Classification of Cycles in Digraphs Associated to Quadratic Polynomials with Coefficients Modulo p^2

Dr. Hamza Daoub[1] Dr. Fathi A. M. Bribesh[1], Dr. Osama Shafah[2]
1, Dept. of Mathematics, Faculty of Science, Zawia University
2, Dept. of Mathematics, Faculty of Science, Sabratha University

Abstract:

The directed graph of the ring $\mathbb{Z}_{p^2}$ is a graphical representation of its additive and multiplicative structure. The digraph for this ring is created by applying the relationship $(a, b) \to (a + b, ab)$. We present the association between finite diagraphs $G(\mathbb{Z}_{p^2})$ and finite commutative rings with unity, $(A = \mathbb{Z}_{p^2})$. The study is concentrated on categorizing the length of cycles explained in the corresponding digraphs form. Some basic number-theoretic notations are involved in the classification of the cycles.

1. Introduction:

It is desired to create a visual illustration of finite rings that preserves ring structure and shows its properties graphically. Besides the Cayley tables, the digraph visualization of a ring may give the ability to look at it from another side. Infact, the association between finite rings and graphs is extensively studied in the last two decades. Some authors investigated the relationship between commutative rings with unity and their divisor graphs. Determining when $G(A)$ have is a complete graph or a star graph [1]. The interplay between ring-theoretic properties of a finite ring and the theoretic properties of its digraph $G(A)$ also been considerably interesting area. Since the most readily distinguishable in digraphs are vertices, some studies place special emphasis on sources and looped vertices [3]. Others interested in using digraph of a ring in showing whether the underlying ring is reduced or not and how many fields the ring is made of [3]. In their paper [6] they introduce another way to deduce ring properties of A from graph properties of G, by determining the number of loops, the number of components, the length of the longest path and longest loop. In our paper we use the same conventions and notations in [6] to describe finite commutative rings, using directed graph representation of rings under the mapping $\psi: (a, b) \to (a + b, a.b)$. We explain classifications of the cycles of $G(\mathbb{Z}_{p^2})$ for a prime p.

Since the properties of primes in number theory play the key role in our study, in the second section we introduce a background which represents some theorems in number theory. The third section will be the

main result where we study the length of all cycles in $G(\mathbb{Z}_{p^2})$. This section is divided into four cases regarding the forms of its vertices in terms of prime numbers.

2. Background:

It is well known in number theory that, for any a, b in $\mathbb{Z}$, with $b > 0$, there exist q, r in $\mathbb{Z}$ such that $a = bq + r$ and $0 < r < b$. Indeed, if bq is the largest multiple of b that does not exceed a then the integer $r = a - bq$ is certainly non-negative and, since $b(q + 1) > a$, we have $r < b$, see reference [2].

Definition 1 *Let $m > 0$ be a positive integer. We say that two integers a and b are congruent modulo m if $b - a$ is divisible by m.*

This definition is an equivalent expression of the following proposition.

Proposition 1 *$a \equiv b \ (mod\ m)$ if and only if $a = b + km$ for some integer k.*

Proof: By definition 1, $a \equiv b \ (mod\ m)$ if and only if $a - b$ is a multiple of m. This means that $a - b = km$ for some integer k, or equivalently $a = b + km$.

Definition 2 *Let n be a positive integer. The Euler $\varphi(n)$ is the number of all non-negative integers b less than n which are prime to n.*

It is clearly seen that $\varphi(1) = 1$ and $\varphi(p) = p - 1$, for any prime p. One can also achieve the following consequence for squired primes by writing $\varphi(p^2) = p^2 - p = p(p - 1)$.

Now, it is important to introduce the following propositions.

Proposition 2 *If a is an integer and m is a positive integer, then there is a unique integer r with $0 \leq r \leq m-1$ so that $a \equiv r(mod\ m)$. This integer r is called the least positive residue of a mod m.*

Proof: See [5].

If p is a prime number, then any $a \in \mathbb{Z}_{p^2}$ can be written in the form

$a = s + n.p$, for some integer $0 \leq n \leq p-1$,

where $s \in \mathbb{Z}p$.

Note that, if $g.c.d(a, p^2) = 1$ then $s \in \varphi(p)$.

Proposition 3 (Fermat's Little Theorem). *Let p be a prime. Any integer a satisfies $a^p \equiv a\ mod\ p$, and any integer a not divisible by p satisfies $a^{p-1} \equiv 1\ mod\ p$.*

Proof: See [4].

Proposition 4 *If $g.c.d(a, m) = 1$, then $a^{\phi(m)} = 1\ \ mod\ m$.*

Proof: See [4].

Proposition 5 *For any integer b and any positive integer $n, bn-1$ is divisible by $b-1$ with quotient $b^{n-1} + b^{n-1} + \cdots + b^2 + b + 1$.*

Proof: See [4].

Theorem 1 (Chinese Remainder Theorem) *Assume that $m_1, m_2, \ldots, m_r$ are positive integers that are pairwise relatively prime (that is, $g.c.d(m_i, m_j) = 1$ if $i \neq j$). Then the system of congruences*

$$x \equiv a_1(mod\ m_1)$$
$$x \equiv a_2(mod\ m_2)$$
$$\ldots$$
$$x \equiv a_r(mod\ m_r)$$

has a unique solution mod $m_1 m_2 \ldots m_r$.

Proof: See [5].

Corollary 1 *Let p be a prime. The congruence $x^2 \equiv 1\ (mod\ p)$ has only the solutions $x = \pm 1\ (mod\ p)$.*

Proof: See [5].

Cycle in graph theory is defined as a closed path. That is, we start and end at the same vertex. In the middle, we do not travel to any vertex twice. In some references a circuit is a path which begins and ends at same vertex, i.e., circuit and cycle are the same. However, we follow their definition of cycles that is mentioned in reference[6], as follows:

Definition 3 *The sequence*

$(a_1, b_1) \rightarrow (a_2, b_2) \rightarrow \ldots (a_k, b_k)$ (1)

of arrows in G defines a cycle of length k (or a k-cycle) if $(a_k + b_k, a_k b_k) = (a_1, b_1)$ and $(a_i + b_i, a_i b_i) \neq (a_j, b_j)$ for all $j \leq i < k$.

The following proposition states that cycles of length one are essential in $G(\mathbb{Z}_p^2)$.

Proposition 6 *i) There are exactly $n = \#\{cycles\ of\ length 1 in\ G\}$, and they correspond to the vertices $(a, 0)$.*

ii) Each connected component of G contains exactly one loop, and the number of connected components is $n + \#\{cycles\ of\ length > 1\}$.

Proof: See [6].

Remark 1 *It is easy to see that there exists a 2-cycle if and only if the ring$A$ has non-trivial nilpotent elements. For, since $(a_2, b_2) \neq (a_1, b_1)$, we have $b_1 \neq 0$, $b_1^2 = 0$ and this is nilpotent in A. Conversely, if c is a nilpotent $c^{k-1} \neq 0$, $c^k = 0$ for $k > 1$, take $b = c^{k-1}$, then $b^2 = 0$ and there is a 2-cycle given by*

$(-1, b) \to (b-1, -b) \to (-1, b)$ [6].

3. Main Results:

The main result of this work is to look at the cycles length in $G(\mathbb{Z}_{p^2})$ using the mapping ψ. The ring $\mathbb{Z}_p$ also plays an important role in this study as there are cycles in $G(\mathbb{Z}_{p^2})$ that are well connected with cycles of $G(\mathbb{Z}_p)$ in addition to primes properties.

Let $\overrightarrow{C_\alpha}$ be any directed cycle in $G(\mathbb{Z}_p)$ of length $\alpha > 1$ and suppose that $\overrightarrow{C_\beta}$ be any directed cycle in $G(\mathbb{Z}_{p^2})$. Since every cycle is a set of vertices direct-connected by the mapping ψ. We will investigate all ordered pairs that existed in $\mathbb{Z}_{p^2}$. The coordinates of any vertex (q, k) in $\mathbb{Z}_{p^2}$ must take one of the following forms.

Case 1 If $g.c.d(q, p^2) \neq 1$ and $g.c.d(k, p^2) \neq 1$. Then, q and k can be written in terms of p as $q = n.p$, $k = m.p$ for some integers $0 \leq n, m \leq p-1$. Thus, $(n.p, m.p) \longrightarrow ((n+m)p, 0)$, which corresponds to cycles of length one as it is proposed in Proposition 6.

Case 2. If $g.c.d(q, p^2) = 1$ and $g.c.d(k, p^2) \neq 1$. Then, $q = s + n.p, k = m.p$ for some integers $0 \leq n, m \leq p-1$ where $s \in \varphi(p)$. Thus,

$$(s + n.p, m.p) \to (s + n.p + m.p, s.m.p) \to (s + n.p + (1+s)m.p, s^2.m.p) \to (s + n.p + (1 + s + s^2)m.p, s^3.m.p) \to \cdots \to (s + n.p + (1 + s + s^2 + \cdots + s^{p-2})m.p, s^{p-1}.m.p) \quad (2)$$

The element s satisfies that $s^2 = 1$,if $s = \pm 1$, Thus, $(-1 + n.p, m.p) \to (-1 + n.p + m.p, -m.p)$. Therefore, we have a cycle of

length 2 ,that corresponds to nilpotent element case as it is mentioned in Remark 1.

According to Fermat's Little Theorem and Proposition 5, we note that sequence (2) is a cycle of length $p-1$. However, such cycle could have length l where $2 < l < p$, that depends on s. Whenever, $s^l = 1$, Proposition 5, is used to obtain $1 + s + \cdots + s^{l-1} = 0$. Therefore, the path gets closed at $(s + n.p, m.p)$, which represent a cycle of length l.

When s satisfies that $s^p = 1$, then Fermat's Little Theorem leads to $s = 1$. Therefore, the sequence $(1 + n.p, m.p) \to \cdots \to (1 + n.p + (p-1)\, m.p, m.p)$ is a cycle of length p.

Case 3 If $g.c.d(q, p^2) \neq 1$ and $g.c.d(k, p^2) = 1$. Then, $q = n.p$, $k = r + m.p$ for some integers $0 \leq n, m \leq p - 1$ where $r \in \varphi(p)$. Thus,

$$(n.p, r + m.p) \to (r + n.p + m.p, r.n.p) \to (r + m.p + (1 + r)n.p, r^2.n.p) \to (r + m.p + (1 + r + r^2)n.p, r^3.n.p) \to \cdots \to (r + m.p + (1 + r + r^2 + \cdots + r^{p-2})n.p, r^{p-1}.n.p) \quad (3)$$

According to Fermat's Little Theorem and Proposition 5, we conclude that sequence (3) gets closed at the vertex $(r + m.p, n.p)$. Note that, both vertices $(r + m.p, n.p)$ and $(n.p, r + m.p)$ are adjacent to the vertex $(r + n.p + m.p, r.n.p)$. Therefore, the length of this cycle is determined by the element r similar to case two.

Case 4 If $g.c.d(q, p^2) = 1$ and $g.c.d(k, p^2) = 1$. Then, $q = s + n.p$, $k = r + m.p$ for some integers $0 \leq n, m \leq p - 1$ where s and $r \in \varphi(p)$. Thus,

$$(s + n.p, r + m.p) \to (s + r + (n+m).p, s.r + (r.n +$$

$s.m)p) \rightarrow \ ... \rightarrow \ (c + n'.p, d + m'.p)$ 4)

where n', m' are integers. If $(s,r) \in \overrightarrow{C_\alpha}$ then the sequence (4) is a cycle of length $\gamma.\alpha$ for some positive integer γ. (To prove this fact one can refer to Chinese Reminder Theorem with the map $h: \mathbb{Z}_{p^2} \rightarrow \mathbb{Z}_p$ defined by $h(a) = [a]_p$).

If $(s,r) \notin \overrightarrow{C_\alpha}$, then the sequence (4) is a path. When sequence (4) represents a cycle then its length is effected by the choice of n and m, therefore the value of the integer γ is affected. The following example illustrates how n and m, and also their order control the value of the integer number γ.

Example 1. *According to* $G(\mathbb{Z}_{13})$ *there is a unique cycle of length greater than* 1, *which is represented by* $\overrightarrow{C_4}$. *In* $G(\mathbb{Z}_{13^2})$, *The choice* $n + m = 12$ *makes sequence (4) a cycle of length* 16. *Note that, the choice* $n = 5$ *and* $m = 7$ *gives a cycle of length* 4, *as a single case. Simultaneously,* $n = 7$ *and* $m = 5$ *give us a cycle of length* 16. *However, the choice* $n + m \neq 12$ *gives cycles of length* 208.

Note that, all cycles in case 4 are cycles of length $j.\alpha$, *where* j *is a positive integer.*

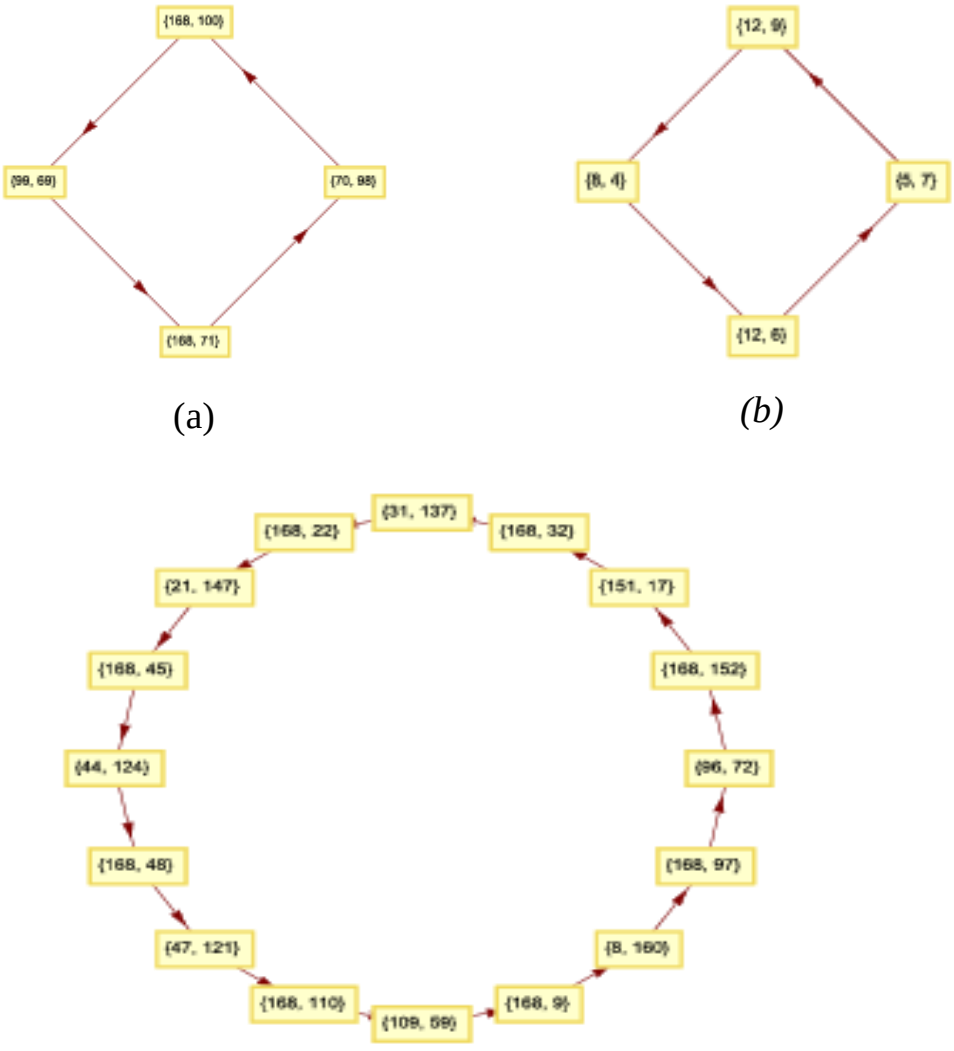

Figure1: shown are, panel (a) is a cycle in $G(\mathbb{Z}_{169})$ with $n = 5$ and $m = 7$, panel (b) is the unique cycle in $G(\mathbb{Z}_{13})$, panel (c) is a cycle in $G(\mathbb{Z}_{169})$ with $n = 7$ and $m = 5$.

References:

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

[2] A. Baker. A concise introduction to the theory of numbers. Cambridge University Press, 1984.

[3] S. Hausken and J. Skinnerb. Directed graphs of commutative rings. Rose-Hulman Undergraduate Mathematics Journal, 14(2), 2013.

[4] N. Koblitz. A course in number theory and cryptography, volume 114. Springer Science & Business Media, 1994.

[5] J. S. Kraft and L. C. Washington. An introduction to number theory with cryptography. CRC Press, 2016.

[6] Lipkovski, Aleksandar T. Digraphs associated with finite rings. Publications de l'Institut Mathematique 92.106 (2012): 35-41.