4} (P_2 - P_1)(D_2 - D_1) + J\left[ \frac{1}{4} (P_1 + P_2)(D_2 - D_1) + \frac{1}{4} (P_2 - P_1)(D_1 + D_2) \right], \]
\[ P \times D \times P^{-1} = \frac{1}{8} (P_1 + P_2)(D_1 + D_2)(P_1^{-1} + P_2^{-1}) + \frac{1}{8} (P_2 - P_1)(D_2 - D_1)(P_1^{-1} + P_2^{-1}) + \frac{1}{8} (P_1 + P_2)(D_2 - D_1)(P_2^{-1} - P_1^{-1}) + \frac{1}{8} (P_2 - P_1)(D_1 + D_2)(P_2^{-1} - P_1^{-1}) + J\left[ \frac{1}{8} (P_1 + P_2)(D_1 + D_2)(P_1^{-1} + P_2^{-1}) + \frac{1}{8} (P_2 - P_1)(D_2 - D_1)(P_1^{-1} + P_2^{-1}) + \frac{1}{8} (P_1 + P_2)(D_2 - D_1)(P_2^{-1} - P_1^{-1}) + \frac{1}{8} (P_2 - P_1)(D_1 + D_2)(P_2^{-1} - P_1^{-1}) \right]. \]

We put

\[ L_1 = \frac{1}{8} (P_1 + P_2)(D_1 + D_2)(P_1^{-1} + P_2^{-1}) + \frac{1}{8} (P_1 + P_2)(D_2 - D_1)(P_2^{-1} - P_1^{-1}) \]
\[ = \frac{1}{8} (P_1 + P_2)[(D_1 + D_2)(P_1^{-1} + P_2^{-1}) + (D_2 - D_1)(P_2^{-1} - P_1^{-1})] \]
\[ = \frac{1}{8} (P_1 + P_2)[2(D_1 + D_2)P_2^{-1} - 2D_1(P_2^{-1} - P_1^{-1})] \]
\[ = \frac{1}{4} (P_1 + P_2)[(D_1 + D_2)P_2^{-1} - D_1(P_2^{-1} - P_1^{-1})] \]
\[ = \frac{1}{4} (P_1 + P_2)(D_1 + D_2)P_2^{-1} - \frac{1}{4} (P_1 + P_2)D_1(P_2^{-1} - P_1^{-1}). \]
On the other hand, we put

\[ L_2 = \frac{1}{8} (P_2 - P_1) (D_2 - D_1) (P_1^{-1} + P_2^{-1}) + \frac{1}{8} (P_2 - P_1) (D_1 + D_2) (P_2^{-1} - P_1^{-1}) \]
\[ = \frac{1}{8} (P_2 - P_1) [(D_1 + D_2 - 2D_1)(P_1^{-1} + P_2^{-1}) + (D_1 + D_2) (P_2^{-1} - P_1^{-1})] \]
\[ = \frac{1}{8} (P_2 - P_1) [2(D_1 + D_2)P_2^{-1} - 2D_1(P_1^{-1} + P_2^{-1})] \]
\[ = \frac{1}{4} (P_2 - P_1) [(D_1 + D_2)P_2^{-1} - D_1(P_1^{-1} + P_2^{-1})]. \]  

(41)

So that

\[ L_1 + L_2 = \frac{1}{4} (2) \frac{1}{4} (P_2)(D_1 + D_2)P_2^{-1} \]
\[ - \frac{1}{4} [P_1D_1P_2^{-1} - P_1D_1P_1^{-1} + P_2D_1P_2^{-1} - P_1D_1P_1^{-1} - P_2D_1P_1^{-1} - P_1D_1P_2^{-1} - P_1D_1P_1^{-1} - P_1D_1P_2^{-1}] \]
\[ = \frac{1}{2} P_2D_2P_2^{-1} + \frac{1}{2} P_1D_1P_1^{-1} = \frac{1}{2} (P_2D_2P_2^{-1} + P_1D_1P_1^{-1}) = \frac{1}{2} (A + B + A - B) = A. \]  

(42)

By a similar discussion, we put

\[ T_1 = \frac{1}{8} (P_1 + P_2) (D_2 - D_1)(P_1^{-1} + P_2^{-1}) + \frac{1}{8} (P_1 + P_2) (D_1 + D_2) (P_2^{-1} - P_1^{-1}) \]
\[ = \frac{1}{8} (P_1 + P_2) [(D_1 + D_2 - 2D_1)(P_1^{-1} + P_2^{-1}) + (D_1 + D_2) (P_2^{-1} - P_1^{-1})] \]
\[ = \frac{1}{4} (P_1 + P_2) [(D_1 + D_2)P_2^{-1} - D_1(P_1^{-1} + P_2^{-1})] \]
\[ = \frac{1}{4} (P_1 + P_2) (D_1 + D_2)P_2^{-1} - \frac{1}{4} (P_1 + P_2)D_1(P_1^{-1} + P_2^{-1}), \]  

(43)

\[ T_2 = \frac{1}{8} (P_2 - P_1) (D_1 + D_2)(P_1^{-1} + P_2^{-1}) + \frac{1}{8} (P_2 - P_1) (D_2 - D_1) (P_2^{-1} - P_1^{-1}) \]
\[ = \frac{1}{8} (P_2 - P_1) [(D_1 + D_2)(P_1^{-1} + P_2^{-1}) + (D_2 - D_1)(P_2^{-1} - P_1^{-1})] \]
\[ = \frac{1}{4} (P_2 - P_1) (D_1 + D_2)P_2^{-1} - \frac{1}{4} (P_2 - P_1)D_1(P_2^{-1} - P_1^{-1}). \]

(44)

So that
\[ T_1 + T_2 = \frac{1}{2} (P_2)(D_1 + D_2)P_2^{-1} \]
\[ -\frac{1}{4} \left[ P_1 D_1 P_1^{-1} + P_1 D_2 P_2^{-1} + P_2 D_1 P_1^{-1} + P_2 D_2 P_2^{-1} - P_2 D_2 P_1^{-1} - P_1 D_2 P_2^{-1} + P_1 D_1 P_2^{-1} \right] \]
\[ = \frac{1}{2} P_2 (D_1 + D_2)P_2^{-1} - \frac{1}{4} \left[ 2P_1 D_1 P_1^{-1} + 2P_2 D_2 P_2^{-1} \right] \]
\[ = \frac{1}{2} (P_2 D_2 P_2^{-1} - P_1 D_1 P_1^{-1}) \]
\[ = \frac{1}{2} [(A + B) - (A - B)] = B. \] (44)

This implies that \( X = PDP^{-1} = A + BJ \) is diagonalizable. \( \square \)

4. Algorithm for the Diagonalization of a Split-Complex Matrix

Let \( X = A + BJ \) be a split-complex matrix with \( A + B, A - B \) are diagonalizable matrices.

To diagonalize \( X \), follow these following steps:

Step 1. Diagonalize \( A + B, A - B \), i.e., find \( P_1, P_2 \) and \( D_1, D_2 \) such that \( A + B = P_2 D_2 P_2^{-1}, A - B = P_1 D_1 P_1^{-1} \).

Step 2. Put \( D = 1/2 (D_1 + D_2) + 1/2 J (D_2 - D_1), P = 1/2 (P_1 + P_2) + 1/2 J (P_2 - P_1) \), where
\[ P^{-1} = \frac{1}{2} (P_1^{-1} + P_2^{-1}) + \frac{1}{2} J (P_2^{-1} - P_1^{-1}) \]. (45)

Step 3. According to the previous theorem, we get \( X = PDP^{-1} \).

Example 9. Consider the following \( 2 \times 2 \) split-complex matrix:

\[ X = A + BJ = \begin{pmatrix} 2 & 1 \\ -1 & 3 \end{pmatrix} + \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} J = \begin{pmatrix} 2 + J & 1 + J \\ -1 + J & 3 + J \end{pmatrix}, \]

\[ A + B = \begin{pmatrix} 3 & 2 \\ 0 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 3 & 0 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^{-1}, \]

\[ A - B = \begin{pmatrix} 1 & 0 \\ -2 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}^{-1}, \]

\[ D_1 = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \]

\[ D_2 = \begin{pmatrix} 3 & 0 \\ 0 & 4 \end{pmatrix}, \]

\[ P_1 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \]

\[ P_2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \]

\[ D = \frac{1}{2} (D_1 + D_2) + \frac{1}{2} J (D_2 - D_1) = \begin{pmatrix} 2 + J & 0 \\ 0 & 3 + J \end{pmatrix}, \]

\[ P = \frac{1}{2} (P_1 + P_2) + \frac{1}{2} J (P_2 - P_1) = \begin{pmatrix} 1 & 1 + J \\ 1 - J & 1 \end{pmatrix}. \] (46)
It is easy to see that $PDP^{-1} = X$.

5. Conclusion

In this paper, we have found many novel properties and applications of split-complex numbers, where we have introduced an algorithm to diagonalize a split-complex real matrix and raising a split-complex matrix to powers. We have shown that a diagonalizable square split-complex matrix $X = A + BJ$ is diagonalizable if and only if $A + B, A - B$ are diagonalizable. Also, a formula of computing the split-complex matrix powers was obtained and proved.

Also, we have presented a generalization of RSA cryptosystem by using split-complex integers with more complexity. In addition, the foundations of split-complex number theory were established and clarified in terms of theorems and examples.

As a future research direction, we aim to use the number theoretical foundations of split-complex integers in generalizing El-Gamal cryptosystem with a novel split-complex version. In addition, the problem of representing split-complex matrices by split-complex linear transformations should be discussed, we recommend researchers to study this important problem to answer the following research question:

How can we represent a square split-complex matrix by split-complex linear function defined between two split-complex vector spaces defined in [5]?

Data Availability

The data used to support the study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

Authors’ Contributions

The contributions of all the authors are equal.

References


