Rose-Hulman Undergraduate Mathematics Journal

Volume 21
Issue 1

Article 4

New Theorems for the Digraphs of Commutative Rings

Morgan Bounds
Indiana Wesleyan University, morgan.bounds@myemail.indwes.edu

New Theorems for the Digraphs of Commutative Rings

Cover Page Footnote

The author would like to thank Dr. Mel Royer and Dr. Bob Mallison for their guidance and Alyssa Tucker for her unwavering support. The author would also like to thank his parents, Chris and Tamara Bounds, for instilling within him the virtue of education.

ℝose-Hulman Undergraduate Mathematics Journal

Volume 21, Issue 1, 2020

New Theorems for the Digraphs of Commutative Rings

By *Morgan Bounds*

Abstract. The digraphs of commutative rings under modular arithmetic reveal intriguing cycle patterns, many of which have yet to be explained. To help illuminate these patterns, we establish a set of new theorems. Rings with relatively prime moduli a and b are used to predict cycles in the digraph of the ring with modulus ab. Rings that use Pythagorean primes as their modulus are shown to always have a cycle in common. Rings with perfect square moduli have cycles that relate to their square root.

1 Introduction

The directed graphs, or **digraphs**, of commutative rings under modular arithmetic create intriguing patterns. Most contain cycles of varying lengths, while a select few contain none at all. Can the cycles of composite moduli be predicted based on the digraphs of their factors? Are cycle lengths determined by special properties of their modulus? Do all Pythagorean primes have cycles in common? This paper presents an array of new theorems that addresses these questions, proves past conjectures, and offers fresh insight into digraph behavior.

The digraphs of commutative rings formed through modular arithmetic were first examined by Hausken and Skinner [5], and Ang and Schulte [1]. They constructed digraphs using the operation $(x, y) \to (x + y, xy) \pmod n$, where x and y are elements from the the ring of all integers (mod n). Haffner and Newnum investigated these cycles [4] and made several compelling conjectures. This research has been heavily influenced by Haffner and Newnum, and this paper offers a proof for two of their major conjectures. Additionally, this paper establishes two theorems that are a continuation of the research conducted by Bounds [2].

This paper will begin by providing background information in Section 2 on the underlying theory of rings, focusing in particular on how to construct the digraphs of commutative rings under modular arithmetic. Later in Section 2, two of Haffner and Newnum's conjectures will be presented with examples. In Section 3, new theorems will

Mathematics Subject Classification. 05C25

Keywords. rings, digraphs, Pythagorean primes, modular arithmetic

be established that prove Haffner and Newnum's conjectures, and other new theorems will be proven as well. Finally, in Section 4, future research directions will be suggested.

2 Background

2.1 Definitions

In this paper a **ring**, denoted by $\mathbb{Z}_\mathbf{n}$, refers to the set of all integers modulo n. Because modular arithmetic is commutative under addition and multiplication, $\mathbb{Z}_\mathbf{n}$ is said to be a **commutative** ring. Now create a **vertex**, denoted $(\mathbf{x}, \mathbf{y})$, where x and y are elements of $\mathbb{Z}_n$. The **mapping** of a vertex (x_1, y_1) onto a new vertex (x_2, y_2), denoted by $(x_1, y_1) \rightarrow (x_2, y_2)$, is an operation which transforms (x_1, y_1) into a new vertex where $x_2 \equiv x_1 + y_1 (\text{mod } n)$ and $y_2 \equiv x_1 y_1 (\text{mod } n)$. The **digraph** of $\mathbb{Z}_\mathbf{n}$, denoted by $\Psi(\mathbb{Z}_\mathbf{n})$, is a graph that shows all the mappings of all the vertices of $\mathbb{Z}_n$. Figure 1 displays the completed digraph of $\mathbb{Z}_5$. A **cycle** occurs when the operation indefinitely loops through a set of two or more vertices.

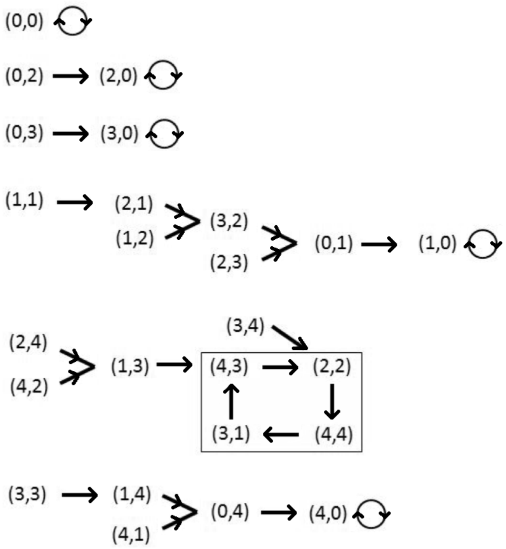

Figure 1: $\Psi(\mathbb{Z}_5)$ [4]

Observe that Figure 1 contains one cycle, enclosed in the box. This cycle can be expressed using the notation: $(4,3) \rightarrow (2,2) \rightarrow (4,4) \rightarrow (3,1) \rightarrow (4,3)$. Note that this mapping of (4,3) in $\Psi(\mathbb{Z}_5)$ leads to a cycle of length 4. In general, a cycle of length c is always of the form $(x_1, y_1) \rightarrow (x_2, y_2) \rightarrow \ldots \rightarrow (x_c, y_c) \rightarrow (x_1, y_1)$. Not every digraph, however, contains cycles. Note that in Figure 2 all the vertices of $\Psi(\mathbb{Z}_3)$ eventually lead to a terminating vertex.

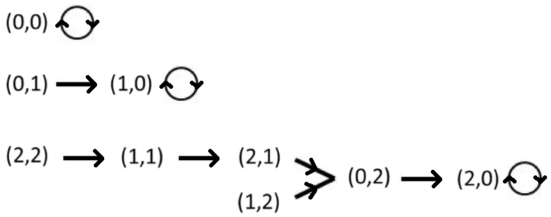

Figure 2: $\Psi(\mathbb{Z}_3)$ [4]

2.2 Past Conjectures

Recall that $\Psi(\mathbb{Z}_5)$ has one cycle of length 4 and that $\Psi(\mathbb{Z}_3)$ contains zero cycles. Observe in Figure 3 what happens when we construct the digraph of $\Psi(\mathbb{Z}_{15})$. We get precisely 3 cycles, all of which are of length 4. It appears that the cycles of $\Psi(\mathbb{Z}_5)$ are triplicated when we multiply the modulus by three. But what if $\Psi(\mathbb{Z}_3)$ had also contained a cycle?

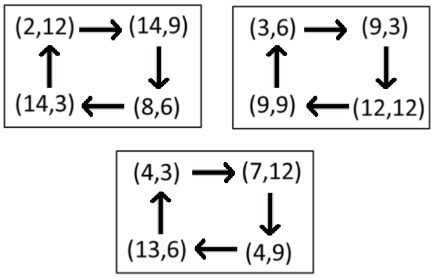

Figure 3: Cycles in $\Psi(\mathbb{Z}_{15})$ [4]

Note that $\Psi(\mathbb{Z}_4)$, displayed in Figure 4, contains one cycle of length 2. Now observe in Figure 5 the cycles found in $\Psi(\mathbb{Z}_{20})$. There are precisely five cycles of length 2 and at least four cycles of length 4. Based on these observations, Haffner and Newnum identified a pattern. They articulated this pattern in their “Relatively Prime with Zero Cycles Conjecture" and “Least Common Multiple Conjecture" [4]. These conjectures are cases of the following assertion, which will later be proven.

Theorem 2. Let a and b be relatively prime positive integers. Suppose for a given cycle length c, $\Psi(\mathbb{Z}_a)$ has N_c cycles of length c and $\Psi(\mathbb{Z}_b)$ has M_c cycles of length c. Then $\Psi(\mathbb{Z}_{ab})$ has at least $b\mathrm{N}_c + a\mathrm{M}_c$ cycles of length c.

3 New Theorems

3.1 Cycles from Coprime Factors of the Modulus

We begin with a simpler case of the main theorem.

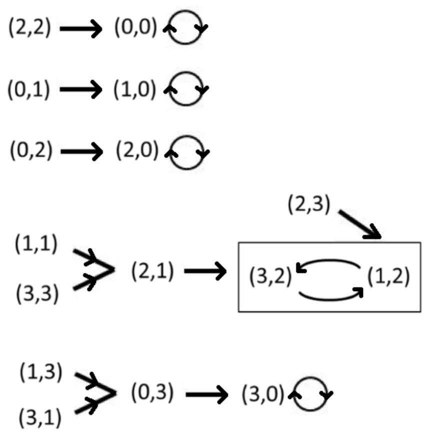

Figure 4: $\Psi(\mathbb{Z}_4)$ [4]

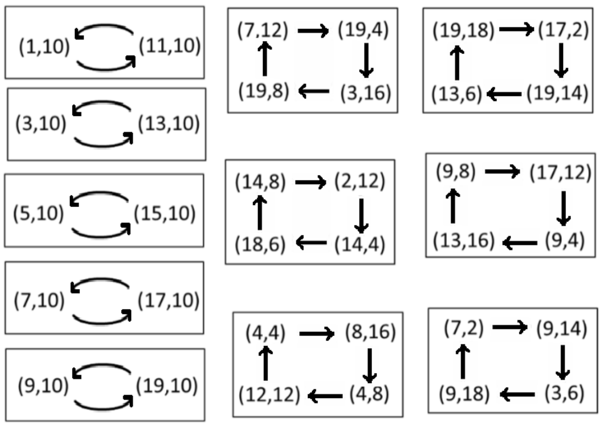

Figure 5: Cycles in $\Psi(\mathbb{Z}_{20})$ [4]

Theorem 1. Let a and b be relatively prime positive integers and suppose $\Psi(\mathbb{Z}_a)$ has N_c cycles of a given length c. Then $\Psi(\mathbb{Z}_{ab})$ will have at least $b\mathrm{N}_c$ cycles of length c.

We begin by establishing some useful identities and a lemma, which we then use to prove the theorem. Each cycle in $\Psi(\mathbb{Z}_a)$ of length c is of the form $(x_1, y_1) \to (x_2, y_2) \to \ldots \to (x_c, y_c) \to (x_{c+1}, y_{c+1})$, where

$$x_{c+1} \equiv x_1 (\text{mod } a) \tag{1}$$

$$y_{c+1} \equiv y_1 (\text{mod } a) \tag{2}$$

Furthermore, the x and y components of an arbitrary vertex in the cycle are defined recursively as follows:

$$x_n = x_{n-1} + y_{n-1} \tag{3}$$

$$y_n = x_{n-1} \cdot y_{n-1} \tag{4}$$

Now, consider the mapping of the vertex $(ka + x_1, b^{\phi(a)} y_1)$ in $\Psi(\mathbb{Z}_{ab})$, where x_1 and y_1 can be selected from any vertex in any cycle of $\Psi(\mathbb{Z}_a)$, ϕ is Euler's totient function, and k is an integer such that $0 \le k \le b-1$. Let $\chi_1 = ka + x_1$ and $\gamma_1 = b^{\phi(a)} y_1$. If we can show that (χ_1, γ_1) leads to a cycle of length c, then we can guarantee at least b cycles of length c in $\Psi(\mathbb{Z}_{ab})$ for every cycle in $\Psi(\mathbb{Z}_a)$ of length c by varying k from 0 to $b-1$. This would prove Theorem 1. Before demonstrating such a mapping of (χ_1, γ_1), we must first establish three helpful identities. First, $b^{\phi(a)} \equiv 1 (\text{mod } a)$ by Euler's Theorem. Then, multiplying both sides and the modulus by b, we get $b^{\phi(a)+1} \equiv b (\text{mod } ab)$. Finally, let us multiply both sides by $b^{\phi(a)-1}$ to obtain

$$b^{2\phi(a)} \equiv b^{\phi(a)} (\text{mod } ab) \tag{5}$$

This result will prove useful later. Now, let us examine Equation (1) more closely. Through subtraction, we easily obtain $x_{c+1} - x_1 \equiv 0(\text{mod } a)$. Next, we multiply both sides and the modulus by b to yield $b(x_{c+1} - x_1) \equiv 0(\text{mod } ab)$. Finally, multiply both sides by $b^{\phi(a)-1}$ to get

$$b^{\phi(a)}(x_{c+1} - x_1) \equiv 0(\text{mod } ab) \tag{6}$$

This result will also prove useful. Now we must consider Equation (2). Multiplying both sides and the modulus by b gives us $by_1 \equiv by_{c+1}(\text{mod } ab)$. From here, we simply multiply both sides by $b^{\phi(a)-1}$ to obtain

$$b^{\phi(a)}y_1 \equiv b^{\phi(a)}y_{c+1}(\text{mod } ab) \tag{7}$$

Now that we have established (5), (6), and (7), we need to establish a lemma that will iterate (χ_1, γ_1) as far as we wish.

Lemma 1. With $(\chi_1, \gamma_1) = (ka + x_1, b^{\phi(a)}y_1)$, we have
$(\chi_j, \gamma_j) = (ka + x_1 + b^{\phi(a)}(x_j - x_1), b^{\phi(a)}y_j))$, for every $j \geq 1$

Proof. Using mathematical induction, note that the conclusion holds for
$j = 1$. Now, assume $(\chi_j, \gamma_j) = (ka + x_1 + b^{\phi(a)}(x_j - x_1), b^{\phi(a)}y_j))$.Then by (3),

$$\chi_{j+1} \equiv \chi_j + \gamma_j \equiv ka + x_1 + b^{\phi(a)}(x_j - x_1) + b^{\phi(a)}y_j \equiv ka + x_1 + b^{\phi(a)}(x_{j+1} - x_1)$$

and by (4) and (5),

$$\gamma_{j+1} \equiv \chi_j\gamma_j \equiv (ka + x_1 + b^{\phi(a)}(x_j - x_1))(b^{\phi(a)}y_j) \equiv b^{\phi(a)}y_{j+1}(\text{mod } ab)$$

□

Now a proof of Theorem 1 will be given.

Proof. In $\Psi(\mathbb{Z}_{ab})$, the vertex $(\chi_1, \gamma_1) = (ka + x_1, b^{\phi(a)}y_1)$ will eventually map onto $(\chi_{c+1}, \gamma_{c+1})$. From Lemma 1,

$$(\chi_{c+1}, \gamma_{c+1}) = (ka + x_1 + b^{\phi(a)}(x_{c+1} - x_1), b^{\phi(a)}y_{c+1})$$

$$\equiv (ka + x_1, b^{\phi(a)}y_1)(\text{mod } ab)$$

by (6) and (7).

This proves that (χ_1, γ_1) leads to a cycle of at most length c in $\Psi(\mathbb{Z}_{ab})$. Now, by contradiction we will show that no vertex in the cycle before $(\chi_{c+1}, \gamma_{c+1})$ is equivalent to the starting vertex. Assume that in the mapping of (χ_1, γ_1), there exists a vertex (χ_d, γ_d), where $1 < d < c + 1$ and
$(\chi_d, \gamma_d) \equiv (\chi_1, \gamma_1)(\text{mod } ab)$. By Lemma 1 and substitution,

$$(\chi_d, \gamma_d) = (ka + x_1 + b^{\phi(a)}(x_d - x_1), b^{\phi(a)}y_d) \equiv (ka + x_1, b^{\phi(a)}y_1)(\text{mod } ab)$$

This implies the following congruence relations:

$$ka + x_1 + b^{\phi(a)}(x_d - x_1) \equiv ka + x_1 (\text{mod } ab) \tag{8}$$

$$b^{\phi(a)} y_d \equiv b^{\phi(a)} y_1 (\text{mod } ab) \tag{9}$$

Subtracting $ka + x_1$ from both sides of (8) yields $b^{\phi(a)}(x_d - x_1) \equiv 0(\text{mod } ab)$. Dividing both sides by $b^{\phi(a)}$ implies $x_d \equiv x_1(\text{mod } a)$. And in (9) dividing both sides by $b^{\phi(a)}$ yields $y_d \equiv y_1(\text{mod } a)$. Now, examining (1) and (2), it becomes clear $d = c + 1$. But this contradicts the definition of d.

Therefore, (χ_1, γ_1) cannot cycle back before producing a full cycle of length c. Now, as k takes on b distinct values, each produces a unique (χ_1, γ_1) (an argument similar to the one used in (8) and (9) confirms their uniqueness). This guarantees at least b cycles of length c in $\Psi(\mathbb{Z}_{ab})$ for each cycle of length c that was in $\Psi(\mathbb{Z}_a)$. □

Theorem 1 will now be demonstrated in the case that $a = 4$, $b = 5$, and $c = 2$. Based on $\Psi(\mathbb{Z}_4)$, which can be observed in Figure 4, we expect $\Psi(\mathbb{Z}_{20})$ to have at least 5 cycles of length 2. From the proof of Theorem 1, we know that we can begin a cycle in $\Psi(\mathbb{Z}_{20})$ by identifying a vertex of the form $(ka + x_1, b^{\phi(a)} y_1)$, where $0 \le k \le 4$, and (x_1, y_1) is an arbitrary vertex from an arbitrary cycle of $\Psi(\mathbb{Z}_4)$. In Figure 4, we see that we can choose $(x_1, y_1) = (3,2)$. Now, using $\phi(4) = 2$, $(ka + x_1, b^{\phi(a)} y_1) \equiv (4k + 3, 10)(\text{mod } 20)$. By substituting in each possible value of k, we can generate the 5 vertices $(3,10), (7,10), (11,10), (15,10)$, and $(19,10)$. And, by referring to Figure 5, we see that each of these vertices leads to a unique cycle of length 2 in $\Psi(\mathbb{Z}_{20})$.

Thus, Theorem 1 is not only capable of predicting a minimum number of cycles and their lengths, but also the vertices of which those cycles are comprised. We have proven that $\Psi(\mathbb{Z}_{ab})$ has at least b cycles of length c for each cycle of length c in $\Psi(\mathbb{Z}_a)$. However, we have yet to show that $\Psi(\mathbb{Z}_{ab})$ will have a unique cycles of length c for each cycle of length c in $\Psi(\mathbb{Z}_b)$. This will now be shown in Theorem 2.

3.2 Both Factors Contribute to Cycle Behavior

Theorem 2. Let a and b be relatively prime positive integers. Suppose for a given cycle length c, $\Psi(\mathbb{Z}_a)$ has N_c cycles of length c and $\Psi(\mathbb{Z}_b)$ has M_c cycles of length c. Then $\Psi(\mathbb{Z}_{ab})$ has at least $b\mathrm{N}_c + a\mathrm{M}_c$ cycles of length c.

Proof. From each cycle of length c in $\Psi(\mathbb{Z}_a)$, we know that we can identify and use a vertex (χ_1, γ_1) to create a cycle in $\Psi(\mathbb{Z}_{ab})$. And, from Lemma 1, we know that each of the vertices of that cycle will be of the form $(\chi_{u_a}, \gamma_{u_a}) = (ka + x_{1_a} + b^{\phi(a)}(x_{u_a} - x_{1_a}), b^{\phi(a)} y_{u_a})$, where x_{1_a}, x_{u_a}, and y_{u_a} were adopted from vertices of a cycle of length c in $\Psi(\mathbb{Z}_a)$ and $1 \le u \le c$. Similarly, using a cycle in $\Psi(\mathbb{Z}_b)$ as our starting point, the vertex (χ_1, γ_1) will create a cycle in $\Psi(\mathbb{Z}_{ab})$ whose vertices are of the form $(\chi_{v_b}, \gamma_{v_b}) = (kb + x_{1_b} + a^{\phi(b)}(x_{v_b} - x_{1_b}), a^{\phi(b)} y_{v_b})$, where x_{1_b}, x_{v_b}, and y_{v_b} were adopted from vertices of a cycle of length c in $\Psi(\mathbb{Z}_b)$ and $1 \leq v \leq c$.

To prove Theorem 2, we must show that $(\chi_{u_a}, \gamma_{u_a})$ will never be equivalent to $(\chi_{v_b}, \gamma_{v_b})$, no matter what values of u, v, x, and y are selected. By contradiction, assume that for some u and v, $(\chi_{u_a}, \gamma_{u_a}) \equiv (\chi_{v_b}, \gamma_{v_b}) (\text{mod } ab)$. Congruence of their γ-components shows that $b^{\phi(a)} y_{u_a} \equiv a^{\phi(b)} y_{v_b} (\text{mod } ab)$, and therefore $b^{\phi(a)} y_{u_a} \equiv 0 (\text{mod } a)$. But since $(x, 0)$ is always a terminal vertex and therefore does not create a cycle, we know that $y_{u_a} \not\equiv 0 (\text{mod } a)$. Since a and b are relatively prime, $b^{\phi(a)} y_{u_a} \not\equiv 0 (\text{mod } a)$, which is a contradiction. □

3.3 Moduli with a Guaranteed Cycle of Length 4

The first two theorems predict the minimum number of cycles of a given length in $\Psi(\mathbb{Z}_{ab})$ based on $\Psi(\mathbb{Z}_a)$ and $\Psi(\mathbb{Z}_b)$. But what if $\Psi(\mathbb{Z}_a)$ and $\Psi(\mathbb{Z}_b)$ are not given? The following theorems help predict a digraph's cycle behavior given only the modulus.

Theorem 3. $\Psi(\mathbb{Z}_n)$ has at least one cycle of length 4 if there exists an integer x such that $x^2 \equiv -1 (\text{mod } n)$.

Proof. In $\Psi(\mathbb{Z}_n)$, map the vertex $(-1, x+1)$ as follows:

$$(-1, x+1) \to (x, -x-1) \to (-1, 1-x) \to (-x, x-1) \to (-1, x+1)$$

Thus, $(-1, x+1)$ leads to a cycle of length 4. □

Note that Theorem 3 applies to all Pythagorean primes, which are primes of the form $4k+1$, where k is an integer. This becomes evident when we examine Wilson's Theorem, which states that $(p-1)! \equiv -1 (\text{mod } p)$ for any prime number p. By expanding and refactoring the factorial on the left, we obtain $((\frac{p-1}{2})!)^2 (-1)^{\frac{p-1}{2}} \equiv -1 (\text{mod } p)$ [3]. Because p is of the form $4k+1$, $\frac{p-1}{2}$ is even and $(-1)^{\frac{p-1}{2}}$ is 1. Now we have $((\frac{p-1}{2})!)^2 \equiv -1 (\text{mod } p)$. Thus, for the digraphs of Pythagorean primes, Theorem 3 will always hold because $((\frac{p-1}{2})!)$ will always satisfy x.

For example, $k = 1$ yields 5, which is the first Pythagorean prime. Furthermore, solving for x yields 2, which anticipates the cycle $(4,3) \to (2,2) \to (4,4) \to (3,1) \to (4,3)$, which can be observed in Figure 1.

3.4 Cycles in Perfect Square Moduli

Theorem 4. $\Psi(\mathbb{Z}_{p^2})$, where p is a prime number, has at least $p-1$ cycles of length p.

Proof. In $\Psi(\mathbb{Z}_{p^2})$, map the vertex $(1,kp)$, where $1 \le k \le p-1$:

$$(1,kp) \to (1+kp,kp) \to (1+2kp,kp) \to (1+3kp,kp) \to \ldots \to (1+(p-1)kp,kp)$$

$$\to (1,kp)$$

Since p is prime, $(1,kp)$ leads to a cycle of length p. And because k can take on $p-1$ distinct values, each producing a different $(1,kp)$, we can guarantee at least $p-1$ cycles of length p in $\Psi(\mathbb{Z}_{p^2})$. □

Digraph	Cycle Length	Cycles of Given length
$\Psi(\mathbf{Z}_4)$	2	1
$\Psi(\mathbf{Z}_9)$	3	2
$\Psi(\mathbf{Z}_{25})$	5	4
$\Psi(\mathbf{Z}_{49})$	7	6
$\vdots$	$\vdots$	$\vdots$

Figure 6: Cycles of length $p-1$ in $\Psi(\mathbf{Z}_{p^2})$

Take, for example, $\Psi(\mathbb{Z}_4)$. Based on Theorem 4, we can predict that $\Psi(\mathbb{Z}_4)$ will have at least one cycle of length 2 of the form $(1,2) \to (3,2) \to (1,2)$. Observing Figure 4, this prediction is verified. Figure 6 further demonstrates the pattern identified in Theorem 4.

4 Future Directions

When presented with $\Psi(\mathbb{Z}_4)$ and $\Psi(\mathbb{Z}_5)$, one can use Theorem 2 to predict that $\Psi(\mathbb{Z}_{20})$ will have at least five cycles of length 2 and at least four cycles of length 4. While $\Psi(\mathbb{Z}_{20})$ has precisely five cycles of length 2, it has more than just the four cycles of length 4 that were predicted. $\Psi(\mathbb{Z}_{20})$ contains six cycles of length 4, to be exact. Where are the two additional cycles coming from? Can a theorem be constructed that predicts such cycles? Under what conditions does Theorem 2 predict a precise number of cycles?

Theorem 2 examines $\Psi(\mathbb{Z}_{ab})$ where a and b are relatively prime. Could a result similar to Theorem 2 be demonstrated in $\Psi(\mathbb{Z}_{abc})$ for relatively prime $a, b,$ and c? Could this be further generalized to predict the cycles of $\Psi(\mathbb{Z}_n)$ given the digraphs of the prime factors of n?

Theorems 3 and 4 predict cycles in the digraphs of moduli that meet special requirements. What other methods exist for predicting how many cycles and what cycle lengths a digraph will have given only the modulus?

All of the theorems in this paper have included the caveat “at least". To prove that a digraph will have at least a certain number of cycles is relatively easy. Relative, that is, to proving that a digraph will have at most a certain number of cycles. Can a theorem be established that predicts at most how many cycles the digraph of an arbitrary modulus will have? Given an arbitrary modulus, can one calculate the upper bound on how long its cycles can get? This direction is explored in part by Lipkovski [6].

References

[1] Christopher Ang and Alex Schulte. Directed graphs of commutative rings with identity. *Rose-Hulman Undergraduate Mathematics Journal*, Vol.14.1, 2013.

[2] Morgan T. Bounds. Predicting cycles in the digraphs of commutative rings. *Unpublished Manuscript. Indiana Wesleyan University*, 2017.

[3] David Burton. Elementary number theory. *McGraw-Hill*, page 95, 1998.

[4] Lauren Haffner and Chelsea Newnum. Directed graphs of commutative rings. *Unpublished Manuscript. Indiana Wesleyan University*, 2015.

[5] Seth Hausken and Jared Skinner. Directed graphs of commutative rings. *Rose-Hulman Undergraduate Mathematics Journal*, Vol.14.1, 2013.

[6] Aleksandar Lipkovski. Structure graphs of rings: Definitions and first results. *Journal of Mathematical Sciences*, Vol.225.4, 2017.

Morgan Bounds
Indiana Wesleyan University
morgan.bounds@myemail.indwes.edu