2009-01-01

A Characterization of Pseudo-Orders in the Ring Zn

Jorge Ivan Vargas
University of Texas at El Paso, jivanvargas@gmail.com

A Characterization of Pseudo-Orders in the Ring $\mathbb{Z}_n$

JORGE IVAN VARGAS

Department of Mathematical Sciences

APPROVED:

Piotr Wojciechowski, Chair, Ph.D.

Emil Daniel Schwab, Ph.D.

Mohamed Amine Khamsi, Ph.D.

Vladik Kreinovich, Ph.D.

Patricia D. Witherspoon, Ph.D.
Dean of the Graduate School

to my

MOTHER and FATHER

with love

A Characterization of Pseudo-Orders in the Ring $\mathbb{Z}_n$

by

JORGE IVAN VARGAS

THESIS

Presented to the Faculty of the Graduate School of

The University of Texas at El Paso

in Partial Fulfillment

of the Requirements

for the Degree of

MASTER OF SCIENCE

Department of Mathematical Sciences

THE UNIVERSITY OF TEXAS AT EL PASO

December 2009

Abstract

Partially ordered sets are widely studied in algebra. The theory of lattice-ordered and partially-ordered rings is an important case. In this paper, we consider a more general relation: pseudo orders, which are relations that are reflexive and antisymmetric, but are not necessarily transitive. Analogously to partially-ordered rings, we study pseudo-ordered rings. We present a general characterization for pseudo-ordered rings, and then we focus on a specific structure: the ring $\mathbb{Z}_n$. Having the constraints of this ring, we are able to give the conditions under which $\mathbb{Z}_n$ can be pseudo-ordered.

Table of Contents

Chapter 1

Introduction

Partial order relations are very familiar structures in many fields of mathematics. By a partial order relation we understand a relation $\leq$ which is reflexive, antisymmetric, and transitive. If we relax the conditions by removing the need for transitivity, we get a more general structure, a *pseudo order*. This relation seems to be often arising in nature.

To begin with an apparently non-mathematical example, consider the sports. If a team A defeats a team B, and the team B defeats a team C, it is not necessarily true – and very often it is not – that team A defeats team C.

In a more formal example, consider the relation "is close to", which we define as $a \leq b$ if and only if $0 \leq b - a < \delta$ for some fixed δ. Clearly, this defines a non-transitive relation, although it is reflexive and antisymmetric. For instance, let $\delta = 5$, then $1 \leq 5$ since $5 - 1 = 4 < 5$; $5 \leq 9$ since $9 - 5 = 4 < 5$; however, $9 - 1 = 8 \not< 5$, hence $1 \not\leq 9$ although we have $1 \leq 5 \leq 9$, that is, $\leq$ is not transitive.

Another example can be the relation defined by stating that $a \leq b$ if and only if $a \equiv b \pmod 3$ or $a \equiv (b + 1) \pmod 3$. It can be easily checked that this relation also defines a reflexive and antisymmetric relation. It is however, non-transitive. Indeed, $2 \leq 7$ and $7 \leq 21$, but $2 \not\leq 21$ as $2 \equiv 7 + 1 \pmod 3$, $7 \equiv 21 + 1 \pmod 3$, but $2 \not\equiv 21 \pmod 3$ and $2 \not\equiv 21 + 1 \pmod 3$.

The above definition and examples appear in [5]. In a restricted context to pseudo-orders with a trichotomy law, the pseudo-ordered rings were studied in [8]. Recently there has been certain amount of interest in these concepts in functional analysis due to their parts played in [6], where some important fixed point theorems were extended.

Let us formally define the relations having the discussed properties.

Definition 1.0.1. *A relation $\leq$ on a set S is said to be a pseudo-order relation if:*

- *For any $a \in S$, $a \leq a$ (reflexive property)*
- *$a, b \in S$, and $a \leq b$ and $b \leq a$ implies $a = b$ (antisymmetric property).*

This is of course a general definition. In the next section, we start considering rings with a compatible pseudo-order and investigate some of their properties.

Chapter 2

Preliminaries

We begin our study of pseudo-order rings by providing a formal definition and basics results.

Definition 2.0.2. *A 4-tuple $(R, +, \cdot, \leq)$ is said to be a pseudo-ordered ring if it satisfies the following*

- $(R, +, \cdot)$ *is a ring*
- $(R, \leq)$ *is a pseudo-order*
- $\forall a, b, c \in R$, $a \leq b$ *implies* $a + c \leq b + c$
- $\forall a, b, c \in R, c > 0, a \leq b$ *implies* $c \cdot a \leq c \cdot b$ *and* $a \cdot c \leq b \cdot c$.

The definition of a *partially ordered* ring is analogous to Definition 2.0.2, having a partial order instead of a pseudo-order. However, there is a significant difference. A non-trivial partially ordered ring, that is, a ring with at least two different, comparable elements, is necessarily infinite. By considering a pseudo-order instead of a partial order we can, as we will see, obtain finite, non-trivial rings with an order.

As we start our study of pseudo-ordered rings, probably the most natural questions is, in what situation can a ring be pseudo-ordered? Although, Definition 2.0.2 states explicitly what a pseudo-ordered ring is, we want to find a characterization that allows us to readily determine when we have a pseudo-ordered ring. The following proposition provides such characterization.

Proposition 2.0.3. *Let R be any ring. Then R is a pseudo-ordered ring if and only if there exists $P \subseteq R$ such that $P \cap -P = \{0\}$ and $P \cdot P \subseteq P$.*

Proof. ($\Rightarrow$) Suppose R is a pseudo-ordered ring, and define $P = \{p \in R; p \geq 0\}$. Let us show this set P satisfies the desired properties. Since $0 \geq 0$, we obtain $0 \in P$. Moreover, since $0 - 0 = 0$, $-0 = 0$, and thus $0 \in -P$, and hence we have $0 \in P \cap -P$. Let us show 0 is the only element that belongs to the intersection. Let $x \in P \cap -P$. Since $x \in P$, we have $x \geq 0$. Moreover, since $x \in -P$, we have $-x \in P$, and hence $-x \geq 0$. Upon adding x to both sides, we obtain $0 \geq x$. Then, by antisymmetry, $x = 0$, therefore $P \cap -P = \{0\}$.

Now, let p, q be arbitrary elements from P. By definition of P, $p \geq 0$ and $q \geq 0$. Also, since R is a pseudo-ordered ring, we have that $p \cdot q \geq r \cdot q$ whenever $p \geq r$, in particular, for $r = 0$. Therefore, $p \cdot q \geq 0 \cdot q = 0$, hence $p \cdot q \in P$. Since p and q are arbitrary elements from P, we have $P \cdot P \subseteq P$.

($\Leftarrow$) Let us define $a \leq b$ if and only if $b - a \in P$, and let us show this relation is reflexive and antisymmetric. Since 0 belongs to $P \cap -P$, 0 belongs to P, and $x - x = 0 \in P$ for any $x \in R$, hence $\leq$ is reflexive.

Now, let $b - a \in P$ and $a - b \in P$. Since $-(a - b) = b - a$, and $P \cap -P = \{0\}$, it must be the case that $b - a = 0$, or $b = a$. Therefore $\leq$ is antisymmetric, and consequently, a pseudo-order.

Finally, let $a \leq b$ and let $c \in P$. By definition of $\leq$, $b - a \in P$ and since $P \cdot P \subseteq P$, $c \cdot b - c \cdot a = c \cdot (b - a) \in P$. But this implies $c \cdot a \leq c \cdot b$. Similarly, $a \cdot c \leq b \cdot c$, hence $(R, +, \cdot, \leq)$ is a pseudo-ordered ring. □

Proposition 2.0.3 provides a very valuable tool to examine properties of pseudo-ordered rings, and, as we will see in the upcoming sections, also to find characterizations of specific pseudo-ordered rings.

A direct application of Proposition 2.0.3 tells us that the smallest pseudo-ordered ring other than the trivial, has to have more than two elements. We present this result in the following proposition.

Proposition 2.0.4. *There is no pseudo-order ring of cardinality 2.*

Proof. Suppose there is some pseudo ordered ring R of cardinality 2. Let $R = \{0, a\}$, but then $a + a = 0$ since $(R, +)$ is a group. If $P \neq \{0\}$, then $a \in P$. But then $a \in -P$, contradicting Proposition 2.0.3. Therefore no such ring R exists. □

At this point, we know that if in a ring R we are able to find a subset P with the properties described above, R can be pseudo-ordered. The question that arises is, can any ring R which have more than 2 elements be pseudo-ordered? The following theorem tells us when a ring with unity can be pseudo-ordered. Before stating the theorem, let us recall that the *characteristic* of a ring R is the least positive integer n such that $n \cdot x = 0$ for all x in R. If no such integer exists, we say that R has characteristic 0. We denote the characteristic of R by $char(R)$.

Theorem 2.0.5. *Let R be a ring with unity. Then, R can be pseudo-ordered if and only if $char(R) \neq 2$.*

Proof. ($\Rightarrow$) Assume $char(R) = 2$ and R is pseudo-ordered. Then, there is $P \subseteq R$ such that $P \cap -P = \{0\}$ and $P \cdot P \subseteq P$. Let $p_0 \in P$. Since $\text{char}(R) = 2$, then $p_0 + p_0 = 1 \cdot p_0 + 1 \cdot p_0 = (1 + 1) \cdot p_0 = 0$. But this implies $-p_0 = p_0$, which is impossible since $p_0 \in P$, therefore R cannot be pseudo-ordered, contradiction. Hence, $char(R) \neq 2$.

($\Leftarrow$) Conversely, assume $char(R) \neq 2$, and let $P = \{0, 1\}$. Clearly, P satisfies the requirements of Proposition 2.0.3, and therefore R can be pseudo-ordered. □

Let us examine some examples that illustrate these statements. Consider $\mathbb{Z}_2[X]$, the ring of polynomials with coefficients over $\mathbb{Z}_2$. Since $\text{char}(R) = 2$, the ring cannot be pseudo-ordered.

On the other hand, since $char(\mathbb{Z}_n) = n$, these rings form a class of examples where 2.0.5 applies positively, provided that $n > 2$. An even more interesting and complicated example is the ring of all n x n matrices.

While Theorem 2.0.5 characterizes nicely the situation when a ring with unity can be pseudo-ordered, the set P can always be taken to be $\{0, 1\}$. While this is indeed enough

for a ring to be pseudo-ordered, we would like to find more interesting sets P having the properties 2.0.3. We will now direct our attention towards the structure of pseudo-ordered rings $\mathbb{Z}_n$, $n > 2$.

Chapter 3

Pseudo-Orderings "by an Element"

In the previous section we obtained a general characterization for pseudo-ordered rings. We wish, however to find more interesting pseudo-orders other than the one guaranteed by Theorem 2.0.5. In this section we explore the structure of the set P having the properties 2.0.3. Our goal is to obtain additional information that allows us to find and construct pseudo-orders on rings. As we will see, it is often more convenient to look at the cases the ring *cannot* be pseudo-ordered instead. By this approach we are able, not only to tell when a ring can be pseudo-ordered, but also to construct the set P with the properties 2.0.3.

3.1 The Structure of P

As it has been stated, in order to find and construct the set P with the properties 2.0.3, we need to have a better understanding of what these sets are. Let us then, describe some natural properties of these sets. To do so, we introduce new terminology.

Definition 3.1.1. *Let R be a ring, and let $a \in R$. We define the set $\hat{a} = \{0, a, a^2, a^3, \ldots\}$.*

Since one of the two required properties for the set P to define a pseudo-order on R is implicitly inherited by the definition of a set $\hat{a}$, namely, the closure under $\cdot$, Definition 3.1.1 is a natural approach to find them. In order to do so, the other property – that only 0 belongs to the intersection – must be satisfied. Our next definition refers precisely to those situations.

Definition 3.1.2. *Let R be a ring, and let $r \in R$. We say that R is pseudo-ordered by r if the set $\hat{r}$ satisfies the property $\hat{r} \cap -\hat{r} = \{0\}$.*

Note that for $\hat{r}$ to have the properties 3.1.2 we only require that the intersection of $\hat{r}$ and $-\hat{r}$ be 0. This is clear since $\hat{r}$ is closed under $\cdot$ by definition, so $\hat{r}$ defines a pseudo-ordered on R if and only if $\hat{r} \cap -\hat{r} = \{0\}$.

Another important observation is that $\hat{r^d} \subseteq \hat{r}$ for any $d \geq 1$, $r \in R$, and consequently $-\hat{r^d} \subseteq -\hat{r}$. Hence, if a ring R is pseudo-ordered by r then it is also pseudo-ordered by r^d. What is uncertain at this point is the situation when R is not pseudo-ordered by r but it is pseudo-ordered by r^d for some $d > 1$. We will come back to this question in the next section.

It can be shown that any set P satisfying the properties of 2.0.3 is of the form

$$P = \hat{r_0} \cup \hat{r_1} \cup \hat{r_2} \cup \dots \tag{3.1}$$

for some elements $r_0, r_1, r_2, \dots \in R$. Indeed, if r is an element of P, then so is $r \cdot r = r^2, r^2 \cdot r = r^3$ and so on since P is closed under $\cdot$, and thus 3.1. Moreover, since $\hat{r_i} \subseteq P$, then $-\hat{r_i} \subseteq -P$, and since by hypothesis $P \cap -P = \{0\}$, then $\hat{r_i} \cap -\hat{r_i} = \{0\}$. Therefore R is pseudo-ordered by any r_i such that $\hat{r_i}$ is a set in the union (3.1).

From the above discussion, it is natural to examine the conditions under which a ring R is pseudo-ordered by an element $r \in R$. In the next section, we will apply this definition to characterize the situation in integral domains.

3.2 An application to Integral Domains

In the previous section, we introduced the concept of the set $\hat{a}$. Applying it to integral domains, let us note the following general fact.

Consider a ring R and an arbitrary element $p \in R$. As stated in the previous section, R is pseudo-ordered by p if and only if $\hat{p} \cap -\hat{p} = \{0\}$. But, this condition is satisfied if and only if

$$x + y \neq 0 \text{ for all elements } x, y \in \hat{p} \tag{3.2}$$

Note that, since $x, y \in \hat{p}$, $x = p^n$ and $y = p^m$, for some $n, m \in \mathbb{N}$. Without loss of generality, assume $m \leq n$. Then (3.2) is equivalent to

$$p^n + p^m \neq 0 \ \forall m, n \in \mathbb{N}. \tag{3.3}$$

If R has unit, then (3.3) can be rewritten as $p^m \cdot (p^{n-m} + 1) \neq 0 \ \forall n \geq m \in \mathbb{N}$. Assuming $p \neq 0$, and that within R $a \cdot b = 0$ implies $a = 0$ or $b = 0$, we can establish that R can be pseudo-ordered by p if and only if $p^n + 1 \neq 0 \ \forall n \in \mathbb{N}$. Hence, we can state the following theorem.

Theorem 3.2.1. *Let R be an integral domain and let $p \in R$, $p \neq 0$. Then R is pseudo-ordered by p if and only if $p^n + 1 \neq 0 \ \forall n \in \mathbb{N}$.*

Proof. R is not pseudo-ordered by p if and only $p^n + p^m = 0$ for some $n, m \in \mathbb{N}$, with $n \geq m$. This is equivalent to $p^n + p^m = p^m \cdot (p^{n-m} + 1) = 0$. Since R is an integral domain, we equivalently have $p^{n-m} + 1 = 0$. □

An immediate consequence of the above theorem is given in the following corollary.

Corollary 3.2.2. *The complex number field $\mathbb{C}$ cannot be pseudo-ordered by i.*

Proof. $i^2 + 1 = -1 + 1 = 0$, by 3.2.1 $\mathbb{C}$ cannot be pseudo-ordered by i. □

Having introduced the concept 3.1.2, we are ready to investigate the pseudo orders of the ring $\mathbb{Z}_n$. In the next section we shall study the conditions under which $\mathbb{Z}_n$ can be pseudo-ordered by an arbitrary element $s \in \mathbb{Z}_n$.

Chapter 4

Pseudo-Orders in the Ring $\mathbb{Z}_n$

In this section we address the question related to the pseudo-orders of $\mathbb{Z}_n$. In the remainder of this text we consider $\mathbb{Z}_n$ with $n > 2$, since $\mathbb{Z}_2$ has cardinality 2 and from Theorem 2.0.4 we already know it cannot be pseudo-ordered, hence there is no need to consider this case.

Given that $\mathbb{Z}_n$ is a finite ring, there are finitely many elements that can pseudo-order it. One approach to find these elements is to consider the prime factorization of n.

4.1 Simple Case: n is a Power of a Prime Number

Let us first start with the simplest case, the case when n contains only one prime number in its prime factorization.

Theorem 4.1.1. *Let $R = \mathbb{Z}_{p^k}$. Then R cannot be pseudo-ordered by p if and only if $p = 2$*

Proof. ($\Rightarrow$) Assume $\mathbb{Z}_{p^k}$ is not pseudo-ordered by p. Then, $n = p^k \mid p^a + p^b$ for some positive integers a and b. Without loss of generality, assume $p^a \not\equiv 0 \pmod{n}$ and $p^b \not\equiv 0 \pmod{n}$ because if, say $p^a \equiv 0 \pmod{n}$ then $p^k \mid p^b$ hence $p^b \equiv 0$ and there is nothing to prove. Also without loss of generality we can assume $a \leq b$. Then $n = p^k \mid p^a + p^b = p^a \cdot (p^{b-a} + 1)$. If $a \neq b$, then $p^k \nmid p^{b-a} + 1$, and we obtain $p^k \mid p^a$, a contradiction. So, a must equal b.

Then we have $n = p^k \mid p^a + p^b = p^a \cdot (p^{b-a} + 1) = 2 \cdot p^a$. If $p \neq 2$, then again we obtain $p^k \mid p^a$, a contradiction. Therefore we must have $p = 2$.

($\Leftarrow$) Assume $p = 2$. Then since $2^k = 2^{k-1} + 2^{k-1}$ and $2^{k-1} \not\equiv 0 \pmod{n}$ and $2^k = n$, we obtained n as a sum of two powers of 2, which proves that $\mathbb{Z}_n$ cannot be pseudo-ordered by 2. □

Example 4.1.2. Consider the ring $R = \mathbb{Z}_{16}$. Since $16 = 2^4$, Theorem 4.1.1 tells us *R is not* pseudo-ordered by 2. We can see it directly by finding $P = \{0, 2, 4, 8\}$ while $-P = \{0, 14, 12, 8\}$ and so $P \cap -P = \{0, 8\}$.

Note that, if in the previous example we attempt to pseudo-order Z_{16} by $4 = 2^2$, then we find out that $\hat{2^2} = \{0, 4\}$ and $-\hat{2^2} = \{0, 12\}$ and therefore $\mathbb{Z}_{16}$ is pseudo-ordered by 2^2. It is therefore natural to ask when can we pseudo-order $\mathbb{Z}_{2^k}$ by 2^d for some $d > 1$. To this end, we need a widely known result from number theory. The proof of this theorem is omitted. However, it can be found in most number theory text books, for instance, in [1] or [2].

Theorem 4.1.3. *(Euclid's Lemma) If* $a \mid b \cdot c$, *with* $\gcd(a, b) = 1$, *then* $a \mid c$.

Theorem 4.1.4. *Let* $R = \mathbb{Z}_{2^k}$. *Then R cannot be pseudo-ordered by* 2^d *for any* $d \geq 1$ *if and only if* $d \mid k - 1$.

Proof. ($\Rightarrow$) Assume R is not pseudo-ordered by 2^d. Then there are $n, m \in \mathbb{Z}$ such that $2^k \mid 2^{d \cdot m} + 2^{d \cdot n}$ with $2^{d \cdot n} \not\equiv 0 \pmod{2^k}$ and $2^{d \cdot m} \not\equiv 0 \pmod{2^k}$. Without loss of generality, let $m \leq n$. Then

$$2^k \mid 2^{d \cdot m} + 2^{d \cdot n} = 2^{d \cdot m} \cdot (2^{d \cdot (n-m)} + 1)$$

Suppose $n \neq m$. Since $\gcd(2^k, 2^{d \cdot (n-m)} + 1) = 1$, by Euclid's lemma we have $2^k \mid 2^{d \cdot m}$, a contradiction. So we must have $n = m$. Thus, $2^k \mid 2 \cdot 2^{d \cdot m} = 2^{d \cdot m + 1}$.

Since $2^k \mid 2^{d \cdot m + 1}$, we have $k \leq d \cdot m + 1$. Also, given $2^k \nmid 2^{d \cdot m}$, we have $d \cdot m < k$. So, we obtain that $d \cdot m < k \leq d \cdot m + 1$. Therefore we must have $k = d \cdot m + 1$, or $k - 1 = d \cdot m$ and the result follows.

($\Leftarrow$) Assume $d \mid k - 1$, then $m \cdot d = k - 1$, so $m \cdot d + 1 = k$ for some m. Hence,

$$n = 2^k = 2^{m \cdot d + 1} = 2^{m \cdot d} + 2^{m \cdot d} = (2^d)^m + (2^d)^m$$

and therefore R cannot be pseudo-ordered by p^d. □

Revisiting our example of $\mathbb{Z}_{16}$, where $n = 2^4$ and $k = 4$, we can see that for $d = 1, 3$, $\mathbb{Z}_{16}$ is not pseudo-ordered by p^d. Indeed, $d = 1 \mid 3 = k - 1$ and $d = 3 \mid 3 = k - 1$. However $2^2 = 4$ pseudo-orders $\mathbb{Z}_{16}$ as we found by computing the set $\hat{2^2} = \{0, 4\}$ and $-\hat{2^2} = \{0, 12\}$.

In order to present a corollary to 4.1.4, we recall the definition of a well-known number theoretic function.

Definition 4.1.5. *Given a positive integer n, let $\tau(n)$ denote the number of positive divisors of n.*

Example 4.1.6. Consider the case $n = 12$. It can be easily seen that the divisors of 12 are $1, 2, 3, 4, 6, 12$, which is a total of 6 divisors. Therefore, $\tau(12) = 6$.

Example 4.1.7. For any prime number p, $\tau(p) = 2$, namely, 1 and p itself.

Corollary 4.1.8. *$\mathbb{Z}_{2^k}$ can be pseudo-ordered in $k - \tau(k-1)$ ways.*

Proof. By 4.1.4, $\mathbb{Z}_{2^k}$ is not pseudo-ordered by p^d when $d \mid k - 1$. There are $\tau(k-1)$ such divisors. Therefore the number of the remaining possibilities is $k - \tau(k-1)$. □

4.2 General Case: n an Arbitrary Number

Now let us turn our attention to more general cases, when n is not limited to be a power of a prime. Let $R = \mathbb{Z}_n$, and let $p_1^{k_1} \cdot p_2^{k_2} \ldots \cdot p_r^{k_r}$ be the prime factorization of n. Consider an arbitrary prime number $p_1, p_2, \ldots, p_r$ from the factorization and call it p. Then, $n = p^k \cdot q$, and $\gcd(p, q) = 1$.

Let us explore the conditions that need to be satisfied in order for p to pseudo-order R. Let us first recall a definition and another widely known result from number theory that will be applied in our results. The proof of the theorem is also omitted. See [1] or [2] for a proof of this theorem.

Definition 4.2.1. *For $n \geq 1$, let $\phi(n)$ denote the number of positive integers not exceeding n that are relatively prime to n.*

Example 4.2.2. Consider the case $n = 30 = 2 \cdot 3 \cdot 5$. Clearly, the numbers relatively prime to 30 not exceeding 30 are those which are not multiples of $2, 3$, and 5, and they are: $1, 7, 11, 13, 17, 19, 23, 29$. There are 8 of them, therefore $\phi(30) = 8$.

Theorem 4.2.3. *(Euler's Theorem) If* $n \geq 1$ *and* $\gcd(a, n) = 1$*, then*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

4.2.1 Pseudo-Orders by a Product of Primes From the Factorization of n

Euler's theorem is a very powerful tool that allows us to simplify expressions when working with congruences. In the following results, we will see how Euler's theorem helps us to find an upper bound of a number in concern, and therefore makes the computation very feasible in practice.

Theorem 4.2.4. *Let* $n = p^k \cdot q$*,* $q > 1$*, with* p *prime,* $k \geq 1$*,* $q > 1$*, and* $\gcd(p, q) = 1$*. Then the ring* $\mathbb{Z}_n$ *cannot be pseudo-ordered by* p^d *if and only if* $q \mid p^{d \cdot c} + 1$*, for some* $c \in [0, \phi(q))$*.*

Proof. ($\Leftarrow$) Assume $q \mid p^{d \cdot c} + 1$ for some $c \geq 1$. Since $p^k \mid p^{k \cdot h}$ for any h, in particular, for $h = d$, it follows that

$$\begin{aligned} n = p^k \cdot q \mid & p^{k \cdot d} \cdot (p^{d \cdot c} + 1) \\ & = p^{d \cdot (k+c)} + p^{d \cdot k} \\ & = (p^d)^{k+c} + (p^d)^k \end{aligned}$$

Let us show that $p^{d \cdot (k+c)}$ and $p^{d \cdot k}$ are not 0 in $\mathbb{Z}_n$. To this end, it suffices to show one of them is not 0 in $\mathbb{Z}_n$ because, if say $p^{d \cdot (k+c)} \equiv 0 \pmod{n}$ and $p^{d \cdot k} \not\equiv 0 \pmod{n}$, we obtain $p^{d \cdot (k+c)} + p^{d \cdot k} \equiv p^{d \cdot k} \equiv 0 \pmod{n}$, a contradiction. Therefore, let us show $p^{d \cdot k} \not\equiv 0 \pmod{n}$. Suppose not. Then $n = p^k \cdot q \mid p^{k \cdot d}$, but this implies $q \mid p^{k \cdot (d-1)}$, which is impossible since $\gcd(p, q) = 1$. Therefore $n \nmid p^{k \cdot d}$.

($\Rightarrow$) Suppose that $\mathbb{Z}_n$ cannot be pseudo-ordered by p^d. Then there exist a and b such that $n \mid p^{d\cdot a} + p^{d\cdot b}$. Note that $p^{d\cdot a}$ and $p^{d\cdot b}$ are not congruent to n.

Without loss of generality, assume $a \leq b$, then $p^{d\cdot a} + p^{d\cdot b} = p^{a\cdot d} \cdot (p^{d\cdot(b-a)} + 1)$. Since $p^k \nmid p^{d\cdot h} + 1$ for any $h > 0$, it follows that $q \mid p^{d\cdot(b-a)} + 1$.

Now let us prove that indeed we have $b - a < \phi(q)$. We apply the division algorithm to divide $b - a$ by $\phi(q)$. We have $b - a = t \cdot \phi(q) + c$ where $0 \leq c < \phi(q)$. Now we represent $q \mid p^{d\cdot(b-a)} + 1$ in its equivalent form using congruences:

$$p^{d\cdot(b-a)} \equiv -1 \pmod{q} \tag{4.1}$$

Hence

$$p^{d\cdot(b-a)} = p^{d\cdot(t\cdot\phi(q)+c)} = (p^{\phi(q)})^{d\cdot t} \cdot p^{d\cdot c} = (p^{d\cdot t})^{\phi(q)} \cdot p^{d\cdot c}. \tag{4.2}$$

But by 4.2.3,

$$(p^{d\cdot t})^{\phi(q)} \equiv 1 \pmod{q}. \tag{4.3}$$

By multiplying (4.3) by $p^{d\cdot c}$ and comparing with (4.1) we obtain $p^{d\cdot c} \equiv -1 \pmod{q}$. Therefore $q \mid p^{d\cdot c} + 1$ with $0 \leq c < \phi(q)$. □

Before generalizing the above result, let us see an example that uses Theorem 4.2.4 to find sets P in $\mathbb{Z}_n$ that defines a pseudo-order.

Example 4.2.5. Consider $n = 300 = 2^2 \cdot 3 \cdot 5^2$. Let us check whether $\mathbb{Z}_{300}$ can be pseudo-ordered by 2. Since, 300 is not a power of 2, the only condition that needs to be checked is whether $q = 3 \cdot 5^2 = 75$ divides a number of the form $2^c + 1$. This is equivalent to $2^c \equiv -1 \pmod{75}$, which means $2^c + 1 = 75 \cdot k$ for some k. It can be easily seen that the multiples of 75 have either 0 or 5 as the last digit, hence we only need to consider the powers of 2 that have either 9 or 4 as the last digit. As the former never happens, we only need to check the powers of 2 with 4 as the last digit. A quick inspection shows that there is no such $c < \phi(75) = 40$ which makes $2^c + 1$ a multiple of 75, therefore, $\mathbb{Z}_{300}$ *can* be pseudo-ordered

by 2. By computing the powers of 2 (mod 300), we generate the set P:

$$P = \{0, 2, 4, 8, 16, 32, 64, 128, 256, 212, 124, 248, 196, 92, 184, 68,$$
$$136, 272, 244, 188, 76, 152\}$$

The set $-P$ obtained by computing $300 - x \ \forall x \in P$ is

$$-P = \{0, 298, 296, 292, 284, 268, 236, 172, 44, 88, 176, 52, 104, 208,$$
$$116, 232, 164, 28, 56, 112, 224, 148\}$$

It can be verified directly that indeed $P \cap -P = \{0\}$.

As we stated earlier, $\hat{r^d} \subseteq \hat{r}$ for any $d \geq 1$. Therefore, since $\mathbb{Z}_{300}$ is pseudo-ordered by 2, it is also pseudo-ordered by $2^2 = 4$. This assertion is verified generating the sets P and $-P$:

$$P = \{0, 4, 16, 64, 76, 124, 136, 184, 196, 244, 256\}$$
$$-P = \{0, 296, 284, 236, 224, 176, 164, 116, 104, 56, 44\}$$

and seeing that $P \cap -P = \{0\}$.

Let us now check whether $\mathbb{Z}_{300}$ is pseudo-ordered by 5. In this case, we have $q = 2^2 \cdot 3 = 12$. We need to see if q divides a number of the form $5^c + 1$. Clearly, the powers of 5 have a 5 as the last digit. Hence, $5^c + 1$ has a 6 as the last digit. Since the multiples of 12 are $12, 24, 36, 48, 60, 72, 84, 96, \ldots$ we can see that the last digit is repeated every 5 numbers. Therefore, the number that is of the form $5^c + 1$, if it exits, must be one of $36, 96, 156, \ldots, 36 + k \cdot 60$. It can be checked that none of these numbers is of the form $5^c + 1$. This is done by looking at the generated sets P and $-P$:

$$P = \{0, 5, 25, 125\}$$
$$-P = \{0, 295, 275, 175\}$$

and $P \cap -P = \{0\}$. Therefore $\mathbb{Z}_{300}$ is pseudo-ordered by 5.

Since $\mathbb{Z}_{300}$ is pseudo-ordered by 5, it also is pseudo-ordered by 5^2:

$$P = \{0, 25\}$$
$$-P = \{0, 275\}.$$

In the previous theorem we considered a pseudo-ordering of the ring $\mathbb{Z}_n$ by a number p^d where p is a prime number coming from the prime factorization of n. A further generalization will be to pseudo-order by $m = p_1^{s_1} \cdot \ldots \cdot p_r^{s_r}$, where the p_i's are prime numbers coming from the prime factorization of n. It turns out, that the condition is analogous to the case when $r = 1$. We present the result in the following theorem.

Theorem 4.2.6. *Let $R = \mathbb{Z}_n$ where $n = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r} \cdot q$, $q > 1$ and $\gcd(p_i, q) = 1$ for $i = 1, \ldots, r$. Let $m = p_1^{s_1} \cdot \ldots \cdot p_r^{s_r}$, $s_i \geq 1$. Then R is not pseudo-ordered by m if and only if $q \mid m^c + 1$ for some $c \in [0, \phi(q))$.*

Proof. ($\Rightarrow$) Suppose $\mathbb{Z}_n$ is not pseudo-ordered by m. Then, there exist a, b, with say, $a \leq b$ such that

$$p_1^{k_1} \cdot \ldots \cdot p_r^{k_r} \cdot q \mid (p_1^{k_1} \cdot \ldots \cdot p_r^{k_r})^a + (p_1^{k_1} \cdot \ldots \cdot p_r^{k_r})^b.$$

Note that $(p_1^{k_1} \cdot \ldots \cdot p_r^{k_r})^a$ and $(p_1^{k_1} \cdot \ldots \cdot p_r^{k_r})^b$ are not 0 in $\mathbb{Z}_n$. Then

$$p_1^{k_1} \cdot \ldots \cdot p_r^{k_r} \cdot q \mid (p_1^{k_1} \cdot \ldots \cdot p_r^{k_r})^a \cdot ((p_1^{k_1} \cdot \ldots \cdot p_r^{k_r})^{b-a} + 1)$$

Since $\gcd(p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}, q) = 1$ we have $q \mid (p_1^{k_1} \cdot \ldots \cdot p_r^{k_r})^a \cdot ((p_1^{k_1} \cdot \ldots \cdot p_r^{k_r})^{b-a} + 1)$. It follows that $q \mid (p_1^{k_1} \cdot \ldots \cdot p_r^{k_r})^{b-a} + 1$. To bound the exponent, divide $b - a$ by $\phi(q)$. Then, $b - a = h \cdot \phi(q) + c$ where $0 \leq c < \phi(q)$. Using congruences, we obtain

$$(p_1^{k_1} \cdot \ldots \cdot p_r^{k_r})^{b-a} \equiv -1 \pmod{q}, \tag{4.4}$$

and

$$(p_1^{k_1} \cdot \ldots \cdot p_r^{k_r})^{b-a} = (p_1^{k_1} \cdot \ldots \cdot p_r^{k_r})^{h \cdot \phi(q) + c} = (p_1^{k_1} \cdot \ldots \cdot p_r^{k_r})^{h \cdot \phi(q)} \cdot (p_1^{k_1} \cdot \ldots \cdot p_r^{k_r})^c. \tag{4.5}$$

Since $\gcd(p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}, q) = 1$, by Theorem 4.2.3,

$$((p_1^{k_1} \cdot \ldots \cdot p_r^{k_r})^h)^{\phi(q)} \equiv 1 \pmod{q}. \tag{4.6}$$

By multiplying (4.6) by $(p_1^{k_1}\cdot\ldots\cdot p_r^{k_r})^c$ and comparing with (4.4) we obtain $(p_1^{k_1}\cdot\ldots\cdot p_r^{k_r})^c \equiv -1 \pmod{q}$. Therefore $q \mid m^c + 1$ with $c \in [0, \phi(q))$.

($\Leftarrow$) Suppose $q \mid m^c + 1$ for some $0 \leq c < \phi(q)$. Let $b = \max(k_1, \ldots, k_r)$, then $p_1^{k_1} \cdot \ldots \cdot p_r^{k_r} \mid p_1^{b \cdot s_1} \cdot \ldots \cdot p_r^{b \cdot s_r} = m^b$. Hence, $p_1^{k_1} \cdot \ldots \cdot p_r^{k_r} \cdot q = n \mid m^b \cdot (m^c + 1)$.

Since $q > 1$, $n \nmid m^b$ and $n \mid m^{b+c} + m^b$, therefore $\mathbb{Z}_n$ is not pseudo-ordered by m. □

4.2.2 Pseudo-Order by a Number Relatively Prime to n

Our next result deals with pseudo-orderings of $\mathbb{Z}_n$ by an arbitrary number s which is relatively prime to n.

Theorem 4.2.7. *Let $R = \mathbb{Z}_n$, and consider a number s such that $\gcd(s, n) = 1$. Then R cannot be pseudo-ordered by s^d if and only if $n \mid s^{d \cdot c} + 1$ where $0 \leq c < \phi(n)$.*

Proof. ($\Rightarrow$) Assume $\mathbb{Z}_n$ is not pseudo-ordered by s^d. Then, there exist $a, b \in \mathbb{Z}$, $a \leq b$ such that $n \mid s^{d \cdot a} + s^{d \cdot b} = s^{d \cdot a} \cdot (s^{d \cdot (b-a)} + 1)$. Since $\gcd(n, s) = 1$, $n \nmid s^{d \cdot a}$, hence $n \mid s^{d \cdot (b-a)} + 1$. If $a = b$, then $n \mid 2$, which is impossible since $n > 2$. Hence, $b - a > 0$. To bound from above the power of s from above, we represent $n \mid s^{d \cdot (b-a)} + 1$ as

$$s^{d \cdot (b-a)} \equiv -1 \pmod{n}.$$

Divide $b - a$ by $\phi(n)$, so $b - a = q \cdot \phi(n) + c$ where $0 \leq c < \phi(n)$ and therefore

$$s^{d \cdot (q \cdot \phi(n) + c)} \equiv -1 \pmod{n} \equiv s^{d \cdot c} \equiv -1 \pmod{n}$$

and the conclusion follows.

($\Leftarrow$) Assume $n \mid s^{d \cdot c} + 1$ for some $c \in \mathbb{Z}$, $0 \leq c < \phi(n)$. Since $n \mid n \cdot s^{d \cdot r}$ for any r and $n \cdot s^{d \cdot r} \mid s^{d \cdot r} \cdot (s^{d \cdot c} + 1)$, it follows that $n \mid s^{d \cdot r} \cdot (s^{d \cdot c} + 1) = s^{d \cdot (c+r)} + s^{d \cdot r}$. Since neither of $s^{d \cdot (c+r)}$ and $s^{d \cdot r}$ is 0 in $\mathbb{Z}_n$, the ring cannot be pseudo-ordered by s^d. □

Note that the number m considered in 4.2.7 can be thought as a number composed of primes *not coming* from the prime factorization of n while the number m in Theorem 4.2.6

is composed from the primes *coming* from the prime factorization of n. We will now mix these two cases.

4.2.3 Pseudo-Order $\mathbb{Z}_n$ by an Arbitrary m

In order to characterize the general case, we shall find a suitable representation for any two numbers n and m that allows us to use the techniques we have applied so far. This representation is stated in the following lemma.

Lemma 4.2.8. *Let n and m be any two positive integers. Then n and m can be expressed as*

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r} \cdot q$$

$$m = p_1^{s_1} \cdot p_2^{s_2} \cdot \ldots \cdot p_r^{s_r} \cdot s$$

where $p_i > 0$, $s_i > 0$, $k_i > 0$, p_i are pairwise different primes for $i = 1, \ldots, r$, $\gcd(q, s) = 1$, and $r \geq 0$.

Proof. If $\gcd(n, m) = 1$, let $q = n$ and $s = m$ with $r = 0$, then n and m are expressed in the desired form.

Suppose $\gcd(n, m) > 1$. By the Fundamental Theorem of Arithmetic, there is at least one common prime number in the prime factorizations of m and n. Let $p_1, p_2, \ldots, p_r$ for $r \geq 1$ be the common primes of m and n and consider the prime factorizations:

$$n = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_r^{n_r} \cdot q_1^{a_1} \cdot \ldots \cdot q_h^{a_h}$$

$$m = p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots \cdot p_r^{m_r} \cdot t_1^{b_1} \cdot \ldots \cdot t_w^{b_w}$$

where $q_1, \ldots, q_h$ and $t_1, \ldots, t_w$ are the remaining primes in the factorization of m and n respectively. Since $p_1, \ldots, p_r$ are all the common prime numbers of n and m, it follows that $\gcd(q_1^{a_1} \cdot \ldots \cdot q_h^{a_h}, t_1^{b_1} \cdot \ldots \cdot t_w^{b_w}) = 1$. Let us put $q = q_1^{a_1} \cdot \ldots \cdot q_h^{a_h}$ and $s = t_1^{b_1} \cdot \ldots \cdot t_w^{b_w}$. Hence n and m are represented in the desired format. □

We are now in a position to prove the main theorem about possibilities of pseudo-ordering $\mathbb{Z}_n$ by an arbitrary number m. As we will see shortly, this theorem splits into cases. We present a lemma that will be useful to prove one of the cases.

Lemma 4.2.9. *Let m, n be positive integers such that $m \leq n$ and let $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$. Then $a \cdot b^m \nmid c \cdot b^n$ if and only if $a \nmid c$ for any $c \in \mathbb{Z}$.*

Proof. ($\Rightarrow$) By contrapositive assume $a \mid c$. Since for any $m \leq n$, $b^m \mid b^n$, then $a \cdot b^m \mid c \cdot b^n$.

($\Leftarrow$) Again by contrapositive suppose $a \cdot b^m \mid c \cdot b^n$ with $m \leq n$. Then $c \cdot b^n = k \cdot a \cdot b^m$ for some k, which implies $c \cdot b^{n-m} = k \cdot a$, so $a \mid c \cdot b^{n-m}$. If $n = m$, then $a \mid c \cdot b^0 = c$. If $n > m$, then $a \mid c \cdot b^s$ for some $s > 0$. Since $1 = \gcd(a, b) = \gcd(a, b^s)$, it follows that $a \mid c$. □

We now proceed to present the main result.

Theorem 4.2.10. *Let $R = \mathbb{Z}_n$, with $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r} \cdot s$, and let $m = p_1^{s_1} \cdot p_2^{s_2} \cdot \ldots \cdot p_r^{s_r} \cdot q$, where $p_1, \ldots, p_r$ are primes, $k_i > 0$, $s_i > 0$, and $\gcd(p_i, s) = \gcd(s, q) = 1$, $i = 1, \ldots, r$. Then, R is not pseudo-ordered by m if and only if one of the following conditions is satisfied,*

$$s = 1, p_1 = 2, s_1 \mid k_1 - 1, \text{ and } k_j \leq \frac{s_j}{s_1} \cdot (k_1 - 1), j = 2, \ldots, r \tag{4.7}$$

$$s > 1 \text{ and } s \mid m^c + 1, \text{ for some } c \in [0, \phi(s)). \tag{4.8}$$

Proof. ($\Rightarrow$) Suppose that R is not pseudo-ordered by m.

Case $s = 1$

Suppose that there are two elements from $\hat{m}$ that add up to 0. So let $n \mid m^a + m^b$.

We have $m^a + m^b = m^a \cdot (m^{b-a} + 1)$ where without loss of generality we may assume $a \leq b$. Let $c = b - a$ and suppose $c > 0$. Then

$$n = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r} \mid p_1^{a \cdot s_1} \cdot \ldots \cdot p_r^{a \cdot s_r} \cdot q^a \cdot (p_1^{c \cdot s_1} \cdot \ldots \cdot p_r^{c \cdot s_r} \cdot q^c + 1).$$

Note that $p_i^{k_i} \nmid m^c + 1$ since $\gcd(p_i^{k_i}, m^c + 1) = 1$, for $i = 1, \ldots, r$, so $n \nmid m^c + 1$. Therefore $n \mid m^a$. But then $m^a \equiv 0 \pmod{n}$, hence $m^a = 0$ in $\mathbb{Z}_n$.

So we must have $a = b$. Then $n \mid 2 \cdot m^a$ and $m^a \not\equiv 0 \pmod{n}$. Therefore n is an even number, and since $s = 1$, so m is also even because m contains all the primes of the prime factorization of n, in particular 2. Without loss of generality, assume $p_1 = 2$. Since $m^a \not\equiv 0 \pmod{n}$, i.e. $n \nmid m^a$, we have

$$2^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r} \mid 2^{a \cdot s_1 + 1} \cdot p_2^{a \cdot s_2} \cdot \ldots \cdot p_r^{a \cdot s_r} \cdot q^a \tag{4.9}$$

$$2^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r} \nmid 2^{a \cdot s_1} \cdot p_2^{a \cdot s_2} \cdot \ldots \cdot p_r^{a \cdot s_r} \cdot q^a. \tag{4.10}$$

Since $\gcd(2, p_i) = \gcd(2, q) = 1$, $i = 1, \ldots, r$, from (4.9) we conclude

$$2^{k_1} \mid 2^{a \cdot s_1 + 1} \text{ and } p_i^{k_i} \mid p_i^{a \cdot s_i},\ i = 2, \ldots, r.$$

It implies

$$k_1 \leq a \cdot s_1 + 1 \text{ and } k_i \leq a \cdot s_i,\ i = 2, \ldots, r.$$

Since $2^{k_1} \cdot p_2^{k_2} \cdot \ldots p_r^{k_r} \nmid 2^{a \cdot s_1} \cdot p_2^{a \cdot s_2} \cdot \ldots \cdot p_r^{a \cdot s_r} \cdot q^a$, by repeatedly applying Lemma 4.2.9 for each p_i, we conclude that $2^{k_1} \nmid 2^{a \cdot s_1} \cdot q^a$. In particular, $2^{k_1} \nmid 2^{a \cdot s_1}$, which implies $a \cdot s_1 < k_1$. Hence we obtain $a \cdot s_1 < k_1 \leq a \cdot s_1 + 1$. Therefore $k_1 = a \cdot s_1 + 1$, so $a = \frac{k_1 - 1}{s_1}$. Thus $s_1 \mid k_1 - 1$ and $k_i \leq \frac{k_1 - 1}{s_1} \cdot s_i$ as claimed.

Case $s > 1$

Let again $a \leq b$ and $n \mid m^a + m^b = m^a \cdot (m^{b-a} + 1)$. So $p_1^{k_1} \cdot \ldots \cdot p_r^{k_r} \cdot s \mid m^a \cdot (m^{b-a} + 1)$. Since $\gcd(s, m) = 1$, it follows that $s \mid m^{b-a} + 1$.

Now, divide $b - a$ by $\phi(s)$, so that $b - a = t \cdot \phi(s) + c$ where $0 \leq c < \phi(s)$. Since $s \mid m^{b-a} + 1$ is equivalent to stating $m^{b-a} \equiv -1 \pmod{s}$, we have

$$(m^{\phi(s)})^t \cdot m^c = m^{t \cdot \phi(s)} \cdot m^c = m^{t \cdot \phi(s) + c} = m^{b-a} \equiv -1 \pmod{s}.$$

Since $\gcd(m, s) = 1$, Euler's theorem applies, and by Theorem 4.2.3

$$m^c = 1^t \cdot m^c = (m^{\phi(s)})^t \cdot m^c = m^{b-a} \equiv -1 \pmod{s}.$$

Therefore $s \mid m^c + 1$ for $c \in [0, \phi(s))$.

($\Leftarrow$) Case (4.7). Suppose $s_1 \mid (k_1 - 1)$ and $k_j \leq \frac{s_j}{s_1} \cdot (k_1 - 1), j = 2, \ldots, r$.

Let $a = \frac{k_1 - 1}{s_1}$. So $k_1 = a \cdot s_1 + 1$ and $k_j \leq s_j \cdot a$, $j = 2, \ldots, r$. Then

$$p_2^{k_2} \cdot \ldots \cdot p_r^{k_r} \mid p_2^{a \cdot s_2} \cdot \ldots \cdot p_r^{a \cdot s_r}$$

$$2^{k_1} \mid 2^{a \cdot s_1 + 1}.$$

So

$$2^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r} \mid 2^{a \cdot s_1 + 1} \cdot p_2^{a \cdot s_2} \cdot \ldots \cdot p_r^{a \cdot s_r}$$

and therefore

$$n = 2^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r} \mid 2 \cdot (2^{s_1} \cdot p_2^{s_2} \cdot \ldots \cdot p_r^{s_r} \cdot q)^a = 2 \cdot m^a = m^a + m^a.$$

Since $k_1 > a \cdot s_1$ and $\gcd(2, q) = 1$, then $2^{k_1} \nmid 2^{a \cdot s_1} \cdot q^a$. By repeatedly applying Lemma 4.2.9 to each p_j for $j = 2, \ldots, r$ we get

$$n = 2^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r} \nmid (2^{s_1} \cdot p_2^{s_2} \cdot \ldots \cdot p_r^{s_r} \cdot q)^a = m^a.$$

Hence, $n \nmid m^a$ and $n \mid m^a + m^a$, that is, $\mathbb{Z}_n$ is not pseudo-ordered by m.

Case (4.8). Suppose $s \mid m^c + 1$ for some $c \in [0, \phi(s))$, and let $b = \max(k_1, \ldots, k_r)$. Since $p_i^{k_i} \mid p_i^{s_i \cdot b}$ for $i = 1, \ldots, r$,

$$p_1^{k_1} \cdot \ldots \cdot p_r^{k_r} \mid p_1^{b \cdot s_1} \cdot \ldots \cdot p_r^{b \cdot s_r} \cdot q^b = m^b$$

and therefore

$$n = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r} \cdot s \mid m^b \cdot (m^c + 1) = m^{b+c} + m^b.$$

Since $s > 1$ and $\gcd(s, q) = 1$, no power of m equals 0 in $\mathbb{Z}_n$. Hence $\mathbb{Z}_n$ is not pseudo-ordered by m.

□

Note that when $q = 1$, Theorem 4.2.6 becomes a particular case of Theorem 4.2.10. Similarly, when $r = 0$ Theorem 4.2.7 becomes a special case of 4.2.10. Furthermore, the other specific case we investigated, Theorem 4.1.4 refers to the case when $s = q = r = 1$.

Let us present a few examples of our results and let us illustrate them by computing the corresponding sets $\hat{m}$ and $-\hat{m}$.

4.2.4 Examples for the Case $s = 1$

Let us first see a few examples for the case (4.7).

Example 4.2.11. Consider $n = 128334375 = 3^5 \cdot 5^5 \cdot 13^2$, $m = 2354625 = 3^2 \cdot 5^3 \cdot 13 \cdot 7 \cdot 23$. Here $s = 1$ and since 2 is not part of the prime factorizations of both n and m, the condition (4.7) is not satisfied, hence $\mathbb{Z}_n$ *is* pseudo-ordered by m. The generated sets $\hat{m}$ and $-\hat{m}$ are:

$$\hat{m} = \{0, 2354625, 85556250\}$$
$$-\hat{m} = \{0, 125979750, 42778125\}.$$

By examining these sets, we can see that indeed $\hat{m} \cap -\hat{m} = \{0\}$.

Example 4.2.12. Consider $n = 16301247872 = 2^7 \cdot 7^3 \cdot 13^5$, $m = 89908 = 2^2 \cdot 7 \cdot 13^2 \cdot 19$. The first condition, that 2 belongs to the prime factorization of both n and m this time is satisfied. We have $k_1 = 7, s_1 = 2$, and $\frac{k_1 - 1}{s_1} = 3$, and, $2 \mid 7 - 1 = 6$, $k_2 = 3 \leq 1 \cdot 3 = s_2 \cdot \frac{k_1 - 1}{s_1}$, and $k_3 = 4 \leq 2 \cdot 3 = s_3 \cdot \frac{k_1 - 1}{s_1}$. Since all the conditions from (4.7) of Theorem 4.2.10 are satisfied, this $\mathbb{Z}_n$ *is not* pseudo-ordered by m. This claim can be directly verified by looking

at the sets $\hat{m}$ and $-\hat{m}$:

$$\hat{m} = \{0, 89908, 8083448464, 8150623936\}$$
$$-\hat{m} = \{0, 16301157964, 8217799408, 8150623936\}.$$

We can see that $\hat{m} \cap -\hat{m} = \{0, 8150623936\}$, so by Theorem 2.0.3 the set $\hat{m}$ does not define a pseudo order.

Example 4.2.13. Consider $n = 114108735104 = 2^7 \cdot 7^4 \cdot 13^5$, $m = 89908 = 2^2 \cdot 7 \cdot 13^2 \cdot 19$. Although this is an almost identical example with 4.2.12, the only difference is the exponent of 7 in the prime factorization of n, changed from 3 to 4. Making this modification, the condition (4.7) of Theorem 4.2.10 is no longer satisfied since $k_2 = 4 \not\leq 1 \cdot 3 = s_2 \cdot \frac{k_1 - 1}{s_1}$. The theorem states then that $\mathbb{Z}_n$ is pseudo-ordered by m. The sets $\hat{m}$ and $-\hat{m}$ are:

$$\hat{m} = \{0, 89908, 8083448464, 8150623936\}$$
$$-\hat{m} = \{0, 114108645196, 106025286640, 105958111168\}.$$

Inspecting these sets, we can see that indeed $\hat{m} \cap -\hat{m} = \{0\}$.

4.2.5 Examples for the Case $s > 1$

We exhibit the use of condition (4.8).

Example 4.2.14. Consider $n = 1210 = 11^2 \cdot 2 \cdot 5$, $m = 11 \cdot 13$. Looking at the prime factorizations, wee can see that $s = 10$, $q = 13$. Since $s = 10 \mid 20449 + 1 = 143^2 + 1 = m^2 + 1$, Theorem 4.2.10 tells us $\mathbb{Z}_n$ *is not* pseudo-ordered by m. The generated sets $\hat{m}$ and $-\hat{m}$ are:

$$\hat{m} = \{0, 121, 143, 363, 847, 1089\}$$
$$-\hat{m} = \{0, 1089, 1067, 847, 363, 121\}.$$

Clearly, $\hat{m} \cap -\hat{m} = \{0, 121, 363, 847, 1089\}$, which agrees with the statement of Theorems 4.2.10 and 2.0.3.

Example 4.2.15. Consider $n = 458,640 = 2^4 \cdot 7^2 \cdot 13 \cdot 3^2 \cdot 5$, $m = 21112 = 2^3 \cdot 7 \cdot 13 \cdot 29$. For this example, we have $s = 45$, $q = 13$. It can be checked that $45 \nmid 21112^c + 1$ for all $c \in [0, \phi(45) = 24)$. Theorem 4.2.10 tells us that $\mathbb{Z}_n$ is pseudo-ordered by m. The sets $\hat{m}$ and $-\hat{m}$ are:

$$\begin{aligned}
\hat{m} = \{&0, 10192, 21112, 40768, 71344, 132496,\\
&163072, 193648, 224224, 285376, 315952,\\
&346528, 377104, 438256\}\\
-\hat{m} = \{&0, 448448, 437528, 417872, 387296,\\
&326144, 295568, 264992, 234416, 173264,\\
&142688, 112112, 81536, 20384\}.
\end{aligned}$$

Chapter 5

Concluding Remarks

We have presented a characterization of pseudo-orders in $\mathbb{Z}_n$. We have started presenting a general characterization for a set $P \subseteq R$ to form a positive cone on a ring R. This characterization proved very useful in finding pseudo-orderings by elements of the ring R.

Although, there are still questions to be answered. An interesting question following this line of research is to determine how to select elements $r_1, r_2, \ldots, r_n$ such that $\hat{r_1} \cup \hat{r_2} \cup \ldots \cup \hat{r_n}$ forms a positive cone. For example, consider the case of $\mathbb{Z}_{16}$. Using the results we have obtained, we can see $\mathbb{Z}_{16}$ is pseudo-ordered by 3 and 5. The generated sets are:

$$\hat{3} = \{0, 1, 3, 9, 11\}$$
$$-\hat{3} = \{0, 15, 13, 7, 5\}$$
$$\hat{5} = \{0, 1, 5, 9, 13\}$$
$$-\hat{5} = \{0, 15, 11, 7, 3\}.$$

Although, we can see that $11 \in \hat{3}$, $5 \in \hat{5}$, and $11 + 5 = 16 \equiv 0 \pmod{16}$. Therefore $\hat{3} \cup \hat{5}$ does not define a pseudo-order on $\mathbb{Z}_{16}$ even though each one of them separately does define a pseudo-order.

At this point it is uncertain what conditions must be satisfied for two sets $\hat{r_i}$ and $\hat{r_j}$ so that their union defines a pseudo-order on $\mathbb{Z}_n$. Examples like the previous one motivate to find a way to determine these conditions.

In our work, we mainly investigated the ring $\mathbb{Z}_n$. However, we have presented some results that apply to algebraic structures in general, like other rings and integral domains. Another direction worth pursuing is to investigate how the results and techniques presented in this work can be generalized.

References

[1] Burton, David M. *Elementary Number Theory*, 5th ed. New York: McGraw-Hill, 2002

[2] Hardy, G.H., Wright E.M. *An Introduction to the Theory of Numbers*, 6th ed. Oxford University Press, USA, 2008

[3] Isaacs, Martin A. *Algebra: A Graduate Course*, Belmont, California: Brooks/Cole, 1993

[4] Gallian, Joseph A. *Contemporary Abstract Algebra*, 5th ed. Boston: Houghton Mifflin, 2002

[5] Skala, Helen. *Trellis Theory*, Memoirs of the American Mathematical Society, No. 121. 1972

[6] Khamsi, Mohamed Amine. *Remarks on Caristi's Fixed Point Theorem*, Nonlinear Analysis, TMA, Vol. 71 (2009), 227-231

[7] Johnson, D. G. *A Structure Theory for a Class of Lattice-Ordered Rings*, Acta Mathematica, Vol. 104, No. 3-4, 163-215, December, 1960

[8] Machtinger, L. A. *Rings Satisfying a Not-Necessarily Transitive Relation*, Monatshefte für Mathematik, Vol. 75, No. 4, pp. 320-323, August, 1972

Appendix A

Source Code

Most of the examples presented in this thesis showed the generated sets P and $-P$. These sets were generated by a computer program.

The purpose of the mentioned program is to verify the results of the theorems and to display the generated sets. The program, however, does not use the theorems presented in this thesis. The program verifies if a generated set P forms a positive cone by means of "*brute force*".

The source code for the software is provided 'as is'. While no errors were found during the time it was used, it cannot be guaranteed the program is bug-free.

The program is written in the *Java* programming language. In order to compile it and run it, the Java SDK must be installed (http://java.sun.com/javase/downloads/index.jsp).

The program was developed and tested under version 1.6_11, however, any version 1.5+ should be able to compile it and run it.

For readers not familiar with computer programming, a diagram that describes the flow of the program is presented. In the diagram, the letter n refers to the modulo of $\mathbb{Z}_n$. The letter m refers to the number that will generate the set $\hat{m}$.

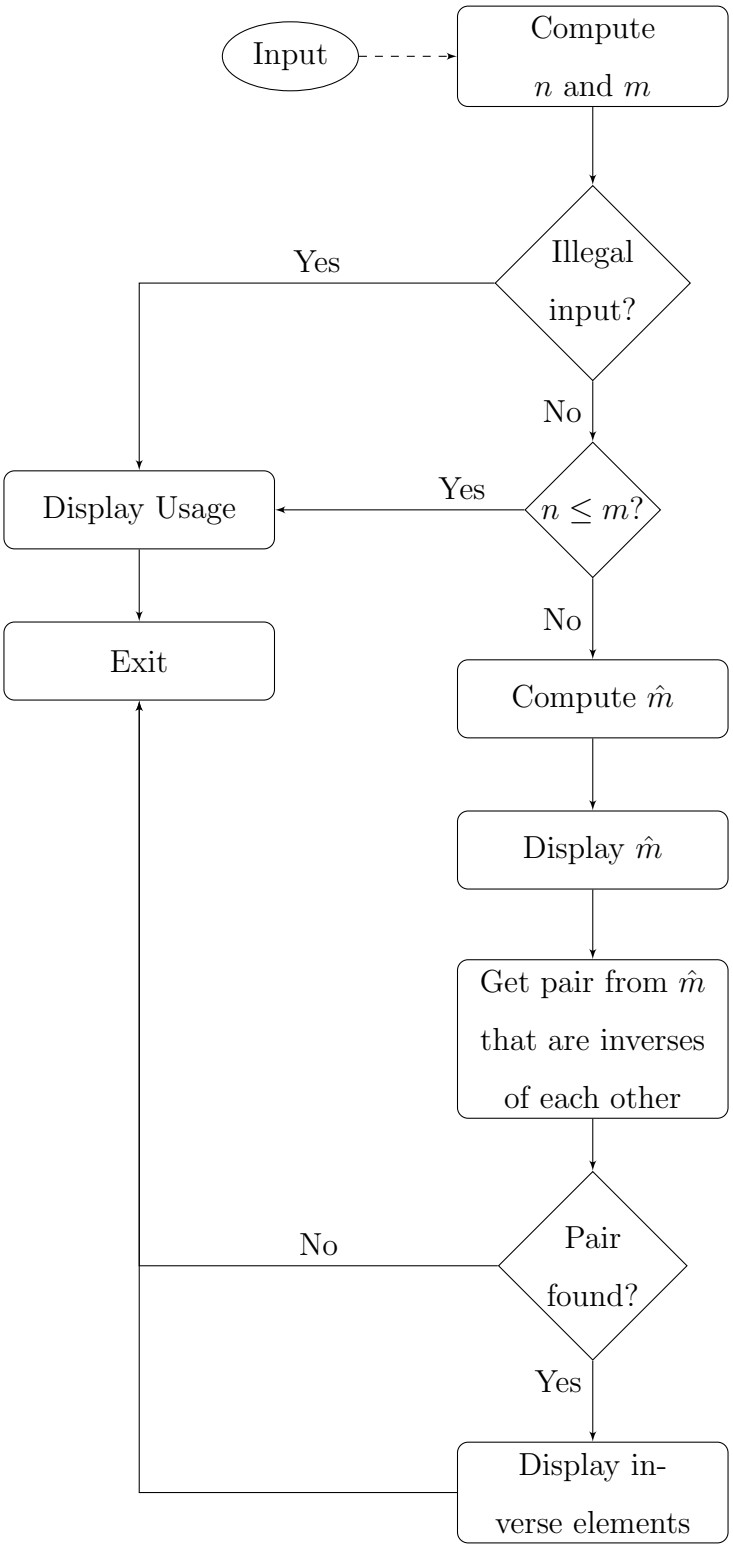

Figure A.1: Flow diagram of the computer program

```
import java.util.ArrayList;
import java.util.Arrays;
import java.util.Locale;

/**
 * This program is used to determine if, given arguments {@code n} and
 * {@code m}, the ring Z_n is pseudo-ordered by {@code m}.
 * There is only one method exposed, {@code main}. Upon receiving the
 * input, this program computes the sets {@code P} and {@code -P} and checks
 * if the set {@code P} forms a positive cone.
 *
 * @author Ivan Vargas
 * @version 1.0
 * @since 1.6.0_11
 */
public class PseudoOrderRings {

    /** ------------------------------------------------------
     *
     * Instance Variables
     *
     * ------------------------------------------------------*/

    /**
     * The set list containing the elements generated by m
     */
    private ArrayList<Long> hatSet;
```

```
/**
 * The modulo of the generated set
 */
private long modulo;

/** ------------------------------------------------------
 *
 * Constructor
 *
 * ------------------------------------------------------*/

/**
 * Creates a new instance
 */
public PseudoOrderRings() {
    hatSet = new ArrayList<Long>();
    modulo = -1;
} // End constructor()

/** ------------------------------------------------------
 *
 * Private Methods
 *
 * ------------------------------------------------------*/

/**
 * Given numbers n and m, compute the set m hat modulo n. The
```

```
 * resulting set is stored in {@link #hatSet}.
 * @param n The modulo.
 * @param m The generator of the set
 * @throws IllegalArgumentException if n is non-positive or if m is
 *         negative.
 */
private void computeSetHat(long n, long m) {
    if(n <= 0 || m < 0) {
        throw new IllegalArgumentException(
              "n must be non negative and m positive");
    }
    modulo = n;
    hatSet.clear();
    hatSet.add(new Long(0));
    long tmp = m;
    while (!hatSet.contains(tmp)) {
        hatSet.add(tmp);
        tmp *= m;
        tmp %= n;
    } // end of while (!hatSet.contains(tmp))
    Long[] sorted = new Long[hatSet.size()];
    hatSet.toArray(sorted);
    Arrays.sort(sorted);
    hatSet.clear();
    // Sort elements to make it easy to read
    for(int i = 0; i < sorted.length; i++) {
        hatSet.add(sorted[i]);
    }
```

```
} // End computeSetHat(long, long)

/**
 * If {@link #hatSet} contains two elements that are inverse of each
 * other, this method returns those elements in an array of
 * {@code long}. If {@link #hatSet} contains no inverses, i.e. it
 * forms a positive cone, it returns {@code null}. If {@link #hatSet}
 * contains more than one pair of inverse elements, it returns the
 * first pair that it finds.
 * @return An array of length two containing two elements in
 *         {@link #hatSet} that inverses of each other. If no inverses
 *         exist, {@code null} is returned.
 */
private long[] getInverseElementsInHatSet() {
    long[] inverses = new long[2];
    for(int i = 0; i < hatSet.size(); i++) {
        for(int j = i; j < hatSet.size(); j++) {
            if((hatSet.get(i) + hatSet.get(j)) % modulo == 0 &&
                    hatSet.get(i) != 0) {
                inverses[0] = hatSet.get(i);
                inverses[1] = hatSet.get(j);
                return inverses;
            }
        }
    }
    return null;
} // End getInverseElementsInHatSet()
```

```
/**
 * Creates a {@link String} representation of the sets {@link #hatSet}
 * and {@code -hatSet}, where the {@code -hatSet} is the set formed by
 * computing {@link #modulo} - {@code hatSet.get(i)} where {@code i}
 * runs from {@literal 0} to {@code hatSet.size()}
 * @return A {@link String} representation of {@link #hatSet} and
 *         {@code -hatSet}
 */
private String setsToString() {
    StringBuilder sb = new StringBuilder("P = { ");
    for (int i = 0; i < hatSet.size(); i++) {
        sb.append(hatSet.get(i));
        if (i + 1 < hatSet.size()) {
            sb.append(", ");
        } // end of if (i + 1 == hatSet.getCount())

    } // end of for (int i = 0; i < hatSet.getCount(); i++)
    sb.append(" }\n");

    sb.append("-P = { ");
    for (int i = 0; i < hatSet.size(); i++) {
        sb.append((modulo - hatSet.get(i)) % modulo);
        if (i + 1 < hatSet.size()) {
            sb.append(", ");
        } // end of if (i + 1 == hatSet.getCount())

    } // end of for (int i = 0; i < hatSet.getCount(); i++)
    sb.append(" }");
```

```
    return sb.toString();
} // End setsToString()

/**
 * Computes the numbers {@literal n} and {@literal m} from the given
 * arguments if they are in the correct format.
 * <p>
 * The correct format of the arguments is the following:<br/>
 * n1 n2 ... ns - m1 m2 ... mr<br/>
 * The ni's and mi's are positive integers, the '-' is the separator
 * so that the program will know when the ni's sequence finish and
 * the mi's sequence starts.
 * </p>
 * <p>
 * The product of the ni's is the resulting number {@literal n}. The
 * product of the mi's is the resulting number {@literal m}
 * </p>
 * @param args The arguments containing the {@link String} representation
 *             of the numbers to compute {@literal n} and {@literal m}
 * @return An array {@code A} of {@code long} values of length 2, where
 *         {@code A[0] = n} and {@code A[1] = m}
 * @throws IllegalArgumentException if one of the following scenarios is
 *         found:
 *         <ol>
 *         <li> {@code args} contains symbols other than whole positive
 *              numbers and '-'</li>
 *         <li> {@code args} does not contain exactly one '-'</li>
 *         </ol>
```

```
 */
private static long[] getNumbers(String[] args) {
   long n = 1, m = 1, tmp = 0;
   int index = 0;
   try {
       for (; index < args.length; index++) {
           if ("-".equals(args[index])) {
               index++;
               break;
           }
           tmp = Long.parseLong(args[index]);
           if(tmp <= 0) {
               String msg = String.format(Locale.getDefault(),
                           "Only positive numbers are accepted. Got %d",
                           tmp);
               throw new IllegalArgumentException(msg);
           }
           n *= tmp;
       }
       if(index == args.length) { // No '-' was given
           throw new IllegalArgumentException("A '-' is required");
       }

       for (; index < args.length; index++) {
           tmp = Long.parseLong(args[index]);
           if(tmp <= 0) {
               String msg = String.format(Locale.getDefault(),
                           "Only positive numbers are accepted. Got %d",
```

```
                                tmp);
                    throw new IllegalArgumentException(msg);
                }
                m *= tmp;
            }
        } catch(NumberFormatException e) {
            String msg =
                    "Only whole positive numbers and one '-' are accepted";
            throw new IllegalArgumentException(msg, e);
        }
        return new long[]{n, m};
    } // End getNumbers(String[])

    /**
     * Creates a {@link String} that contains the usage of the program
     * @return The {@link String} describing the usage of the program
     */
    private static String getUsage() {
        StringBuilder sb = new StringBuilder("Usage: ");
        sb.append("java PseudoOrderRings n1 ... nk - m1 ... ms");
        sb.append("\n\twhere 'n1 ... nk' and 'm1 ... ms' are sequence");
        sb.append(" of positive integers");
        sb.append("\nThe product of the ni's will be the resulting ");
        sb.append("number n. The product of the mi's will be the ");
        sb.append("resulting number m\nn must be greater than m");
        return sb.toString();
    } // End getUsage()
```

```
/** ------------------------------------------------------
 *
 * Main Method
 *
 * ------------------------------------------------------*/

/**
 * Runs the application
 * @param args The arguments to run the application. The expected
 *             arguments are: n1 n2 .... nk - m1 m2 .... ms
 *             where the ni's and mi's are integers, the '....' means
 *             that an arbitrary number of integers are accepted, and
 *             the '-' is the separator. From these sequence of integers,
 *             the numbers n and m will be created, where n will be the
 *             product of the ni's and m will be the product of the mi's.
 *             All ni's and mi's are expected to be positive numbers
 */
public static void main(String[] args) {
    long[] input = null;
    try {
        input = getNumbers(args);
    } catch(IllegalArgumentException e) {
        System.out.println(getUsage());
        System.exit(0);
    }

    long n = input[0], m = input[1];
    System.out.println(String.format(Locale.getDefault(), "n: %d m: %d",
```

```
                                        n, m));

        if (n <= m) {
            System.err.println(String.format(Locale.getDefault(),
                               "n must be grater than m. Got: n: %d, m: %d",
                               n, m));
            System.exit(0);
        } // End if (n < m)

        PseudoOrderRings ps = new PseudoOrderRings();
        ps.computeSetHat(n, m);
        System.out.println(ps.setsToString());
        long[] inverses = ps.getInverseElementsInHatSet();
        boolean isPseudoOrdered = (inverses == null);
        System.out.println(String.format(Locale.getDefault(),
                                         "%d psuedo-ordered by %d? %s",
                                         n, m, isPseudoOrdered));
        if(inverses != null) {
            System.out.println(String.format(Locale.getDefault(),
                                             "n = %d = %d + %d",
                                             n, inverses[0], inverses[1]));
        } // End if (inverses != null)
    } // End main(String[])

} // End class PseudoOrderRings
```

Curriculum Vitae

Jorge Ivan Vargas was born on October 2, 1981. The second son of Miguel and Concepcion Vargas. He entered The University of Texas at El Paso in the fall 2000. While pursuing his bachelor's in Computer Science he worked as a Math Tutor at the Tutoring and Learning Center located at the University library and as a Teaching Assistant for undergraduate courses. He was a member of one the two UTEP teams that participated in a programming competition held at New Mexico State University on October 4, 2003. In April 3, 2004 he was inducted into the Upsilon Pi Epsilon Computer Science Honor Society UTEP chapter. He received his bachelor's degree in Computer Science in spring 2005.

In the fall 2005, he entered Graduate School at The University of Texas at El Paso to pursue a master's degree in Computer Science. Supported by the National Science Foundation *Bridge to the Doctorate* fellowship program, he received his master's degree in Computer Science in the summer 2007.

In the spring 2007, he was accepted in the master's program in the Mathematical Sciences department at The University of Texas at El Paso. While pursuing the master's degree in Mathematics he worked as a Software Engineer for Phillips and Computer Sciences Corporation.

Permanent address: 9951 Rosa M. Richardson
El Paso, Texas 79927