Vol. 3(Iss. 1) 2026, pp.147-164, African Scientific Annual Review www.asarev.net ISSN: 3007-0902

Enumeration of Subrings and Subring Identities of Strongly Unital Commutative Finite Rings

[1*]Daisy Ingado Binayo
[2]Michael Onyango Ojiema
[3]Maurice Owino Oduor

[1,2] Department of Mathematics, Masinde Muliro University of Science and Technology.
[3]Department of Mathematics and Computer Science, University of Kabianga

[1*] daisybinayo1@gmail.com

https://doi.org/10.51867/asarev.3.1.15

Abstract

In this paper, we derive explicit formulas for the number of subrings of a given strongly unital ring and for the identities of those subrings. From the classification results, every finite commutative strongly unital ring R is isomorphic to $R \cong \prod_{i=1}^{k} \mathbb{Z}_{p_i}$, where $k \geq 2$ and $p_1, \ldots, p_k$ are distinct primes. Equivalently, by the Chinese Remainder Theorem, $R \cong \mathbb{Z}_n$ with $n = p_1 p_2 \cdots p_k$ (square-free and composite). This paper provides closed form formulas for the number of subrings, describes the subrings explicitly, gives the identity of each subring, and discusses combinatorial and algorithmic aspects.

MSC2010 Subject Classification: 16P10, 16B99
Keywords: Strongly unital finite rings, Finite commutative rings, Ring enumeration, Square-free integers.

1 Introduction

The structural analysis of finite commutative rings has long been guided by the fundamental dichotomy established by Wilson [19], wherein every element is classified either as a unit or a zero divisor. While this binary partition provides a useful initial lens, the deeper challenge lies in understanding how the interplay between additive and multiplicative structures gives rise to the rich variety of ring morphologies observed in the finite setting. Over the past five decades, researchers have progressively refined the classification programme, moving from general associative frameworks to increasingly specific invariants. Raghavendran [18] laid the groundwork by systematically studying finite associative rings through their decomposition into local components, while subsequent contributions, such as those of Chikunji [3], extended these ideas by imposing radical restrictions to obtain tractable classes of completely primary rings. Work on unit groups of such rings by Oduor, Ojiema and Mmasi [11], Oduor and Onyango [12], and Were and Oduor [8] has further refined our understanding of the algebraic invariants associated with these structures. Despite these advances, a complete characterisation of all

finite commutative rings in terms of well-understood algebraic building blocks—such as direct products of fields or group rings—remains elusive, particularly when one demands explicit information about the subring structure alongside the global decomposition. A pivotal refinement in this classification effort concerns the behaviour of subrings with respect to multiplicative identities. Corbas [5, 6] provided some of the earliest insights into rings with constrained zero-divisor products, but his work did not systematically address the question of whether subrings necessarily inherit or possess identities. The classical example of $\mathbb{Z}_6$ vividly illustrates the subtlety of this problem: its subrings $\{0, 3\}$ and $\{0, 2, 4\}$ possess identities 3 and 4, respectively, neither of which coincides with the ambient identity 1. This phenomenon demonstrates that the identity of a subring, when it exists, is an independent algebraic datum rather than a derived one, and its determination requires a separate analysis beyond mere ideal membership. Corbas's foundational investigations into rings with finite zero divisors and rings in which products of zero divisors vanish, while important, did not extend to a comprehensive treatment of subring identities, leaving a significant gap that subsequent researchers would begin to address.

The notion of a *strongly unital* ring—a ring in which every subring has a (not necessarily shared) multiplicative identity—was formally investigated by Oman and Stroud [14]. Their principal classification theorem states that a finite ring is strongly unital if and only if it is isomorphic to a finite direct product of absolutely algebraic fields of prime characteristic. In the commutative setting, this reduces to the elegant form

$$R \cong \prod_{i=1}^{k} \mathbb{Z}_{p_i},$$

where $p_1, \ldots, p_k$ are distinct primes. Furthermore, they established that any subring S of such a ring possesses an identity of the form $(e_1, \ldots, e_r, 0, \ldots, 0)$, with the e_i being non-zero idempotents corresponding to the non-trivial coordinates of S. While this result completely characterises the class of rings under consideration, it leaves a significant gap: it does not enumerate the subrings, nor does it provide a closed-form formula for the identity of each subring in terms of the ambient parameters. In short, the classification answers *what* the rings are, but not *how many* subrings they have or *how to compute* their identities explicitly.

This enumeration gap is particularly evident in the cyclic case $R = \mathbb{Z}_n$ with n square-free and composite. By the Chinese Remainder Theorem, such rings fall directly into the strongly unital class. Recent work by Choi and Walker [4] has advanced our understanding of the ideal structure of $\mathbb{Z}_n$ through the lens of n-absorbing ideals, yet their focus on prime-like ideals does not address the comprehensive enumeration of all subrings. Moreover, while it is a standard fact that ideals of $\mathbb{Z}_n$ correspond to divisors of n, the additional fact that *every* subring is an ideal in this setting is rarely highlighted, and the computation of the unique identity element for each divisor-based subring via the Chinese Remainder Theorem has not been systematically developed in the context of strong unitality. Dobbs [7] has contributed to our understanding of when rings are products of fields, and the monographs of McDonald [10] and Karpilovsky [9] provide comprehensive treatments of finite rings and group rings respectively, yet none of these works explicitly addresses the enumeration of subrings and their identities in the canonical strongly unital class. Consequently, there exists no unified reference that explicitly lists the subrings of $\mathbb{Z}_n$ for square-free n, gives their identities, and proves that these

identities are all distinct—a property that is essential for verifying the strong unitality condition.

Beyond the cyclic case, the broader problem of enumerating subrings in direct products of fields with repeated prime factors reveals further unexplored territory. For products of the form $\prod_{i=1}^{h} \mathbb{Z}_{2p_i}$, where the prime 2 appears multiple times, the ring is no longer strongly unital according to the Oman–Stroud criterion. In such settings, subrings such as the diagonal embedding in $(\mathbb{Z}_{2p})^2$ are not direct products of subrings of the individual factors, and their enumeration requires sophisticated combinatorial techniques that have not yet been developed. Recent extensions by Oman and Senkoff [15] to the class of *almost strongly unital* rings—where every proper subring has an identity—demonstrate that the subring identity problem continues to generate new structural questions. However, their work remains focused on classification rather than on explicit counting. Concurrently, the graph-theoretic investigations of zero-divisors initiated by Beck [2] and subsequently advanced by Anderson and Livingston [1] and others such as Owino and Walwenda [17] have enriched our understanding of the combinatorial properties of finite rings, but they operate at a different level of abstraction and do not address the algebraic enumeration problem central to this paper.

A careful synthesis of the literature thus reveals a clear and coherent research gap. While significant strides have been made in classifying finite rings [18, 3], characterising strong unitality [14], studying unit groups [11, 12, 13, 8], investigating ideal structures [4], and exploring zero-divisor graphs [2, 1, 17], no single work provides an explicit, complete, and accessible enumeration of all subrings—along with their identities—for the canonical class of strongly unital finite commutative rings. Moreover, the intrinsic Boolean lattice structure of the subring poset in this class has not been formally articulated, nor has its combinatorial richness been exploited to derive counting formulas. The existing references either treat the classification independently of enumeration or focus on graph-theoretic invariants that are orthogonal to the subring identity problem. This paper is designed to fill these lacunae.

In this paper, we provide a complete solution to the enumeration problem for finite commutative strongly unital rings. We prove that for $R \cong \prod_{i=1}^{k} \mathbb{Z}_{p_i}$ with distinct primes p_i, the subrings are precisely the direct products $S_I = \prod_{i \in I} \mathbb{Z}_{p_i} \times \prod_{i \notin I} \{0\}$ indexed by subsets $I \subseteq \{1, \ldots, k\}$. Consequently, the number of subrings is exactly 2^k, and the multiplicative identity of S_I is the vector with 1 in the i-th coordinate exactly when $i \in I$, and 0 otherwise. We show that these identities are all distinct, thereby confirming the strong unitality condition from an enumerative perspective. In the cyclic case, this yields a divisor-based parametrisation where the subring $d\mathbb{Z}_n$ has identity e_d uniquely determined by $e_d \equiv 0 \pmod{d}$ and $e_d \equiv 1 \pmod{n/d}$.

2 Subrings and Their Identities

Proposition 1. *For $k \in \mathbb{Z}^+$ such that $2k+1$ is a prime integer, the ring $\mathbb{Z}_{2(2k+1)}$ is strongly unital.*

Proof. The ring $\mathbb{Z}_{2(2k+1)}$ has exactly four subrings: $\{0\}$, $2\mathbb{Z}_{2(2k+1)}$, $(2k+1)\mathbb{Z}_{2(2k+1)}$, and $\mathbb{Z}_{2(2k+1)}$. It is easy to verify that:

i. The identity of $\{0\}$ is 0.

ii. The identity of $2\mathbb{Z}_{2(2k+1)}$ is $2k+2$.

iii. The identity of $(2k+1)\mathbb{Z}_{2(2k+1)}$ is $2k+1$.

iv. The identity of $\mathbb{Z}_{2(2k+1)}$ is 1.

So each subring has a distinct identity. □

Proposition 2. *The ring $\mathbb{Z}_{2p}$ has exactly four subrings:*

i. $\{0\}$ *with identity 0.*

ii. $p\mathbb{Z}_{2p} = \{0, p\}$ *with identity p.*

iii. $2\mathbb{Z}_{2p} = \{0, 2, 4, \ldots, 2(p-1)\}$ *with identity* $p+1$.

iv. $\mathbb{Z}_{2p}$ *with identity 1.*

Proof. The divisors of $2p$ are $1, 2, p, 2p$. Since each corresponding ideal has an identity, we can compute these identities. For $d = p$, we solve $e \equiv 0 \pmod{p}$ and $e \equiv 1 \pmod{2}$. The unique solution modulo $2p$ is $e = p$. For $d = 2$, we solve $e \equiv 0 \pmod{2}$ and $e \equiv 1 \pmod{p}$. The solution is $e = p+1$. □

Remark 1. The ring $\mathbb{Z}_{2(2k+1)}$ is strongly unital if and only if $2k+1$ is an odd prime integer.

Example 2.1. *Consider the ring $\mathbb{Z}_{18}$. In this case $2k+1 = 9$ which is not prime. Now, $6\mathbb{Z}_{18}$ is a subring of $\mathbb{Z}_{18}$ without identity. In fact, $6\mathbb{Z}_{18}$ is a nilpotent ideal of $\mathbb{Z}_{18}$. Therefore $\mathbb{Z}_{18}$ is not strongly unital.*

2.1 Properties of the Subrings

Proposition 3. *$2\mathbb{Z}_{2(2k+1)}$ is a subring of $\mathbb{Z}_{2(2k+1)}$ with identity $2k+2$.*

Proof. Let $2t \in 2\mathbb{Z}_{2(2k+1)}$ be an arbitrary element. We need to show that $(2k+2)(2t) = 2t \pmod{2(2k+1)}$. Indeed,

$$2t(2k+2) = 4tk + 4t = 4tk + 2t + 2t = (4k+2)t + 2t = 2t \pmod{4k+2}$$

since the characteristic of the ring $\mathbb{Z}_{2(2k+1)}$ is $4k+2$. □

Proposition 4. *For an odd prime integer $2k+1$, the ring $(2k+1)\mathbb{Z}_{2(2k+1)}$ is a subring of $\mathbb{Z}_{2(2k+1)}$ with identity $2k+1$.*

Proof. Clearly $(2k+1)\mathbb{Z}_{2(2k+1)}$ is closed under subtraction, addition and multiplication. Let $(2k+1)t \in (2k+1)\mathbb{Z}_{2(2k+1)}$. Then

$$((2k+1)t)(2k+1) = 4k^2t + 2kt + 2kt + t = (4k+2)kt + (2k+1)t = (2k+1)t \pmod{4k+2}$$

since $\mathbb{Z}_{2(2k+1)} = 4k+2$. □

Proposition 5. *The subring $2\mathbb{Z}_{2p}$ is a field isomorphic to $\mathbb{Z}_p$.*

Proof. If $2k+1$ is an odd prime integer, then $\gcd(2, 2k+1) = 1$ and the order of the subring $2\mathbb{Z}_{2(2k+1)}$ is $2k+1$. So $2\mathbb{Z}_{2(2k+1)}$ is a field. The order of the group of units $(2\mathbb{Z}_{2(2k+1)})^\times$ is $2k$, so that $2\mathbb{Z}_{2(2k+1)} \cong \mathbb{Z}_{2k}$. Actually, since it's a field of order $p = 2k+1$, it is isomorphic to $\mathbb{Z}_p$. □

Proposition 6. *The subring $p\mathbb{Z}_{2p}$ is isomorphic to $\mathbb{Z}_2$.*

Proof. It has two elements: 0 and p. Since $p^2 \equiv p \pmod{2p}$, p acts as the identity. Thus it is a ring with two elements and identity p, hence isomorphic to $\mathbb{Z}_2$. □

2.2 Maximal Ideals

Proposition 7. *For an odd prime integer $2k+1$, the subring $2\mathbb{Z}_{2(2k+1)}$ is a maximal ideal of $\mathbb{Z}_{2(2k+1)}$.*

Proof. Let $x, y \in 2\mathbb{Z}_{2(2k+1)}$. Then $x = 2t_1$ and $y = 2t_2$ where $t_1, t_2 \in \mathbb{Z}_{2(2k+1)}$. So $x \pm y = 2t_1 \pm 2t_2 = 2(t_1 \pm t_2) \in 2\mathbb{Z}_{2(2k+1)}$, since $t_1 \pm t_2 \in \mathbb{Z}_{2(2k+1)}$.

Suppose $r \in \mathbb{Z}_{2(2k+1)}$, then $rx = r(2t_1) = 2rt_1 \in 2\mathbb{Z}_{2(2k+1)}$ since $rt_1 \in \mathbb{Z}_{2(2k+1)}$. The maximality of $2\mathbb{Z}_{2(2k+1)}$ follows from the fact that the subring consists of zero divisors and any other ideal that contains $2\mathbb{Z}_{2(2k+1)}$ must contain the identity 1 mod $2(2k+1)$, which is $\mathbb{Z}_{2(2k+1)}$ itself. So $\{0\} \subset 2\mathbb{Z}_{2(2k+1)} \subset \mathbb{Z}_{2(2k+1)}$. □

Proposition 8. *The subring $(2k+1)\mathbb{Z}_{2(2k+1)}$ is a maximal ideal of $\mathbb{Z}_{2(2k+1)}$.*

Proof. Let $x, y \in (2k+1)\mathbb{Z}_{2(2k+1)}$. Then $x = (2k+1)t_1$ and $y = (2k+1)t_2$, $t_1, t_2 \in \mathbb{Z}_{2(2k+1)}$. So $x \pm y = (2k+1)t_1 \pm (2k+1)t_2 = (2k+1)(t_1 \pm t_2) \in (2k+1)\mathbb{Z}_{2(2k+1)}$ since $t_1 \pm t_2 \in \mathbb{Z}_{2(2k+1)}$.

Let $r \in \mathbb{Z}_{2(2k+1)}$. Then $rx = r((2k+1)t_1) = (2k+1)rt_1 \in (2k+1)\mathbb{Z}_{2(2k+1)}$ since $rt_1 \in \mathbb{Z}_{2(2k+1)}$. Similarly, $xr \in (2k+1)\mathbb{Z}_{2(2k+1)}$. The inclusion $\{0\} \subset (2k+1)\mathbb{Z}_{2(2k+1)} \subset \mathbb{Z}_{2(2k+1)}$ implies that $(2k+1)\mathbb{Z}_{2(2k+1)}$ is a maximal ideal. □

2.3 Homomorphisms and Isomorphisms

Lemma 1. *The map $f : \mathbb{Z}_{2(2k+1)} \to \mathbb{Z}_{2(2k+1)}/2\mathbb{Z}_{2(2k+1)}$ defined by $x \mapsto x + 2\mathbb{Z}_{2(2k+1)}$ is a ring homomorphism.*

Proof. Let $x_1, x_2 \in \mathbb{Z}_{2(2k+1)}$. Then

$$f(x_1 + x_2) = (x_1 + x_2) + 2\mathbb{Z}_{2(2k+1)} = (x_1 + 2\mathbb{Z}_{2(2k+1)}) + (x_2 + 2\mathbb{Z}_{2(2k+1)}) = f(x_1) + f(x_2).$$

Also

$$f(x_1x_2) = (x_1x_2) + 2\mathbb{Z}_{2(2k+1)} = (x_1 + 2\mathbb{Z}_{2(2k+1)})(x_2 + 2\mathbb{Z}_{2(2k+1)}) = f(x_1)f(x_2).$$

□

Lemma 2. *Consider the canonical projection homomorphism*

$$f : \mathbb{Z}_{2(2k+1)} \longrightarrow \mathbb{Z}_{2(2k+1)}/2\mathbb{Z}_{2(2k+1)}, \qquad f(x) = x + 2\mathbb{Z}_{2(2k+1)}.$$

Then $\ker f = 2\mathbb{Z}_{2(2k+1)}$.

Proof. By definition of the quotient ring,

$$\ker f = \{x \in \mathbb{Z}_{2(2k+1)} \mid x + 2\mathbb{Z}_{2(2k+1)} = 2\mathbb{Z}_{2(2k+1)}\}.$$

The equality $x + 2\mathbb{Z}_{2(2k+1)} = 2\mathbb{Z}_{2(2k+1)}$ holds iff $x \in 2\mathbb{Z}_{2(2k+1)}$. Hence $\ker f = 2\mathbb{Z}_{2(2k+1)}$. □

Lemma 3. *With the same homomorphism f as above, the image of f is isomorphic to $\mathbb{Z}_2$; i.e., $f(\mathbb{Z}_{2(2k+1)}) \cong \mathbb{Z}_2$.*

Proof. By the First Isomorphism Theorem for rings,

$$\mathbb{Z}_{2(2k+1)}/\ker f \cong \mathrm{Im}(f).$$

From Lemma 2, $\ker f = 2\mathbb{Z}_{2(2k+1)}$. Therefore

$$\mathrm{Im}(f) \cong \mathbb{Z}_{2(2k+1)}/2\mathbb{Z}_{2(2k+1)}.$$

The quotient $\mathbb{Z}_{2(2k+1)}/2\mathbb{Z}_{2(2k+1)}$ has exactly two cosets: $2\mathbb{Z}_{2(2k+1)}$ and $1 + 2\mathbb{Z}_{2(2k+1)}$. Hence it is isomorphic to $\mathbb{Z}_2$. □

Lemma 4. *The map*

$$g : \mathbb{Z}_{2(2k+1)} \longrightarrow \mathbb{Z}_{2(2k+1)}/(2k+1)\mathbb{Z}_{2(2k+1)}, \qquad g(x) = x + (2k+1)\mathbb{Z}_{2(2k+1)},$$

is a ring homomorphism.

Proof. For any $x, y \in \mathbb{Z}_{2(2k+1)}$,

$$g(x+y) = (x+y) + (2k+1)\mathbb{Z}_{2(2k+1)} = \big(x + (2k+1)\mathbb{Z}_{2(2k+1)}\big) + \big(y + (2k+1)\mathbb{Z}_{2(2k+1)}\big) = g(x) + g(y),$$

and

$$g(xy) = xy + (2k+1)\mathbb{Z}_{2(2k+1)} = \big(x + (2k+1)\mathbb{Z}_{2(2k+1)}\big)\big(y + (2k+1)\mathbb{Z}_{2(2k+1)}\big) = g(x)g(y).$$

Thus g preserves addition and multiplication; it also maps 1 to $1 + (2k+1)\mathbb{Z}_{2(2k+1)}$, the identity of the quotient ring. Hence g is a ring homomorphism. □

Lemma 5. *For the homomorphism g defined above,*

$$\ker g = (2k+1)\mathbb{Z}_{2(2k+1)}, \qquad \operatorname{Im} g \cong \mathbb{Z}_{2k+1}.$$

Proof. By definition of the quotient ring,

$$\ker g = \{x \in \mathbb{Z}_{2(2k+1)} \mid x + (2k+1)\mathbb{Z}_{2(2k+1)} = (2k+1)\mathbb{Z}_{2(2k+1)}\}.$$

The coset equality holds iff $x \in (2k+1)\mathbb{Z}_{2(2k+1)}$. Hence $\ker g = (2k+1)\mathbb{Z}_{2(2k+1)}$.

The ring $\mathbb{Z}_{2(2k+1)}$ has $2(2k+1)$ elements. The ideal $(2k+1)\mathbb{Z}_{2(2k+1)}$ consists of all multiples of $2k+1$ modulo $2(2k+1)$; its size is 2 because $(2k+1)\cdot 2 = 2(2k+1) \equiv 0$ and $(2k+1)\cdot 1 = 2k+1 \not\equiv 0$. Therefore the quotient ring $\mathbb{Z}_{2(2k+1)}/(2k+1)\mathbb{Z}_{2(2k+1)}$ has

$$\frac{2(2k+1)}{2} = 2k+1$$

elements. Since the quotient of a finite commutative ring by a maximal ideal is a field, this quotient is the field of order $2k+1$, i.e., $\mathbb{Z}_{2k+1}$. By the First Isomorphism Theorem,

$$\operatorname{Im} g \cong \mathbb{Z}_{2(2k+1)}/\ker g = \mathbb{Z}_{2(2k+1)}/(2k+1)\mathbb{Z}_{2(2k+1)} \cong \mathbb{Z}_{2k+1}.$$

□

2.4 Chinese Remainder Theorem Decomposition

Proposition 9. *For any odd prime p, the ring $\mathbb{Z}_{2p}$ decomposes as a direct product:*

$$\mathbb{Z}_{2p} \cong \mathbb{Z}_2 \times \mathbb{Z}_p.$$

Proof. Since 2 and p are distinct primes, $\gcd(2,p) = 1$. The Chinese Remainder Theorem states that for coprime integers m and n, the map

$$\varphi : \mathbb{Z}_{mn} \longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n, \qquad \varphi(x) = (x \bmod m,\ x \bmod n)$$

is a ring isomorphism. Taking $m = 2$ and $n = p$ gives $\mathbb{Z}_{2p} \cong \mathbb{Z}_2 \times \mathbb{Z}_p$.

Alternatively, in terms of ideals, the ideals (2) and (p) in $\mathbb{Z}_{2p}$ satisfy $(2) \cap (p) = \{0\}$ because 2 and p are coprime, and $(2) + (p) = \mathbb{Z}_{2p}$. Hence by the Chinese Remainder Theorem for rings,

$$\mathbb{Z}_{2p} \cong \mathbb{Z}_{2p}/(2) \times \mathbb{Z}_{2p}/(p) \cong \mathbb{Z}_2 \times \mathbb{Z}_p.$$

□

Proposition 10. *Let $k \in \mathbb{Z}^+$ be such that $2k+1$ is prime. Then the ring $\mathbb{Z}_{2(2k+1)}$ is reduced (i.e., it has no nonzero nilpotent elements).*

Proof. Set $p = 2k+1$. By Proposition 9, $\mathbb{Z}_{2p} \cong \mathbb{Z}_2 \times \mathbb{Z}_p$. Both $\mathbb{Z}_2$ and $\mathbb{Z}_p$ are fields, hence have no nonzero nilpotent elements. An element $(a,b) \in \mathbb{Z}_2 \times \mathbb{Z}_p$ is nilpotent iff $(a,b)^n = (a^n, b^n) = (0,0)$ for some $n \geq 1$. Since $\mathbb{Z}_2$ and $\mathbb{Z}_p$ are reduced, $a^n = 0$ implies $a = 0$, and $b^n = 0$ implies $b = 0$. Thus the only nilpotent element in the product is $(0,0)$. Therefore $\mathbb{Z}_{2(2k+1)}$ has no nonzero nilpotent elements; it is reduced. □

2.5 Unit Group of $\mathbb{Z}_{2(2k+1)}$

Theorem 1. *Let $p = 2k+1$ be an odd prime. Then the unit group of $\mathbb{Z}_{2p}$ is cyclic of order $2k$; i.e.,*

$$(\mathbb{Z}_{2p})^\times \cong \mathbb{Z}_{2k}.$$

Proof. Since $\gcd(2,p) = 1$, the Chinese Remainder Theorem yields a ring isomorphism

$$\mathbb{Z}_{2p} \cong \mathbb{Z}_2 \times \mathbb{Z}_p.$$

The unit group of a direct product of rings is the direct product of the unit groups:

$$(\mathbb{Z}_{2p})^\times \cong (\mathbb{Z}_2)^\times \times (\mathbb{Z}_p)^\times.$$

Now $(\mathbb{Z}_2)^\times = \{1\}$ (the trivial group), and because p is prime, $\mathbb{Z}_p$ is a field, so its multiplicative group $(\mathbb{Z}_p)^\times$ is cyclic of order $p-1 = 2k$. Hence

$$(\mathbb{Z}_{2p})^\times \cong \{1\} \times \mathbb{Z}_{2k} \cong \mathbb{Z}_{2k}.$$

Thus the unit group is cyclic of order $2k$. □

Remark 2. The integer k is positive because $p \geq 3$; therefore $2k$ is even. For example, when $p = 3$ $(k = 1)$, $(\mathbb{Z}_6)^\times \cong \mathbb{Z}_2$; when $p = 5$ $(k = 2)$, $(\mathbb{Z}_{10})^\times \cong \mathbb{Z}_4$; and when $p = 7$ $(k = 3)$, $(\mathbb{Z}_{14})^\times \cong \mathbb{Z}_6$.

3 Direct Products and Counting Subrings

3.1 General Formulas for Subrings and Identities

Let $R = \prod_{i=1}^{h} \mathbb{Z}_{2p_i}$ where each p_i is an odd prime (not necessarily distinct). Each factor $\mathbb{Z}_{2p_i}$ has exactly four subrings, which we denote as:

(i) $S_i(0) = \{0\}$ with identity 0_i.

(ii) $S_i(2) = 2\mathbb{Z}_{2p_i}$ with identity $e_i(2) = p_i + 1 \pmod{2p_i}$.

(iiii) $S_i(p) = p_i\mathbb{Z}_{2p_i}$ with identity $e_i(p) = p_i \pmod{2p_i}$.

(iv) $S_i(1) = \mathbb{Z}_{2p_i}$ with identity 1_i.

3.2 Subring Structure of the Canonical Strongly Unital Ring

Theorem 2 (Subring Formula for Direct Products of Distinct Prime Fields)**.** *Let $R = \prod_{i=1}^{k} \mathbb{Z}_{p_i}$ where $p_1, \ldots, p_k$ are distinct primes and $k \geq 2$. Then every subring S of R is of the form*

$$S = \prod_{i=1}^{k} S_i,$$

where each S_i is either $\{0\}$ or $\mathbb{Z}_{p_i}$. Consequently, R has exactly 2^k subrings. Moreover, the identity of such a subring is the vector with 1 in the i-th coordinate precisely when $S_i = \mathbb{Z}_{p_i}$.

Proof. For each index i $(1 \leq i \leq k)$, let $\pi_i : R \to \mathbb{Z}_{p_i}$ be the canonical projection onto the i-th coordinate. Since $\mathbb{Z}_{p_i}$ is a field, its only subrings are $\{0\}$ and $\mathbb{Z}_{p_i}$ itself. Let S be any subring of R. For each i, the image $\pi_i(S)$ is a subring of $\mathbb{Z}_{p_i}$; therefore

$$\pi_i(S) \in \big\{\{0\},\ \mathbb{Z}_{p_i}\big\}.$$

Define $I = \{i \mid \pi_i(S) = \mathbb{Z}_{p_i}\}$. We claim that

$$S = \prod_{i=1}^{k} \pi_i(S) = \Big(\prod_{i\in I} \mathbb{Z}_{p_i}\Big) \times \Big(\prod_{i\notin I} \{0\}\Big).$$

The inclusion $S \subseteq \prod_i \pi_i(S)$ is obvious because each coordinate of any element of S lies in $\pi_i(S)$. Conversely, for each $i \in I$, there exists an element $s^{(i)} \in S$ such that $\pi_i(s^{(i)}) = 1$ (since the projection is onto $\mathbb{Z}_{p_i}$). Consider the product $t = \prod_{i\in I} s^{(i)}$ (taken in R). Because different coordinates have independent components, the element t has 1 in every coordinate $i \in I$ and some value (possibly 0) in coordinates $j \notin I$. However, note that for $j \notin I$, we have $\pi_j(S) = \{0\}$, so every element of S has 0 in those coordinates. Hence t actually has 0 in coordinates $j \notin I$. Thus t is the vector with 1 in coordinates I and 0 elsewhere. Now let $x = (x_1, \ldots, x_k)$ be any element of $\prod_i \pi_i(S)$. Then for each $i \in I$, $x_i \in \mathbb{Z}_{p_i}$ can be written as $x_i = a_i \cdot 1$ with $a_i \in \mathbb{Z}_{p_i}$. The element $\sum_{i\in I} a_i(t_i)$ (where t_i is the vector with 1 in coordinate i and 0 elsewhere) belongs to S because S is closed under addition and multiplication by scalars from $\mathbb{Z}$ (since it is a subring). More directly, the element $\big(\sum_{i\in I} a_i e_i\big) \cdot t$ (where e_i are the standard basis vectors) lies in S. This yields an element whose coordinates are exactly $(x_1, \ldots, x_k)$. Hence $\prod_i \pi_i(S) \subseteq S$. Therefore $S = \prod_i \pi_i(S)$.

Thus every subring is determined by the subset I of indices where the projection is the whole field, giving precisely 2^k distinct subrings. The identity of such a subring is the vector with 1 in coordinates

$i \in I$ and 0 elsewhere, which is clearly idempotent and acts as the multiplicative identity on the subring. □

Corollary 3. *Let $R = \prod_{i=1}^{k} \mathbb{Z}_{p_i}$ where $p_1, p_2, \ldots, p_k$ are distinct primes and $k \geq 2$. Then the number of subrings of R is exactly 2^k. For any subset $I \subseteq \{1, 2, \ldots, k\}$, the subring*

$$S_I = \prod_{i \in I} \mathbb{Z}_{p_i} \times \prod_{i \notin I} \{0\}$$

has multiplicative identity $\mathbf{1}_{S_I} = (e_1, \ldots, e_k)$ with $e_i = 1$ if $i \in I$ and $e_i = 0$ otherwise. Distinct subsets yield distinct identities.

Remark 3. Although not strongly unital, the ring $R = (\mathbb{Z}_{2p})^h$ (with p an odd prime) has 4^h subrings, each obtained by choosing for each coordinate one of the four subrings of $\mathbb{Z}_{2p}$ (namely $\{0\}, 2\mathbb{Z}_{2p}, p\mathbb{Z}_{2p}, \mathbb{Z}_{2p}$). Their identities are tuples where each entry is $0, p+1, p$, or 1 respectively.

3.3 Counting Subrings in the Canonical Class

Let $R = \prod_{i=1}^{k} \mathbb{Z}_{p_i}$ where $p_1, \ldots, p_k$ are distinct primes and $k \geq 2$. We determine all subrings of R and count them.

Lemma 6. *For each i, let $\pi_i : R \to \mathbb{Z}_{p_i}$ be the projection. If S is a subring of R, then*

$$S = \prod_{i=1}^{k} \pi_i(S).$$

Moreover, for each i, $\pi_i(S)$ is either $\{0\}$ or $\mathbb{Z}_{p_i}$.

Proof. The projection π_i is a ring homomorphism, so $\pi_i(S)$ is a subring of $\mathbb{Z}_{p_i}$. Since $\mathbb{Z}_{p_i}$ is a field, its only subrings are $\{0\}$ and $\mathbb{Z}_{p_i}$ itself. Hence $\pi_i(S) \in \{\{0\}, \mathbb{Z}_{p_i}\}$.

Clearly $S \subseteq \prod_{i=1}^{k} \pi_i(S)$. For the reverse inclusion, define $I = \{i \mid \pi_i(S) = \mathbb{Z}_{p_i}\}$. For each $i \in I$ choose an element $s^{(i)} \in S$ with $\pi_i(s^{(i)}) = 1$. Because distinct coordinates are independent, the product

$$e = \prod_{i \in I} s^{(i)}$$

has 1 in every coordinate belonging to I and, because for $j \notin I$ we have $\pi_j(S) = \{0\}$ and thus every element of S has zero in those coordinates, we also have $\pi_j(e) = 0$ for $j \notin I$. Hence e is the vector with 1 in coordinates I and 0 elsewhere; in particular $e \in S$.

Now take any element $x = (x_1, \ldots, x_k)$ with $x_i \in \pi_i(S)$. For $i \in I$ write $x_i = a_i \cdot 1$ with $a_i \in \mathbb{Z}_{p_i}$. The element

$$x' = \sum_{i \in I} a_i \big(e \cdot (0, \ldots, 0, 1_i, 0, \ldots, 0)\big)$$

lies in S because it is a combination of products of elements of S. A direct computation shows that $\pi_i(x') = x_i$ for all i, and $\pi_j(x') = 0$ for $j \notin I$. Thus $x = x' \in S$. Therefore $\prod_i \pi_i(S) \subseteq S$. Equality follows. □

Definition 1. For a subset $I \subseteq \{1, \ldots, k\}$ define

$$S_I = \prod_{i=1}^{k} T_i, \qquad T_i = \begin{cases} \mathbb{Z}_{p_i}, & i \in I, \\ \{0\}, & i \notin I. \end{cases}$$

Lemma 7. *The map $I \mapsto S_I$ is a bijection between the power set $\mathcal{P}(\{1, \ldots, k\})$ and the set of all subrings of R.*

Proof. Lemma 6 shows that every subring has the form S_I with $I = \{i \mid \pi_i(S) = \mathbb{Z}_{p_i}\}$. Different subsets give different subrings (e.g., they differ in the zero pattern). Hence the correspondence is bijective. □

Theorem 4 (Number of Subrings)**.** *Let $R = \prod_{i=1}^{k} \mathbb{Z}_{p_i}$ with distinct primes p_i and $k \geq 2$. Then R has exactly 2^k subrings. Moreover, each subring S_I has multiplicative identity*

$$\mathbf{1}_{S_I} = (e_1, \ldots, e_k), \qquad e_i = \begin{cases} 1, & i \in I, \\ 0, & i \notin I. \end{cases}$$

Proof. The bijection of Lemma 7 gives 2^k subrings. The identity property is verified directly: for any $(x_i) \in S_I$, coordinates with $i \in I$ are multiplied by 1, and coordinates with $i \notin I$ are already 0. Uniqueness of the identity is standard. □

Corollary 5. *If $R \cong \mathbb{Z}_n$ where $n = p_1 p_2 \cdots p_k$ is square-free and composite, then the number of subrings of $\mathbb{Z}_n$ equals the number of divisors of n, which is 2^k. The subring corresponding to a divisor d of n is the ideal $d\mathbb{Z}_n$, and its identity is the unique element e_d satisfying $e_d \equiv 0 \pmod{d}$, $e_d \equiv 1 \pmod{n/d}$ (Chinese Remainder Theorem).*

3.4 Remark on Products of $\mathbb{Z}_{2p}$

For a ring of the form $T = \prod_{i=1}^{h} \mathbb{Z}_{2p_i}$ where each p_i is an odd prime (not necessarily distinct), the situation differs from the canonical case. Such a ring is not strongly unital unless $h = 1$ and the factorisation yields distinct primes. Indeed, when $h \geq 2$ the prime 2 appears at least twice, which introduces a diagonal subring (e.g., in the two copies of $\mathbb{Z}_2$) that shares an identity with a larger subring, violating condition (3) of strong unitality [14]. For $h = 1$ we obtain $\mathbb{Z}_{2p_1}$, which is strongly unital because $\mathbb{Z}_{2p_1} \cong \mathbb{Z}_2 \times \mathbb{Z}_{p_1}$ with distinct primes.

Although each factor $\mathbb{Z}_{2p_i}$ has exactly four subrings $(\{0\}, 2\mathbb{Z}_{2p_i}, p_i\mathbb{Z}_{2p_i}, \mathbb{Z}_{2p_i})$, subrings of a direct product are not necessarily direct products of subrings of the factors. For example, the diagonal subring $\{(a, a) \mid a \in \mathbb{Z}_{2p}\}$ inside $(\mathbb{Z}_{2p})^2$ is a subring that cannot be expressed as $S \times T$ with S, T

subrings of $\mathbb{Z}_{2p}$. Consequently, the enumeration formulas developed here apply only to the canonical strongly unital rings $\prod_{i=1}^{k} \mathbb{Z}_{p_i}$ with distinct primes p_i and $k \geq 2$.

4 Identities of Subrings

We now determine the multiplicative identity of each subring S_I in the canonical decomposition.

Theorem 6 (Identity of a Subring)**.** *Let $R = \prod_{i=1}^{k} \mathbb{Z}_{p_i}$ with distinct primes p_i and $k \geq 2$. For a subset $I \subseteq \{1, \ldots, k\}$, the subring*

$$S_I = \prod_{i \in I} \mathbb{Z}_{p_i} \times \prod_{i \notin I} \{0\}$$

has multiplicative identity

$$\mathbf{1}_{S_I} = (e_1, \ldots, e_k), \qquad e_i = \begin{cases} 1, & \text{if } i \in I, \\ 0, & \text{if } i \notin I. \end{cases}$$

Proof. Take any $(x_1, \ldots, x_k) \in S_I$. By definition, $x_i = 0$ for all $i \notin I$. Then

$$(e_1, \ldots, e_k) \cdot (x_1, \ldots, x_k) = (e_1 x_1, \ldots, e_k x_k).$$

If $i \in I$, then $e_i = 1$ and $1 \cdot x_i = x_i$. If $i \notin I$, then $e_i = 0$ and $0 \cdot 0 = 0 = x_i$. Hence the product equals $(x_1, \ldots, x_k)$. The same computation holds for multiplication on the left. Uniqueness of the identity element forces $\mathbf{1}_{S_I}$ to be exactly this tuple. □

Corollary 7. *Distinct subrings have distinct identities. Moreover, the identity of any proper nontrivial subring differs from the identity $\mathbf{1}_R = (1, 1, \ldots, 1)$ of the whole ring.*

Proof. If $I \neq J$, then there exists an index i in the symmetric difference $I \triangle J$. In that coordinate, one identity has 1 and the other 0; therefore they are different. For a proper subset $I \subsetneq \{1, \ldots, k\}$, pick $j \notin I$. Then $\mathbf{1}_{S_I}$ has 0 in coordinate j while $\mathbf{1}_R$ has 1; thus $\mathbf{1}_{S_I} \neq \mathbf{1}_R$. □

5 The Cyclic Ring Case: $\mathbb{Z}_n$ with Square-Free Composite n

When $R \cong \mathbb{Z}_n$ where $n = p_1 p_2 \cdots p_k$ is square-free and composite ($k \geq 2$), the Chinese Remainder Theorem gives an explicit description of subrings in terms of divisors of n.

Theorem 8 (Subrings of $\mathbb{Z}_n$)**.** *Let $n = p_1 p_2 \cdots p_k$ be a product of distinct primes with $k \geq 2$. Then the subrings of $\mathbb{Z}_n$ are precisely the ideals $d\mathbb{Z}_n$ for each positive divisor d of n. Each such subring is isomorphic to $\mathbb{Z}_{n/d}$ and has a multiplicative identity e_d, which is the unique element of $\mathbb{Z}_n$ satisfying*

$$e_d \equiv 0 \pmod{d}, \qquad e_d \equiv 1 \pmod{n/d}.$$

Moreover, the number of subrings is 2^k *(the number of divisors of* n*).*

Proof. Since $\mathbb{Z}_n$ is a principal ideal ring, every subring is an ideal $d\mathbb{Z}_n$ for some divisor d of n. Because n is square-free, $\gcd(d, n/d) = 1$ for every divisor d. Hence each $d\mathbb{Z}_n$ possesses a unique identity e_d given by the two congruences. The Chinese Remainder Theorem guarantees existence and uniqueness of such an element modulo n.

Under the CRT isomorphism $\mathbb{Z}_n \cong \prod_{i=1}^{k} \mathbb{Z}_{p_i}$, the divisor d corresponds to the subset $J = \{i : p_i \mid d\}$. The ideal $d\mathbb{Z}_n$ maps to the subring where coordinates in J are forced to 0 and coordinates not in J are the full $\mathbb{Z}_{p_i}$. Its identity is the vector with 1 in coordinates not in J and 0 in J; the pre-image of this vector under the CRT is precisely e_d. The number of divisors of a square-free number with k prime factors is 2^k, which matches the number of subrings. □

Example 5.1 ($\mathbb{Z}_{30}$)**.** *Let* $n = 30 = 2 \cdot 3 \cdot 5$*. The divisors are* $1, 2, 3, 5, 6, 10, 15, 30$*. We compute the identity* e_d *for each divisor* d *using the CRT.*

(i) $d = 1$*:* $1\mathbb{Z}_{30} = \mathbb{Z}_{30}$*, identity* $e_1 = 1$*.*

(ii) $d = 2$*: Solve* $e \equiv 0 \pmod 2$*,* $e \equiv 1 \pmod{15}$*. The numbers congruent to* 1 *modulo* 15 *are* $1, 16, 31, \ldots$*. The even one is* 16*. Hence* $e_2 = 16$*.*

(iii) $d = 3$*: Solve* $e \equiv 0 \pmod 3$*,* $e \equiv 1 \pmod{10}$*. Numbers* $\equiv 1 \pmod{10}$*:* $1, 11, 21, 31, \ldots$*. The multiple of* 3 *among these is* 21*. Thus* $e_3 = 21$*.*

(iv) $d = 5$*: Solve* $e \equiv 0 \pmod 5$*,* $e \equiv 1 \pmod 6$*. Numbers* $\equiv 1 \pmod 6$*:* $1, 7, 13, 19, 25, 31, \ldots$*. The multiple of* 5 *is* 25*. Hence* $e_5 = 25$*.*

(v) $d = 6 = 2{\cdot}3$*: Solve* $e \equiv 0 \pmod 6$*,* $e \equiv 1 \pmod 5$*. Numbers* $\equiv 0 \pmod 6$*:* $0, 6, 12, 18, 24, 30, \ldots$*. The one congruent to* 1 *modulo* 5 *is* 6 *(since* $6 \equiv 1 \pmod 5$*). Hence* $e_6 = 6$*.*

(vi) $d = 10 = 2 \cdot 5$*: Solve* $e \equiv 0 \pmod{10}$*,* $e \equiv 1 \pmod 3$*. Multiples of* 10*:* $0, 10, 20, 30, \ldots$*. The one congruent to* 1 *modulo* 3 *is* 10 *(since* $10 \equiv 1 \pmod 3$*). Thus* $e_{10} = 10$*.*

(vii) $d = 15 = 3 \cdot 5$*: Solve* $e \equiv 0 \pmod{15}$*,* $e \equiv 1 \pmod 2$*. Multiples of* 15*:* $0, 15, 30, \ldots$*. The odd one is* 15*. Hence* $e_{15} = 15$*.*

(viii) $d = 30$*:* $30\mathbb{Z}_{30} = \{0\}$*, identity* $e_{30} = 0$*.*

All identities are distinct, and only the identity of the whole ring ($d = 1$) *equals* 1*; proper subrings have identities different from* 1*. This confirms that* $\mathbb{Z}_{30}$ *is strongly unital.*

6 Extended Construction: Products of $\mathbb{Z}_{2p_i}$ (Not All Strongly Unital)

A ring of the form $R = \prod_{i=1}^{h} \mathbb{Z}_{2p_i}$ where each p_i is an odd prime (not necessarily distinct) is generally not strongly unital. Indeed, after factoring each $\mathbb{Z}_{2p_i} \cong \mathbb{Z}_2 \times \mathbb{Z}_{p_i}$ (Chinese Remainder Theorem, since $\gcd(2, p_i) = 1$), the total prime factorisation of R contains the prime 2 at least h times. If $h \geq 2$,

the prime 2 repeats, which (by the classification) prevents strong unitality. The only way R can be strongly unital is when $h = 1$ and the prime p_1 is such that the factorisation yields distinct primes (which it does, because $\mathbb{Z}_{2p_1} \cong \mathbb{Z}_2 \times \mathbb{Z}_{p_1}$ gives the two distinct primes 2 and p_1). Thus for $h \geq 2$, the ring R is not strongly unital.

Nevertheless, it is a combinatorial exercise to count the number of subrings that are *direct products of subrings of the factors*. Each factor $\mathbb{Z}_{2p_i}$ has exactly four subrings: $\{0\}$, $2\mathbb{Z}_{2p_i}$, $p_i\mathbb{Z}_{2p_i}$, $\mathbb{Z}_{2p_i}$. The Cartesian product of any choice of subrings from each factor gives a subring of R that is itself a direct product. Such subrings are called **product subrings**. There are 4^h of them. However, we caution that not every subring of a direct product is necessarily a product of subrings of the factors. For example, in $(\mathbb{Z}_{2p})^2$, the diagonal subring $\{(a, a) \mid a \in \mathbb{Z}_{2p}\}$ is a subring that cannot be expressed as $S \times T$ with S, T subrings of $\mathbb{Z}_{2p}$.
The following theorem is therefore stated only for product subrings, not for all subrings.

Theorem 9 (Product Subrings of $\prod \mathbb{Z}_{2p_i}$)**.** *Let $R = \prod_{i=1}^{h} \mathbb{Z}_{2p_i}$ where each p_i is an odd prime. The set of subrings of R that are direct products of subrings of the factors has cardinality 4^h. Each such subring corresponds to an h-tuple $(t_1, \ldots, t_h)$ with $t_i \in \{0, 2, p, 1\}$, where the subring is $\prod_{i=1}^{h} S_i(t_i)$ and $S_i(0) = \{0\}$, $S_i(2) = 2\mathbb{Z}_{2p_i}$, $S_i(p) = p_i\mathbb{Z}_{2p_i}$, $S_i(1) = \mathbb{Z}_{2p_i}$. The identity of such a product subring is the tuple of identities of the factors (namely 0, $p_i + 1$, p_i, 1 respectively).*

Proof. Each factor has exactly four subrings, and the product of subrings is a subring of the product. The identity of a direct product is the tuple of the identities of the factors. Distinct tuples give distinct subrings and distinct identities. Hence there are exactly 4^h such product subrings. □

7 Examples and Verification

We illustrate the classification and enumeration with concrete examples.

Example 7.1 ($\mathbb{Z}_6$ (canonical strongly unital ring))**.** *Let $R = \mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$. The primes are 2 and 3 (distinct, $k = 2$). According to Theorem 4, R has $2^2 = 4$ subrings. Under the CRT isomorphism $x \mapsto (x \bmod 2, x \bmod 3)$, we obtain:*

i. $\emptyset$*:* $\{0\}$ *(identity 0).*

ii. $\{2\}$*: elements with $x \equiv 0 \pmod 2$ (i.e., $2\mathbb{Z}_6 = \{0, 2, 4\}$). The identity is the element that maps to $(0, 1)$, namely $x \equiv 0 \pmod 2, x \equiv 1 \pmod 3 \Rightarrow x = 4$.*

iii. $\{3\}$*: elements with $x \equiv 0 \pmod 3$ (i.e., $3\mathbb{Z}_6 = \{0, 3\}$). The identity is the element that maps to $(1, 0)$, namely $x \equiv 1 \pmod 2, x \equiv 0 \pmod 3 \Rightarrow x = 3$.*

iv. $\{2, 3\}$*: the whole ring $\mathbb{Z}_6$ with identity 1.*

All identities are distinct, and proper subring identities differ from 1.

Example 7.2 ($\mathbb{Z}_{30}$ (canonical strongly unital ring))**.** *Let $n = 30 = 2 \cdot 3 \cdot 5$. Then $k = 3$ and $R = \mathbb{Z}_{30}$ is strongly unital. It has $2^3 = 8$ subrings, corresponding to subsets of $\{2, 3, 5\}$. For a subset I, the identity is the unique residue e modulo 30 satisfying $e \equiv 1 \pmod{p}$ for $p \in I$ and $e \equiv 0 \pmod{p}$ for $p \notin I$.*

Take $I = \{2, 3\}$. Then we require $e \equiv 1 \pmod 2$, $e \equiv 1 \pmod 3$, $e \equiv 0 \pmod 5$. The first two give $e \equiv 1 \pmod 6$. Write $e = 5t$. Then $5t \equiv 1 \pmod 6$. Since $5 \equiv -1 \pmod 6$, we have $-t \equiv 1 \pmod 6$ $\Rightarrow t \equiv -1 \equiv 5 \pmod 6$. The smallest positive solution is $t = 5$, yielding $e = 25$. Hence the subring corresponding to $\{2, 3\}$ has identity 25 modulo 30. Similar computations give all eight identities, all distinct.

Example 7.3 (Non-strongly unital product: $(\mathbb{Z}_6)^2$)**.** *Consider $R = \mathbb{Z}_6 \times \mathbb{Z}_6 \cong (\mathbb{Z}_2 \times \mathbb{Z}_3)^2$. The prime 2 appears twice, so R is not strongly unital. Indeed, the diagonal subring $\{(a, a) \mid a \in \mathbb{Z}_6\}$ has identity $(1, 1)$, which equals the whole ring's identity, violating condition (2). This illustrates why repeated primes are forbidden.*

8 Algorithmic Enumeration

From the theoretical formulas, we can design a simple algorithm to enumerate all subrings and their identities.

Algorithm 1 Enumerate subrings of a finite commutative strongly unital ring R

Given R expressed as $\prod_{i=1}^{k} \mathbb{Z}_{p_i}$ with distinct primes p_i (or as $\mathbb{Z}_n$ with square-free composite n).

1. Compute the set of prime factors $\{p_1, \ldots, p_k\}$.
2. For each subset $I \subseteq \{1, \ldots, k\}$ (represented as a bitmask from 0 to $2^k - 1$):
   i. Construct the subring $S_I = \prod_{i \in I} \mathbb{Z}_{p_i} \times \prod_{i \notin I} \{0\}$.
   ii. Compute the identity $\mathbf{1}_{S_I}$ as the vector with 1 in coordinates $i \in I$ and 0 elsewhere.
   iii. If the ring is given as $\mathbb{Z}_n$, compute the corresponding integer identity via Chinese remainder solving.
3. Output the list of subrings and their identities.

The time complexity is $O(2^k \cdot k)$ for the product representation, which is optimal because the output size is 2^k.

9 Connection with the Boolean Lattice

Let $R = \prod_{i=1}^{k} \mathbb{Z}_{p_i}$ where $p_1, \ldots, p_k$ are distinct primes and $k \geq 2$. For each subset $I \subseteq \{1, \ldots, k\}$, define the subring

$$S_I = \prod_{i \in I} \mathbb{Z}_{p_i} \times \prod_{i \notin I} \{0\}.$$

By Lemma 6 and Lemma 7, the map $\Phi : \mathcal{P}(\{1, \ldots, k\}) \to \mathrm{Sub}(R)$ given by $\Phi(I) = S_I$ is a bijection.

Proposition 11. *The subring lattice* $(\mathrm{Sub}(R), \subseteq)$ *is isomorphic to the Boolean lattice* $(\mathcal{P}(\{1,\ldots,k\}), \subseteq)$. *Moreover, for any* $I, J \subseteq \{1,\ldots,k\}$*:*

$$S_I \vee S_J = S_{I\cup J}, \qquad S_I \wedge S_J = S_{I\cap J}, \qquad \neg S_I = S_{I^c},$$

where $\vee$ *and* $\wedge$ *denote join and meet in the subring lattice (i.e., the smallest subring containing the union, and the intersection, respectively).*

Proof. The map Φ is order-preserving because $I \subseteq J$ implies $S_I \subseteq S_J$ (an element with support in I also has support in J). It is a bijection, hence an order isomorphism. Therefore $\mathrm{Sub}(R)$ inherits the Boolean lattice structure of $\mathcal{P}(\{1,\ldots,k\})$.

Explicitly, the join $S_I \vee S_J$ is the smallest subring containing both S_I and S_J. The subset corresponding to this subring must be the smallest subset containing both I and J, which is $I \cup J$. Thus $S_I \vee S_J = S_{I\cup J}$. The meet (intersection) satisfies $S_I \cap S_J = S_{I\cap J}$ because an element belongs to both subrings exactly when it is nonzero only on coordinates belonging to $I \cap J$. The complement in the Boolean lattice corresponds to the subring with support $I^c = \{1,\ldots,k\} \setminus I$, i.e., $\neg S_I = S_{I^c}$. □

A direct consequence is that the subring lattice is distributive, complemented, and its Möbius function is the same as that of the power set lattice. The identity map $S_I \mapsto \mathbf{1}_{S_I}$ provides an embedding of the Boolean lattice into the idempotent semiring of R, since $\mathbf{1}_{S_I} \cdot \mathbf{1}_{S_J} = \mathbf{1}_{S_{I\cap J}}$ and $\mathbf{1}_{S_I} + \mathbf{1}_{S_J} - \mathbf{1}_{S_I}\mathbf{1}_{S_J} = \mathbf{1}_{S_{I\cup J}}$.

10 Conclusion and Recommendations

10.1 Conclusion

In this paper, we have provided a complete and explicit enumeration of all subrings of finite commutative strongly unital rings, together with closed-form formulas for the multiplicative identity of each subring. We established that every finite commutative strongly unital ring is isomorphic to $R \cong \prod_{i=1}^{k} \mathbb{Z}_{p_i}$, where $p_1,\ldots,p_k$ are distinct primes, and demonstrated that the subrings of R are precisely the direct products $S_I = \prod_{i\in I} \mathbb{Z}_{p_i} \times \prod_{i\notin I}\{0\}$ indexed by subsets $I \subseteq \{1,\ldots,k\}$. Consequently, the number of subrings is exactly 2^k, and the identity of S_I is the vector with 1 in coordinates $i \in I$ and 0 elsewhere. We further showed that distinct subrings possess distinct identities, thereby confirming the strong unitality condition from an enumerative perspective. In the cyclic ring case $\mathbb{Z}_n$ with n square-free and composite, this yields a divisor-based parametrisation where subrings correspond to divisors $d \mid n$, with identities uniquely determined by the congruences $e_d \equiv 0 \pmod{d}$ and $e_d \equiv 1 \pmod{n/d}$. Moreover, we established that the subring lattice is isomorphic to the Boolean lattice, revealing a rich combinatorial structure that connects subring inclusion, intersection, and join to set operations on the prime factors. These results bridge a significant gap in the literature by providing explicit enumeration formulas that complement the classification theorems of Oman and Stroud [14].

10.2 Recommendations

The results presented in this paper open several avenues for future research. First, the enumeration problem for products of the form $\prod_{i=1}^{h} \mathbb{Z}_{2p_i}$, where the prime 2 appears multiple times, remains largely unexplored. A comprehensive combinatorial classification of subrings in this setting would be a significant contribution to the theory. Second, the Boolean lattice structure of the subring poset in the canonical class suggests that the subring lattice can serve as a useful framework for studying other algebraic invariants, such as the automorphism group or the ideal lattice of R. Investigating the interplay between the subring lattice and these invariants could yield further insights. Third, the algorithmic approach outlined can be extended to compute subring identities for larger values of k, and an efficient implementation would be valuable for computational experiments. Finally, it would be interesting to explore whether similar enumeration techniques can be applied to other classes of finite rings, such as $\mathbb{Z}_{p^m}$ or products of chain rings, where the subring structure is more complex but may still admit closed-form enumeration formulas.

References

[1] Anderson, D. D., & Livingston, P. S. (1999). The zero-divisor graph of a commutative ring. *Journal of Algebra*, **217**(2), 434–447.

[2] Beck, I. (1988). Coloring of commutative rings. *Journal of Algebra*, **116**(1), 208–226.

[3] Chikunji, C. J. (2005). A classification of cube radical zero completely primary finite rings. *Demonstratio Mathematica*, **XXXVIII**, 7–20.

[4] Choi, H. S., & Walker, A. (2020). THE RADICAL OF AN n-ABSORBING IDEAL. *Journal of Commutative Algebra*, 12(2), 171-177.

[5] Corbas, B. (1969). Rings with finite zero divisors. *Mathematische Annalen*, **181**, 1–7.

[6] Corbas, B. (1970). Finite rings in which the product of any two zero divisors is zero. *Archiv der Mathematik*, **21**, 466–469.

[7] Dobbs, D. E. (2007). When is a ring a product of fields? *Houston Journal of Mathematics*, **33**(3), 657–671.

[8] Were, H. S., & Oduor, M. O. (2022). Classification of Unit Groups of Five Radical Zero Completely Primary Finite Rings Whose First and Second Galois Ring Module Generators Are of the Order pk, k= 2, 3, 4. *Journal of Mathematics*, 2022(1), 7867431.

[9] Karpilovsky, G. (1989). *The algebraic structure of group rings*. Marcel Dekker.

[10] McDonald, B. R. (1974). *Finite rings with identity*. Marcel Dekker.

[11] Oduor, M. O., Ojiema, M. O., & Mmasi, E. (2013). Units of commutative completely primary finite rings of characteristic p^n. *International Journal of Algebra*, **7**(6), 259–266.

[12] Oduor, M. O., & Onyango, M. O. (2014). Unit groups of some classes of power four radical zero commutative completely primary finite rings. *International Journal of Algebra*, **8**, 357–363.

[13] Ojiema, M. O., Owino, M. O., & Odhiambo, P. O. (2016). Automorphisms of the unit groups of square radical zero finite commutative completely primary finite rings. *International Journal of Pure and Applied Mathematics*, **108**(1), 39–48.

[14] Oman, G., & Stroud, J. (2020). Rings whose subrings have an identity. *Involve: A Journal of Mathematics*, **13**(5), 823–830.

[15] Oman, G., & Senkoff, E. (2023). Almost strongly unital rings. *Involve: A Journal of Mathematics*, **16**(3), 453–465.

[16] Owino, M. O., Omamo, A. L., & Musoga, C. (2013). On the regular elements of rings in which the product of any two zero divisors lies in the Galois subring. *International Journal of Pure and Applied Mathematics*, **86**(1), 7–18.

[17] Owino, M. O., & Walwenda, S. O. (2016). On the zero divisor graphs of class of commutative completely primary finite rings. *Journal of Advances in Mathematics*, **12**(3), 6021–6022.

[18] Raghavendran, R. (1969). Finite associative rings. *Compositio Mathematica*, **21**(2), 195–229.

[19] Wilson, R. S. (1973). On the structure of finite rings. *Compositio Mathematica*, **26**, 79–93.