Quadratic residues and squares of the ring of dual numbers modulo n

Basem Alkhamaiseh
Department of Mathematics
Yarmouk University
Irbid
Jordan basem.m@yu.edu.jo

Abstract. For an integer $n \geq 1$, we denote the ring of dual numbers over the integers modulo n by $\mathbb{Z}_n[\alpha]$. The ring $\mathbb{Z}_n[\alpha]$ is a commutative extension for the ring $\mathbb{Z}_n$. We introduce and study square and quadratic residue elements in $\mathbb{Z}_n[\alpha]$. We also find multiplicative functions that count squares and quadratic residues for the ring $\mathbb{Z}_n[\alpha]$.

Keywords: squares, quadratic residues, ring of dual numbers.

1. Introduction

Let $\mathbb{Z}_n$ be the ring of integers modulo n , where $n \geq 1$. An element $a \in \mathbb{Z}_n$ is called a square element if and only if there exists $c \in \mathbb{Z}_n$ such that $a \equiv c^2 (\mathrm{mod}\, n)$. Square elements of $\mathbb{Z}_n$ that are units are called quadratic residues. Quadratic residues and squares have many interested applications in cryptography, factoring of large numbers and in acoustical engeneering, see for example [6, 5]. W.D. Stangl in [1] obtained multiplicative functions, $s(n)$ and $q(n)$, that count number of squares and number of quadratic residues in $\mathbb{Z}_n$, respectively. In [2], a full characterization for the quadratic residues in $\mathbb{Z}_n$ has been given.

In this paper, our work is based on the well-studied ring $\mathbb{Z}_n[\alpha]$, the ring of dual numbers of $\mathbb{Z}_n$, see [7, 8]. Every element in $\mathbb{Z}_n[\alpha]$ is of the form $a + b\alpha$ where $a, b \in \mathbb{Z}_n$, and $\alpha^2 = 0$, with addition and multiplication defined as

$$\begin{aligned} (a + b\alpha) + (c + d\alpha) &= (a + c) + (b + d)\alpha, \\ (a + b\alpha)(c + d\alpha) &= (ac) + (ad + bc)\alpha \end{aligned}$$

$\mathbb{Z}_n[\alpha]$ is a commutative ring extension of $\mathbb{Z}_n$ with unity 1. Motivated by W.D. Stangl work in [1], we want to make an analogous attempt to study and count squares and quadratic residues for the ring $\mathbb{Z}_n[\alpha]$. Thus, we will see the strong relationship between squares and quadratic residues in $\mathbb{Z}_n$ and those over the ring of dual numbers $\mathbb{Z}_n[\alpha]$. For definitions and terms of general number theory consult [2],[4] and [3].

2. The ring $\mathbb{Z}_n[\alpha]$

Our purpose in this section is only to collect results in one place concerning the ring $\mathbb{Z}_n[\alpha]$.

The ring of dual numbers modulo n, $\mathbb{Z}_n[\alpha] = \{a + b\alpha : a, b \in \mathbb{Z}_n$, with $\alpha^2 = 0\}$, is a commutative ring under addition and multiplication modulo n. This ring is a natural commutative extension of the ring $\mathbb{Z}_n$. Hence we will generalize some concepts in a natural way concerning the ring $\mathbb{Z}_n$ to be suitable for the ring $\mathbb{Z}_n[\alpha]$.

The following definition is a natural generalization of the congruence concept over the ring $\mathbb{Z}_n[\alpha]$, you can see [9].

Definition 2.1. *For $n > 1$, let $a + b\alpha$ and $c + d\alpha$ be two elements of $\mathbb{Z}_n[\alpha]$. Then $a + b\alpha$ is congruent to $c + d\alpha$ modulo n if and only if $a \equiv c \ (mod n)$ and $b \equiv d \ (mod n)$. We will use the notation $a + b\alpha \overset{\alpha}{\equiv} c + d\alpha (mod n)$ to say that $a + b\alpha$ is congruent to $c + d\alpha$ modulo n.*

The following proposition talks about the units of $\mathbb{Z}_n[\alpha]$, and it is probably well known.

Proposition 2.1. *Let $n > 1$. Then $a + b\alpha$ is a unit of $\mathbb{Z}_n[\alpha]$ if and only if a is a unit of $\mathbb{Z}_n$, that is $a + b\alpha$ is a unit of $\mathbb{Z}_n[\alpha]$ if and only if a is relatively prime to n.*

Now, we can generalize the squares and quadratic residues concepts for the ring $\mathbb{Z}_n[\alpha]$

Definition 2.2. *Let $n > 1$. Then*

1. *An element $a + b\alpha$ is a square in $\mathbb{Z}_n[\alpha]$ if and only if*

$$a + b\alpha \overset{\alpha}{\equiv} (c + d\alpha)^2 \ (mod n)$$

   for some $c + d\alpha \in \mathbb{Z}_n[\alpha]$.

2. *An element $a + b\alpha$ is a quadratic residue in $\mathbb{Z}_n[\alpha]$ if and only if $a + b\alpha$ is a square in $\mathbb{Z}_n[\alpha]$ and a is relatively prime to n.*

We will use the notations: $s_\alpha(n)$ to indicate number of squares in $\mathbb{Z}_n[\alpha]$, and $q_\alpha(n)$ to indicate number of quadratic residues in $\mathbb{Z}_n[\alpha]$.

Recall that the number-theoretic function f is multiplicative if $f(mn) = f(m)f(n)$, for any two relatively prime integers m and n.

Theorem 2.1. *Let $n \in \mathbb{Z}$. Then $s_\alpha(n)$ and $q_\alpha(n)$ are multiplicative functions.*

Proof. Suppose that $\gcd(m, n) = 1$. Then one can check that$\mathbb{Z}_{mn}[\alpha]$ is isomorphic to $\mathbb{Z}_m[\alpha] \times \mathbb{Z}_n[\alpha]$ under the ring isomorphism $f : \mathbb{Z}_{mn}[\alpha] \longrightarrow \mathbb{Z}_m[\alpha] \times \mathbb{Z}_n[\alpha]$ which is defined by $f(a + b\alpha(\mathrm{mod}\, mn)) = (a + b\alpha(\mathrm{mod}\, m), a + b\alpha(\mathrm{mod}\, n))$.

Now, suppose $a+b\alpha \in \mathbb{Z}_m[\alpha]$ and $c+d\alpha \in \mathbb{Z}_n[\alpha]$ are squares. Then there exist $x_0+x_1\alpha \in \mathbb{Z}_m[\alpha]$ and $y_0+y_1\alpha \in \mathbb{Z}_n[\alpha]$ such that $a+b\alpha \overset{\alpha}{\equiv} (x_0+x_1\alpha)^2 (\mathrm{mod}\, m)$ and $c+d\alpha \overset{\alpha}{\equiv} (y_0+y_1\alpha)^2 (\mathrm{mod}\, n)$. So $\big((x_0+x_1\alpha)^2 (\mathrm{mod}\, m), (y_0+y_1\alpha)^2 (\mathrm{mod}\, n)\big) = (a+b\alpha (\mathrm{mod}\, m), c+d\alpha (\mathrm{mod}\, n)) \in \mathbb{Z}_m[\alpha] \times \mathbb{Z}_n[\alpha]$. Hence

$$\begin{aligned} & f^{-1}(a+b\alpha (\mathrm{mod}\, m), c+d\alpha (\mathrm{mod}\, n)) \\ & = f^{-1}((x_0+x_1\alpha)^2 (\mathrm{mod}\, m), (y_0+y_1\alpha)^2 (\mathrm{mod}\, n)) \\ & = [f^{-1}((x_0+x_1\alpha) (\mathrm{mod}\, m), (y_0+y_1\alpha) (\mathrm{mod}\, n))]^2 \end{aligned}$$

Thus, $f^{-1}(a+b\alpha (\mathrm{mod}\, m), c+d\alpha (\mathrm{mod}\, n))$ is squre in $\mathbb{Z}_{mn}[\alpha]$. Therefore, $s_\alpha(n).s_\alpha(m) \leq s_\alpha(nm)$.

To prove the other inclusion, let $a+b\alpha$ be square in $\mathbb{Z}_{mn}[\alpha]$. Then, there exists $x+y\alpha \in \mathbb{Z}_{mn}[\alpha]$, such that $a+b\alpha \overset{\alpha}{\equiv} (x+y\alpha)^2 (\mathrm{mod}\, mn)$

Now, since f is a function from $\mathbb{Z}_{mn}[\alpha]$ onto $\mathbb{Z}_m[\alpha] \times \mathbb{Z}_n[\alpha]$, we have

$$(w_0+w_1\alpha (\mathrm{mod}\, m), z_0+z_1\alpha (\mathrm{mod}\, n)) \in \mathbb{Z}_m[\alpha] \times \mathbb{Z}_n[\alpha]$$

such that

$$\begin{aligned} (w_0+w_1\alpha (\mathrm{mod}\, m), z_0+z_1\alpha (\mathrm{mod}\, n)) &= f(a+b\alpha (\mathrm{mod}\, mn)) \\ &= f((x+y\alpha)^2 (\mathrm{mod}\, mn)) \\ &= [f((x+y\alpha) (\mathrm{mod}\, mn))]^2, \end{aligned}$$

so, $(w_0+w_1\alpha (\mathrm{mod}\, m), z_0+z_1\alpha (\mathrm{mod}\, n))$ is square in $\mathbb{Z}_m[\alpha] \times \mathbb{Z}_n[\alpha]$. Thus, $s_\alpha(nm) \leq s_\alpha(n).s_\alpha(m)$. The previous two inclusions lead us to the result $s_\alpha(nm) = s_\alpha(n).s_\alpha(m)$.

It is clear that any quadratic residue is a square modulo n. Hence to prove that $q_\alpha(n)$ is a multiplicative function, we used Proposition [2.1] and the fact that $\gcd(a, nm) = 1$ if and only if $\gcd(a, n) = 1$ and $\gcd(a, m) = 1$. □

Since both $s_\alpha(n)$ and $q_\alpha(n)$ are multiplicative functions, we can compute $s_\alpha(n)$ and $q_\alpha(n)$ for any n, based on the prime factorization of n. So if we can find a closed-form formulas of these functions on the powers of primes, then our job will be hold.

3. Quadratic residues in $\mathbb{Z}_n[\alpha]$

In this section, we will study and count the quadratic residues in the ring $\mathbb{Z}_n[\alpha]$.

The quadratic residues in the ring $\mathbb{Z}_n$ have been completely characterized in [2]. W.D. Stangl in [1] derived a closed-form formula for the function $q(n)$, for any n, based on the prime factorization of n.

Proposition 3.1. *Let p be a prime number. Then:*

$$q(p^k) = \begin{cases} 1, & \text{if } p = 2 \text{ and } k = 1 \text{ or } 2, \\ 2^{k-3}, & \text{if } p = 2 \text{ and } k \geq 3 \\ \frac{(p^k - p^{k-1})}{2}, & \text{if } p \neq 2 \text{ and } k \geq 1. \end{cases}$$

The following theorem gives us the strong relationship between the quadratic residues in $\mathbb{Z}_{p^k}$ and $\mathbb{Z}_{p^k}[\alpha]$, where p is an odd prime.

Theorem 3.1. *Let p be an odd prime and $k \geq 1$, then $a + b\alpha$ is a quadratic residue in $\mathbb{Z}_{p^k}[\alpha]$ if and only if a is a quadratic residue in $\mathbb{Z}_{p^k}$.*

Proof. Suppose a is a quadratic residue in $\mathbb{Z}_{p^k}$, then $a \equiv c^2 (\mathrm{mod}\, p^k)$ for some $c \in \mathbb{Z}_{p^k}$. Since $\gcd(a, p^k) = 1$, one can easily prove that $\gcd(c, p^k) = 1$, so c is a unit in $\mathbb{Z}_{p^k}$. Thus,$a + b\alpha \overset{\alpha}{\equiv} \left(c^2 + b\alpha\right) (\mathrm{mod}\, p^k) \overset{\alpha}{\equiv} \left(c + (2c)^{-1} b\alpha\right)^2 (\mathrm{mod}\, p^k)$.

It is clear that $a + b\alpha$ is a quadratic residue in $\mathbb{Z}_n[\alpha]$. For the other direction, we leave it as an easy excercise to the reader. □

The following corollary is a natural consequence of Theorem [3.1].

Corollary 3.1. *Let p be an odd prime. Then $q_\alpha(p^k) = p^k q(p^k)$ for all $k \geq 1$.*

Theorem 3.2. *For all $k \geq 1$, $a + b\alpha$ is a quadratic residue in $\mathbb{Z}_{2^k}[\alpha]$ if and only if a is a quadratic residue in $\mathbb{Z}_{2^k}$ and b is even.*

Proof. Suppose that $a + b\alpha$ is a quadratic residue in $\mathbb{Z}_{2^k}[\alpha]$. Then, there exists a unit $c + d\alpha$ in $\mathbb{Z}_{2^k}[\alpha]$ such that

$$a + b\alpha \overset{\alpha}{\equiv} [c + d\alpha]^2 (\mathrm{mod}\, 2^k)$$

so,

$$\begin{aligned} a &\equiv c^2 (\mathrm{mod}\, 2^k) \quad \text{and} \\ b &\equiv 2cd (\mathrm{mod}\, 2^k). \end{aligned}$$

It is obvious that a is a quadratic residue in $\mathbb{Z}_{2^k}$ and $2|b$, so b is even. Conversely, suppose that a is a quadratic residue in $\mathbb{Z}_{2^k}$ and b is even. Then there exists a unit c in $\mathbb{Z}_{2^k}$ such that $a \equiv c^2 (\mathrm{mod}\, 2^k)$. Also, since b is even, $b = 2t$ for some $t \in \mathbb{Z}_{2^k}$. Hence

$$\begin{aligned} a + b\alpha &\overset{\alpha}{\equiv} c^2 + b\alpha (\mathrm{mod}\, 2^k) \\ &\overset{\alpha}{\equiv} c^2 + 2t\alpha (\mathrm{mod}\, 2^k) \\ &\overset{\alpha}{\equiv} [c + c^{-1} t\alpha]^2 (\mathrm{mod}\, 2^k). \end{aligned}$$

So, $a + b\alpha$ is a quadratic residue in $\mathbb{Z}_{2^k}[\alpha]$. □

Corollary 3.2. *$q_\alpha(2^k) = 2^{k-1} q(2^k)$ for all $k \geq 1$.*

Proof. By Theorem [3.2], one can deduce that

$$\begin{aligned} q_\alpha(2^k) &= [\text{number of even elements in } \mathbb{Z}_{2^k}[\alpha]].q(2^k) \\ &= [2^k - \phi(2^k)].q(2^k) \\ &= 2^{k-1} q(2^k). \quad \square \end{aligned}$$

Using Proposition [3.1], we can summarize the results in Corollary [3.1] and Corollary [3.2] in the following theorem

Theorem 3.3. *Let p be a prime number. Then:*

$$q_\alpha(p^k) = \begin{cases} 1, & \text{if } p = 2 \text{ and } k = 1, \\ 2, & \text{if } p = 2 \text{ and } k = 2, \\ 2^{2k-4}, & \text{if } p = 2 \text{ and } k \geq 3, \\ \frac{p^k\left(p^k - p^{k-1}\right)}{2}, & \text{if } p \neq 2 \text{ and } k \geq 1. \end{cases}$$

Hence, if we write n as product of its prime factors, then it is easy to count all quadratic residues in $\mathbb{Z}_n[\alpha]$.

4. Squares in $\mathbb{Z}_n[\alpha]$

In this section, we will study and count the squares in the ring $\mathbb{Z}_n[\alpha]$.

Firstly, we introduce a proposition, see [1], concerning the number of squares $s(p^k)$ in the ring $\mathbb{Z}_{p^k}$ for any prime p.

Proposition 4.1. *1. If p is an odd prime, then*

(a) $s(p) = \frac{p+1}{2}$;

(b) $s(p^2) = \frac{p^2-p+2}{2}$;

(c) For $k \geq 3$, $s(p^k) = \begin{cases} \frac{p^{k+1}+p+2}{2(p+1)}, & \text{if } k \text{ is even}, \\ \frac{p^{k+1}+2p+1}{2(p+1)}, & \text{if } k \text{ is odd}. \end{cases}$;

2. $s(2^k) = \begin{cases} \frac{2^{k-1}+4}{3}, & \text{if } k \text{ is even}, \\ \frac{2^{k-1}+5}{3}, & \text{if } k \text{ is odd and } k \geq 3 \end{cases}$.

The following lemma is obtained directly and it will help us to investigate the squares in the ring $\mathbb{Z}_n[\alpha]$.

Lemma 4.1. *Let p be any prime integer. Then the sets $A_i = \{x \in \mathbb{Z}_{p^k} : gcd(x, p^k) = p^i\}$ where $0 \leq i \leq k-1$, and $A_k = \{0\}$ form a partition for the ring $\mathbb{Z}_{p^k}$.*

Recall that the set A_0 is called the set of units, and its group under multiplication modulo p^k.

Now, we will use the notation: $s(A_i)$ to indicate number of squares of $\mathbb{Z}_{p^k}$ in the set A_i.

Lemma 4.2. *Let p be any prime integer and let k be an even integer. Then for $0 \leq i \leq k-1$, we have* $s(A_i) = \begin{cases} q(p^{k-i}), & \text{if } i \text{ is even}, \\ 0, & \text{if } i \text{ is odd}. \end{cases}$

Proof. By Lemma [4.1], $A_i = \{x \in \mathbb{Z}_{p^k} : \gcd(x, p^k) = p^i\}$. Hence

$$\begin{aligned} A_i &= \{x \in \mathbb{Z}_{p^k} : \gcd(\frac{x}{p^i}, p^{k-i}) = 1\} \\ &= \{p^i y \in \mathbb{Z}_{p^k} : \gcd(y, p^{k-i}) = 1\} \\ &= p^i\{y \in \mathbb{Z}_{p^k} : \gcd(y, p^{k-i}) = 1\} \\ &= p^i U(\mathbb{Z}_{p^{k-i}}). \end{aligned}$$

Thus, it is obvious that if i is even, then the squares in A_i are identical with the squares in $p^i U(\mathbb{Z}_{p^{k-i}})$. that is because p^i is square in $\mathbb{Z}_{p^k}$. So, number of squares in A_i is equivalent to the number of quadratic residues in $\mathbb{Z}_{p^{k-i}}$, i.e. $s(A_i) = q(p^{k-i})$. On the other hand, if i is odd, then A_i will never be have squares. Since p^i is not square in $\mathbb{Z}_{p^k}$. □

Lemma 4.3. *Let p be an odd prime, k be an even integer and let $a \in A_{2j}$ (as defined in Lemma [4.1]) for $1 \leq j \leq \frac{k}{2}$. Then $a + b\alpha$ is a square in $\mathbb{Z}_{p^k}[\alpha]$ if and only if a is a square in $\mathbb{Z}_{p^k}$ and $p^j | b$.*

Proof. Suppose that $a + b\alpha$ is a square in $\mathbb{Z}_{p^k}[\alpha]$. Then, there exists $c + d\alpha \in \mathbb{Z}_{p^k}[\alpha]$ such that $a + b\alpha \overset{\alpha}{\equiv} [c + d\alpha]^2 (\mathrm{mod}\, p^k)$. Hence

$$\begin{aligned} a &\equiv c^2 (\mathrm{mod}\, p^k) \quad \text{and} \\ b &\equiv 2cd (\mathrm{mod}\, p^k). \end{aligned}$$

Obviously, a is a square in $\mathbb{Z}_{p^k}$. Now, because $a \in A_{2j}$, we have $p^{2j} | a$. So $p^j | c$. Thus, by the second congruence above, $p^j | b$.

Conversely, suppose a is a square in $\mathbb{Z}_{p^k}$ and $p^j | b$. Then $a \equiv c^2 (\mathrm{mod}\, p^k)$ for some $c \in \mathbb{Z}_{p^k}$ and $b = p^j t$ for some $t \in \mathbb{Z}$. Since $a \in A_{2j}$, one can deduce that $c = p^j r$ with $\gcd(r, p) = 1$. Thus, we get

$$\begin{aligned} a + b\alpha &\overset{\alpha}{\equiv} c^2 + b\alpha (\mathrm{mod}\, p^k) \\ &\overset{\alpha}{\equiv} (p^j r)^2 + p^j t\alpha (\mathrm{mod}\, p^k) \\ &\overset{\alpha}{\equiv} [p^j r + 2^{-1} r^{-1} t\alpha]^2 (\mathrm{mod}\, p^k). \end{aligned}$$

Hence, $a + b\alpha$ is a square in $\mathbb{Z}_{p^k}[\alpha]$. □

The previous lemmas (Lemma [4.1], Lemma [4.2] and Lemma [4.3]) will play a key role in counting the number of squares in $\mathbb{Z}_{p^k}[\alpha]$. We will use the notation: $s_\alpha(A_i)$ to denote number of the squares in $\mathbb{Z}_{p^k}[\alpha]$ that has the form $a + b\alpha$, where $a \in A_i$, (Note that by Lemma [4.2] and Lemma [4.3]: If i is odd, then $s_\alpha(A_i) = 0$). Now, let us define the set $D_i = \{b \in \mathbb{Z}_{p^k} : p^i | b\}$. It is clear that $D_i = \bigcup_{r=i}^{k} A_r$. Note that $D_0 = \mathbb{Z}_{p^k}$. Also, since the sets $A_0, A_1, \ldots, A_k$ are disjoint, then $D_i = D_{i-1} - A_{i-1}$, for $i \geq 1$. Hence, we have the following lemma.

Lemma 4.4. *For any positive integer k, $|D_i| = p^{k-i}$, for $i \geq 1$.*

Proof. By the definition of A_i, one can prove $|A_i| = \phi(p^{k-i})$. Thus, the result can be obtained easily by induction. □

Theorem 4.1. *Let p be an odd prime. If k is even, then*

$$s_\alpha(p^k) = \frac{p^{2(k+1)} + p^{\frac{k}{2}}(p^2+2p+2)}{2(p^2+p+1)}.$$

Proof.

$$\begin{aligned}
s_\alpha(p^k) &= \sum_{i=0}^{k} s_\alpha(A_i), \\
&= s_\alpha(A_0) + s_\alpha(A_2) + s_\alpha(A_4) + \cdots + s_\alpha(A_{k-2}) + s_\alpha(A_k) \\
&= s_\alpha(A_0) + |D_1|\, s(A_2) + |D_2|\, s(A_4) + \cdots + \left|D_{\frac{k-2}{2}}\right| s(A_{k-2}) + \left|D_{\frac{k}{2}}\right| s(A_k) \\
&= q_\alpha(p^k) + p^{k-1}s(A_2) + p^{k-2}s(A_4) + \cdots + p^{k-(\frac{k-2}{2})}s(A_{k-2}) + p^{\frac{k}{2}} \\
&= p^k q(p^k) + p^{k-1}q(p^{k-2}) + p^{k-2}q(p^{k-4}) + \cdots + p^{\frac{k+2}{2}}q(p^2) + p^{\frac{k}{2}} \\
&= \frac{\left(p^{2k} - p^{2k-1}\right) + \left(p^{2k-3} - p^{2k-4}\right) + \cdots + \left(p^{\frac{k+6}{2}} - p^{\frac{k+4}{2}}\right) + 2p^{\frac{k}{2}}}{2} \\
&= \frac{p^{2k+2} + p^{\frac{k+4}{2}} + 2p^{\frac{k+2}{2}} + 2p^{\frac{k}{2}}}{2(p^2+p+1)} \\
&= \frac{p^{2(k+1)} + p^{\frac{k}{2}}(p^2+2p+2)}{2(p^2+p+1)}.
\end{aligned}$$

□

To count number of squares in $\mathbb{Z}_{p^k}[\alpha]$ where p is an odd prime and k is odd, we need the following lemmas.

The following lemma is probably well known but does not seem to appear in the literature.

Lemma 4.5. *Let p be any prime. If $p^{2t+1}|c^2$, then $p^{t+1}|c$.*

Lemma 4.6. *Let p be an odd prime, $k = 2t+1$ be an odd integer and let $a \in A_{2j}$ (as defined in Lemma [4.1]). Then, for $1 \le j \le t$, we have*

1. *$a + b\alpha$ is a square in $\mathbb{Z}_{p^k}[\alpha]$ if and only if a is a square in $\mathbb{Z}_{p^k}$ and $p^j|b$.*
2. *$b\alpha$ is a square in $\mathbb{Z}_{p^k}[\alpha]$ if and only if $p^{\frac{k+1}{2}}|b$.*

Proof. The proof is similar to the proof of Lemma [4.3]. Hence it is omitted. □

Lemma 4.7. *Let p be any prime integer and let k be an odd integer. Then, for $1 \le j \le \frac{k-1}{2}$, we have* $s(A_i) = \begin{cases} q(p^{k-i}), & \text{if } i \text{ is even}, \\ 0, & \text{if } i \text{ is odd}. \end{cases}$

Proof. Similar to the proof of Lemma [4.2]. □

Theorem 4.2. *Let p be an odd prime. If k is odd, then*

$$s_\alpha(p^k) = \frac{p^{2(k+1)} + p^{\frac{k-1}{2}}(2p^2+p+2)}{2(p^2+p+1)}.$$

Proof.

$$\begin{aligned}
s_\alpha(p^k) &= \sum_{i=0}^{k} s_\alpha(A_i), \\
&= s_\alpha(A_0) + s_\alpha(A_2) + s_\alpha(A_4) + \cdots + s_\alpha(A_{k-1}) + s_\alpha(A_k) \\
&= s_\alpha(A_0) + |D_1|\, s(A_2) + |D_2|\, s(A_4) + \cdots + \left|D_{\frac{k-1}{2}}\right| s(A_{k-1}) + \left|D_{\frac{k+1}{2}}\right| s(A_k) \\
&= q_\alpha(p^k) + p^{k-1}s(A_2) + p^{k-2}s(A_4) + \cdots + p^{k-(\frac{k-1}{2})}s(A_{k-1}) + p^{k-(\frac{k+1}{2})} \\
&= p^k q(p^k) + p^{k-1}q(p^{k-2}) + p^{k-2}q(p^{k-4}) + \cdots + p^{\frac{k+1}{2}}q(p) + p^{\frac{k-1}{2}} \\
&= \frac{\left(p^{2k} - p^{2k-1}\right) + \left(p^{2k-3} - p^{2k-4}\right) + \cdots + \left(p^{\frac{k+3}{2}} - p^{\frac{k+1}{2}}\right) + 2p^{\frac{k-1}{2}}}{2} \\
&= \frac{p^{2k+2} + 2p^{\frac{k+3}{2}} + p^{\frac{k+1}{2}} + 2p^{\frac{k-1}{2}}}{2(p^2+p+1)} \\
&= \frac{p^{2(k+1)} + p^{\frac{k-1}{2}}(2p^2+p+2)}{2(p^2+p+1)}.
\end{aligned}$$

□

For completeness, let us study the case when $p = 2$. To do this, we present the following lemmas.

Lemma 4.8. *Let k be an even integer and let $a \in A_{2j}$ (as defined in Lemma [4.1]), for $1 \leq j \leq \frac{k}{2}$. Then, $a + b\alpha$ is a square in $\mathbb{Z}_{2^k}[\alpha]$ if and only if a is a square in $\mathbb{Z}_{2^k}$ and $2^{j+1}|b$.*

Proof. Suppose that $a + b\alpha$ is a square in $\mathbb{Z}_{2^k}[\alpha]$. Then, there exists $c + d\alpha \in \mathbb{Z}_{2^k}[\alpha]$ such that $a + b\alpha \overset{\alpha}{\equiv} [c + d\alpha]^2 (\mathrm{mod}\, 2^k)$. Hence

$$\begin{aligned}
a &\equiv c^2 (\mathrm{mod}\, 2^k) \quad \text{and} \\
b &\equiv 2cd (\mathrm{mod}\, 2^k)
\end{aligned}$$

Obviously, a is a square in $\mathbb{Z}_{2^k}$. Now, because $a \in A_{2j}$, we have $2^{2j}|a$. So, $2^j|c$. Thus, by the second congruence above, $2^{j+1}|b$.

Conversely, suppose a is a square in $\mathbb{Z}_{2^k}$ and $2^{j+1}|b$. Then, $a \equiv c^2 (\mathrm{mod}\, 2^k)$ for some $c \in \mathbb{Z}_{2^k}$ and $b = 2^{j+1}t$ for some $t \in \mathbb{Z}$. Since $a \in A_{2j}$, one can deduce that $c = 2^j r$ with $\gcd(r, 2) = 1$. Thus, we get

$$\begin{aligned}
a + b\alpha &\overset{\alpha}{\equiv} c^2 + b\alpha (\mathrm{mod}\, 2^k) \\
&\overset{\alpha}{\equiv} (2^j r)^2 + 2^{j+1}t\alpha (\mathrm{mod}\, 2^k) \\
&\overset{\alpha}{\equiv} [2^j r + r^{-1}t\alpha]^2 (\mathrm{mod}\, 2^k).
\end{aligned}$$

Hence, $a + b\alpha$ is a square in $\mathbb{Z}_{2^k}[\alpha]$. □

Lemma 4.9. *Let $k = 2t + 1$ be an odd integer and let $a \in A_{2j}$ (as defined in Lemma [4.1]) for $1 \leq j \leq t$ $(= \frac{k-1}{2})$. Then*

1. *$a + b\alpha$ is a square in $\mathbb{Z}_{2^k}[\alpha]$ if and only if a is a square in $\mathbb{Z}_{2^k}$ and $2^{j+1}|b$.*
2. *$b\alpha$ is a square in $\mathbb{Z}_{2^k}[\alpha]$ if and only if $2^{\frac{k+3}{2}}|b$.*

Proof. Using Lemma [4.5], then the idea of the proof of (1) is similar to the proof of Lemma [4.6] above. So, we skip it. Thus, we will only prove (2). Suppose that $b\alpha$ is a square in $\mathbb{Z}_{2^k}[\alpha]$. So, there exists $c + d\alpha \in \mathbb{Z}_{2^k}[\alpha]$ such that $b\alpha \overset{\alpha}{\equiv} [c + d\alpha]^2 (\mathrm{mod}\, 2^k)$. Hence $b\alpha \overset{\alpha}{\equiv} c^2 + 2cd\alpha (\mathrm{mod}\, 2^k)$. It is clear that $2^k|c^2$, and $b \equiv 2cd (\mathrm{mod}\, 2^k)$. Since k is odd and by Lemma [4.5], we get $2^{\frac{k+1}{2}}|c$. Now because of $b \equiv 2cd (\mathrm{mod}\, 2^k)$, we have $2^{\frac{k+1}{2}+1}|b$. Thus $2^{\frac{k+3}{2}}|b$. To prove the other implication, suppose that $2^{\frac{k+3}{2}}|b$. So $b = 2^{\frac{k+1}{2}+1}r$ for some $r \in \mathbb{Z}$. Hence

$$\begin{aligned} b\alpha &\overset{\alpha}{\equiv} 2^{\frac{k+1}{2}+1} r\alpha (\mathrm{mod}\, 2^k) \\ &\overset{\alpha}{\equiv} [2^{\frac{k+1}{2}} + r\alpha]^2 (\mathrm{mod}\, 2^k). \end{aligned}$$

Thus, $b\alpha$ is a square in $\mathbb{Z}_{2^k}[\alpha]$. □

Now, we are ready to count the number of squares in the ring $\mathbb{Z}_{2^k}[\alpha]$.

Theorem 4.3. *Let k be a positive integer. Then*

1. *$s_\alpha(2) = 2$, and $s_\alpha(2^2) = 3$.*
2. *If k is even and $k \geq 3$, then $s_\alpha(2^k) = \frac{2^{2k-1} - 2^{2k-(\frac{3k}{2}-2)}}{7} + 3(2^{\frac{k}{2}-1})$.*
3. *If k is odd and $k \geq 3$, then $s_\alpha(2^k) = \frac{2^{2k-1} - 2^{2k-(\frac{3k-1}{2})}}{7} + 3(2^{\frac{k-3}{2}})$.*

Proof. (1) Obvious

(2) Suppose that, k is even. Then:

$$\begin{aligned} s_\alpha(2^k) &= \sum_{i=0}^{k} s_\alpha(A_i), \text{ by Lemma [4.2], we have} \\ &= \sum_{j=0}^{\frac{k-2}{2}} s_\alpha(A_{2j}) + s_\alpha(A_k) \\ &= s_\alpha(A_0) + s_\alpha(A_2) + s_\alpha(A_4) + \cdots s_\alpha(A_{k-4}) + s_\alpha(A_{k-2}) + s_\alpha(A_k) \\ &= q_\alpha(2^k) + |D_2|\, s(A_2) + |D_3|\, s(A_4) + \cdots \left|D_{\frac{k-4}{2}+1}\right| s(A_{k-4}) + \\ &\left|D_{\frac{k-2}{2}+1}\right| s(A_{k-2}) + \left|D_{\frac{k}{2}+1}\right| s(A_k) \\ &= q_\alpha(2^k) + 2^{k-2} s(A_2) + 2^{k-3} s(A_4) + \cdots 2^{k-(\frac{k}{2}-1)} s(A_{k-4}) + \\ &2^{k-(\frac{k}{2})} s(A_{k-2}) + 2^{k-(\frac{k+2}{2})} \end{aligned}$$

$$= 2^{2k-4} + 2^{k-2}q(2^{k-2}) + 2^{k-3}q(2^{k-4}) + \cdots + 2^{k-(\frac{k}{2}-1)}q(2^{k-(k-4)}) +$$
$$2^{\frac{k}{2}}q(2^2) + 2^{k-(\frac{k+2}{2})}$$
$$= 2^{2k-4} + 2^{k-2}2^{(k-2)-3} + 2^{k-3}2^{(k-4)-3} + \cdots + 2^{k-(\frac{k}{2}-1)}2 +$$
$$2^{\frac{k}{2}} + 2^{\frac{k}{2}-1}$$
$$= 2^{2k-4} + 2^{2k-7} + 2^{2k-10} + \cdots + 2^{2k-(\frac{3k}{2}-2)} + 2^{\frac{k}{2}} + 2^{\frac{k}{2}-1}$$
$$= \frac{2^{2k-2} + 2^{2k-3} + 2^{2k-4} + 2^{2k-5} + 2^{2k-6} + 2^{2k-7}}{7} + \cdots +$$
$$\frac{2^{2k-(\frac{3k}{2}-4)} + 2^{2k-(\frac{3k}{2}-3)} + 2^{2k-(\frac{3k}{2}-2)}}{7} + 2^{\frac{k}{2}} + 2^{\frac{k}{2}-1}$$
$$= \frac{2^{2k-(\frac{3k}{2}-2)}[2^{(\frac{3k}{2}-4)} + 2^{(\frac{3k}{2}-5)} + 2^{(\frac{3k}{2}-6)} + \cdots + 2 + 1]}{7} + 2^{\frac{k}{2}} + 2^{\frac{k}{2}-1}$$
$$= \frac{2^{2k-(\frac{3k}{2}-2)}[2^{(\frac{3k}{2}-4)+1} - 1]}{7} + 2^{\frac{k}{2}} + 2^{\frac{k}{2}-1}$$
$$= \frac{2^{2k-(\frac{3k}{2}-2)}[2^{(\frac{3k}{2}-3)} - 1]}{7} + 2^{\frac{k}{2}} + 2^{\frac{k}{2}-1}$$
$$= \frac{2^{2k-1} - 2^{2k-(\frac{3k}{2}-2)}}{7} + 2^{\frac{k}{2}} + 2^{\frac{k}{2}-1}$$
$$= \frac{2^{2k-1} - 2^{2k-(\frac{3k}{2}-2)}}{7} + 3(2^{\frac{k}{2}-1}).$$

(3) Suppose that k is odd. Then

$$s_\alpha(2^k) = \sum_{i=0}^{k} s_\alpha(A_i), \quad \text{by Lemma [4.2], we have}$$
$$= \sum_{j=0}^{\frac{k-1}{2}} s_\alpha(A_{2j}) + s_\alpha(A_k)$$
$$= s_\alpha(A_0) + s_\alpha(A_2) + s_\alpha(A_4) + \cdots s_\alpha(A_{k-3}) + s_\alpha(A_{k-1}) + s_\alpha(A_k)$$
$$= q_\alpha(2^k) + |D_2|\, s(A_2) + |D_3|\, s(A_4) + \cdots \left|D_{\frac{k-3}{2}+1}\right| s(A_{k-3})$$
$$+ \left|D_{\frac{k-1}{2}+1}\right| s(A_{k-1}) + \left|D_{\frac{k+3}{2}}\right| s(A_k)$$
$$= q_\alpha(2^k) + 2^{k-2}s(A_2) + 2^{k-3}s(A_4) + \cdots 2^{k-(\frac{k-1}{2})}s(A_{k-3})$$
$$+ 2^{k-(\frac{k+1}{2})}s(A_{k-1}) + 2^{k-(\frac{k+3}{2})}$$
$$= 2^{2k-4} + 2^{k-2}q(2^{k-2}) + 2^{k-3}q(2^{k-4}) + \cdots + 2^{k-(\frac{k-1}{2})}q(2^{k-(k-3)})$$
$$+ 2^{\frac{k-1}{2}}q(2) + 2^{k-(\frac{k+3}{2})}$$
$$= 2^{2k-4} + 2^{k-2}2^{(k-2)-3} + 2^{k-3}2^{(k-4)-3} + \cdots + 2^{k-(\frac{k-1}{2})}.1$$

$$
\begin{aligned}
&+ 2^{\frac{k-1}{2}} + 2^{\frac{k-3}{2}} \\
&= 2^{2k-4} + 2^{2k-7} + 2^{2k-10} + \cdots + 2^{2k-(\frac{3k-1}{2})} + 2^{\frac{k-1}{2}} + 2^{\frac{k-3}{2}} \\
&= \frac{2^{2k-2} + 2^{2k-3} + 2^{2k-4} + 2^{2k-5} + 2^{2k-6} + 2^{2k-7}}{7} \\
&+ \cdots + \frac{2^{2k-(\frac{3k-5}{2})} + 2^{2k-(\frac{3k-3}{2})} + 2^{2k-(\frac{3k-1}{2})}}{7} + 2^{\frac{k-1}{2}} + 2^{\frac{k-3}{2}} \\
&= \frac{2^{2k-(\frac{3k-1}{2})}[2^{(\frac{3k-1}{2}-2)} + 2^{(\frac{3k-1}{2}-3)} + 2^{(\frac{3k-1}{2}-5)} + \cdots + 2 + 1]}{7} + 2^{\frac{k-1}{2}} + 2^{\frac{k-3}{2}} \\
&= \frac{2^{2k-(\frac{3k-1}{2})}[2^{(\frac{3k-1}{2}-2)+1} - 1]}{7} + 2^{\frac{k-1}{2}} + 2^{\frac{k-3}{2}} \\
&= \frac{2^{2k-(\frac{3k-1}{2})}[2^{(\frac{3k-1}{2}-1)} - 1]}{7} + 2^{\frac{k-1}{2}} + 2^{\frac{k-3}{2}} \\
&= \frac{2^{2k-1} - 2^{2k-(\frac{3k-1}{2})}}{7} + 2^{\frac{k-1}{2}} + 2^{\frac{k-3}{2}} \\
&= \frac{2^{2k-1} - 2^{2k-(\frac{3k-1}{2})}}{7} + 3(2^{\frac{k-3}{2}}).
\end{aligned}
$$

□

References

[1] D. Stangl, *Counting squares in $\mathbb{Z}_n$*, Math. Mag., 69 (1996), 285-289.

[2] D.M. Burton, *Elementary number theory*, Tata McGraw-Hill Education, 2006.

[3] K.H. Rosen, *Elementary number theory and its applications*, Addison-Wesley, 1993.

[4] G.H. Hardy, E.M. Wright, *An introduction to the theory of numbers*, Oxford University Press, 1979.

[5] T.J. Cox, Y.W. Lam, *Prediction and evaluation of the scattering from quadratic residue diffusers*, J. Acoust. Soc. Am., 95 (1994), 297-305.

[6] S.J. Sepherd, P.W. Sanders, C.T. Stockel, *The quadratic residue cipher and some notes on implementation*, Cryptologia, 17 (1993), 264-282.

[7] E. Pennestri, R. Stefanelli, *Linear algebra and numerical algorithms using dual numbers*, Multibody Syst. Dyn., 18 (2007), 323-344.

[8] Y.L. Gu, J. Luh, *Dual-number transformation and its applications to robotics*, IEEE Journal on Robotics and Automation, 3 (1987), 615-623.

[9] A. Maqtry, *Polynomial functions of the ring of dual numbers over some rings modulo M*, M.S. Jordan University, 2013.

Accepted: December 29, 2019