Self-quasi-regularity in Certain Rings

Allen K. Hoffmeyer

Abstract

Let R be an associative ring, not necessarily commutative and not necessarily having unity. Recall an element $x \in R$ is called *quasi-regular* if and only if solutions y and z exist for the equations $x + y - x * y = 0$ and $x + z - z * x = 0$. In this case $y = z$, and the unique element $\hat{x} = y$ is called the *quasi-inverse* for x. It is well known that $\mathbf{J}(R)$, the Jacobson radical of R, is the unique largest ideal in R consisting entirely of quasi-regular elements. In this paper, we explore the implications of the case $x = \hat{x}$, that is, when a ring element is its own quasi-inverse. We call such elements *self-quasi-regular*. We determine some properties of $sq(R)$, the set of all self-quasi-regular elements, for a general ring, and also compare this set to $\mathbf{J}(R)$. Then, we completely characterize the set $sq(R)$ for all homomorphic images of $\mathbb{Z}$, the integers, including the cardinality and membership of the set $sq(\mathbb{Z}_n)$ for each choice of n.

1 Introduction

In the radical theory of rings, the most common, most useful, and most studied radical is the Jacobson radical. Many characterizations of the Jacobson radical are well known, including that which defines it as the unique largest ideal in a ring consisting entirely of quasi-regular elements. By *ring*, we mean an associative ring R, not necessarily commutative and not necessarily having unity (although many of the concrete examples of this paper are indeed commutative and with 1). By *radical*, we mean an Amitsur-Kurosh radical, as defined in Szász [3], and we denote the Jacobson radical by $\mathbf{J}(R)$. Recall that $x \in R$ is *quasi-regular* if and only if there exists $\hat{x} \in R$ such that $x+\hat{x}-x*\hat{x} = x+\hat{x}-\hat{x}*x = 0$. It is well known that if such an $\hat{x}$ exists, then it is unique. The primary focus of this paper is the study of a certain subset of the collection of quasi-regular elements in a ring R. Thus, we introduce the following

Definition An element $x \in R$ is *self-quasi-regular* if and only if $x = \hat{x}$.

[1] *2000 Mathematics Subject Classifications:* 16U99, 16N20
Keywords and phrases: ring, quasi-regular, Jacobson radical

Thus, an element is self-quasi-regular precisely when it is its own quasi-inverse. We denote the set of all the self-quasi-regular elements of R by $sq(R)$. It is obvious that $sq(R)$ is contained in the set of quasi-regular elements for any ring R, and it easily seen that in many cases this containment is proper. It is of interest to compare $sq(R)$ to $\mathbf{J}(R)$ for a given ring R, although it's easy to see that neither $sq(R) \subseteq \mathbf{J}(R)$ nor $\mathbf{J}(R) \subseteq sq(R)$ holds in general.

Note, the simple substitution of $\hat{x} = x$ reduces the definition of self-quasi-regularity to the following: an element $x \in R$ is self-quasi-regular if and only if $2x - x^2 = 0$ if and only if $x^2 = 2x$. This fact will be useful in many of our proofs, and hence the equation $x^2 = 2x$ will often directly follow the assumption $x \in sq(R)$. Next, observe that $0 + 0 - 0 * 0 = 0$. Hence 0 is self-quasi-regular in any ring. Similarly, if R has unity, say 1_R, then $2 * 1_R \in sq(R)$ because $2 * 1_R + 2 * 1_R - (2 * 1_R)(2 * 1_R) = 4 * 1_R - 4 * 1_R = 0$. Since these elements are self-quasi-regular in any ring (if R has unity), we say that 0 and $2 * 1_R$ are the *trivial* self-quasi-regular elements of R. For emphasis, what we have just proved is the following

Lemma 1.1. *In any ring R, 0 is self-quasi-regular. If R has unity, then $2 * 1_R$ is also self-quasi-regular.*

Some notation will be used frequently throughout the paper. For an element a in a ring R we denote by $\langle a \rangle$ the principal ideal generated by a. Let $\mathbb{N}$ denote the set of natural numbers and let $\mathbb{Z}$ denote the set of integers. Let $\mathbb{Z}_n$ be the proper homomorphic image of $\mathbb{Z}$, such that for $n \in \mathbb{Z}$ the homomorphism has as its kernel the ideal $\langle n \rangle$. For $k \in \mathbb{Z}$, we denote by $\bar{k}$ the equivalence class of k in some $\mathbb{Z}_n$, and we thus distinguish between elements of $\mathbb{Z}$ and their images under a homomorphism. We denote the greatest common divisor of two natural numbers a and b by (a, b).

Next, we now look at some results for self-quasi-regularity in general rings.

2 Self-quasi-regularity in General Rings

In some sense, as far as self-quasi-regularity is concerned, the most trivial kind of ring that we may consider is a field F or a division ring D (also known as a *skew field*), in which case the non-zero elements elements form a multiplicative group. Let 1_D be the unity of D. We claim that the only two self-quasi-regular elements of D are 0 and $2 * 1_D$.

Lemma 2.1. *If D is a division ring and 1_D is the unity of D, then $sq(D) = \{0, 2 * 1_D\}$.*

Proof. We already know that $0, 2 * 1_D \in sq(D)$ from Lemma 1.1. Next, let $0 \neq x \in sq(D)$. Since x is self-quasi-regular, we know that

$x^2 = 2x$. Also, we know that $0 \neq x$ is invertible, that is there exists an $x^{-1} \in D$ such that $x * x^{-1} = x^{-1} * x = 1_D$. So, we have

$$\begin{aligned} & x^2 && = 2x \\ \Leftrightarrow \quad & x^2(x^{-1}) && = 2x(x^{-1}) \\ \Leftrightarrow \quad & x && = 2 * 1_D. \end{aligned}$$

□

So there really is no mystery or intrigue when considering the self-quasi-regular elements of a division ring. It is of interest to note, however, that nearly all elements in a division ring are quasi-regular. Indeed, it is readily shown (using the defining equation for "quasi-regular") that only the unity element 1_D fails to be quasi-regular in a division ring. Thus, although such examples have "many" quasi-regular elements, they have very "few" self-quasi-regular elements. Now, if we relax our restrictions on the ring and consider an arbitrary commutative ring R, then we get much more interesting results. We might ask when the set $sq(R)$ is closed under addition or multiplication.

Lemma 2.2. *Let R be commutative and let $a, b \in sq(R)$. Then $a + b \in sq(R)$ if and only if $2ab = 0$ and $ab \in sq(R)$ if and only if $2ab = 0$.*

Proof. Suppose $a, b \in sq(R)$. Then $a^2 = 2a$ and $b^2 = 2b$. Observe, this gives $a + b \in sq(R)$ if and only if

$$\begin{aligned} & (a+b)^2 && = 2(a+b) \\ \Leftrightarrow \quad & a^2 + 2ab + b^2 && = 2a + 2b \\ \Leftrightarrow \quad & 2a + 2ab + 2b && = 2a + 2b \\ \Leftrightarrow \quad & 2ab && = 0. \end{aligned}$$

Similarly, we have $ab \in sq(R)$ if and only if

$$\begin{aligned} & (ab)^2 && = 2(ab) \\ \Leftrightarrow \quad & a^2b^2 && = 2ab \\ \Leftrightarrow \quad & (2a)(2b) && = 2ab \\ \Leftrightarrow \quad & 4ab && = 2ab \\ \Leftrightarrow \quad & 2ab && = 0. \end{aligned}$$

□

It is interesting to note (especially in the proofs) how self-quasi-regularity allows one to treat multiplication of the elements of $sq(R)$ by using addition. Actually, for any $a \in sq(R)$, we can treat powers of a by considering multiples of a.

Lemma 2.3. *Let R be a ring (not necessarily commutative). Let $a \in sq(R)$. Then, we have $a^m = 2^{m-1}a$ for all $m > 1$.*

Proof. We prove by induction. Let $a \in sq(R)$. Observe, since $a^2 = 2a$, the inductive hypothesis holds for $m = 2$. Now, suppose that $a^k = 2^{k-1}a$ for some $k > 2$. So, we have

$$\begin{aligned} a^{k+1} &= a^k a \\ &= (2^{k-1}a)a \\ &= 2^{k-1}a^2 \\ &= 2^{k-1}(2a) \\ &= 2^k a. \end{aligned}$$

So, by the Principle of Mathematical Induction, we obtain the result $a^m = 2^{m-1}a$ for all $m > 1$. □

Lemma 2.4. *Let R be a commutative ring with unity and let $x \in sq(R)$. Then the following are equivalent:*

a) $x + 2 * 1_R \in sq(R)$

b) $4x = 0$

c) $x^3 = 0$.

Proof. We first prove a) if and only if b). Since $x \in sq(R)$, we know that $x^2 = 2x$. So, observe $x + 2 * 1_R \in sq(R)$ if and only if

$$\begin{aligned} & (x + 2 * 1_R)^2 && = 2(x + 2 * 1_R) \\ \Leftrightarrow\ & x^2 + 4x + 4 * 1_R && = 2x + 4 * 1_R \\ \Leftrightarrow\ & x^2 + 2x && = 0 \\ \Leftrightarrow\ & 2x + 2x && = 0 \\ \Leftrightarrow\ & 4x && = 0. \end{aligned}$$

Lastly, observe that $x^3 = 4x$ by Lemma 2.3, and hence $4x = 0$ if and only if $x^3 = 0$. □

After looking at the closure of $sq(R)$ under the two binary ring operations (i.e. multiplication and addition), it natural to ask what properties would $sq(R)$ have if it were a subring of R.

Corollary 2.5. *Let R be a commutative ring with unity. If $sq(R)$ is a subring of R, then $sq(R)$ has characteristic 4 and is nilpotent of index 3. In particular, if $\mathbf{J}(R) = sq(R)$, then $4\mathbf{J}(R) = 0$ and $\mathbf{J}(R)^3 = 0$.*

Proof. Let $x \in sq(R)$. Since $sq(R)$ is closed with respect to addition and $2 * 1_R \in sq(R)$ in any ring with unity, then $x + 2 * 1_R \in sq(R)$. Thus $4x = 0$ and $x^3 = 0$ by Lemma 2.4, and it is immediate that R has characteristic 4 and is nilpotent of index 3. The last assertion follows because any ideal, including $\mathbf{J}(R)$, must be a subring. □

This corollary illustrates some of the limitations on $sq(R)$ being a subring or ideal in any commutative ring with unity. If we ask when it is possible that $sq(R) = \mathbf{J}(R)$, it is clear that the characteristic and nilpotency play a very strong role for the radical. For example, no commutative domain will have $\mathbf{J}(R) = sq(R)$, even though, in general in a domain, the Jacobson radical can be "large" inside the ring.

We have looked at some general properties of self-quasi-regularity in certain rings with and without unity. We now consider the property of self-quasi-regularity in a certain class of rings, namely those of the form $\mathbb{Z}_n$.

3 Self-quasi-regularity in $\mathbb{Z}_n$

Our goal in the next two sections is to characterize all of the self-quasi-regular elements of each of the rings $\mathbb{Z}_n, n \in \mathbb{N}$. We start with some basic properties of self-quasi-regular elements in $\mathbb{Z}_n$. Recall that we use (a, b) for the greatest common divisor of $a, b \in \mathbb{N}$. Observe $\bar{x} \in sq(\mathbb{Z}_n)$ if and only if $\overline{2x - x^2} = \overline{0}$ if and only if $x^2 - 2x \equiv 0 \pmod{n}$ if and only if $x^2 \equiv 2x \pmod{n}$. However, before we continue it is imperative that we know some cancellation properties for equations of the form $ax \equiv b \pmod{m}$ where $m \in \mathbb{N}$ and $m > 1$. Note the following lemmas (proofs can be found in Dudley [2]):

Lemma 3.1. *If $(a, m) \nmid b$, then $ax \equiv b \pmod{m}$ has no solutions.*

Lemma 3.2. *If $(a, m) = 1$, then $ax \equiv b \pmod{m}$ has exactly one solution.*

Lemma 3.3. *If $ac \equiv bc \pmod{m}$ and $(c, m) = 1$, then $a \equiv b \pmod{m}$.*

Lemma 3.4. *If $ac \equiv bc \pmod{mc}$, then $a \equiv b \pmod{m}$.*

The preceeding four lemmas are vital to the understanding of the following material. We start with some simple observations about self-quasi-regularity in $\mathbb{Z}_n$.

Lemma 3.5. *If $\overline{x} \in sq(\mathbb{Z}_n)$ with $(x, n) = 1$, then $\overline{x} = \overline{2}$.*

Proof. Let $\overline{x} \in sq(\mathbb{Z}_n)$ with $(x, n) = 1$. Since $(x, n) = 1$, we know $x \neq 0$ from which we cancel the x in the equation $x^2 \equiv 2x \pmod{n}$ using Lemma 3.3 to get $x \equiv 2 \pmod{n}$ (or rather, $\overline{x} = \overline{2}$). □

Observe that the previous lemma implies that if $\overline{x} \in sq(\mathbb{Z}_n)$, $\overline{x} \neq \overline{0}$ and $\overline{x} \neq \overline{2}$, then $(x, n) > 1$. This fact will be important in many of the following results.

Lemma 3.6. *If $\overline{x} \in sq(\mathbb{Z}_{2m})$ where $m \in \mathbb{N}$, then $\overline{x} = \overline{2k}$ for some $k \in \mathbb{Z}$.*

Proof. Let $\bar{x} \in sq(\mathbb{Z}_{2m})$ and suppose $\overline{x} = \overline{2k+1}$ for some $k \in \mathbb{Z}$. So, we have

$$\begin{aligned} & (2k+1)^2 && \equiv 2(2k+1) \pmod{2n} \\ \Leftrightarrow \quad & 4k^2+4k+1 && \equiv 4k+2 \pmod{2n} \\ \Leftrightarrow \quad & 4k^2+1 && \equiv 2 \pmod{2n} \\ \Leftrightarrow \quad & 4k^2 && \equiv 1 \pmod{2n}. \end{aligned}$$

Observe that $(4k^2, 2n) \geq 2$ and so $(4k^2, 2n) \nmid 1$ by Lemma 3.1. This contradicts the assumption that $\overline{x}$ was odd. Therefore, we must have $\overline{x} = \overline{2k}$ for some $k \in \mathbb{Z}$. □

Proposition 3.7. *The set $sq(\mathbb{Z}_n)$ is a subring of $\mathbb{Z}_n$ if and only if $n \in \{1, 2, 4, 8\}$.*

Proof. Suppose that $sq(\mathbb{Z}_n)$ is a subring of $\mathbb{Z}_n$, for some $n \in \mathbb{N}$. If $n = 1$ (i.e. the trivial, one element ring), we know that $\{\overline{0}\} = sq(\mathbb{Z}_1) = \mathbb{Z}_1$, and hence $sq(\mathbb{Z}_1)$ is a subring of $\mathbb{Z}_1$. Likewise, if $n = 2$ (i.e. the two element field), then it is easily seen that $\{\overline{0}\} = sq(\mathbb{Z}_2)$ is a subring of $\mathbb{Z}_2$.

Now, assume $n > 2$. We know by closure of the additive group $(sq(\mathbb{Z}_n), +)$, and the fact that $\overline{2} \in \mathbb{Z}_n$ for all $n > 2$, that the set $\{\overline{0}, \overline{2}, \overline{4}, \ldots, \overline{n-4}, \overline{n-2}\} \subseteq sq(\mathbb{Z}_n)$. Now by Lemma (2.2), for each $\overline{x} \in sq(\mathbb{Z}_n)$, since $\overline{2} \in sq(\mathbb{Z}_n)$, we must have that $2 \cdot (\overline{2x}) = \overline{0}$. This implies $4\overline{x} = \overline{0}$, for all $\overline{x} \in sq(\mathbb{Z}_n)$, since $sq(Z_n)$ is assumed to be a subring. However, if $n \geq 9$, for $\overline{x} = \overline{2}$, it is clear that $4 \cdot \overline{2} = \overline{8} \neq \overline{0}$. Thus for any $n \geq 9$, $sq(\mathbb{Z}_n)$ is not a subring of $\mathbb{Z}_n$.

Lastly, we check the values $3 \leq n \leq 8$. It is evident that $\{\overline{0}, \overline{2}\} = sq(\mathbb{Z}_3)$, but the three element field has no proper, nontrivial subrings. Next, it is easily calculated that $\overline{4} \notin sq(Z_n)$ for any $n \in \{5, 6, 7\}$, so that the subring generated by $\overline{2}$ is not entirely self-quasi-regular, and hence $sq(\mathbb{Z}_n)$ is not a subring in these cases. Finally, it is easily checked that $sq(Z_4) = \{\overline{0}, \overline{2}\}$ and that $sq(\mathbb{Z}_8) = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$ and that these are indeed subrings of their respective rings. Thus only for n in the set $\{1, 2, 4, 8\}$ do we have that $sq(\mathbb{Z}_n)$ is a subring of $\mathbb{Z}_n$. It is worth noting that in each of these four cases, $sq(\mathbb{Z}_n) = \mathbf{J}(\mathbb{Z}_n)$, and so $sq(\mathbb{Z}_n)$ is in fact an ideal in $\mathbb{Z}_n$. □

Having taken care of some preliminaries, we are ready to dive into some of the deeper results. We now begin characterizing the self-quasi-regular elements of $\mathbb{Z}_n$ based on the prime power decomposition of n. We begin with two rather simple decompositions $n = p^r$ for some $r > 0$, with p an odd prime and $n = 2^k$ with $k > 2$.

Proposition 3.8. *The only self quasi-regular elements of $\mathbb{Z}_{p^r}$, with $r > 0$ and p an odd prime, are $\bar{0}$ and $\bar{2}$.*

Proof. First, we show the lemma is true for $r = 1$. Observe $\mathbb{Z}_p$ is a field and so by Lemma 2.1 we know that $sq(\mathbb{Z}_p) = \{\overline{0}, \overline{2}\}$. Now, suppose $r > 1$ and let $\overline{x} \in sq(\mathbb{Z}_{p^r})$ with $\overline{x} \neq \overline{0}$ and $\overline{x} \neq \overline{2}$. So, we have $\overline{x} = \overline{sp^k}$ (since $(x, p^r) \neq 1$) where $0 < k < r$, $0 < s < p^{r-k}$, and $(s, p) = 1$. Observe, since $\overline{x} \in sq(\mathbb{Z}_{p^r})$ we obtain

$$\begin{aligned} & x^2 && \equiv 2x \pmod{p^r} \\ \Leftrightarrow\ & (sp^k)^2 && \equiv 2sp^k \pmod{p^r} \\ \Leftrightarrow\ & s^2p^{2k} && \equiv 2sp^k \pmod{p^r} \\ \Leftrightarrow\ & s^2p^k && \equiv 2s \pmod{p^{r-k}}, \text{ by Lemma 3.4,} \\ \Leftrightarrow\ & sp^k && \equiv 2 \pmod{p^{r-k}} \text{ by Lemma 3.3.} \end{aligned} \tag{1}$$

Observe that $p \mid sp^k$ and $p \mid p^{r-k}t$ and so the equivalence (1) implies that $p \mid 2$. However, we know that p is an odd prime and so $p \nmid 2$. Thus, we have contradicted the assumption that $\overline{x} \neq \overline{0}$ and $\overline{x} \neq \overline{2}$. Hence, there does not exist such an $\bar{x} \in sq(\mathbb{Z}_{p^r})$. It follows that $sq(\mathbb{Z}_{p^r}) = \{\overline{0}, \overline{2}\}$ whenever p is an odd prime and $r > 0$. □

Theorem 3.9. *Suppose $n = 2^k$ with $k > 2$. Then $|sq(\mathbb{Z}_n)| = 4$ and in particular $sq(\mathbb{Z}_n) = \{\overline{0}, \overline{2}, \overline{2^{k-1}}, \overline{2^{k-1} + 2}\}$.*

Proof. Suppose $\overline{x} \in sq(\mathbb{Z}_n)$. Since n is even, we know x is even by Lemma 3.6. So $\overline{x} = \overline{2m}$ for some $m \in \mathbb{Z}$. Using substitution gives

$$\begin{aligned} & (2m)^2 && \equiv 2(2m) \pmod{2^k} \\ \Leftrightarrow\ & 4m^2 && \equiv 4m \pmod{2^k} \\ \Leftrightarrow\ & m^2 && \equiv m \pmod{2^{k-2}}, \text{ by Lemma 3.4,} \\ \Leftrightarrow\ & m^2 - m && \equiv 0 \pmod{2^{k-2}} \\ \Leftrightarrow\ & m(m-1) && \equiv 0 \pmod{2^{k-2}} \end{aligned}$$

We now consider two cases:
Case I: Suppose that m is odd. Since m is odd, we have $(m, 2^{k-2}) = 1$ and we obtain

$$\begin{aligned} & m(m-1) && \equiv 0 \pmod{2^{k-2}} \\ \Leftrightarrow\ & m - 1 && \equiv 0 \pmod{2^{k-2}}, \text{ by Lemma 3.3,} \\ \Leftrightarrow\ & m && \equiv 1 \pmod{2^{k-2}} \\ \Leftrightarrow\ & m && = 2^{k-2}r + 1 \end{aligned}$$

for some $r \in \mathbb{Z}$. Observe that $\overline{x} = \overline{2m} = \overline{2^{k-1}r + 2}$. If $r = 2s$ for some $s \in \mathbb{Z}$, then $\overline{x} = \overline{2^{k-1}r + 2} = \overline{2^{k-1}(2s) + 2} = \overline{2^k s + 2} = \overline{2}$. If $r = 2s + 1$ for some $s \in \mathbb{Z}$, then $\overline{x} = \overline{2^{k-1}r + 2} = \overline{2^{k-1}(2s + 1) + 2} = \overline{2^k s + 2^{k-1} + 2} = \overline{2^{k-1} + 2}$. Thus, in Case I, we must have $\overline{x} = \overline{2}$ or $\overline{2^{k-1} + 2}$.

Case II: Suppose that m is even. So, we have $m-1$ is odd, $(m-1, 2^{k-2}) = 1$, and

$$\begin{aligned} & m(m-1) && \equiv 0 \pmod{2^{k-2}} \\ \Leftrightarrow \quad & m && \equiv 0 \pmod{2^{k-2}}, \text{ by Lemma 3.3,} \\ \Leftrightarrow \quad & m && = 2^{k-2}r \end{aligned}$$

where $r \in \mathbb{Z}$. We now have $\overline{x} = \overline{2m} = \overline{2^{k-1}r}$. If $r = 2s$ for some $s \in \mathbb{Z}$, then $\overline{x = 2^{k-1}(2s)} = \overline{2^k s} = \overline{0}$. If $r = 2s+1$ for some $s \in \mathbb{Z}$, then $\overline{x} = \overline{2^{k-1}(2s+1)} = \overline{2^k s + 2^{k-1}} = \overline{2^{k-1}}$. Thus, in Case II, we must have $\overline{x} = \overline{0}$ or $\overline{2^{k-1}}$.

So, all cases being exhausted, if $\overline{x} \in sq(\mathbb{Z}_n)$, with $n = 2^k$ and $k > 2$, then $\overline{x} \in \{\overline{0}, \overline{2}, \overline{2^{k-1}}, \overline{2^{k-1}+2}\}$. □

Observe that $|sq(\mathbb{Z}_2)| = 1$ because $\overline{0}$ is the only self-quasi-regular element of $\mathbb{Z}_2$. Also, $|sq(\mathbb{Z}_{2^2})| = |sq(\mathbb{Z}_4)| = 2$ since $\overline{0}$ and $\overline{2}$ are the only self-quasi-regular elements of $\mathbb{Z}_4$. Thus, we know the set $sq(\mathbb{Z}_{2^k})$ for all $k \in \mathbb{N}$. Next, we consider an n of the form $n = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_k^{\lambda_k}$ where $k \in \mathbb{N}$, the p_i terms are distinct odd primes for all $i = 1, 2, \ldots, k$, and $\lambda_i \in \mathbb{N}$ for all $i = 1, 2, \ldots, k$.

4 Main Results

In this section, we completely characterize the sets $sq(\mathbb{Z}_n)$, for each choice of $n \in \mathbb{N}$. We determine the cardinality of the set, and by our proof techniques, we can explicitly construct the membership of the set $sq(\mathbb{Z}_n)$, given any $n \in \mathbb{N}$.

Theorem 4.1. *Suppose $n = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_k^{\lambda_k}$, where the p_i terms are distinct odd primes and $\lambda_i \in \mathbb{N}$ for all $i = 1, 2, \ldots, k$. Then $|sq(\mathbb{Z}_n)| = 2^k$.*

Proof. First, let $\overline{0} \neq \overline{x} \in sq(\mathbb{Z}_n)$ with $(x, n) = p_b^{e_b} t$ where $0 < e_b < \lambda_b$, $(t, p_b) = 1$ and $b \in \{1, 2, \ldots, k\}$. We show that $e_b < \lambda_b$ leads to a contradiction and so it turns out that if some p_i divides x for $\overline{0} \neq \overline{x} \in sq(\mathbb{Z}_n)$, then it follows that $p_i^{\lambda_i}$ must also divide x. Thus, we need only consider $(x, n) = P$ where $n = PQ$, $P, Q > 1$, and $(P, Q) = 1$. Now, we prove our assertion. Assume $\overline{0} \neq \overline{x} \in sq(\mathbb{Z}_n)$ such that $(x, n) = p_b^{e_b} t$, $0 < e_b < \lambda_b$, $(t, p_b) = 1$, and $b \in \{1, 2, \ldots, k\}$. Since $\overline{x} \in sq(\mathbb{Z}_n)$, we have $x^2 \equiv 2x \pmod{n}$. Observe, since $(x, n) = p_b^{e_b} t$, we have $\overline{x} = \overline{p_b^{e_b} ts}$, where $(s, p_b) = 1$. So, we have

$$\begin{aligned} & x^2 && \equiv 2x \pmod{n} \\ \Leftrightarrow \quad & p_b^{2e_b} t^2 s^2 && \equiv 2p_b^{e_b} ts \pmod{n} \end{aligned}$$

Observe that $p_b^{e_b+1} \mid p_b^{2e_b} t^2 s^2$ and $p_b^{e_b+1} \mid n$, but $p_b^{e_b+1} \nmid 2p_b^{e_b} ts$ and so the equation above has no solution. This is a contradiction of

the fact that $\overline{0} \neq \overline{x} \in sq(\mathbb{Z}_n)$. Hence the assumption $(x,n) = p_b^{e_b}t$ for some $b \in \{1,2,\ldots,k\}$ implies $e_b = 0$ or $e_b = \lambda_b$. So, the only possibilities for (x,n) for some nonzero $\overline{x} \in sq(\mathbb{Z}_n)$ are

$$\begin{aligned}(x,n) &= 1\\ (x,n) &= p_{i_1}^{\lambda_{i_1}}\\ (x,n) &= p_{i_1}^{\lambda_{i_1}}p_{i_2}^{\lambda_{i_2}}\\ &\vdots\\ (x,n) &= p_{i_1}^{\lambda_{i_1}}p_{i_2}^{\lambda_{i_2}}\cdots p_{i_{k-1}}^{\lambda_{i_{k-1}}}.\end{aligned}$$

We now consider each possibility. Observe $(x,n) = 1$ implies that $x = 2$ by Lemma 3.5. Let us consider the general case; that is, we consider $(x,n) = p_{i_1}^{\lambda_{i_1}}p_{i_2}^{\lambda_{i_2}}\cdots p_{i_m}^{\lambda_{i_m}} = P > 1$ where $0 < m < k$ and $n = PQ$ with $(P,Q) = 1$. Note that we may now write $\overline{x} = \overline{sP}$ for some $s \in \mathbb{N}$ with $(s,Q) = 1$. Since $\overline{x} \in sq(\mathbb{Z}_n)$, we have

$$\begin{aligned} & x^2 && \equiv 2x \pmod{n}\\ \Leftrightarrow\ & (sP)^2 && \equiv 2sP \pmod{PQ}\\ \Leftrightarrow\ & s^2P^2 && \equiv 2sP \pmod{PQ}\\ \Leftrightarrow\ & s^2P && \equiv 2s \pmod{Q}, \text{ by Lemma 3.4,}\\ \Leftrightarrow\ & sP && \equiv 2 \pmod{Q}, \text{ by Lemma 3.3.} \end{aligned} \tag{2}$$

We know (2) has a unique solution since $(P,Q) = 1$ and so there does exist a self-quasi-regular element $\overline{x}$ of $\mathbb{Z}_n$ such that $(x,n) = p_{i_1}^{\lambda_{i_1}}p_{i_2}^{\lambda_{i_2}}\cdots p_{i_m}^{\lambda_{i_m}}$ where $0 < m < k$ namely $\overline{x} = \overline{sP}$ where $s \equiv 2P^{-1} \pmod{Q}$. We now count how many such self-quasi-regular elements exist that these equations will generate. Since there are k primes, there are $\binom{k}{1}$ ways for $(x,n) = p_{i_1}^{\lambda_{i_1}}$. Similarly, there are $\binom{k}{2}$ ways for $(x,n) = p_{i_1}^{\lambda_{i_1}}p_{i_2}^{\lambda_{i_2}}$. For the general case, there are $\binom{k}{a}$ ways for $(x,n) = p_{i_1}^{\lambda_{i_1}}p_{i_2}^{\lambda_{i_2}}\cdots p_{i_a}^{\lambda_{i_a}}$ where $0 < a < k$. Summing all of the cases and including the special case where $(x,n) = 1$, there are $1+\binom{k}{1}+\binom{k}{2}+\cdots+\binom{k}{k-1} = 2^k-1$ possibilities where k is the number of distinct primes in the factorization of n. We need also include the other trivial self-quasi-regular element $\bar{0}$. This gives a total of 2^k possible cases that each generate a self quasi-regular element. We now need to show that each equation generates a unique self quasi-regular element. This will demonstrate that $|sq(\mathbb{Z}_n)| = 2^k$.

Our only concern is that two distinct equations of the form of (2) will generate the same self-quasi-regular element of $\mathbb{Z}_n$. We now show that this cannot happen. For the purpose of contradiction, suppose that two distinct equations of the form of (2) generate the same self-quasi-regular element. Consider $n = P_1Q_1 = P_2Q_2$ where

$(P_i, Q_i) = 1$ for $i = 1, 2$, $P_1 \neq P_2$, and $1 < P_1, P_2, < n$. So, we have $\overline{x} = \overline{s_1 P_1} = \overline{s_2 P_2}$ for some $s_1, s_2 \in \mathbb{Z}$ with $(s_1, P_1 Q_1) = (s_2, P_2 Q_2) = 1$. Since $P_1 \neq P_2$, there exists p_i such that that $p_i \mid P_1$ and $p_i \nmid P_2$. However, the odd prime $p_i \mid n$ and hence $p_i \mid Q_2$. Also, we know $p_i \mid x$ and since $(p_i, P_2) = 1$ we know $p_i \mid s_2$. Together, the observed $p_i \mid s_2$ and $p_i \mid Q_2$ imply that $(s_2, P_2 Q_2) \geq p_i > 1$. This is a contradiction of the assumption that one self-quasi-regular element of $\mathbb{Z}_n$ could be generated by two distinct equations of the form of (2). Therefore, we must have that each equation of the form of (2) generates a unique self-quasi-regular element. Thus, we have that $|sq(\mathbb{Z}_n)| = 2^k$ where $n = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_k^{\lambda_k}$, where the p_i's are distinct odd primes and $\lambda_i > 0$ for all $i = 1, 2, \ldots, k$. □

Probably the most striking part of this theorem is that the number of self-quasi-regular elements of $\mathbb{Z}_n$ (for the above prime power decomposition) depends not on the specific primes or their powers. The number of self-quasi-regular elements depends entirely on the number of primes in the prime power decomposition! This is a rather remarkable fact, which will prove to be true for other factorizations of n as well. Next, we look at $n = 2p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_k^{\lambda_k}$, where the p_i terms are distinct odd primes and $\lambda_i > 0$ for all $i = 1, 2, \ldots, k$.

Theorem 4.2. *Suppose $n = 2p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_k^{\lambda_k}$, where the p_i terms are distinct odd primes and $\lambda_i > 0$ for all $i = 1, 2, \ldots, k$. Then $|sq(\mathbb{Z}_n)| = 2^k$.*

Proof. This proof follows the exact same form of the proof of the previous theorem. Let $\overline{0} \neq \overline{x} \in sq(\mathbb{Z}_n)$. The only difference is that the possible values of (x, n) are all multiplied by 2. In a fashion quite analagous to that in the previous theorem, $(x, n) = 2p_b^{e_b} t$ for some $b \in \{1, 2, \ldots, k\}$ implies $e_b = 0$ or λ_b. So, the only possibilities for (x, n) for some nonzero $\overline{x} \in sq(\mathbb{Z}_n)$ are

$$\begin{aligned} (x, n) &= 2 \\ (x, n) &= 2p_{i_1}^{\lambda_{i_1}} \\ &\vdots \\ (x, n) &= 2p_{i_1}^{\lambda_{i_1}} p_{i_2}^{\lambda_{i_2}} \cdots p_{i_{k-1}}^{\lambda_{i_{k-1}}}. \end{aligned}$$

We solve the appropriate linear congruence equations to find the self-quasi-regular elements. A similar counting argument to the one from the last theorem gives that there are 2^k possibilities for the number of self-quasi-regular elements and a similar uniqueness argument guarantees that $|sq(\mathbb{Z}_n)| = 2^k$. □

The next theorem is similarly striking in that it completely constructs what the self-quasi-regular elements of $\mathbb{Z}_n$ are for the remaining prime power decompositions of n. That is, we consider $sq(\mathbb{Z}_n)$

where $n = 2^{\lambda}p_1^{\lambda_1}p_2^{\lambda_2}\cdots p_k^{\lambda_k}$ where the p_i terms are all distinct odd primes and $\lambda_i > 0$ for all $i = 1, 2, \ldots, k$.

Theorem 4.3. *Suppose $n = 2^{\lambda}p_1^{\lambda_1}p_2^{\lambda_2}\cdots p_k^{\lambda_k}$ where the p_i terms are distinct odd primes, $\lambda_i > 0$ for all $i = 1, 2, \ldots, k$, and $\lambda \geq 3$. Then $|sq(\mathbb{Z}_n)| = 2^{k+2}$. Similarly, if $\lambda = 2$, then $|sq(\mathbb{Z}_n)| = 2^{k+1}$.*

Proof. Let $R = p_1^{\lambda_1}p_2^{\lambda_2}\cdots p_k^{\lambda_k}$ and so $n = 2^{\lambda}R$. Since n is even, we know $x \in sq(\mathbb{Z}_n)$ implies $x = 2s$ for some $s \in \mathbb{Z}$, by Lemma 3.6. So, we have $(x, n) = 2^m t$ where $(t, n) = 1$ and $1 \leq m \leq \lambda$. However, it is easily shown that all values of m except for $m \in \{1, \lambda - 1, \lambda\}$ lead to a contradiction. So, we need only consider those m listed above. Let $R = PQ$ where $(P, Q) = 1$ and $Q, P > 1$. We consider all of the possibilities for (x, n) where $0 \neq x \in sq(\mathbb{Z}_n)$. We have the following possibilities:

$$(x, n) = 2 \tag{3}$$
$$(x, n) = 2P \tag{4}$$
$$(x, n) = 2R \tag{5}$$
$$(x, n) = 2^{\lambda-1} \tag{6}$$
$$(x, n) = 2^{\lambda-1}P \tag{7}$$
$$(x, n) = 2^{\lambda-1}R \tag{8}$$
$$(x, n) = 2^{\lambda} \tag{9}$$
$$(x, n) = 2^{\lambda}P \tag{10}$$

We now consider each case.

Case (3): Consider $(x, n) = 2$. So, we have $x = 2t$ where $(t, n) = 1$, for some $t \in \mathbb{Z}$. So, observe

$$\begin{aligned}
& x^2 && \equiv 2x \pmod{n} \\
& 4t^2 && \equiv 4t \pmod{2^{\lambda}R} \\
\Leftrightarrow\ & t^2 && \equiv t \pmod{2^{\lambda-2}R} \\
\Leftrightarrow\ & t && \equiv 1 \pmod{2^{\lambda-2}R} \\
\Leftrightarrow\ & t && = 2^{\lambda-2}Rs + 1, \text{ for some } s \in \mathbb{Z} \\
\Leftrightarrow\ & x = 2t && = 2^{\lambda-1}Rs + 2.
\end{aligned}$$

Observe, if s is even, then $s = 2a$ for some $a \in \mathbb{Z}$ and $\overline{x} = \overline{2^{\lambda}Ra + 2} = \overline{2}$. If s is odd, then $s = 2a+1$ for some $a \in \mathbb{Z}$ and $\overline{x} = \overline{2^{\lambda}Ra + 2^{\lambda-1}R + 2} = \overline{2^{\lambda-1}R + 2}$. So, for $(x, n) = 2$ we obtain two self-quasi-regular elements.

Case (4): Consider $(x, n) = 2P$. So, we have $x = 2Pt$ where

$(t, n) = 1$, for some $t \in \mathbb{Z}$. Observe

$$\begin{array}{rcll} & x^2 & \equiv 2x \pmod{n} \\ \Leftrightarrow & 4P^2t^2 & \equiv 4Pt \pmod{2^\lambda PQ} \\ \Leftrightarrow & Pt & \equiv 1 \pmod{2^{\lambda-2}Q} \\ \Leftrightarrow & t & \equiv P' \pmod{2^{\lambda-2}Q} \\ & & \text{where } PP' \equiv 1 \pmod{2^{\lambda-2}Q}, \\ & & \text{(note: } P' \text{ is guaranteed by Lemma 3.2)}, \\ \Leftrightarrow & t & = 2^{\lambda-2}Qs + P', \text{ for some } s \in \mathbb{Z}, \\ \Leftrightarrow & x & = 2Pt = 2^{\lambda-1}PQs + 2PP'. \end{array}$$

Observe, in a fashion similar to the last case, s even implies $\overline{x} = \overline{2PP'}$ and s odd implies $\overline{x} = \overline{2^{\lambda-1}PQ + 2PP'}$. So, for each different P, there are two self-quasi-regular elements associated with $(x, n) = 2P$.

Case (5): Consider $(x, n) = 2R$. So, we have $x = 2Rt$ where $(t, n) = 1$, for some $t \in \mathbb{Z}$. Observe

$$\begin{array}{rcll} & x^2 & \equiv 2x \pmod{n} \\ \Leftrightarrow & 4R^2t^2 & \equiv 4Rt \pmod{2^\lambda R} \\ \Leftrightarrow & Rt & \equiv 1 \pmod{2^{\lambda-2}} \\ \Leftrightarrow & t & \equiv R' \pmod{2^{\lambda-2}} \\ & & \text{where } RR' \equiv 1 \pmod{2^{\lambda-2}} \\ \Leftrightarrow & t & = 2^{\lambda-2}s + R' \\ \Leftrightarrow & x & = 2Rt = 2^{\lambda-1}Rs + 2RR'. \end{array}$$

Observe, in a fashion similar to the last case, s even implies $\overline{x} = \overline{2RR'}$ and s odd implies $\overline{x} = \overline{2^{\lambda-1}R + 2RR'}$. So, for $(x, n) = 2R$ we obtain two self-quasi-regular elements.

Case (6): Consider $(x, n) = 2^{\lambda-1}$. So, we have $x = 2^{\lambda-1}t$ where $(t, n) = 1$, for some $t \in \mathbb{Z}$. Observe

$$\begin{array}{rcll} & x^2 & \equiv 2x \pmod{n} \\ \Leftrightarrow & 2^{2\lambda-2}t^2 & \equiv 2^\lambda t \pmod{2^\lambda R} \\ \Leftrightarrow & 2^{\lambda-2}t & \equiv 1 \pmod{R} \\ \Leftrightarrow & t & \equiv 2' \pmod{R} \\ & & \text{where } 2^{\lambda-2}2' \equiv 1 \pmod{R} \\ \Leftrightarrow & t & = Rs + 2' \\ \Leftrightarrow & x & = 2^{\lambda-1}t = 2^{\lambda-1}Rs + 2^{\lambda-1}2'. \end{array}$$

Observe, in a fashion similar to the last case, s even implies $\overline{x} = \overline{2^{\lambda-1}2'}$ and s odd implies $\overline{x} = \overline{2^{\lambda-1}R + 2^{\lambda-1}2'}$. So, for $(x, n) = 2^{\lambda-1}$

we obtain two self-quasi-regular elements.

Case (7): Consider $(x,n) = 2^{\lambda-1}P$. So, we have $x = 2^{\lambda-1}Pt$ where $(t,n) = 1$. Observe

$$\begin{aligned}
& x^2 && \equiv 2x \pmod{n} \\
\Leftrightarrow\ & 2^{2\lambda-2}P^2t^2 && \equiv 2^{\lambda}Pt \pmod{2^{\lambda}PQ} \\
\Leftrightarrow\ & 2^{\lambda-2}Pt && \equiv 1 \pmod{Q} \\
\Leftrightarrow\ & t && \equiv A \pmod{Q} \\
& && \text{where } 2^{\lambda-2}PA \equiv 1 \pmod{Q} \\
\Leftrightarrow\ & t && = Qs + A \\
\Leftrightarrow\ & x && = 2^{\lambda-1}Pt = 2^{\lambda-1}PQs + 2^{\lambda-1}PA.
\end{aligned}$$

Observe,in a fashion similar to the last case, s even implies $\overline{x} = \overline{2^{\lambda-1}PA}$ and s odd implies $\overline{x} = \overline{2^{\lambda-1}PQ + 2^{\lambda-1}PA}$. So, for each different P, there are two self-quasi-regular elements associated with $(x,n) = 2^{\lambda-1}P$.

Case (8): Consider $(x,n) = 2^{\lambda-1}R$. Then $\overline{x} = \overline{2^{\lambda-1}Rs}$ for some $s \in \mathbb{Z}$. Observe s odd gives $\overline{x} = \overline{2^{\lambda-1}R}$, the integer s even gives $\overline{x} = \overline{0}$ and so either way $x \in sq(\mathbb{Z}_n)$ since $x^2 \equiv 2^{2\lambda-2}R^2 \equiv (2^{\lambda}R)(2^{\lambda-2}R) \equiv 0 \pmod{n}$ and $2x \equiv 2^{\lambda}R \equiv 0 \pmod{n}$.

We claim that even though $(x,n) = 2^{\lambda}$ and $(x,n) = 2^{\lambda}P$ do not lead to a contradiction, they do lead to redundant self-quasi-regular elements already generated by equations (6) and (7). It is straightforward to verify that this is the case.

Now, having exhausted all possible cases for $1 < (x,n) < n$, we proceed with counting the number of elements that each case gives. Observe $(x,n) = 2$ gives $\overline{x} = \overline{2}$ and so case (3) generates one self-quasi-regular element. For case (4), observe that each distinct choice for P generates 2 self-quasi-regular elements. We now need to determine how many different choices of "P" exist. The total number of ways that $(x,n) = p_{i_1}^{\lambda_{i_1}}$ is $\binom{k}{1}$, the total number of ways that $(x,n) = p_{i_1}^{\lambda_{i_1}}p_{i_2}^{\lambda_{i_2}}$ is $\binom{k}{2}$, and in general the total number of ways that $(x,n) = p_{i_1}^{\lambda_{i_1}}p_{i_2}^{\lambda_{i_2}}\cdots p_{i_a}^{\lambda_{i_a}}$ where $a < k$ is $\binom{k}{a}$. So, counting all the different possibilites for P and remembering that each separate P generates 2 self-quasi-regular elements we get $2(\binom{k}{1}+\binom{k}{2}+\cdots+\binom{k}{k-1}) = 2(2^k-2) = 2^{k+1}-4$. Case (5) generates two quasi-regular-elements as does case (6). Case (7) generates, $2^{k+1}-4$ from the same argument used above. Case (8) generates one self-quasi-regular element, namely $2^{\lambda-1}R$. Observe that cases (9) and (10) are redundant. We finally include the trivial self-quasi-regular element, $\overline{0}$. So, we have

$|sq(\mathbb{Z}_n)| \leq 2+2^{k+1}-4+2+2^{k+1}-4+2+1+1 = 2^{k+1}+2^{k+1} = 2^{k+2}$. Furthermore, an argument similar to that in Theorem (4.1) shows that the self-quasi-regular elements found in the last step are indeed distinct.

Lastly, consider $n = 2^{\lambda}p_1p_2\cdots p_k$ where $\lambda = 2$. We again have cases (3) through (8) generating distinct self-quasi-regular elements. However, for $\lambda = 2$, observe that cases (3), (4), and (5) are the same as cases (6), (7), and (8) respectively. So, there are exactly half as many self-quasi-regular elements as the case where $\lambda \geq 3$. Therefore, there are $\frac{2^{k+2}}{2} = 2^{k+1}$ self-quasi-regular elements for $\lambda = 2$.

□

We summarize the results of this section in a rather concise form in order to understand the pattern that emerges naturally.

Theorem 4.4. *Let n be any positive integer. By the Fundamental Theorem of Arithmetic, we may write $n = 2^{\lambda}p_1^{\lambda_1}p_2^{\lambda_2}\cdots p_k^{\lambda_k}$, where the p_i terms are distinct odd primes, $\lambda \geq 0$, and $\lambda_i > 0$ for all $i = 1, 2, \ldots, k$. (Let $k = 0$ if $n = 2^{\lambda}$.) Then, we have the following:*

$$|sq(\mathbb{Z}_n)| = \begin{cases} 2^k & \text{if } \lambda = 0 \text{ or } 1 \\ 2^{k+1} & \text{if } \lambda = 2 \\ 2^{k+2} & \text{if } \lambda \geq 3 \end{cases}$$

5 Examples and Another Approach

Here, we demonstrate how our proof techniques may explicitly determine the membership of some choice of $sq(\mathbb{Z}_n)$. We have already seen that $\bar{0}$ and $\bar{2}$ are always in $sq(\mathbb{Z}_n)$, and thus we consider only the non-trivial self-quasi-regular elements.

Example Suppose $n = 2250 = 2 \cdot 3^2 \cdot 5^3$. Our main Theorem 4.4 tells us that there should be four elements in the set $sq(\mathbb{Z}_{2250})$, including the trivial self-quasi-regular elements. We now find the other two members of this set. If we consider each case of the proof we realize that we need only consider $P = 3^2$ and $P = 5^3$. We need to solve the equations $3^2s \equiv 1 \pmod{5^3}$ and $5^3t \equiv 1 \pmod{3^2}$ and then substitute these values s, t into $\overline{x} = \overline{2 \cdot 3^2 \cdot s}$ and $\overline{x} = \overline{2 \cdot 5^3 \cdot t}$. It is easy to calculate that the solution to the first linear congruence equation is $s = 14$ which gives $\overline{x} = \overline{252}$. It is also easy to see that $252^2 - 2*252 \equiv 0 \pmod{2250}$. Observe the second congruence equation has the solution of $t = 8$ which gives $\overline{x} = \overline{2 \cdot 5^3 \cdot 8} = \overline{1750}$ and this, too, is easily checked for the property of self-quasi-regularity.

Example Suppose $n = 784 = 2^4 \cdot 7^2$. Our main Theorem 4.4 tells us that there should be eight elements in the set $sq(\mathbb{Z}_{784})$, including the trivial self-quasi-regular elements. Ahead of time, we go ahead

and give $sq(\mathbb{Z}_{784}) = \{0, 2, 98, 296, 392, 394, 490, 688\}$ and show that the linear congruence equations give the desired elements. Following the proof of Theorem 4.3 we consider the different cases (we use $\overline{x}$ to denote an element of $sq(\mathbb{Z}_{784})$):

Case (4): We consider $(x, 2^4 7^2) = 2$. We know $\overline{x} = \overline{2}$ or $\overline{x} = \overline{2 + 2^3 7^2} = \overline{394}$.

Case (5) or (6): These cases are the same because there is only one odd prime to consider. Consider $(x, 2^4 7^2) = 2 \cdot 7^2$ which gives $\overline{x} = \overline{2 \cdot 7^2 \cdot t}$ or $\overline{x} = \overline{2 \cdot 7^2 \cdot t + 2^3 7^2}$. In the form of the proof of the theorem, we need to solve $7^2 t \equiv 1 \pmod{2^2}$ which has the solution $t = 1$ and gives $\overline{x} = \overline{2 \cdot 7^2 \cdot 1} = 98$ Also, we have $\overline{98 + 2^3 7^2} = \overline{490}$ is self-quasi-regular.

Case (7): Consider $(x, 2^4 7^2) = 2^3$ and so $\overline{x} = \overline{2^3 t}$ or $\overline{x} = \overline{2^3 t + 2^3 7^2}$. We need to solve $2^2 t \equiv 1 \pmod{7^2}$ which has the solution of $t = 37$. So, we substitute and obtain $\overline{x} = \overline{2^3 37} = \overline{296}$ or $\overline{x} = \overline{296 + 2^3 7^2}$.

Case(8) or (9): Consider $(x, 2^4 7^2) = 2^3 7^2$ and so $\overline{x} = 2^3 7^2 = 392$ or $\overline{392 + 2^3 7^2} = \overline{0}$.

So, we showed that $sq(\mathbb{Z}_{784})$ is exactly as listed above. So the problem of finding the exact self-quasi-regular elements of $\mathbb{Z}_n$ reduces to the problem of solving linear congruence equations. Indeed, one of the merits of our somewhat labor-intensive approach is the constructive nature of the proofs. For any n, we may construct the set $sq(\mathbb{Z}_n)$ with the methods illustrated in the two previous examples.

Another Approach Dr. David Anderson solved the problem of counting self-quasi-regular elements in $\mathbb{Z}_n$ rather elegantly. He personally communicated this solution via email after we discussed the problem in person at a conference. We include his proof of the theorem both for its beauty and conciseness.

Proof. (Sketch.) Let n be as the theorem states. For any two rings R and S, we have $|sq(R \times S)| = |sq(R)||sq(S)|$. A simple induction argument extends this fact to any number of rings, i.e. if $R_1, R_2, \ldots, R_t$ are any rings, then $|sq(R_1 \times R_2 \times \cdots \times R_t)| = |sq(R_1)||sq(R_2)| \cdots |sq(R_t)|$. By the Chinese Remainder Theorem, for $n = 2^\lambda p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_k^{\lambda_k}$, we have $\mathbb{Z}_n \cong \mathbb{Z}_{2^\lambda} \times \mathbb{Z}_{p_1^{\lambda_1}} \times \mathbb{Z}_{p_2^{\lambda_2}} \times \cdots \times \mathbb{Z}_{p_k^{\lambda_k}}$. Recall that $\mathbb{Z}_2$ has only $\overline{0}$ as a self-quasi-regular element and so $|sq(\mathbb{Z}_2)| = 1$. Also, $|sq(\mathbb{Z}_4)| = 2$ and our Theorem 3.9 gives that $|sq(\mathbb{Z}_{2^\lambda})| = 4$, for any $\lambda > 2$. Recall, our Proposition 3.8 gives that the only self-quasi-regular elements in $\mathbb{Z}_{p^r}$ are $\bar{0}$ and $\bar{2}$. Hence

$|sq(\mathbb{Z}_{p_i^{\lambda_i}})| = 2$ for any i. So, using all of these facts, we know that

$$\begin{aligned} |sq(\mathbb{Z}_n)| &= |sq(\mathbb{Z}_{2^\lambda})||sq(\mathbb{Z}_{p_1^{\lambda_1}})||sq(\mathbb{Z}_{p_2^{\lambda_2}})|\cdots|sq(\mathbb{Z}_{p_k^{\lambda_k}})| \\ &= \begin{cases} 2^k & \text{if } \lambda = 0 \text{ or } 1 \\ 2^{k+1} & \text{if } \lambda = 2 \\ 2^{k+2} & \text{if } \lambda \geq 3 \end{cases} \end{aligned}$$

□

References

[1] Bhattacharya, P.B., S.K. Jain, and S.R. Nagpaul, *Basic Abstract Algebra, 2e*, Cambridge University Press, (New York, 1994).

[2] Dudley, Underwood, *Elementary Number Theory, 2e*, W.H. Freeman and Company, (New York, 1978).

[3] Szász, F.A., *Radicals of Rings*, John Wiley, (New York, 1981).