Abstract:

The objective of this paper is to study for the first time the foundational concepts of number theory in 2-plithogenic rings of integers, where concepts such as symbolic 2-plithogenic congruencies, division, semi primes, and greatest common divisors.

In addition, many elementary properties will be discussed in details through many theorems and examples.

Keywords: Symbolic 2-plithogenic integer, symbolic 2-plithogenic divison, symbolic 2-plithogenic semi prime.

Introduction and basic concepts

The concept of symbolic plithogenic sets was defined by Smarandache in [13-17,30], and he suggested an algebraic approach of these sets. Laterally, the concept of symbolic 2-plithogenic rings [31]. In general, we can say that symbolic plithogenic structures are very close to neutrosophic algebraic structures with many differences in the definition of multiplication operation [1-10].

Let $R$ be a ring, the symbolic 2-plithogenic ring is defined as follows:

$2 - SP_R = \{a_0 + a_1P_1 + a_2P_2; a_i \in R, P_j^2 = P_j, P_1 \times P_2 = P_{\max(1,2)} = P_2\}$.

Smarandache has defined algebraic operations on $2 - SP_R$ as follows:
Addition:
\[ [a_0 + a_1p_1 + a_2p_2] + [b_0 + b_1p_1 + b_2p_2] = (a_0 + b_0) + (a_1 + b_1)p_1 + (a_2 + b_2)p_2. \]

Multiplication:
\[ [a_0 + a_1p_1 + a_2p_2][b_0 + b_1p_1 + b_2p_2] = a_0b_0 + a_0b_1p_1 + a_0b_2p_2 + a_1b_0p_1 + a_1b_1p_1^2 + a_1b_2p_1p_2 + a_2b_0p_2 + a_2b_1p_1p_2 + a_2b_2p_2^2 + a_1b_1p_1p_1 = a_0b_0 + (a_0b_1 + a_1b_0 + a_1b_1)p_1 + (a_0b_2 + a_1b_2 + a_2b_0 + a_2b_1 + a_2b_2)p_2. \]

It is clear that \((2 - SP_R)\) is a ring.

Also, if \( R \) is commutative, then \( 2 - SP_R \) is commutative, and if \( R \) has a unity (1), than \( 2 - SP_R \) has the same unity (1).

If \( R \) is a field, then \( 2 - SP_R \) is called a symbolic 2-plithogenic field.

In this paper, we study the symbolic 2-plithogenic number theoretical concepts according to many points of view, where congruencies, Euclidean division, Euler’s function, and greatest common divisors will be presented in terms of theorems. In addition, many examples will be illustrated to explain the novelty of these ideas. In addition, we suggest many future applications of symbolic 2-plithogenic integers in cryptography and public key neutrosophic cryptography.

**Main Discussion**

**Definition.**

Let \( A = a_0 + a_1p_1 + a_2p_2, B = b_0 + b_1p_1 + b_2p_2 \in 2 - SP_Z \), we say that \( A \setminus B \) if and only if there exists \( C \in 2 - SP_Z \) such that \( A \times B = C \).

**Definition.**

Let \( A = a_0 + a_1p_1 + a_2p_2, B = b_0 + b_1p_1 + b_2p_2, C = c_0 + c_1p_1 + c_2p_2 \) be three symbolic 2-plithogenic integers, then \( A \equiv B (\text{mod } C) \) if and only if \( C \setminus A \setminus B \).

Also, \( C = gcd(A, B) \) if and only if \( C \setminus A \) and \( C \setminus B \) and for any \( D \setminus A, D \setminus B \), then \( D \setminus C \).

**Definition.**

We say that \( A \leq B \) if \( a_0 \leq b_0, a_0 + a_1 \leq b_0 + b_1, a_0 + a_2 \leq b_0 + b_1 + b_2 \).

**Theorem.**

Let \( A = a_0 + a_1p_1 + a_2p_2, B = b_0 + b_1p_1 + b_2p_2, C = c_0 + c_1p_1 + c_2p_2 \in 2 - SP_Z \), then:

1. \( \leq \) is a partial order relation.

2. \( A \setminus B \) if and only if \( a_0 \setminus b_0, a_0 + a_1 \setminus b_0 + b_1, a_0 + a_1 + a_2 \setminus b_0 + b_1 + b_2 \).
3). \( \gcd(A, B) = C \) if and only if \( \gcd(a_0, b_0) = c_0, \gcd(a_0 + a_1, b_0 + b_1) = c_1, \gcd(a_0 + a_1 + a_2, b_0 + b_1 + b_2) = c_0 + c_1 + c_2. \)

4). \( A \equiv B(\text{mod } C) \) if and only if:

\[
\begin{align*}
& a_0 \equiv b_0 \text{ (mod } c_0) \\
& a_0 + a_1 \equiv b_0 + b_1 \text{ (mod } c_0 + c_1) \\
& a_0 + a_1 + a_2 \equiv b_0 + b_1 + b_2 \text{ (mod } c_0 + c_1 + c_2)
\end{align*}
\]

\textbf{Proof.}

1). \( A \leq A \) that is because \( a_0 \leq a_0, a_0 + a_1 \leq a_0 + a_1, a_0 + a_1 + a_2 \leq a_0 + a_1 + a_2. \)

If \( A \leq B \) and \( B \leq A \), then:

\[
\begin{align*}
& a_0 \leq b_0, b_0 \leq a_0, \text{thus } a_0 = b_0 \\
& a_0 + a_1 \leq b_0 + b_1, b_0 + b_1 \leq a_0 + a_1, \text{thus } a_0 + a_1 = b_0 + b_1, \text{ hence } a_1 = b_1 \\
& a_0 + a_1 + a_2 \leq b_0 + b_1 + b_2, b_0 + b_1 + b_2 \leq a_0 + a_1 + a_2, \text{ thus } a_0 + a_1 + a_2 = b_0 + b_1 + b_2, \text{ hence } a_2 = b_2
\end{align*}
\]

Hence \( A = B. \)

If \( A \leq B \) and \( B \leq C \), then \( a_0 \leq b_0 \leq c_0, a_0 + a_1 \leq b_0 + b_1 \leq c_0 + c_1, a_0 + a_1 + a_2 \leq b_0 + b_1 + b_2 \leq c_0 + c_1 + c_2, \) thus \( A \leq C. \)

2). If \( A \setminus B \), then there exists \( C \) such that \( A.C = B. \) This equivalents:

\[ a_0c_0 + P_1(a_0c_1 + a_1c_0 + a_1c_1) + P_2(a_0c_2 + a_2c_0 + a_2c_2 + a_1c_2 + a_2c_1) = b_0 + b_1P_1 + b_2P_2 \]

there for:

\[
\begin{align*}
& a_0c_0 = b_0 \ldots (1) \\
& a_0c_1 + a_1c_0 + a_1c_1 = b_1 \ldots (2) \\
& a_0c_2 + a_2c_0 + a_2c_2 + a_1c_2 + a_2c_1 = b_2 \ldots (3)
\end{align*}
\]

We add (1) to (2) and (1) to (2) to (3), to get:

\[
\begin{align*}
& a_0c_0 = b_0 \\
& (a_0 + a_1)(c_0 + c_1) = b_0 + b_1 \\
& (a_0 + a_1 + a_2)(c_0 + c_1 + c_2) = b_0 + b_1 + b_2
\end{align*}
\]

Thus \( a_0 \setminus b_0, a_0 + a_1 \setminus b_0, a_0 + a_1 + a_2 \setminus b_0 + b_1 + b_2. \)

3). Assume that \( \gcd(A, B) = C \), then for any \( D = d_0 + d_1P_1 + d_2P_2 \in 2 \setminus SP_z \) such that \( D \setminus A, D \setminus B \) implies \( D \setminus C. \)

According to (2), we get \( d_0 \setminus c_0, d_0 + d_1 \setminus c_0 + c_1, d_0 + d_1 + d_2 \setminus c_0 + c_1 + c_2, \) so that

\[ \gcd(a_0, b_0) = c_0, \gcd(a_0 + a_1, b_0 + b_1) = c_0 + c_1, \gcd(a_0 + a_1 + a_2, b_0 + b_1 + b_2) = c_0 + c_1 + c_2. \]

This implies that \( \gcd(A, B) = \gcd(a_0, b_0) + P_1[\gcd(a_0 + a_1, b_0 + b_1) - \gcd(a_0, b_0)] + P_2[\gcd(a_0 + a_1 + a_2, b_0 + b_1 + b_2) - \gcd(a_0 + a_1, b_0 + b_1)]. \)

4). \( A \equiv B(\text{mod } C) \) if and only if \( C \setminus A - B, \) thus:

\[ c_0 \setminus a_0 - b_0, c_0 + c_1 \setminus (a_0 + a_1) - (b_0 + b_1), c_0 + c_1 + c_2 \setminus (a_0 + a_1 + a_2) - (b_0 + b_1 + b_2) \]
So that:
\[
\begin{align*}
    a_0 &\equiv b_0 \pmod{c_0} \\
    a_0 + a_1 &\equiv b_0 + b_1 \pmod{c_0 + c_1} \\
    a_0 + a_1 + a_2 &\equiv b_0 + b_1 + b_2 \pmod{c_0 + c_1 + c_2}
\end{align*}
\]

**Theorem.**

Let \( A = a_0 + a_1 P_1 + a_2 P_2, B = b_0 + b_1 P_1 + b_2 P_2 \in 2 - SP_Z \), then \( \gcd(A, B) = 1 \) if and only if \( \gcd(a_0, b_0) = 1, \gcd(a_0 + a_1, b_0 + b_1) = 1, \gcd(a_0 + a_1 + a_2, b_0 + b_1 + b_2) = 1 \).

The proof is clear.

**Theorem.**

Let \( A, B, C, D, E \in 2 - SP_Z \), where:
\( A = a_0 + a_1 P_1 + a_2 P_2, B = b_0 + b_1 P_1 + b_2 P_2, C = c_0 + c_1 P_1 + c_2 P_2, D = d_0 + d_1 P_1 + d_2 P_2, E = e_0 + e_1 P_1 + e_2 P_2; c_i, a_i, b_i, d_i, e_i, i \in Z \), then:

1. If \( A \equiv B \pmod{C}, D \equiv E \pmod{C} \), then \( A + D \equiv B + E \pmod{C}, A - D \equiv B - E \pmod{C} \).
2. \( A, D \equiv B, E \pmod{C} \).
3. If \( \gcd(A, B) = 1 \), then:
\[
A^{-1}(\pmod{B}) = a_0^{-1}(\pmod{b_0}) + P_1 [(a_0 + a_1)^{-1}(\pmod{b_0 + b_1}) - a_0^{-1}(\pmod{b_0})] + P_2 [(a_0 + a_1 + a_2)^{-1}(\pmod{b_0 + b_1 + b_2}) - (a_0 + a_1)^{-1}(\pmod{b_0 + b_1})]
\]

**Proof.**

1. Assume that \( A \equiv B \pmod{C}, D \equiv E \pmod{C} \), thus:
\[
\begin{align*}
    a_0 &\equiv b_0 \pmod{c_0} \\
    a_0 + a_1 &\equiv b_0 + b_1 \pmod{c_0 + c_1} \\
    a_0 + a_1 + a_2 &\equiv b_0 + b_1 + b_2 \pmod{c_0 + c_1 + c_2}
\end{align*}
\]

And
\[
\begin{align*}
    d_0 &\equiv e_0 \pmod{c_0} \\
    d_0 + d_1 &\equiv e_0 + e_1 \pmod{c_0 + c_1} \\
    d_0 + d_1 + d_2 &\equiv e_0 + e_1 + e_2 \pmod{c_0 + c_1 + c_2}
\end{align*}
\]

This implies:
\[
\begin{align*}
    a_0 + d_0 &\equiv b_0 + e_0 \pmod{c_0} \\
    a_0 + a_1 + d_0 + d_1 &\equiv b_0 + b_1 + e_0 + e_1 \pmod{c_0 + c_1} \\
    a_0 + a_1 + a_2 + d_0 + d_1 + d_2 &\equiv b_0 + b_1 + b_2 + e_0 + e_1 + e_2 \pmod{c_0 + c_1 + c_2}
\end{align*}
\]

So that \( A + D \equiv B + E \pmod{C} \).

We can prove that \( A - D \equiv B - E \pmod{C} \) by a similar.

2. By using a similar discussion, we can write:
\[
\begin{align*}
    a_0 d_0 &\equiv b_0 e_0 \pmod{c_0} \\
    (a_0 + a_1)(d_0 + d_1) &\equiv (b_0 + b_1)(e_0 + e_1) \pmod{c_0 + c_1} \\
    (a_0 + a_1 + a_2)(d_0 + d_1 + d_2) &\equiv (b_0 + b_1 + b_2)(e_0 + e_1 + e_2) \pmod{c_0 + c_1 + c_2}
\end{align*}
\]
Thus \( A \cdot D \equiv B \cdot E (\text{mod } C) \).

3). Suppose that \( \gcd(A, B) = 1 \), then \( \gcd(a_0, b_0) = \gcd(a_0 + a_1, b_0 + b_1) = \gcd(a_0 + a_1 + a_2, b_0 + b_1 + b_2) = 1 \).

We put

\[
T = a_0^{-1} (\text{mod } b_0) + P_1[(a_0 + a_1)^{-1} (\text{mod } b_0 + b_1) - a_0^{-1} (\text{mod } b_0)] \\
+ P_2[(a_0 + a_1 + a_2)^{-1} (\text{mod } b_0 + b_1 + b_2) - (a_0 + a_1)^{-1} (\text{mod } b_0 + b_1)]
\]

\[
A \cdot T = a_0 a_0^{-1} (\text{mod } b_0) + P_1[(a_0 + a_1)(a_0 + a_1)^{-1} (\text{mod } b_0 + b_1) - a_0 a_0^{-1} (\text{mod } b_0)] \\
+ P_2[(a_0 + a_1 + a_2)(a_0 + a_1 + a_2)^{-1} (\text{mod } b_0 + b_1 + b_2) \\
- (a_0 + a_1)(a_0 + a_1)^{-1} (\text{mod } b_0 + b_1)] = 1 + P_1(1 - 1) + P_2(1 - 1) = 1
\]

Thus \( T = A^{-1} \).

Example.

Consider \( A = 5 + 4P_1 + 2P_2, B = 2 + P_1 + P_2, C = 3 + 4P_2 \), we have:

\[
5 \equiv 2 (\text{mod } 3), 5 + 4 = 9 \equiv (2 + 1)(\text{mod } 3 + 0), 5 + 4 + 2 = 11 \equiv (2 + 1 + 1)(\text{mod } 3 + 0 + 4), \text{ thus } A \equiv B (\text{mod } C).
\]

\[
\gcd(A, B) = \gcd(5, 2) + P_1[\gcd(9, 3) - \gcd(5, 2)] + P_2[\gcd(11, 4) - \gcd(9, 3)] = 1 + P_1(3 - 1) + P_2(1 - 3) = 1 + 2P_1 - 2P_2.
\]

Example.

Consider \( A = 2 + P_1 + P_2, B = 3 + P_1 + P_2 \), it is clear that \( \gcd(A, B) = 1 \).

\[
A^{-1} (\text{mod } B) = 2^{-1} (\text{mod } 3) + P_1[3^{-1} (\text{mod } 4) - 2^{-1} (\text{mod } 3)] + P_2[4^{-1} (\text{mod } 5) - 3^{-1} (\text{mod } 4)] = 2 + P_1(3 - 2) + P_2(4 - 3) = 2 + P_1 + P_2.
\]

Definition.

Let \( A = a_0 + a_1 P_1 + a_2 P_2 > 0 \) be a symbolic 2-plithogenic integer, we define \( \varphi_5: 2 - SP_2 \rightarrow 2 - SP_2 \) such that:

\[
\varphi_5(A) = \varphi(a_0) + P_1[\varphi(a_0 + a_1) - \varphi(a_0)] + P_2[\varphi(a_0 + a_1 + a_2) - \varphi(a_0 + a_1)].
\]

Where \( \varphi \) is the classical phi-Euler's function.

Example.

Take \( A = 3 + 5P_1 - P_2, a_0 = 3, a_1 = 5, a_2 = -1 \). We have:

\[
a_0 = 3 > 0, a_0 + a_1 = 8 > 0, a_0 + a_1 + a_2 = 7 > 0, \text{ so that } A > 0.
\]

\[
\varphi(a_0) = 2, \varphi(a_0 + a_1) = 4, \varphi(a_0 + a_1 + a_2) = 6, \text{ hence:}
\]

\[
\varphi_5(A) = 2 + P_1[4 - 2] + P_2[6 - 4] = 2 + 2P_1 + 2P_2.
\]

Theorem.

Let \( A = a_0 + a_1 P_1 + a_2 P_2, M = m_0 + m_1 P_1 + m_2 P_2 \in 2 - SP_2 \) such that \( \gcd(A, M) = 1 \), then
\[ A^{\varphi_3(M)} \equiv 1 \pmod{M}. \]

**Proof.**

According to [ ],

\[ A^{\varphi_3(M)} = a_0^{\varphi(m_0)} + P_1[(a_0 + a_1)^{\varphi(m_0+m_1)} - a_0^{\varphi(m_0)}] \]
\[ + P_2[(a_0 + a_1 + a_2)^{\varphi(m_0+m_1+m_2)} - (a_0 + a_1)^{\varphi(m_0+m_1)}] \]

Since \( \gcd(A,M) = 1 \), then \( \gcd(a_0, m_0) = \gcd(a_0 + a_1, m_0 + m_1) = \gcd(a_0 + a_1 + a_2, m_0 + m_1 + m_2) = 1 \), so that:

\[
\begin{align*}
(a_0 &\equiv 1 \pmod{m_0}) \\
(a_0 + a_1) &\equiv 1 \pmod{m_0 + m_1} \\
(a_0 + a_1 + a_2) &\equiv 1 \pmod{m_0 + m_1 + m_2}
\end{align*}
\]

Thus \( A^{\varphi_3(M)} \equiv 1 + P_1(1 - 1) + P_2(1 - 1)( \pmod{M} ) \equiv 1( \pmod{M} ) \)

**Example.**

Take \( A = 2 + 3P_1 - 2P_2, M = 3 + 4P_1 + 4P_2 \), we have \( \gcd(A,M) = 1 \).

\( \varphi_3(M) = 2 + P_1(6 - 2) + P_2(10 - 6) = 2 + 4P_1 + 4P_2 \)

\( A^{\varphi_3(M)} = 2^2 + P_1[5^6 - 2^2] + P_2[3^{10} - 5^6] \)

\( 2^2 \equiv 1( \pmod{3} ), 5^6 \equiv 1( \pmod{7} ), 3^{10} \equiv 1( \pmod{11} ) \), thus \( A^{\varphi_3(M)} \equiv 1( \pmod{M} ) \)

**Theorem.**

Let \( C = \gcd(A,B) \in 2 - SP_2 \), then there exists \( M, N \in 2 - SP_2 \) such that \( C = MA + NB \).

**Proof.**

We assume that \( C = \gcd(A,B) \), then:

\[
\begin{align*}
c_0 &= \gcd(a_0, b_0) \\
c_1 &= \gcd(a_0 + a_1, b_0 + b_1) - \gcd(a_0, b_0) \\
c_2 &= \gcd(a_0 + a_1 + a_2, b_0 + b_1 + b_2) - \gcd(a_0 + a_1, b_0 + b_1)
\end{align*}
\]

So there exists \( m_0, n_0, m_1, n_1, m_2, n_2 \in \mathbb{Z} \) such that:

\[
\begin{align*}
c_0 &= m_0a_0 + n_0b_0 \\
c_0 + c_1 &= m_1(a_0 + a_1) + n_1(n_0 + n_1) \\
c_0 + c_1 + c_2 &= m_2(a_0 + a_1 + a_2) + n_2(b_0 + b_1 + b_2)
\end{align*}
\]

We put \( M = m_0 + (m_1 - m_0)P_1 + (m_2 - m_1)P_2, N = n_0 + (n_1 - n_0)P_1 + (n_2 - n_1)P_2 \), now let us compute:

\[
\begin{align*}
M.A &= [m_0 + (m_1 - m_0)P_1 + (m_2 - m_1)P_2][a_0 + a_1P_1 + a_2P_2] \\
M.A &= m_0a_0 + P_1(m_0a_1 + m_1a_0 - m_0a_0 + m_1a_1 - m_0a_1) \\
&\quad + P_2(m_0a_2 + m_2a_0 - m_1a_0 + m_2a_1 - m_1a_1 + m_1a_2 - m_0a_2 + m_2a_2 - m_1a_2) \\
M.A &= m_0a_0 + P_1(m_1a_0 + m_1a_1 - m_0a_0) \\
&\quad + P_2(m_2a_0 - m_1a_0 + m_2a_1 - m_1a_1 + m_1a_2 + m_2a_2) \\
N.B &= n_0b_0 + P_1(n_1b_0 + n_1b_1 - n_0b_0) + P_2(n_2b_0 - n_1b_0 + n_2b_1 - n_1b + n_1b_2 + n_2b_2)
\end{align*}
\]
\[ MA + NB = (m_0a_0 + n_0b_0) + p_1[m_1(a_0 + a_1) + n_1(b_0 + b_1) - n_0b_0 - m_0a_0] \\
+ p_2[m_2(a_0 + a_1 + a_2) + n_2(b_0 + b_1 + b_2) - m_1(a_0 + a_1) - n_1(b_0 + b_1)] \\
= c_0 + c_1p_1 + c_2p_2 = C \]

**Example.**

Consider \( A = 3 + 2p_1 + p_2, B = 3 + p_1 + 3p_2 \), we have:

\[ a_0 = 3, a_1 = 2, a_2 = 1, b_0 = 3, b_1 = 1, b_2 = 3. \]

\[ gcd(a_0, b_0) = 3, gcd(a_0 + a_1, b_0 + b_1) = gcd(5, 4) = 1, gcd(a_0 + a_1 + a_2, b_0 + b_1 + b_2) = gcd(6, 7) = 1 \]

Thus \( gcd(A, B) = 3 + (1 - 3)p_1 + (1 - 1)p_2 = 3 - 2p_1. \)

On the other hand, we have:

\[ \begin{align*}
3 &= \frac{1.3}{0.3} \text{ hence } m_0 = 1, n_0 = 0 \\
1 &= \frac{1.5 - 1.4}{1} \text{ hence } m_1 = 1, n_1 = -1 \\
1 &= \frac{-1.6 + 1.7}{1} \text{ hence } m_2 = -1, n_2 = 1
\end{align*} \]

Thus \( M = 1 + (1 - 3)p_1 + (-1 - 1)p_2 = 1 - 2p_2, N = 0 + (-1 - 0)p_1 + (1 + 1)p_2 = -p_1 + 2p_2 \)

We can see that:

\[ MA + NB = (1 - 2p_2)(3 + 2p_1 + p_2) + (-p_1 + 2p_2)(3 + p_1 + 3p_2) \\
= 3 + 2p_1 + p_2 - 6p_2 - 4p_2 - 2p_2 - 3p_1 - p_1 - 3p_1 + 6p_2 + 2p_2 + 6p_2 \\
= 3 - 2p_1 = C = gcd(A, B) \]

**Definition.**

Let \( S = s_0 + s_1p_1 + s_2p_2 \in 2 - SP_2 \), we say that \( S \) is a 2-plithogenic semi prime if \( s_0, s_0 + s_1, s_0 + s_1 + s_2 \) are primes.

**Example.**

The 2-plithogenic integer \( S = 2 + p_1 + 2p_2 \) is a semi prime, that is because \( s_0 = 2, s_0 + s_1 = 3, s_0 + s_1 + s_2 = 5 \) are primes.

**Application In Future Studies**

Symbolic 2-plithogenic number theory as a new research direction maybe very useful branches of knowledge.

We suggest the following research points that symbolic 2-plithogenic integers may have a very big effect on it.

1). How can we use symbolic 2-plithogenic integers in the improvement of crypto-systems [39-41], for example:

a). How can we build a 2-plithogenic version of RSA algorithm.

b). How can we build a 2-plithogenic version of Diffie-Hellman key exchange algorithm.
c). How can we build a 2-plithogenic version of EL-Gamal algorithm for cryptography.

2-). How can we a solve non-linear symbolic 2-plithogenic Diophantine equations and congruencies.

References


Received: December 26, 2022. Accepted: March 29, 2023