Smarandache idempotent in the ring of integers modulo n

Shaban.A.Traina Department of mathematics University of Garyounis E-mail: Shabantraina@yahoo.com Abir.K.Salibi Department of mathematics University of Omar-El Mukhtar E-mail: Abir_sss@yahoo.com

Abstract.

In this paper we analyze and study the Smarandache idempotents (S-idempotents) in the ring of integers modulo n, \Box_n . We have shown in general that an idempotent element in a ring R may not be an S-idempotent. Also we have establish the existence of S-idempotents in \Box_n for a specific value n. We have proved that \Box_n has an S-idempotents with n is a perfect number, and n is of the form $2^i p$, (where p be an odd prime), or $3^i p$ (p a prime greater than 3), or in general when $n = p_1^i p_2$ (p_1 and p_2 are distinct odd primes). We provide many interesting properties and illustrate them with several examples.

Keywords : idempotent, Smarandache idempotent.

1. Introduction.

This section is devoted to the introduction of the basic notions concerning the Smarandache ring. The concept of Smarandache idempotents and Smarandache co- idempotents inis introduced. We recall only those results and definitions, which \Box_n are very basically needed in this paper.

Definition 1.1 [2] : Let *R* be a ring, an element $a \in R \setminus \{0\}$ is called an *idempotent* in *R* if $a^2 = a$. If 1 is in *R* then 1 is called a *trivial idempotent*.

Definition 1.2 [3]: Let *R* be a ring with unit. An element $a \in R \setminus \{0,1\}$ is a *Smarandache idempotent* (*S-idempotent*) of *R* if,

- 1. $a^2 = a$
- 2. There exists $b \in R \setminus \{0, 1, a\}$ such that:
 - i) $b^2 = a$ and
 - *ii)* ab = a (ba = a) or ab = b (ba = b).

Definition 1.3 [3]: Let $a \in R \setminus \{0,1\}$ be a Smarandache idempotent i.e. $a^2 = a$ and there exists $b \in R \setminus \{0,1,a\}$ such that $b^2 = a$ and ab = a (ba = a) or ab = b (ba = b). We call b the *Smarandache co-idempotent* (*S-co-idempotent*) and denote the pair by (a,b).

Example 1.4 : Let $\Box_{10} = \{0, 1, 2, ..., 9\}$ be the ring of integers modulo 10, then $6 \in \Box_{10}$ is an S-idempotent of \Box_{10} for $6^2 \equiv 6 \pmod{10}$ and $4 \in \Box_{10}$ is an S-co-idempotent such that $4^2 \equiv 6 \pmod{10}$ and $6.4 \equiv 4 \pmod{10}$.

Definition 1.5 [3] : Let *R* be a commutative ring with unit and *G* be a group. The group ring *RG* of the group *G* over the ring *R* consists of all finite formal sums of the form $\sum_{i} \alpha_{i} g_{i}$ (*i*-runs over a finite number), where $\alpha_{i}, \beta_{i} \in R$ and $g_{i} \in G$ satisfying the following conditions:

 $i) \qquad \sum_{i} \alpha_{i} g_{i} = \sum_{i} \beta_{i} g_{i} \Leftrightarrow \alpha_{i} = \beta_{i}.$

ii)
$$\left(\sum_{i} \alpha_{i} g_{i}\right) + \left(\sum_{i} \beta_{i} g_{i}\right) = \sum_{i} (\alpha_{i} + \beta_{i}) g_{i}.$$

iii)
$$\left(\sum_{i} \alpha_{i} g_{i}\right) \left(\sum_{j} \beta_{j} g_{j}\right) = \sum_{k} \gamma_{k} g_{k}$$
 where $\gamma_{k} = \sum \alpha_{i} \beta_{j}, g_{k} = g_{i} g_{j}.$

iv) $\alpha_i g_i = g_i \alpha_i$.

v)
$$\alpha \sum_{i} \alpha_{i} g_{i} = \sum_{i} (\alpha \alpha_{i}) g_{i}$$
 for $\alpha, \alpha_{i} \in R$ and $\sum \alpha_{i} g_{i} \in RG$.

RG is a ring with $0 \in R$ as its additive identity.

Since $1 \in R$ we have G = 1. $G \subset RG$ and R = R. $e \subseteq RG$ where *e* is the identity element of *G*.

Note that definition 1.1.5 can be defined for a semigroup with a unit.

Example 1.6 : Let \Box_3 be the prime field of characteristic 3, $G = \{g / g^2 = 1\}$ be the cyclic group of order 2. $\Box_3 G = \{0, 1, 2, g, 2g, 1+g, 1+2g, 2+g, 2+2g\}$, clearly 2+2g is an S-idempotent of $\Box_3 G$ as $(2+2g)^2 = 2+2g$ and (2+2g)(1+g) = 1+g. Hence the claim.

Example 1.7 : Consider the group ring QG of the group G over Q, where $G = \{g / g^2 = 1\}$ be the cyclic group of order 2 and Q be the field of rationals. QG has S-idempotent.

Take $a = \frac{1}{2}(1+g) \in QG$, $b = \frac{-1}{2}(1+g) \in QG$.

Now we have $a^2 = a$, $b^2 = a$, ab = b. So *a* is an S-idempotent in *QG*.

Theorem 1.8 [3] : Let *F* be a field. *F* has no S-idempotent.

Note : Let \square_p be the ring of integers modulo *p*, *p* a prime, then \square_p has no idempotents. For example $\square_2, \square_3, \square_5$ has no idempotents, so has no S-idempotents.

Now we have the following theorem.

Theorem 1.9 [3] : In a ring *R*, every S-idempotent is an idempotent and not vice versa.

Example 1.10 : In \square_{10} , $5 \in \square_{10}$ is an idempotent since $5^2 \equiv 5 \pmod{10}$ but it is not an S-idempotent.

Example 1.11 : Let $S_3 = \{1, p_1, p_2, p_3, p_4, p_5\}$, S_3 be the symmetric group of degree 3 where

$$1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} , \quad p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} , \quad p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} ,$$
$$p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} , \quad p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \text{ and } p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} .$$

 $\Box_2 = \{0,1\}$ be the prime field of characteristic two. Clearly the group ring $\mathbf{Z}_2 S_3$ has idempotents which are S-idempotents.

Now $a = (1 + p_4 + p_5)$ is an S-idempotent in $\mathbb{Z}_2 S_3$ since $(1 + p_4 + p_5)^2 = 1 + p_4 + p_5$, and $b_1 = 1 + p_1 + p_2 \in \mathbb{Z}_2 S_3$ is an S-co idempotent of a, such that $b_1^2 = a$, $ab_1 = a$.

One can see that the element $b_2 = p_1 + p_2 + p_3$ is also an S-co-idempotent of a, such that $b_2^2 = a$, $ab_2 = a$.

This leads us to an interesting results that S-co-idempotent are not unique for a given S-idempotent.

Theorem 1.12 [3] : Let *R* be a ring. $a \in R$ be an S-idempotent. The S-co-idempotents of *a* in general is not unique.

Example 1.13 : In \square_{40} , 25 is an S-idempotent has two S-co-idempotent 5 and 15.

Theorem 1.14 : Let \square_{p^n} be the set of integers modulo p^n , p a prime. Then \square_{p^n} has no non trivial idempotent element.

Proof : Let *a* be an idempotent element in \Box_{p^n}

 $a^2 \equiv a \pmod{p^n}$

Then

$$a(a-1) = kp^n \quad , \quad k \in \Box \, .$$

So we have $a \equiv 1 \pmod{p^n}$ or $a \equiv 0 \pmod{p^n}$. Then \Box_{p^n} has no non trivial idempotent. **Example 1.15 :** Let $\Box_9 = \{0, 1, 2, ..., 9\}$ be the ring of integers modulo 9. It can easily be verified that \Box_9 has no idempotents and so has no S-idempotents.

Theorem 1.16 : Let \Box_n be the ring of integers modulo n, n = 3p, 6p where p odd prime greater than 3, n = 4p where p odd prime and n = 5p where p a prime > 5. If a is an S-idempotent and b an S-co-idempotent of a, then $a+b \equiv n \pmod{n}$.

Proof: Since *a* is an idempotent, then $a^2 \equiv a \pmod{n}$ and $b \in \square_n \setminus \{0,1,a\}$ such that $b^2 \equiv a \pmod{n}$ and $ab \equiv a \pmod{n}$ or $ab \equiv b \pmod{n}$.

i.e. $a^2 \equiv b^2 \pmod{n}$.

So $a^2-b^2=kn$, $k\in \Box$,

i.e. (a-b)(a+b) = kn.

Since $a - b = k_1, k_1 \in \Box, k_1 < n$,

then $a+b=k_2n$, $k_2\in \Box$, with $k_1k_2=k$.

So $a+b \equiv n \pmod{n}$.

Example 1.17 : In \square_{15} ; 10 is an S-idempotent, 5 is an S-co-idempotent and 10+5=15.

Remark 1.18 : The last theorem is not true for all *n*. The case if $n = 2m^2$, $m^2 \neq 2^i$, $i \in \Box$, we have m^2 is an S-idempotent and *m* is an S-co idempotent, but $m^2 + m \not\equiv n \pmod{n}$. For example in $\Box_{18}, (18 = 2.3^2)$, a = 9 is an S-idempotent since $9^2 \equiv 9 \pmod{18}$ and b = 3 is an S-co-idempotent with $3^2 = 9, 3.9 \equiv 9 \pmod{18}$, but $9+3=12 \not\equiv 18 \pmod{18}$.

Note : In \square_n , if *a* is an S-idempotent which has two S-co-idempotent, then one of them must satisfies the condition $a + b \equiv n \pmod{n}$.

Theorem 1.19 : Let \square_n be the ring of integers modulo *n*, and let *a* be an idempotent element, then (n+1)-a is also an idempotent.

Proof : If *a* is an idempotent, then

$$\begin{aligned} a^{2} - a &= kn , \ k \in \Box \\ [(n+1)-a]^{2} - [(n+1)-a] &= (n+1)^{2} - 2a(n+1) + a^{2} - (n+1) + a \\ &= (n+1)^{2} - 2na - (n+1) + a^{2} - a \\ &= n^{2} + n - 2na + nk \\ &= (n+1-2a+k)n \\ &= hn , \ h = n+1-2a+k . \end{aligned}$$

Then (n+1)-a is an idempotent in \Box_n .

2. The existence of S-idempotent in \square_n .

In this section we have proved the existence of an S-idempotent in the ring \Box_n , when $n = 5p \ (p > 5), \ n = 8p \ (p \text{ odd prime})$, and some more cases have been proved.

Theorem 2.20 : Let \Box_{2p} be a ring of integers modulo 2p, where p is an odd prime, then

- i) p and p+1 are two idempotents.
- *ii)* p+1 is an S-idempotent.

Proof: i) Since
$$2 \setminus (p-1)$$
, then $2p \setminus p(p-1)$.
So $p^2 - p = 2pk$, $k \in \Box$, i.e. $p^2 \equiv p \pmod{2p}$.
Also $2 \setminus (p+1)$, then $p^2 + p = 2pk$, $k \in \Box$.
So $(p+1)^2 \equiv p+1 \pmod{2p}$.
Hence p and $p+1$ are idempotents in \Box_{2p} .

ii) Take $a = p + 1 \in \square_{2p}$ and $b = p - 1 \in \square_{2p}$ $a^2 = (p+1)^2 \equiv p + 1 \pmod{2p}$ Therefore, $a^2 \equiv a \pmod{2p}$.

Also $b^2 = (p-1)^2 \equiv (p+1) \pmod{2p}$

Therefore $b^2 \equiv a \pmod{2p}$.

And ab = (p-1)(p+1)

$$= p^2 - 1$$
$$\equiv p - 1 \pmod{2p}.$$

Therefore

$$ab \equiv b \pmod{2p}$$
.

So a = p + 1 is an S-idempotent in \Box_{2p} .

Then \Box_{2p} has idempotents which are not S-idempotent.

Example 2.21 : In \square_{14} ; 7 and 8 are two idempotents. On the other hand, only 8 is an S-idempotents since $6 \in \square_{14}$, $6^2 \equiv 8 \pmod{14}$ and $6.8 \equiv 6 \pmod{14}$.

Theorem 2.22 : In the ring of integers modulo 5p, with p > 5. If the first digit of p is

- i) 1, then p is an idempotent.
- *ii)* 9, then p^2 is an idempotent.
- *iii*) 3,7, then p^4 is an idempotent.

proof: i) If *p* starts with 1, then $5 \setminus (p-1)$. So *p* is an idempotent.

ii) If *p* starts with 9, then $5 \times p$ and $5 \setminus (p-1)$. Hence *p* is not an idempotent. But $5 \setminus (p+1)$. So p^2 is an idempotent.

iii) If *p* start with 3, 7 then $5 \times p$, $5 \times (p-1)$, and $5 \times (p+1)$, i.e. *p* and p^2 are not idempotents. On the other hand, $5 \setminus (p^2 + 1)$, i.e. p^4 is an idempotent. A similar result can be obtain for the ring \Box_{10p} .

Example 2.23 : In \Box_{55} , (55 = 5.11), 11 is an idempotent. In \Box_{95} , (95 = 5.19), (19)² = 76 (mod 95) is an idempotent. Also in \Box_{65} , (65 = 5.13), (13)⁴ = 26 (mod 65) is an idempotent.

Theorem 2.24: Let \Box_{8p} be the ring of integers modulo 8p, p be an odd prime, then p^2 is an idempotent.

Proof: Let p = 2r + 1, $r \in \mathbb{Z}$. Then p(p-1)(p+1) = 4r(2r+1)(r+1)If r is odd $\Rightarrow r+1$ is even $\Rightarrow r+1=2l$, $l \in \mathbb{Z}$. So we have p(p-1)(p+1) = 8(2r+1)(r)(l). Then $8 \setminus p(p-1)(p+1)$. If r is even $\Rightarrow r = 2m$, $m \in \mathbb{Z}$. So $8 \setminus p(p-1)(p+1)$.

Then p^2 is an idempotent.

Example 2.25 : In \square_{24} , (24 = 8.3), (3)² = 9 is an idempotent which is an S-idempotent.

Similar result one can establish from the last theorem are given in the next two corollaries.

Corollary 2.26 : In \square_n , n = 3p, 4p, 12p, 24p where p is an odd prime, p^2 is an idempotent.

Clearly $(2p)^4$ and $(3p)^2$ is also an idempotent in \Box_{24n} .

Corollary 2.27 : In \square_n , n = 5p, 10p, 16p, 48p, where p is an odd prime, p > 5, p^4 is an idempotent.

Example 2.28 : Consider \Box_{120} , (120 = 24.5), it can be calculated that $p^2 \equiv 25 \pmod{120}$, $(2p)^4 \equiv 40 \pmod{120}$ and $(3p)^2 \equiv 105 \pmod{120}$ as non-trivial idempotents, and 96,81 and 16 are the other idempotents in \Box_{120} . One can easily verified that all these idempotents are S-idempotents. Now the S-co-idempotent for 25 is 95, for 40 is 80, 150 it is 15, for 96 the S-co-idempotent is 24, for 81 is 39, and for 16 the S-co-idempotent is 104.

Theorem 2.29 : In the ring of integers modulo 2pq, p,q are odd primes, pq is an idempotent.

Proof: Since $2 \setminus (pq-1)$, then pq(pq-1) = 2pqk, $k \in \Box$. Hence pq is an idempotent.

Example 2.30 : Consider \Box_{30} , (30 = 2.3.5), 15 is an idempotent which is not an S-idempotent.

Theorem 2.31: In the ring of integers modulo $2p^iq^j$, p,q are odd primes, p^iq^j is an idempotent.

Proof: Since $2 \setminus (p^i q^j - 1)$, then $p^i q^j (p^i q^j - 1) = 2p^i q^j k$, $k \in \square$. Hence $p^i q^j$ is an idempotent.

Example 2.32 : Consider \Box_{90} , $(90 = 2.3^2.5)$, 45 is an idempotent which is not an S-idempotent.

Definition 2.33 [5] : A positive integer *n* is said to be a *perfect number* if *n* is equal to the sum of all its positive divisors, excluding *n* itself. e.g. 6 is a perfect number. As 6 = 1 + 2 + 3.

Theorem 2.34 : Let \Box_n be the ring of integers modulo *n*, where *n* is an even perfect number of the form $n = 2^t (2^{t+1} - 1)$, where $2^{t+1} - 1$ is a prime, for some $t \ge 1$, then $a = 2^{t+1} \in \Box_n$ is an S-idempotent.

Proof: For $a = 2^{t+1} \in \square_n,$ choose $b = (n - 2^{t+1}) \in \square_n.$ Clearly $a^2 = (2^{t+1})^2$ $= 2^2 \cdot 2^{2t} \quad (\because 2^t \cdot 2^{t+1} \equiv 2^t \pmod{n})$ $\equiv 2 \cdot 2^t \pmod{n}$ = a.Now $b^2 = (n - 2^{t+1})^2$ $\equiv 2 \cdot 2^t \pmod{n}$ =a.

Also

$$ab = 2^{t+1}(n - 2^{t+1})$$

= b (mod n).

So we get $a^2 \equiv a \pmod{n}$, $b^2 \equiv a \pmod{n}$ and $ab \equiv b \pmod{n}$.

Therefore $\alpha = 2^{s+1}$ is an S- idempotent.

Example 2.35 : Take the ring \Box_6 . Here 6 is an even perfect number . As $6 = 2.(2^2 - 1)$, so $a = 2^2$ is an S-idempotent. Since $a^2 \equiv a \pmod{6}$. For b = 2. Then $a^2 \equiv a \pmod{6}$, $b^2 \equiv a \pmod{6}$ and $ab \equiv b \pmod{6}$. So a = 4 is an S-idempotent.

Theorem 2.36 : Let $\Box_{2^i p}$ be a ring of integers modulo $2^i p$, where p is an odd prime with $p \setminus (2^{t+1}-1)$ for some $t \ge i$, then $a = 2^{t+1} \in \Box_{2^i p}$ is an S-idempotent.

Proof: Note that $p \setminus (2^{t+1}-1)$ for some $t \ge i$.

Therefore

$$2^{t+1} \equiv 1 \pmod{p} \text{ for some } t \ge i .$$

$$\Leftrightarrow 2^t \cdot 2^{t+1} \equiv 2^t \pmod{2^i p} \text{ as gcd } (2^t \cdot 2^i p) = 2^i \text{ , } t \ge i$$

Now take $a = 2^{t+1} \in \square_{2^{i}p}$ and $b = (2^{i}p - 2^{t+1}) \in \square_{2^{i}p}$.

Then it easy to see that :

 $a^2 \equiv a \pmod{2^i p}$, $b^2 \equiv a \pmod{2^i p}$ and $ab \equiv b \pmod{2^i p}$.

Hence $a = 2^{t+1}$ is an idempotent.

Example 2.37 : Take the ring $\Box_{2^{3}.7}$. Here $7 \setminus (2^{5+1} - 1)$, so t = 5. Take a = 8, b = 48.

Then it easy to see that $a^2 \equiv a \pmod{2^3.7}$, $b^2 \equiv a \pmod{2^3.7}$ and $ab \equiv b \pmod{2^3.7}$.

Theorem 2.38 : Let $\Box_{3^i p}$ be the ring of integers modulo $3^i p$, where *p* is an odd prime such that $p \setminus (2.3^t - 1)$ for some $t \ge i$, then $a = 2.3^t \in \Box_{3^i p}$ is an S-idempotent.

Proof: Suppose $p \setminus (2.3^t - 1)$ for some $t \ge i$.

Take $a = 2.3^t \in \square_{3^i p}$ and $b = (3^i p - 2.3^t) \in \square_{3^i p}$.

Then

$$a^{2} = (2.3^{t})^{2}$$

= 2². 3^{2t}
= 2.3^t (mod 3^t p)
= a.

As $2.3^t \equiv 1 \pmod{p}$ for some $t \ge i$

 $\Leftrightarrow 2.3^{t}.3^{t} \equiv 3^{t} \pmod{3^{i} p} \text{ as gcd } (3^{t},3^{i} p) = 3^{i}, t \ge i.$ Similarly $b^{2} \equiv b \pmod{3^{i} p}$ and $ab \equiv b \pmod{3^{i} p}$. So $a = 2.3^{t}$ is an S-idempotent.

Example 2.39 : Take the ring $\Box_{3^2,5}$. Here $5 \setminus 2.3^5 - 1$, so t = 5. Take $\alpha = 2.3^5 \equiv 36 \pmod{45}$ and $b = (3^2.5 - 2.3^5) \equiv 9 \pmod{45}$. $a^2 \equiv a \pmod{45}$, $b^2 \equiv a \pmod{45}$ and $ab \equiv b \pmod{45}$.

We can generalize Theorem 2.36, 2.38 as follows :

Theorem 2.40 : Let $\Box_{p^i q}$ be the ring of integers modulo $p^i q$, Where p,q are distinct odd primes and $q \setminus 2.p^t - 1$ for some $t \ge i$, then $a = 2p^t \in \Box_{p^i q}$ is an S-idempotent.

Proof: Suppose $q \setminus 2.p^t - 1$ for some $t \ge i$.

Take $a = 2p^t \in \square_{p^i q}$ and $b = (p^i q - 2p^t) \in \square_{p^i q}$.

Easily we can show that

 $a^2 \equiv a \pmod{p^i q}$, $b^2 \equiv a \pmod{p^i q}$ and $ab \equiv b \pmod{p^i q}$. So $a = 2p^t$ is an S- idempotent.

3. Conclusion .

One can see in the last section, we have establish the existence of at last one non-trivial S-idempotent. On the other hand, the existence of S-idempotent in the ring \Box_n for every *n* has not been yet established.

References

- [1] Padella, R., *Smarandache Algebraic Structures*, Smarandache Notions Journal, Vol.
 9, No 1-2-3, (1998), 36-38.
- [2] Saracino, D.H., Abstract Algebra : A first Course, Addison Wesley publishers, Inc., (1980).
- [3] Vasantha Kandasamy, W.B., *Smarandache Rings*, American Research Press, Rehoboth, (2002).
- [4] Vasantha Kandasamy, W.B., Bialgebraic structures and Smarandache Bialgebraic structures, American Research Press, Rehoboth, (2003).
- [5] Vasantha Kandasamy, W.B., and M.K. Chetry, Smarandache idempotents in Loop Rings Z_t L_n (m) of the Loops L_n (m), Scientia Magna, Vol. 1, No.2, (2005), 179-187.
- [6] Vasantha Kandasamy, W.B., and T.Subramaniyam, *S-Rings and their properties*, National Symposium on Mathematical Methods and Applications, Indian Institute of Technology ,India , (2003).