Smarandache Rings and Smarandache Elements

Parween A. Hummadi
College of Education
University of Salahaddin
Iraq

Shadan A. Osman
College of Science
University of Salahaddin
Iraq

Received on: 21/6/2012
Accepted on: 18/9/2012

ABSTRACT

In this paper, we study some Smarandache (S) notions in some types of rings. Conditions are given under which $\mathbb{Z}_n$ is a Smarandache ring. We study Smarandache ideals, Smarandache subrings and Smarandache weakly Boolean rings. We discuss some types of Smarandache elements in rings. Moreover, we get some other results.

Keywords: Smarandache ring, Smarandache ideal, Smarandache subring, Smarandache weakly Boolean ring, Smarandache SS-element, Smarandache super idempotent and Smarandache semi idempotent.

1. Introduction

Smarandache ring (S-ring) is introduced by F. Smarandache [1], it is defined to be a ring $\mathcal{R}$ (not necessary commutative), such that a proper subset of $\mathcal{R}$ is a field with respect to the operations induced. In [2] Vasantha Kandasamy introduced many Smarandache concepts such as; S-ideal (A Smarandache ideal is defined as an ideal $\mathcal{J}$, such that a proper subset of $\mathcal{J}$ is a field with respect with the same operations induced), S-subring( Let $\mathcal{R}$ be a ring. A proper subset $\mathcal{S}$ of $\mathcal{R}$ is said to be a Smarandache subring of $\mathcal{R}$ if $\mathcal{S}$ has a proper subset $\mathcal{F}$ which is a field and $\mathcal{S}$ is a subring of $\mathcal{R}$), weakly Boolean rings (Let $\mathcal{R}$ be a ring. We say $\mathcal{R}$ is a weakly Boolean ring if $x^{n(x)} = x$ for all $x \in \mathcal{R}$ and some natural number $n(x) > 1$), Smarandache weakly Boolean rings (Let $\mathcal{R}$ be a ring. We say $\mathcal{R}$ is Smarandache weakly Boolean ring, if we have a S-subring $\mathcal{S}$ of $\mathcal{R}$ such that $\mathcal{S}$ is a weakly Boolean ring). In section one of this paper we give conditions under which $\mathbb{Z}_n$, is a Smarandache ring and we study Smarandache ideals, Smarandache subrings and Smarandache weakly Boolean rings. In section two, we discuss some types of Smarandache elements in rings such as Smarandache SS-element, S-super idempotent and S-semi idempotent elements.

2. Substructures in Smarandache rings

In this section we give conditions under which $\mathbb{Z}_n$ is a Smarandache ring and which answer an open problem given by W. B. Vasantha Kandasamy [2] and we get some other results.

Theorem 2.1
If $n$ has the prime factorization $n = p_1^{a_1} p_2^{a_2} \ldots p_m^{a_m}$ $q$ ($p_i, q$ are distinct primes), $a_i \geq 1(1 \leq i \leq m)$, then $\mathbb{Z}_n$ is an S-ring.

Proof: Let $\mathcal{H}$ be the principal ideal of $\mathbb{Z}_n$ generated by $= p_1^{a_1} p_2^{a_2} \ldots p_m^{a_m}$. This means that $\mathcal{H} = \{0, \gamma, 2\gamma, \ldots, (q-1)\gamma\}$. We claim that $\mathcal{H}$ is a field. Suppose there exist $a, b \in \mathcal{H}$ such that $a \neq 0$, $b \neq 0$ and $ab \equiv 0 \pmod{n}$. Since $a, b \in \mathcal{H}$ then $a = r_1 p_1^{a_1} p_2^{a_2} \ldots p_m^{a_m}$ and $b = r_2 p_1^{a_1} p_2^{a_2} \ldots p_m^{a_m}$ for some $r_1, r_2 \in \{1, 2, \ldots, q-1\}$. Thus

\[ r_1 r_2 p_1^{2a_1} p_2^{2a_2} \ldots p_m^{2a_m} \equiv 0 \pmod{n}, \]

so

\[ r_1 r_2 p_1^{a_1} p_2^{a_2} \ldots p_m^{a_m} = k \]

for some integer $k$, thus

\[ q \mid r_1 r_2 p_1^{a_1} p_2^{a_2} \ldots p_m^{a_m} = k q, \]

so $q \mid r_1 r_2$ since each $p_i$ is a prime number. Hence either $q \mid r_1$ or $q \mid r_2$, which is a contradiction. Therefore $\mathcal{H}$ has no divisors of zero. Since $(\gamma, q) = 1$, the linear congruence $\gamma x \equiv 1 \pmod{q}$, has a unique solution modulo $q$ say $x_0 \equiv 1$. Now, $\gamma x_0 \in \mathcal{H}$ and $\gamma x_0 = 1 + kq$ for some integer $k$. Hence for each $\gamma \in \mathcal{H}$ ($1 \leq i \leq q-1$),

\[ iy = i y (1+qk) = iy + ikq = iy \pmod{q}. \]

Therefore $\gamma x_0$ is an identity element of $\mathcal{H}$, therefore $\mathcal{H}$ is an integral domain. Consequently it is a field.

Example 2.1

Consider $\mathbb{Z}_{180} = \mathbb{Z}_{2^2 \cdot 3^2 \cdot 5}$. Using the notations in Theorem 2.1, $\mathcal{H} = \langle 2^2 \cdot 3^2 \rangle$, $q = 5$, thus $\mathcal{H} = \{0, 36, 72, 108, 144\}$ is a field. Since $5 \mid (36-1)$, hence 36 acts as the identity element. This implies that $\mathbb{Z}_{180}$ is an S-ring.

We remark that $\mathbb{Z}_n$ is not an S-ring where $p$ is prime, since it has no non-trivial ideals.

Theorem 2.2

If $n = p_1^{a_1} p_2^{a_2} \ldots p_m^{a_m}$, $a_i \geq 2$, $p_i$ are distinct prime numbers ($1 \leq i \leq m$), then $\mathbb{Z}_n$ is not an S-ring.

Proof: Since $\mathbb{Z}_n$ is a principal ideal ring, every ideal of $\mathbb{Z}_n$ is of the form $(p_1^{\beta_1} p_2^{\beta_2} \ldots p_m^{\beta_m})$ where $(0 \leq \beta_i \leq a_i)$ and $(1 \leq i \leq m)$. If $J$ is an ideal of $\mathbb{Z}_n$, then $J$ contains an element $x$ of the form $x = p_1 p_2 \ldots p_n$. Put $r = \max \{a_1, a_2, \ldots, a_n\}$. Hence $x^r = (p_1 p_2 \ldots p_n)^r = k p_1^{a_1} \ldots p_m^{a_m}$, for some positive integer $k$, which implies that $x^r \equiv 0 \pmod{n}$, hence each ideal $J$ contains a non zero nilpotent element, therefore no ideal of $\mathbb{Z}_n$ is a field.

Proposition 2.3

If $\mathcal{R}$ is a Boolean ring different from $\mathbb{Z}_2$, then $\mathcal{R}$ is an S-ring.

Proof: Suppose $\mathcal{R}$ is finite. Since $\mathcal{R} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \ldots \oplus \mathbb{Z}_2$ [4]. Consider $\mathcal{F} = \mathbb{Z}_2 \oplus \{0\} \oplus \ldots \oplus \{0\}$. $\mathcal{F}$ is a subring of $\mathcal{R}$ which is isomorphic to $\mathbb{Z}_2$. Thus $\mathcal{F}$ is a subfield of $\mathcal{R}$, hence $\mathcal{R}$ is an S-ring.

Now, suppose $\mathcal{R}$ is an infinite Boolean ring and let $0 \neq a \in \mathcal{R}$. Consider $\mathcal{F} = \{0, a\}$. Then $a + a = 0$ and $a^2 = a$, hence $a$ acts as the identity element, this implies that $\mathcal{F}$ is a subfield of $\mathcal{R}$.

Lemma 2.4

Let $m$ and $n$ be positive integers. If $m$ divides $n$, then there exists a ring homomorphism from $\mathbb{Z}_n$ onto $\mathbb{Z}_m$.

Proof: Define $\phi: \mathbb{Z}_n, +, \cdot \rightarrow (\mathbb{Z}_m, +, \cdot)$ by $\phi(x) = x \pmod{m}$. It is easy to show that $\phi$ is an onto ring homomorphism [5].

Proposition 2.5
If \( n = pq \) or \( n = p^m \) (\( p \) and \( q \) are distinct primes), \( m \geq 2 \), then there exists an ideal \( I \) of \( \mathbb{Z}_n \) such that \( \mathbb{Z}_n/I \) is not an \( S \)-ring.

**Proof:** If \( n = pq \), then \( \mathbb{Z}_n \cong \langle p \rangle \oplus \langle q \rangle \). Consequently, \( \mathbb{Z}_n/(\langle p \rangle \oplus \langle q \rangle) \cong \langle p \rangle \oplus \langle q \rangle \cong \langle p \rangle \). Clearly \( \langle p \rangle = \langle q \rangle = \langle p \rangle \), which implies that \( \langle p \rangle \cong \mathbb{Z}_n \) and \( \langle q \rangle \cong \mathbb{Z}_n \). Therefore, \( \mathbb{Z}_n/I \) is not an \( S \)-ring. If \( n = p^m \), let \( r = p^i \) (\( 1 \leq i \leq m \)). Then by Lemma 2.4 there exists an onto ring homomorphism \( \phi: (\mathbb{Z}_n,+) \to (\mathbb{Z}_r,+). \) Hence \( \mathbb{Z}_n/\ker \phi \cong \mathbb{Z}_{p^i} \) (by fundamental theorem on ring homomorphism). Therefore \( \mathbb{Z}_n/\ker \phi \) is not an \( S \)-ring.

**Proposition 2.6**

If \( p \), \( q \), and \( r \) are distinct primes and \( p^i \) is not of the form \( pq \), then \( \mathbb{Z}_n/I \) is an \( S \)-ring for some ideal \( I \) of \( \mathbb{Z}_n \).

**Proof:** By Lemma 2.4, there exists an onto ring homomorphism \( \phi: (\mathbb{Z}_n,+) \to (\mathbb{Z}_{p^i},+). \) Hence \( \mathbb{Z}_n/\ker \phi \cong \mathbb{Z}_{p^i} \), consequently, is an \( S \)-ring.

**Lemma 2.7**

The number of ideals of the ring \( \mathbb{Z}_n \), where \( n = p_1 p_2 \ldots p_m \), is equal to \( (\alpha_1+1)(\alpha_2+1)\ldots(\alpha_m+1) \).

**Proof:** \( (\mathbb{Z}_n,+) \) is a cyclic group of order \( n \), hence by [5] for each divisor \( k \) of \( n \), \( \mathbb{Z}_n \) contains exactly one subgroup of order \( k \) and by [3] the number of positive divisors of \( n \) is \( (\alpha_1+1)(\alpha_2+1)\ldots(\alpha_m+1) \). But each subgroup of \( \mathbb{Z}_n \) is an ideal of the ring \( \mathbb{Z}_n \), therefore the number of ideals is \( (\alpha_1+1)(\alpha_2+1)\ldots(\alpha_m+1) \).

**Theorem 2.8**

The number of \( S \)-ideals of the ring \( \mathbb{Z}_n \), where \( n = p_1 p_2 \ldots p_r \), \( r \geq 2 \) and \((p_1 < p_2 < \cdots < p_r)\) equal to \( \sum_{i=1}^{r} \binom{r}{i} - r \).

**Proof:** By Theorem 1.1 the number of ideals of \( \mathbb{Z}_n \) which are fields is \( r \), namely \( \langle p_1 \rangle, \langle p_2 \rangle, \ldots, \langle p_r \rangle \). Clearly no ideal of them is \( S \)-ideal. The ideal \( \langle p_i \rangle \) generated by \( p_i \) is of order \( p_1 p_2 \ldots p_r \), so it contains the element \( p_1 p_2 \ldots p_{i-1} \). Hence \( \langle p_1 p_2 \ldots p_{i-1} \rangle \subseteq \langle p_i \rangle \), but \( \langle p_1 p_2 \ldots p_{i-1} \rangle \) is a field, therefore \( \langle p_i \rangle \) is a \( S \)-ideal. A similar argument shows that all \( \langle p_i \rangle, (2 \leq i \leq r) \) are \( S \)-ideals.

Now, consider \( \langle p_1 p_2 \rangle \), the ideal generated by \( p_1 p_2 \), its order is \( p_1 p_2 \ldots p_r \), so it also contains \( p_1 p_2 \ldots p_{i-1} \), hence \( \langle p_1 p_2 \rangle \subseteq \langle p_i \rangle \). Therefore \( \langle p_1 p_2 \rangle \) is \( S \)-ideal. By similar way if we choose any two distinct primes \( p_i, p_j \) from \( \{p_1, p_2, \ldots, p_r\} \), then \( \langle p_i p_j \rangle \) is a \( S \)-ideal for \( 1 \leq i, j \leq r, i \neq j \). Continuing in this manner the ideal generated by multiple of \( r - 2 \) primes from \( \{p_1, p_2, \ldots, p_r\} \) is \( S \)-ideal. Consequently we get that the number of \( S \)-ideals is \( \sum_{i=1}^{r} \binom{r}{i} - r \).

Note that, by Lemma 2.7, the number of non zero ideals of \( \mathbb{Z}_n \) is \( 2^r - 1 = \sum_{i=1}^{r} \binom{r}{i} \).

**Theorem 2.9**

Let \( \mathcal{R} = F_1 \oplus F_2 \oplus \ldots \oplus F_n \) where \( n \geq 2 \) and \( F_i \) is a non prime field. Then every non-trivial ideal of \( \mathcal{R} \) is an \( S \)-ideal.

**Proof:** Let \( J \) be a non zero proper ideal of the ring \( \mathcal{R} \). Then by [6] \( J \) is of the form \( J = I_1 \oplus I_2 \oplus \ldots \oplus I_n \), where \( I_i \) is an ideal of \( F_i \), \( 1 \leq i \leq n \). Hence at least one of \( I_i \) say \( I_k \neq \{0\} \), then \( I_k = F_k \), but \( F_k \) is not a prime field. If \( F_k \) is of characteristic 0 then by [7] \( F_k \) contains a proper subfield which is isomorphic to \( \mathbb{Q} \), hence \( \{0\} \oplus \ldots \oplus \{0\} \oplus \mathbb{Q} \oplus \{0\} \oplus \ldots \oplus \{0\} \) can be considered as a subfield of \( J \). If \( F_k \) has a prime characteristic \( p \), then by [7] \( F_k \) contains a proper subfield which is isomorphic to \( \mathbb{Z}_p \), hence \( \{0\} \oplus \ldots \oplus \{0\} \oplus \mathbb{Z}_p \oplus \{0\} \oplus \ldots \oplus \{0\} \) is a subfield of \( J \). Consequently, \( J \) is an \( S \)-ideal.
Theorem 2.10
Let $\mathcal{R} = F_1 \oplus F_2$, where $F_1$ and $F_2$ are prime fields. Then no ideal of $\mathcal{R}$ is an $S$-ideal.

**Proof:** Since each $F_i$ is a prime field, $\mathcal{R}$ has only two nonzero proper ideals, namely $J_i = F_i \oplus \{0\}$ and $J_2 = \{0\} \oplus F_2$, and clearly $J_i, i = 1, 2$ never contains a subfield, hence $J_i, i = 1, 2$ is not an $S$-ideal

Theorem 2.11
Let $n = p^m q r$ $(m \geq 2)$, $p, q$ and $r$ are distinct primes $(p < q < r)$. If $q - 1 | r - 1$, then $\mathbb{Z}_n$ is an $S$-weakly Boolean ring.

**Proof:** By Theorem 2.1 $\mathbb{Z}_n$ is an $S$-ring and $F = \langle p^m q \rangle$ is a subfield of $\mathbb{Z}_n$. It is clear that the subring $\mathcal{H} = \langle p^m \rangle$ generated by $p^m$ is a $S$-subring. We claim that $(ip^m)^{r - i \mod n}, (1 \leq i \leq qr)$.

Case 1: $(i, qr) = 1$ consequently $(ip^m \mod qr) = 1$. Then by $[3]$ $(ip^m)^{r - 1 \mod qr}$, which implies that $(ip^m)^{r - 1 \mod qr} = 1 + kqr$, for some integer $k$, hence $(ip^m)^{r - 1 \mod qr} = ip^m + ikp^m qr$, therefore $(ip^m)^{r - 1 \mod qr} = ip^m (mod n)$.

Case 2: $(i, qr) \neq 1$, in this case either $(i, q) \neq 1$ or $(i, r) \neq 1$, if $(i, r) \neq 1$, then $i = br$, for some integer $l < q$.

Now, $\frac{i^r (ip^m)^{r - i \mod qr}}{p^m qr} = \frac{(br)^r (p^m)^{r - 1 \mod qr}}{qr} = \frac{l (br)^r (p^m)^{r - 1 \mod qr}}{q}$ \hspace{1cm} (1).

Since $q \not\mid lrp^m$ hence by $[3]$ $(lrp^m)^{q - 1 \mod qr} = 1 \mod q$, then $(lrp^m)^{q - 1 \mod qr} = k_1 q$,
for some integer $k_1$, substituting in equation (1) we get $\frac{i^r (ip^m)^{r - i \mod qr}}{p^m qr} = \frac{k_1 ((lrp^m)^{r - 1 \mod qr}}{((lrp^m)^{q - 1 \mod qr})}$.

But by hypothesis $q - 1 | r - 1$, we obtain $\frac{i^r (ip^m)^{r - i \mod qr}}{p^m qr} = k_2$,
for some integer $k_2$, therefore $(ip^m)^r \equiv ip^m \mod n$.

If $(i, q) \neq 1$, then $i = tq$, for some positive $t < r$. By the same way, we get $\frac{i^r (ip^m)^{r - i \mod qr}}{p^m qr} = \frac{t k_3 ((tpq)^{r - 1 \mod qr}}{((tpq)^{q - 1 \mod qr})}$.

Therefore $\frac{i^r (ip^m)^{r - i \mod qr}}{p^m qr} = k_3$ for some integer $k_3$, which implies that $(ip^m)^r \equiv ip^m \mod n$. This completes the proof.

Theorem 2.12
The group ring $\mathbb{Z}_2 G$, where $G = \langle g \mid g^m = 1 \rangle$ is a cyclic group of an odd order \hspace{1cm} $m > 1$ is an $S$-weakly Boolean ring.

**Proof:** Let $\mathcal{S} = \{0, 1, g + g^2 + \cdots + g^{m - 1}, 1 + g + g^2 + \cdots + g^{m - 1} \}$. It is clear that $(\mathcal{S} , +)$ is an additive group, we must prove that $\mathcal{S}$ is closed under multiplication,

$$(g + g^2 + \cdots + g^{m - 1})(1 + g + g^2 + \cdots + g^{m - 1}) =$$

$$= 1 + g + \cdots + g^{m - 1} + g + g^2 + \cdots + g^{m - 1} + 1 + \cdots + g + g^2 + \cdots + g^{m - 1} + 1 =$$

$$(m - 1) + (m - 1)g + (m - 1)g^2 + \cdots + (m - 1)g^{m - 1} = 0,$$

since $m - 1 \equiv 0 \mod 2$. Hence $\mathcal{S}$ is a subring of $\mathbb{Z}_2 G$, but $\{0, 1\} \subset \mathcal{S}$, thus $\mathcal{S}$ is a $S$-subring. Now

$$(g + g^2 + \cdots + g^{m - 1})^2 = g^2 + g^4 + \cdots + \left(\frac{m - 1}{2}\right)^2 + \left(g^{m - 1}/2\right)^2 + \cdots + (g^{m - 1})^2$$

$$= g^2 + g^4 + \cdots + g^{m - 1} + g + \cdots + g^{m - 2}$$

and also

$$(1 + g + g^2 + \cdots + g^{m - 1})^2 = 1 + g + g^2 + \cdots + g^{m - 1}.$$
Definition 3.1 [2]
Let \( R \) be a ring. An element \( x \in R \) is said to be a Smarandache SS-\( x \) element of \( R \), if there exists \( y \in R \setminus \{x\} \) with \( xy = x + y \). An element \( a \in R \setminus \{0, 2\} \) is an SS-element if \( a^2 = a + a \).

Definition 3.2 [2]
Let \( R \) be a ring. If \( R \) has at least one nontrivial Smarandache SS-element we call \( R \) a Smarandache SS-ring.

Definition 3.3 [2]
Let \( R \) be a ring. An element \( 0 \neq x \in R \) is a Smarandache idempotent (S-idempotent) of \( R \) if
1) \( x^2 = x \).
2) There exists \( y \in R \setminus \{0, 1, x\} \)
   i) \( y^2 = x \) and
   ii) \( xy = y \) (\( xy = y \)) or \( yx = x \) (\( xy = x \)).

Definition 3.4 [2]
Let \( R \) be a ring. An element \( 0 \neq \alpha \in R \) is called a Smarandache super idempotent (S- super idempotent) of \( R \), if \( \alpha^2 = \alpha \) is an S-idempotent of \( R \).

Proposition 3.5
If \( n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_m^{\alpha_m} \) is the prime factorization of \( n \), not all \( \alpha_i = 1 \), and \( n \) is not of the form \( 2^{2a} \), then \( \mathbb{Z}_n \) is Smarandache SS-ring.

Proof: First if \( \alpha_i \neq 1 \) for each \( 1 \leq i \leq m \), take
\[ x = p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \ldots p_m^{\alpha_m - 1}, \quad y = n - x. \]
Thus \( x + y \equiv 0 \pmod{n} \) and
\[ xy = n - n p_1^{\alpha_1 - 2} p_2^{\alpha_2 - 2} \ldots p_m^{\alpha_m - 2} \equiv 0 \pmod{n}. \]
Therefore \( x + y = xy \). Hence \( x \) is Smarandache SS-element.

Second if \( \alpha_i = 1 \) for some \( 1 \leq i \leq m \), let \( \mathcal{A} = \{\alpha_j : \alpha_j = 1\} \).
Take \( x = \prod_{\alpha_i \in \mathcal{A}} p_i^{\alpha_i - 1} \prod_{\alpha_j \in \mathcal{A}} p_j^{\alpha_j} \), \( y = n - x \).
Hence \( x + y \equiv 0 \pmod{n} \) and
\[ xy = x n - k n, \quad \text{for some integer } k, \]
\[ \equiv 0 \pmod{n}. \]
Hence \( x \) is a Smarandache SS-element.

Proposition 3.6
Let \( \mathbb{Z}_2 \) be the ring of integers modulo 2 and \( G = \langle g \mid g^n = 1 \rangle \) be the cyclic group of order \( n \). Then the group ring \( \mathbb{Z}_2 G \) is a Smarandache SS-ring.

Proof: Let \( a = 1 + g \) and \( b = 1 + g^{n-1} \). Then \( a + b = g + g^{n-1} \) and \( ab = (1 + g)(1 + g^{n-1}) = g + g^{n-1} \), this implies that \( x + y = xy \). Hence \( \mathbb{Z}_2 G \) has nontrivial Smarandache SS-element, therefore \( \mathbb{Z}_2 G \) is a Smarandache SS-ring.

When we search for Smarandache SS-elements of \( \mathbb{Z}_p \), we form an opinion that \( \mathbb{Z}_p \) has the maximum number of pairs of Smarandache SS-elements, by using MATLAB program for testing many \( p \). This program is very important because implementing Smarandache SS-element of \( \mathbb{Z}_p \) for large \( p \) is difficult, but due to this program we obtain the result in a short period of time. For a prime number of the form \( n^2 + n - 1(n \geq 4) \), we obtain six pairs of Smarandache SS-elements as it is shown in the following theorem.

Theorem 3.7
Let \( p \) be a prime of the form \( n^2 + n - 1 \) \((n \geq 4)\). Then each of the following pairs \( \left(\frac{p+1}{2}, p-1\right), \left(3\frac{p+1}{2} + 1\right), (n+1, n+2), (n+3, n^2+1), (n, n^2-2) \) and \((n^2-1, n^2)\) is Smarandache SS-elements of \( \mathbb{Z}_p \).

**Proof:** Let \( x = \frac{p+1}{2} \) and \( y = p - 1 \). Thus \( xy - x - y = \frac{p+1}{2}(p-1) - \frac{p+1}{2} - (p-1) = \frac{p-3}{2} p \equiv 0 \pmod{p} \), since \( \frac{p-3}{2} \in \mathbb{Z}^+ \). Hence \( xy \equiv x + y \pmod{p} \).

Let \( x = 3 \) and \( y = \frac{p+1}{2} + 1 \). Then \( xy - x - y = 3 \frac{p+1}{2} + 3 - 3 \frac{p+1}{2} - 1 \equiv 0 \pmod{p} \).

This implies that \( xy \equiv x + y \pmod{p} \). Let \( x = n + 1 \) and \( y = n + 2 \). Then \( xy - x - y = n^2 + 3n + 2 - 2n - 3 \equiv 0 \pmod{p} \). Therefore, \( xy \equiv x + y \pmod{p} \).

Let \( x = n + 3 \) and \( y = n^2 + 1 \). Thus \( xy - x - y = n^3 + 3n^2 + n + 3 - n - 3 - n^2 - 1 = (n+1)p \equiv 0 \pmod{p} \). Hence \( xy \equiv x + y \pmod{p} \).

Let \( x = n \) and \( y = n^2 - 2 \). Then \( xy - x - y = n^3 - 2n - n - n^2 + 2 = (n-2)p \equiv 0 \pmod{p} \). Therefore \( xy \equiv x + y \pmod{p} \). Let \( x = n^2 - 1 \) and \( y = n^2 \). Then \( xy - x - y = n^4 - n^2 - n^2 + 1 - n^2 = n^2 + n - 1 + n^4 - 4n^2 - n + 2 \equiv 0 \pmod{p} \).

This implies that \( xy \equiv x + y \pmod{p} \).

The following example shows the existence of more than six pairs of Smarandache SS-elements.

**Example 3.1**

Consider \( \mathbb{Z}_{71} \). We use the following MATLAB program for evaluating the pairs of Smarandache SS-elements, and we plot them.

**MATLAB program**

```matlab
function g = ss-element(p)
    k=0;
    for i = 3 : p-2
        for j = i+1:p-1
            if mod(i + j, p)==mod(i+j, p)
                k = k+1;
                a(k, :)=[i j];
            end
        end
    end
    a=[a a];
    g1=a(:,1);
    g2=a(:,2);
    plot(g1,g2)
end
```
In the following figure we plot all Smarandache SS-elements

Hence we obtain 34 pairs of SS-elements, they are
(3, 37), (4, 25), (5, 19), (6, 58), (7, 13), (8, 62), (9, 10), (11, 65), (12, 14), (15, 67), (16, 20), (17, 41), (18, 47), (21, 33), (22, 45), (23, 43), (24, 35), (26, 55), (27, 42), (28, 51),
(29, 34), (30, 50), (31, 46), (32, 56), (36, 70), (38, 49), (39, 44), (40, 52), (48, 69), (53, 57),
(54, 68), (59, 61), (60, 66) and (63, 64).

**Definition 3.8** [2]

Let \( \mathcal{R} \) be a ring. An element \( \alpha \in \mathcal{R} \setminus \{0\} \) is said to be a Smarandache semi
idempotent (S-semi idempotent), if the ideal generated by \((\alpha^2 - \alpha)\) that is \(\mathcal{R}(\alpha^2 - \alpha)\mathcal{R}\) is an S-ideal and \(\alpha \notin \mathcal{R}(\alpha^2 - \alpha)\mathcal{R}\) or \(\mathcal{R} = \mathcal{R}(\alpha^2 - \alpha)\mathcal{R}\).

**Example 3.2**

Let \( \mathbb{Z}_{24} \) be the ring of integers modulo 24. Take \( \alpha = 5 \in \mathbb{Z}_{24} \), and consider the ideal generated by \(\alpha^2 - \alpha\). Thus \(\langle \alpha^2 - \alpha \rangle = \langle 20 \rangle = \{0, 20, 16, 12, 4, 8\} = \mathcal{J}\) is an S-ideal, since \(\mathcal{F} = \{0, 8, 16\} \subset \mathcal{J}\) is a field. Hence \(5 \in \mathbb{Z}_{24}\) is an S-semi idempotent elements of \(\mathbb{Z}_{24}\).

**Theorem 3.9**

If \(\mathcal{R}\) has S-semi idempotent elements, then \(\mathcal{R}\) has an S-ideal.

**Proof:** The proof is an immediate consequence of the definition of S-semi idempotent element.

The converse of this theorem is not true in general, for example, if we take \(\mathcal{R} = \mathbb{Z}_{18}\), then \(\mathcal{R}\) has an S-ideal but has no S-semi idempotent element.

**Theorem 3.10**

Let \(\mathbb{Z}_n\) be the ring of integers modulo \(n\) and \(n = p_1^{\alpha_1} \ldots p_m^{\alpha_m} q\) be the prime factorization of \(n\) not of the form \(pq\). If there exists \(i\) \((1 \leq i \leq m)\) such that \((p_i - 1, n) = 1\), then \(\mathbb{Z}_n\) has an S-semi idempotent element.
Proof: Choose $p_i$ such that $(p_i - 1, n) = 1$ and let $\alpha = n - (p_i - 1)$.

Thus $(\alpha^2 - \alpha) = ((n - (p_i - 1))^2 - n + (p_i - 1))$

$= \langle p_i^2 - p_i \rangle = \langle p_i(p_i - 1) \rangle$.

We will show that $\langle p_i \rangle = \langle p_i(p_i - 1) \rangle$. By [7] the ideal $\langle p_i \rangle$ generated by $p_i$ contains $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{i-1}^{\alpha_{i-1}} \cdots p_m^{\alpha_m} q$ elements. Also the ideal $\langle p_i(p_i - 1) \rangle$ generated by

$p_i(p_i - 1)$ likewise contains $p_1^{\alpha_1} \cdots p_{i-1}^{\alpha_{i-1}} \cdots p_m^{\alpha_m} q$ elements, hence $o(\langle p_i \rangle) = o(\langle p_i(p_i - 1) \rangle)$. Then by [5], $\langle p_i \rangle = \langle p_i(p_i - 1) \rangle$. Clearly $\alpha \notin \langle p_i \rangle$ and

$\langle p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}, p_i \rangle \subset \langle p_i \rangle$, hence $\langle p_i \rangle$ is an S-ideal, therefore $\mathbb{Z}_n$ has S-semi idempotent.

Remark 3.11

A Boolean ring has no S-semi idempotent elements, since $\langle \alpha^2 - \alpha \rangle = \langle 0 \rangle$ is not an S-ideal.

Theorem 3.12

If $\mathbb{Z}_n$ has an S-idempotent element which is the product of two consecutive numbers, then $\mathbb{Z}_n$ has super idempotent.

Proof: Let $k = l(l + 1)$ be an S-idempotent. Thus $k^2 = l(l + 1)$. Since

$(l + 1)^2 - (l + 1) = l^2 + l = k$, then $l + 1$ is super idempotent which is a S-idempotent, also $n - l$ is super idempotent since

$(n - l)^2 - (n - l) = n^2 - 2nl + l^2 - n + l = l(l + 1) = k$.

Theorem 3.13

If $\alpha$ is an S-super idempotent of $\mathbb{Z}_n$, then $1 - \alpha$ is super idempotent.

Proof: Suppose $\alpha$ is an S-super idempotent, then $\alpha^2 - \alpha$ is an S-idempotent hence $(\alpha^2 - \alpha)^2 = \alpha^2 - \alpha$.

Now, $((1 - \alpha)^2 - (1 - \alpha))^2 = (1 - 2\alpha + \alpha^2 - 1 + \alpha)^2 = (\alpha^2 - \alpha)^2 = \alpha^2 - \alpha$.

Therefore $1 - \alpha$ is super idempotent.

Finally, we have the following result.

Theorem 3.14

The group ring $\mathbb{Z}_n G$, where $G = \langle g \mid g^m = 1 \rangle$ is a cyclic group of an odd order $m > 1$ has no S-super idempotent element.

Proof: The proof is an immediate consequence of [8].
REFERENCES


