Smarandache Idempotents in finite ring Z_n and in Group Ring Z_nG

W.B.Vasantha and Moon K.Chetry

Department of Mathematics I.I.T. Madras, Chennai

Abstract In this paper we analyze and study the Smarandache idempotents (S-idempotents) in the ring Z_n and in the group ring Z_nG of a finite group G over the finite ring Z_n . We have shown the existance of Smarandache idempotents (S-idempotents) in the ring Z_n when $n = 2^m p$ (or 3p), where p is a prime > 2 (or p a prime > 3). Also we have shown the existance of Smarandache idempotents (S-idempotents) in the group ring Z_2G and Z_2S_n where $n = 2^m p$ (p a prime of the form $2^m t + 1$).

§1. Introduction

This paper has 4 sections. In section 1, we just give the basic definition of S-idempotents in rings. In section 2, we prove the existence of S-idempotents in the ring Z_n where $n = 2^m p, m \in N$ and p is an odd prime. We also prove the existence of S-idempotents for the ring Z_n where n is of the form n = 3p, p is a prime greater than 3. In section 3, we prove the existence of S-idempotents in group rings Z_2G of cyclic group G over Z_2 where order of G is $n, n = 2^m p$ (p a prime of the form $2^m t + 1$). We also prove the existence of S-idempotents for the group ring Z_2S_n where $n = 2^m p$ (p a prime of the form $2^m t + 1$). In the final section, we propose some interesting number theoretic problems based on our study.

Here we just recollect the definition of Smarandache idempotents (S-idempotent) and some basic results to make this paper a self contained one.

Definition 1.1[5]. Let R be a ring. An element $x \in R$ 0 is said to be a Smarandache idempotent (S-idempotent) of R if $x^2 = x$ and there exist $a \in R$ x, 0 such that

$$i. \quad a^2 = x$$
$$ii. \quad xa = x \quad or \quad ax = a.$$

Example 1.1. Let $Z_1 0 = \{0, 1, 2, ..., 9\}$ be the ring of integers modulo 10. Here

$$6^2 \equiv 6 \pmod{10}, \quad 4^2 \equiv 6 \pmod{10}$$

and

$$6 \cdot 4 \equiv 4 \pmod{10}.$$

So 6 is a S-idempotent in Z_{10} .

Example 1.2. Take $Z_{12} = \{0, 1, 2, ..., 11\}$ the ring of integers modulo 12. Here

$$4^2 \equiv 4 \pmod{12}, \quad 8^2 \equiv 4 \pmod{12}$$

and

$$4 \cdot 8 \equiv 8 \pmod{12}.$$

So 4 is a S-idempotent in Z_{12} .

Example 1.3. In $Z_{30} = \{0, 1, 2, \dots, 29\}$ the ring of integers modulo 30, 25 is a S-idempotent. As

$$25^2 \equiv 25 \pmod{30}, \quad 5^2 \equiv 25 \pmod{30}$$

and

$$25 \cdot 5 \equiv 5 \pmod{30}.$$

So 25 is a S-idempotent in Z_{30} .

Theorem 1.1 [5]. Let R be a ring. If $x \in R$ is a S-idempotent then it is an idempotent in R.

Proof. From the very definition of S-idempotents.

§2. S-idempotents in the finite ring Z_n

In this section, we find conditions for Z_n to have S-idempotents and prove that when n is of the form $2^m p$, p a prime 2^{i} or n = 3p (p a prime 3^{i}) has S-idempotents. We also explicitly find all the S-idempotents.

Theorem 2.1. $Z_p = \{0, 1, 2, ..., p-1\}$, the prime field of characteristic p, where p is a prime has no non-trivial S-idempotents.

Proof. Straightforward, as every S-idempotents are idempotents and Z_p has no non-trivial idempotents.

Theorem 2.2: The ring Z_{2p} , where p is an odd prime has S-idempotents.

Proof. Here p is an odd prime, so p must be of the form 2m + 1 i.e p = 2m + 1. Take

$$x = p + 1$$
 and $a = p - 1$.

Here

$$p^{2} = (2m + 1)^{2} = 4m^{2} + 4m + 1$$

= $2m(2m + 1) + 2m + 1$
= $2pm + p$
= $p(mod2p).$

 So

Again

$$x^{2} = (p+1)^{2} \equiv p^{2} + 1 \pmod{2p}$$
$$\equiv p + 1 \pmod{2p}.$$

Therefore

 $x^2 = x.$

Also

$$a^{2} = (p-1)^{2} \equiv p + 1 \pmod{2p},$$

 $a^2 = x.$

therefore

And

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

therefore

$$xa = a$$
.

So x = p + 1 is a S-idempotent in Z_{2p} .

Example 2.1. Take $Z_6 = Z_{2\cdot 3} = \{0, 1, 2, 3, 4, 5\}$ the ring of integers modulo 6. Then x = 3 + 1 = 4 is a S-idempotent. As

$$x^2 = 4^2 \equiv 4 \pmod{6},$$

take a = 2, then $a^2 = 2^2 \equiv 4 \pmod{6}$. Therefore

 $a^2 = x,$

and

$$xa = 4 \cdot 2 \equiv 2 \pmod{6}$$

i.e

$$xa = a$$
.

Theorem 2.3. The ring Z_{2^2p} , p a prime > 2 and is of the form 4m + 1 or 4m + 3 has (at least) two S-idempotents.

Proof. Here p is of the form 4m + 1 or 4m + 3. If p = 4m + 1, then $p^2 \equiv p \pmod{2^2 p}$. As

$$p^{2} = (4m + 1)^{2}$$

= $16m^{2} + 8m + 1$
= $4m(4m + 1) + 4m + 1$
= $4pm + p$
= $p(mod2^{2}p),$

therefore

$$p^2 \equiv p(\bmod 2^2 p).$$

Now, take x = 3p + 1 and a = p - 1 then

$$x^{2} = (3p+1)^{2} = 9p^{2} + 6p + 1$$

$$\equiv 9p + 6p + 1(\text{mod}2^{2}p)$$

$$\equiv 3p + 1(\text{mod}2^{2}p)$$

therefore

 $a^2 = x.$

And

$$xa = (3p+1)(p-1)$$
$$= 3p^2 - 3p + p - 1$$
$$\equiv p - 1(\text{mod}2^2p)$$

therefore

xa = a.

So x is an S-idempotent.

Similarly, we can prove that y = p, (here take a = 3p) is another S-idempotent. These are the only two S-idempotents in Z_{2^2p} when p = 4m + 1. If p = 4m + 3, then $p^2 \equiv 3p \pmod{2^2 p}$.

As above, we can show that x = p + 1, (a = 3p - 1) and y = 3p, (a = p) are the two S-idempotents. So we are getting a nice pattern here for S-idempotents in Z_{2^2p} :

I. If p = 4m + 1, then x = 3p + 1, (a = p - 1) and y = p, (a = 3p) are the two S-idempotents.

II. If p = 4m+3, x = p+1, (a = 3p-1) and y = 3p, (a = p) are the two S-idempotents. **Example 2.2.** Take $Z_{2^2.5} = \{0, 1, \dots, 19\}$, here $5 = 4 \cdot 1 + 1$. So $x = 3 \cdot 5 + 1 = 16$, (a = 5 - 1 = 4) is an S-idempotent. As $16^2 \equiv 16 \pmod{20}$, $4^2 \equiv 16 \pmod{20}$ and $16 \cdot 4 \equiv 4 \pmod{20}$. Also y = 5, $(a = 3 \cdot 5 = 15)$ is another S-idempotent. As $5^2 \equiv 5 \pmod{20}$, $15^2 \equiv 5 \pmod{20}$ and $5 \cdot 15 \equiv 15 \pmod{20}$.

Example 2.3. In the ring $Z_{2^2.7} = \{0, 1, \dots, 27\}$, here $7 = 4 \cdot 1 + 3, x = 7 + 1 = 8, (a = 3 \cdot 7 - 1 = 20)$ is an S-idempotent. As $8^2 \equiv 8 \pmod{28}, 20^2 \equiv 8 \pmod{28}$ and $8 \cdot 20 \equiv 20 \pmod{28}$. Also $y = 3 \cdot 7 = 21, (a = 7)$ is another S-idempotent. As $21^2 \equiv 21 \pmod{28}, 7^2 \equiv 21 \pmod{28}$ and $21 \cdot 7 \equiv 7 \pmod{28}$.

Theorem 2.4. The ring Z_{2^3p} , p a prime > 2 has (at least) two S-idempotents of $\phi(2^3)$ types (where $\phi(n)$ is the number of integer less than n and relatively prime to n).

Proof. As p is prime > 2. So p is one of the 8m + 1, 8m + 3, 8m + 5, 8m + 7. Now we will get the following two S-idempotents for each $\phi(2^3) = 4$ types of prime p.

I. If p = 8m + 1, then x = 7p + 1, (a = p - 1) and y = p, (a = 7p) are S-idempotents. *II.* If p = 8m + 3, then x = 5p + 1, (a = 3p - 1) and y = 3p, (a = 5p) are S-idempotents. *III.* If p = 8m + 5, then x = 3p + 1, (a = 5p - 1) and y = 5p, (a = 3p) are S-idempotents.

IV. If p = 8m + 7, then x = p + 1, (a = 7p - 1) and y = 7p, (a = p) are S-idempotents.

Example 2.4. In the ring $Z_{2^3.3} = \{0, 1, ..., 23\}$, here $3 = 8 \cdot 0 + 3$. So $x = 5 \cdot 3 + 1 = 16, (a = 3 \cdot 3 - 1 = 8)$ is an S-idempotent. As $16^2 \equiv 16 \pmod{24}, 8^2 \equiv 16 \pmod{24}$ and $16 \cdot 8 \equiv 8 \pmod{24}$. Also $y = 3 \cdot 3 = 9, (a = 5 \cdot 3 = 15)$ is another S-idempotent. As $9^2 \equiv 9 \pmod{24}, 15^2 \equiv 9 \pmod{24}$ and $9 \cdot 15 \equiv 15 \pmod{24}$.

Example 2.5. Take $Z_{2^3 \cdot 13} = Z_{104} = \{0, 1, \dots, 103\}$, here $13 = 8 \cdot 1 + 5$. So $x = 3 \cdot 13 + 1 = 40$, $(a = 5 \cdot 13 - 1 = 64)$ is an S-idempotent. As $40^2 \equiv 40 \pmod{104}$, $64^2 \equiv 40 \pmod{104}$ and $40 \cdot 64 \equiv 64 \pmod{104}$. Also $y = 5 \cdot 13 = 65$, $(a = 3 \cdot 13 = 39)$ is another S-idempotent. As $65^2 \equiv 65 \pmod{104}$, $39^2 \equiv 65 \pmod{104}$ and $65 \cdot 39 \equiv 39 \pmod{104}$.

Theorem 2.5. The ring Z_{2^4p} , p a prime > 2 has (at least) two S-idempotents for each of $\phi(2^4)$ types of prime p.

Proof. As above, we can list the S-idempotents for all $\phi(2^4) = 8$ types of prime p.

 $\begin{array}{l} I. \mbox{ If } p = 16m+1, \mbox{ then } x = 15p+1, \mbox{ } (a = p-1) \mbox{ and } y = p, \mbox{ } (a = 15p) \mbox{ are S-idempotents.} \\ II. \mbox{ If } p = 16m+3, \mbox{ then } x = 13p+1, \mbox{ } (a = 3p-1) \mbox{ and } y = 3p, \mbox{ } (a = 13p) \mbox{ are S-idempotents.} \\ III. \mbox{ If } p = 16m+5, \mbox{ then } x = 11p+1, \mbox{ } (a = 5p-1) \mbox{ and } y = 5p, \mbox{ } (a = 11p) \mbox{ are S-idempotents.} \\ IV. \mbox{ If } p = 16m+7, \mbox{ then } x = 9p+1, \mbox{ } (a = 7p-1) \mbox{ and } y = 7p, \mbox{ } (a = 9p) \mbox{ are S-idempotents.} \\ V. \mbox{ If } p = 16m+9, \mbox{ then } x = 7p+1, \mbox{ } (a = 9p-1) \mbox{ and } y = 9p, \mbox{ } (a = 7p) \mbox{ are S-idempotents.} \\ VI. \mbox{ If } p = 16m+11, \mbox{ then } x = 5p+1, \mbox{ } (a = 11p-1) \mbox{ and } y = 11p, \mbox{ } (a = 5p) \mbox{ are S-idempotents.} \\ VII. \mbox{ If } p = 16m+13, \mbox{ then } x = 3p+1, \mbox{ } (a = 13p-1) \mbox{ and } y = 13p, \mbox{ } (a = 13p) \mbox{ are S-idempotents.} \\ VII. \mbox{ If } p = 16m+13, \mbox{ then } x = 3p+1, \mbox{ } (a = 13p-1) \mbox{ and } y = 13p, \mbox{ } (a = 13p) \mbox{ are S-idempotents.} \\ VII. \mbox{ If } p = 16m+13, \mbox{ then } x = 3p+1, \mbox{ } (a = 13p-1) \mbox{ and } y = 13p, \mbox{ } (a = 13p) \mbox{ are S-idempotents.} \\ \end{array}$

VIII. If p = 16m + 15, then x = p + 1, (a = 15p - 1) and y = 15p, (a = p) are S-idempotents. **Example 2.6.** In the ring $Z_{2^4 \cdot 17} = Z_{272} = \{0, 1, \dots, 271\}$, here $17 = 16 \cdot 1 + 1$. So $x = 15 \cdot 17 + 1 = 256$, (a = 17 - 1 = 16) is an S-idempotent. As $256^2 \equiv 256 \pmod{272}$, $16^2 \equiv 256 \pmod{272}$ and $256 \cdot 16 \equiv 16 \pmod{272}$. Also y = 17, $(a = 15 \cdot 17 = 255)$ is another S-idempotent. As $17^2 \equiv 17 \pmod{272}$, $255^2 \equiv 17 \pmod{272}$ and $17 \cdot 255 \equiv 255 \pmod{272}$.

We can generalize the above result as followings:

Theorem 2.6. The ring $Z_{2^n p}$, p a prime > 2 has (at least) two S-idempotents for each of $\phi(2^n)$ types of prime p.

Proof. Here p is one of the $\phi(2^n)$ form:

$$2^{n}m_{1}+1, \quad 2^{n}m_{2}+3, \quad \dots \quad 2^{n}m_{\phi(2^{n})}+(2^{n}-1).$$

We can find the two S-idempotents for each p as above. We are showing here for the prime $p = 2^n m_1 + 1$ only. If

$$p = 2^n m_1 + 1$$
,

then

$$x = (2^n - 1)p + 1, \quad (a = p - 1)$$

and

$$y = p$$
, $(a = (2^n - 1)p)$

are S-idempotents.

Similarly we can find S-idempotents for each of the $\phi(2^n)$ form of prime p.

Theorem 2.7. The ring Z_{3p} , p a prime > 3 has (at least) two S-idempotents of $\phi(3)$ types.

Proof. Here p can be one of the form 3m + 1 or 3m + 2. We can apply the Theorem 2.6 for Z_{3p} also.

I. If p = 3m + 1, then x = 2p + 1, (a = p - 1) and y = p, (a = 2p) are S-idempotents.

II. If p = 3m + 2, then x = p + 1, (a = 2p - 1) and y = 2p, (a = p) are S-idempotents.

Example 2.7. In the ring $Z_{3\cdot 5} = Z_{15} = \{0, 1, \dots, 14\}$, here $5 = 3 \cdot 1 + 2$. So x = 5 + 1 = 6, $(a = 2 \cdot 5 - 1 = 9)$ is an S-idempotent. As $6^2 \equiv 6 \pmod{15}$, $9^2 \equiv 6 \pmod{15}$ and $6 \cdot 9 \equiv 9 \pmod{15}$. Also $y = 2 \cdot 5 = 10$, (a = 5) is another S-idempotent. As $10^2 \equiv 10 \pmod{5}$, $5^2 \equiv 10 \pmod{15}$ and $10 \cdot 5 \equiv 5 \pmod{15}$.

Remark: The above result is not true for the ring Z_{3^2p} , p prime > 3. As, for p = 9m + 5; x = 4p + 1, (a = 5p - 1) should be an S-idempotent from the above result. But we see it is not the case in general; for take the ring $Z_{3^2 \cdot 23} = Z_{207} = \{0, 1, \dots, 206\}$. Here $p = 9 \cdot 2 + 5$. Now take

$$x = 4 \cdot 23 + 1 = 93$$
 and $a = 5 \cdot 23 - 1 = 114$.

But

$$x^2 \not\equiv x \pmod{207}$$
.

So x is not even an idempotent. So x = 4p + 1 is not an S-idempotent of Z_{3^2p} .

§3. S-idempotents in the group rings Z_2G

Here we prove the existance of Smarandache idempotents for the group rings Z_{3^2p} of the cyclic group G of order $2^n p$ where p is a prime of the form $2^n t + 1$.

Example 3.2. Let $G = \{g/g^{52} = 1\}$ be the cyclic group of order $2^2 \cdot 13$. Consider the group ring Z_2G of the group G over Z_2 . Take

$$x = 1 + g^4 + g^8 + g^{12} + \ldots + g^{44} + g^{48}$$

and

$$a = 1 + g^2 + g^4 + \ldots + g^{22} + g^{24}$$

then

$$x^2 = x$$
, and $a^2 = x$

 $x \cdot a = x.$

also

So $x = 1 + g^4 + g^8 + g^{12} + \ldots + g^{44} + g^{48}$ is a S-idempotent in Z_2G .

Theorem 3.1. Let Z_2G be the group ring of the finite cyclic group G of order 2^2p , where p is a prime of the form $2^2m + 1$, then the group ring Z_2G has non-trivial S-idempotents.

Proof. Here G is a cyclic group of order 2^2p , where p of the form $2^2m + 1$. Take

$$x = 1 + g^4 + g^8 + \ldots + g^{16m}$$

and

$$a = 1 + g^2 + g^4 + \ldots + g^{8m}$$

then

$$x^{2} = (1 + g^{4} + g^{8} + \dots + g^{16m})^{2}$$

= 1 + g^{4} + g^{8} + \dots + g^{16m}
= x.

 $= 1 + (g^2)^2 + (g^4)^2 + \ldots + (g^{8m})^2$

 $a^2 = (1 + g^2 + g^4 + \ldots + g^{8m})^2$

And

Also

$$\begin{aligned} x \cdot a &= (1 + g^4 + g^8 + \ldots + g^{16m})(1 + g^2 + g^4 + \ldots + g^{8m}) \\ &= 1 + g^4 + g^8 + \ldots + g^{16m} \\ &= x. \end{aligned}$$

So $x = 1 + g^4 + g^8 + \ldots + g^{16m}$ is a S-idempotent in Z_2G .

= x.

Example 3.3. Let $G = \{g/g^{136} = 1\}$ be the cyclic group of order $2^3 \cdot 17$. Consider the group ring Z_2G of the group G over Z_2 .

Take

$$x = 1 + g^8 + g^{16} + \ldots + g^{128}$$

and

$$a = 1 + g^4 + g^8 + \ldots + g^{64}$$

then

$$\begin{aligned} x^2 &= (1+g^8+g^{16}+\ldots+g^{128})^2 \\ &= 1+g^8+g^{16}+\ldots+g^{128} \\ &= x. \end{aligned}$$

And

$$a^{2} = (1 + g^{4} + g^{8} + \ldots + g^{64})^{2}$$

= 1 + (g^{4})^{2} + (g^{8})^{2} + \ldots + (g^{64})^{2}
= x.

 Also

$$x \cdot a = (1 + g^8 + g^{16} + \dots + g^{128})(1 + g^4 + g^8 + \dots + g^{64})$$

= 1 + g^8 + g^{64} + \dots + g^{128}
= x.

So $x = 1 + g^8 + g^{16} + ... + g^{128}$ is a S-idempotent in Z_2G .

Theorem 3.2. Let Z_2G be the group ring of a finite cyclic group G of order 2^3p , where p is a prime of the form $2^3m + 1$, then the group ring Z_2G has non-trivial S-idempotents.

Proof. Here G is a cyclic group of order 2^3p , where p of the form $2^3m + 1$.

Take

$$x = 1 + g^8 + g^{16} + \ldots + g^{8(p-1)}$$

and

$$a = 1 + g^4 + g^8 + \ldots + g^{4(p-1)}$$

then

$$\begin{aligned} x^2 &= (1 + g^8 + g^{16} + \ldots + g^{8(p-1)})^2 \\ &= 1 + g^8 + g^{16} + \ldots + g^{8(p-1)} \\ &= x. \end{aligned}$$

And

$$a^{2} = (1 + g^{4} + g^{8} + \dots + g^{4(p-1)})^{2}$$

= 1 + (g^{4})^{2} + (g^{8})^{2} + \dots + (g^{8(p-1)})^{2}
= x.

 Also

$$\begin{aligned} x \cdot a &= (1 + g^8 + g^{16} + \ldots + g^{8(p-1)})(1 + g^4 + g^8 + \ldots + g^{4(p-1)}) \\ &= 1 + g^8 + g^{16} + \ldots + g^{8(p-1)} \\ &= x. \end{aligned}$$

So $x = 1 + g^8 + g^{16} + \ldots + g^{8(p-1)}$ is a S-idempotent in Z_2G .

We can generalize the above two results as followings:

Theorem 3.3. Let Z_2G be the group ring of a finite cyclic group G of order $2^n p$, where p is a prime of the form $2^n t + 1$, then the group ring Z_2G has non-trivial S-idempotents.

Proof. Here G is a cyclic group of order $2^n p$, where p of the form $2^n t + 1$.

Take

$$x = 1 + g^{2^n} + g^{2^n \cdot 2} + \ldots + g^{2^n(p-1)}$$

and

$$a = 1 + g^{2^{n-1}} + g^{2^{n-1} \cdot 2} + \ldots + g^{2^{n-1} \cdot (p-1)}$$

then

$$x^{2} = (1 + g^{2^{n}} + g^{2^{n} \cdot 2} + \dots + g^{2^{n}(p-1)})^{2}$$

= $1 + g^{2^{n}} + g^{2^{n} \cdot 2} + \dots + g^{2^{n}(p-1)}$
= x .

And

$$a^{2} = (1 + g^{2^{n-1}} + g^{2^{n-1} \cdot 2} + \dots + g^{2^{n-1} \cdot (p-1)})^{2}$$

= 1 + (g^{2^{n-1}})^{2} + (g^{2^{n-1} \cdot 2})^{2} + \dots + (g^{2^{n-1} \cdot (p-1)})^{2}
= x.

Also

$$\begin{aligned} x \cdot a &= (1 + g^{2^n} + g^{2^n \cdot 2} + \ldots + g^{2^n (p-1)})(1 + g^{2^{n-1}} + g^{2^{n-1} \cdot 2} + \ldots + g^{2^{n-1} \cdot (p-1)}) \\ &= 1 + g^{2^n} + g^{2^n \cdot 2} + \ldots + g^{2^n (p-1)} \\ &= x. \end{aligned}$$

So $x = 1 + g^{2^n} + g^{2^n \cdot 2} + \ldots + g^{2^n (p-1)}$ is a S-idempotent in Z_2G .

Corollary 3.1. Let Z_2S_n be the group ring of a symmetric group S_n where $n = 2^n p$, and p is a prime of the form $2^n t + 1$, then the group ring Z_2S_n has non-trivial S-idempotents.

Proof. Here Z_2S_n is a group ring where $n = 2^n p$, and p of the form $2^n t + 1$. Clearly Z_2S_n contains a finite cyclic group of order $2^n p$. Then by the Theorem 3.3, Z_2S_n has a non-trivial S-idempotent.

§4. Conclusions

Here we have mainly proved the existance of S-idempotents in certain types of group rings. But it is interesting to enumerate the number of S-idempotents for the group rings Z_2G and Z_2S_n in the Theorem 3.3 and Corollary 3.1. We feel that Z_2G can have only one S-idempotent but we are not in a position to give a proof for it. Also, the problem of finding S-idempotents in Z_pS_n (and Z_pG) where (p, n) = 1 (and (p, |G|) = 1) or $(p, n) = d \neq 1$ (and $(p, |G|) = d \neq 1$) are still interesting number theoretic problems.

References

[1] I.G.Connel, On the group ring, Can.J.Math. 15(1963), 650-685.

[2] Kim E.T., Idempotents in some group rings, Bull Korean math.soc., 2(1987), 77-81.

[3] C.P.Milies and S.K.Sehgal, An Introduction to group rings, algebras and applications, Kluwer Academic Publishers, Dordrecht, Netherlands, (2002).

[4] D.S.Passman, The algebraic structure of group rings, Wiley interscience (1997).

[5] W.B.Vasantha Kandasamy, Smarandache rings, American research press, Rehoboth (2002).