Quadratic Polynomials with Coefficients Modulo *n*

Hamza Daoub *
Osama Shafah *

Abstract:

If A is a finite commutative ring with unity. The directed graph of this ring is a graphical representation of its additive and multiplicative structure. Using the map $\varphi: A^2 \to A^2$, which is defined by $(a, b) \to (a + b, ab)$; a directed graph with vertices A^2 and arrows defined by φ can be created for every ring. In this work we are going to present more results, and use Mathematica Software ® to improve the algorithm which is used to calculate the directed graph of A.

Keywords: Graph; Homomorphism; Cycle; Theorem; Length.

Introduction:

This kind of associations between digraphs and finite rings has been studied and proposed previously [e.g [1], [2]]. However, further properties and results are presented here using only the finite commutative ring $\mathbb{Z}_n$. Some results are quoted from [2] for the sake of completeness.

Let $n < \infty$ be a natural number. Define the mapping $\varphi: \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n \times \mathbb{Z}_n$ by $\varphi(a, b) = (a + b, a.b)$. Since $\mathbb{Z}_n$ is finite, so φ can interpret as finite digraph $G_n = G(\mathbb{Z}_n)$ with vertices $\mathbb{Z}_n \times \mathbb{Z}_n$ and arrows defined by φ.

* Department of Mathematics- Zawia University

The outgoing (incoming) degree of a vertex (a, b) is the number of arrows going out (coming in) this vertex. Since G is a function, so it is clear that the outgoing degree of each vertex is one. The incoming degree of the vertex (a, b) is the number of different roots of $x^2 - ax + b$.

The characteristic of $\mathbb{Z}_n$ is n. If n is not a prime, then $\mathbb{Z}_n$ has zero divisors and $\mathbb{Z}_n[x]$ is not a unique factorization domain, so the quadratic polynomial $x^2 - ax + b$ has not a unique solution.
Since $\mathbb{Z}_p$ is a field, a polynomial of the form $x^2 - ax + b \in \mathbb{Z}_p[x]$ is reducible if and only if there exist $c, d \in \mathbb{Z}_p$ so that, $x^2 - ax + b = (x - c)(x - d)$. There are $\binom{p}{2}$ such polynomials for which $c \neq d$ and p for which $c = d$. Therefore, there are exactly

$$\binom{p}{2} + p = \frac{p(p-1)}{2} + p = \frac{p(p+1)}{2}$$

reducible monic quadratic polynomials in $\mathbb{Z}_p[x]$. Since there are p^2 polynomials of the form $x^2 - ax + b$ and each one is either reducible or irreducible, we conclude there are

$$p^2 - \frac{p(p+1)}{2} = \frac{p(p-1)}{2}$$

irreducible monic degree 2 polynomials in $\mathbb{Z}_p[x]$.

The starting vertices (a, b) (with incoming degree 0) correspond to quadratic polynomials $x^2 - ax + b$ irreducible in $\mathbb{Z}_p[x]$. This gives us rough upper estimate for the number of components of the graph $G(\mathbb{Z}_p)$.

Basic Properties:

Theorem 1 If p is an odd prime, then the solutions to the quadratic congruence $\mathrm{x}^2 - \mathrm{ax} + \mathrm{b} = 0 \bmod \mathrm{p}$ with a non congruent to $0 \bmod \mathrm{p}$ are given by

$$\mathrm{x} = \frac{-\mathrm{b} \pm \sqrt{\mathrm{b}^2 - 4\mathrm{ac}}}{2\mathrm{a}}.$$

In particular, if $b^2 - 4ac$ is a quadratic non residue $mod\ p$ then $x^2 - ax + b = 0$ has no solutions $mod\ p$.

Proof. See [2]

We let $N_f(m)$ denote the number of solutions of $x^2 - ax + b = 0\ mod\ m$. If $m = p^{n_1}p^{n_2}\dots p_k^{n_k}$ is the prime decomposition of m, then $N_f(m) = N_f(p^{n_1})N_f(p^{n_2})\dots N_f(p_k^{n_k})$.

Since the incoming degree of a vertex (a, b) is the number of roots of the quadratic polynomial $x^2 - ax + b = 0\ mod\ p$, then we have the following.

Theorem 2 Let $\mathrm{p_1, p_2, \dots, p_k}$ be the composition of the number n. Then the highest degree of a vertex $\mathrm{(a, b)}$ in the graph $\mathrm{G(\mathbb{Z}_n)}$ is less than or equal to 2^{k}

Proof. Let $\mathrm{x^2 - ax + b = 0}$ be an reducible quadratic polynomial over $\mathbb{Z}_{\mathrm{n}}$. From Theorem 1, we have

$$deg(a, b) = 2 \times 2 \times \dots \times 2 \quad (k - times) = 2^k \square$$

Notation: The sequence:

$$(a_1, b_1) \to (a_2, b_2) \to \dots \to (a_k, b_k) \tag{1}$$

of arrows in G defines a cycle of length k (or 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 $j \leq i < k$. In addition, $\overrightarrow{C_k}$ will be referred to the directed cycle with vertices $0, 1, \dots, k - 1$.

Let p and q be relatively prime numbers, such that $n = pq$, $p < q$. Define a map

$$\varphi_1 : \mathbb{Z}_n \to \mathbb{Z}_p$$

that maps representatives $0 \leq a < n$ in $\mathbb{Z}_n$ to $(a\ mod\ p)$ in $\mathbb{Z}_p$. Since p divides n, then φ_1 is a homomorphism. Moreover, $ker\varphi_1 = p\mathbb{Z}_n < \mathbb{Z}_n$, and $|ker\varphi_1| = p$.

Similarly, the same holds for $\varphi_2 : \mathbb{Z}_n \to \mathbb{Z}_q$.

Observe that mappings φ_1 and φ_2 induce mappings of corresponding graphs, which will be denoted again by φ_1 and φ_2.

We will denote to the longest cycle in the digraph $G(\mathbb{Z}_n)$ by $\overrightarrow{C_\gamma}$ for short, and all our discussion later will be based on the construction of φ_1 and φ_2. Furthermore, we will refer to $\mathbb{Z}_n$, $\mathbb{Z}_p$ and $\mathbb{Z}_q$ as sets of natural numbers.

Since a closed walk might be a cycle, so according to the structure of φ_1 and φ_2 and the sequence 1, we have the following:
Corollary 1 *A mapping $f: V(\vec{C}_k) \rightarrow V(G)$ is a homomorphism of $\vec{C}_k$ to G if and only if $f(1), f(2), \ldots, f(k)$ is a cycle in G.*

That means, a closed walk, which is mapped by $\varphi_1(\varphi_2)$ is a cycle. This consequence will be used in this work from now on.

Main Results:

If we suppose that $\alpha|\beta$, $\alpha \neq 1$ (α might equal to β), then it is not proved yet that the maps φ_1 and φ_2 send the longest cycle $\vec{C}_\gamma$ in $G(\mathbb{Z}_n)$ to longest cycles $\vec{C}_\alpha$ and $\vec{C}_\beta$ in $G(\mathbb{Z}_p)$ and $G(\mathbb{Z}_q)$ respectively. Because the cycles in $G(\mathbb{Z}_p)$ and $G(\mathbb{Z}_q)$ which are smaller than $\vec{C}_\alpha$ and $\vec{C}_\beta$ might have a pre-image which is a cycle with length longer than the pre-image of $\vec{C}_\alpha$ and $\vec{C}_\beta$ themselves. For instance, in $G(\mathbb{Z}_{47})$ the longest cycle is $\vec{C}_{12}$, and in $G(\mathbb{Z}_{11})$ the longest cycle is $\vec{C}_6$. While in $G(\mathbb{Z}_{517})$ the longest cycle is $\vec{C}_{30}$. Because, there is a cycle $\vec{C}_{10}$ in $G(\mathbb{Z}_{47})$ has a pre-image with $\vec{C}_6$ in $G(\mathbb{Z}_{517})$; that is exactly a multiple of these two.

This case is not considerable in the following proposition. As a matter of fact the computer calculations show that for n from 1 to 200 this exception case does not exist.

Proposition 1[Ref 2] Let p be a prime number such that $\mathrm{m} = \mathrm{pq}$. The mapping $\varphi: \mathrm{G}(\mathbb{Z}_\mathrm{m}) \rightarrow \mathrm{G}(\mathbb{Z}_\mathrm{p})$ is a homomorphism. So that φ maps the longest cycle in the graph $\mathrm{G}(\mathbb{Z}_\mathrm{m})$ to the longest cycle in $\mathrm{G}(\mathbb{Z}_\mathrm{p})$ If and only if p and q are relatively primes.

Theorem 3 Let p be a prime number, and $\overrightarrow{\mathrm{C}_\alpha}$ is the longest cycle in the graph $\mathrm{G}(\mathbb{Z}_\mathrm{p})$. The longest cycle in the graph $\mathrm{G}(\mathbb{Z}_\mathrm{p} \times \mathbb{Z}_\mathrm{p})$ is a cycle of length:

1. $k = LCM(\alpha, \gamma)$, if there is a cycle of length γ such that $1 < \gamma < \alpha$ and $(\alpha, \gamma) = 1$.
2. $k = \alpha$ if there is no such a cycle $\overrightarrow{C_\gamma}$, $1 < \gamma < \alpha$. Or the

only cycles which are shorter than $\overrightarrow{C_\alpha}$ are cycles of length divides α.

Proof. Define the maps $\varphi_1: \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p$, by $\varphi_1((a,b)) = [a]_p$, and $\varphi_2: \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p$, by $\varphi_2((a,b)) = [b]_p$.

The maps φ_1 and φ_2 are homomorphisms and onto. Consider that $\overrightarrow{C_r}$ is the longest cycle in $G(\mathbb{Z}_p \times \mathbb{Z}_p)$; that is, $(a_1, b_1) \to (a_2, b_2) \to \ldots \to (a_r, b_r)$, where $a_i, b_i \in Z_p \times \mathbb{Z}_p$.

Since φ_1 is a homomorphism then,

$$\begin{aligned}\varphi_1((a_1, b_1)) &= (\varphi_1(a_1), \varphi_1(b_1)) \\ &= (\varphi_1(a_r + b_r), \varphi_1(a_r . b_r)) \\ &= (\varphi_1(a_r) + \varphi_1(b_r), \varphi_1(a_r) . \varphi_1(b_r)) \qquad (2)\end{aligned}$$

We will use the same notations as we mentioned in the last theorem. a_{i1} refers to the first coordinate in the element a_i. Similarly, b_{i1} refers to the first coordinate of b_i.a_{i2} refers to the second coordinate in the element a_i, similarly, b_{i2} refers to the first coordinate of b_i.

Thus, from (2) we get

$$(a_{11}, b_{11}) = (a_{r1} + b_{r1}, a_{r1} . b_{r1} \qquad (3)$$

It is clear that $\varphi_1(\overrightarrow{C_r})$ is a cycle in $G(\mathbb{Z}_p)$, also it satisfies (3). That shows us $\varphi_1(\overrightarrow{C_r})$ divides $\overrightarrow{C_r}$.

If we repeat the same process on φ_2, we get

$$\begin{aligned}\varphi_2((a_1, b_1)) &= (\varphi_2(a_1), \varphi_2(b_1)) \\ &= (\varphi_2(a_r + b_r), \varphi_2(a_r . b_r)) \\ &= (\varphi_2(a_1) + \varphi_2(b_r), \varphi_2(a_r) . \varphi_2(b_r)) \qquad (4)\end{aligned}$$

Therefore:

$$(a_{12}, b_{12}) = (a_{r2} + b_{r2}, a_{r2}.b_{r2}). \quad (5)$$

It is clear that $\varphi_2(\overrightarrow{C_r})$ is a cycle in $G(\mathbb{Z}_q)$, it satisfies (5). That shows us $\varphi_2(\overrightarrow{C_r})$ divides $\overrightarrow{C_r}$.

Considering that φ_1 and φ_2 are onto, and $\overrightarrow{C_r}$ is multiple of $\varphi_1(\overrightarrow{C_r})$ and $\varphi_2(\overrightarrow{C_r})$. Then, by Chinese Reminder Theorem we have the following:

If $G(\mathbb{Z}_p)$ contains at least a cycle $\overrightarrow{C_\gamma}$, such that $1 < \gamma < \alpha$, and $(\alpha, \gamma) = 1$. Then $m = LCM(\alpha, \gamma)$.

If $G(\mathbb{Z}_p)$ contains no cycles or contains cycle $\overrightarrow{C_\gamma}$ such that $1 < \gamma < \alpha$, or $\gamma|\alpha$ Then $m = LCM(\alpha, \gamma) = \alpha$.

The largest multiple that we can get is the longest cycle in $G(\mathbb{Z}_p)$, which means that the length of $\overrightarrow{C_r}$ is exactly the length of the longest cycle in $G(\mathbb{Z}_p)$. □

Theorem 4:

Let $p_1^{n_1}, p_2^{n_2}, \ldots, p_r^{n_r}$ be coprimes, such that $p_i \neq p_j$ for $i \neq j$, Then, the longest cycle $\overrightarrow{C_n}$ in $G(\mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \ldots \mathbb{Z}_{p_r^{n_r}})$ has a length $m = LCM(\alpha_1, \alpha_2, \ldots, \alpha_n)$, where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the lengths of the longest cycles in $G(\mathbb{Z}_{p_1^{n_1}})$, $G(\mathbb{Z}_{p_2^{n_2}})$, ..., $G(\mathbb{Z}_{p_r^{n_r}})$ respectively.

Proof.

Define a mapping $\varphi: \mathbb{Z}_{p_1^{n_1} p_2^{n_2} \ldots p_r^{n_r}} \to \mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \ldots \mathbb{Z}_{p_r^{n_r}}$ by $\varphi([a]_{p_1^{n_1} p_2^{n_2} \ldots p_r^{n_r}}) = ([a]_{p_1^{n_1}}, [a]_{p_2^{n_2}}, \ldots, [a]_{p_r^{n_r}})$. This mapping is well defined. Furthermore, it is an isomorphism. We know that the longest cycle in $G(\mathbb{Z}_{p_1^{n_1} p_2^{n_2} \ldots p_r^{n_r}})$ is the least common multiple of the length of the longest cycles in the digraphs $G(\mathbb{Z}_{p^{n_1}})$, $G(\mathbb{Z}_{p^{n_2}})$, ..., and $G(\mathbb{Z}_{p^{n_r}})$ Since φ is bijection, Then the longest cycle in $G(\mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times$

$\ldots \mathbb{Z}_{p_r^{n_r}})$ has a length equal to the length of the longest cycle in $G(\mathbb{Z}_{p_1^{n_1} p_2^{n_2} \ldots p_r^{n_r}})$. □

Theorem 5:

Let p and q be any two prime numbers. Then the longest cycle in the graph $G(\mathbb{Z}_p \times \mathbb{Z}_q)$ is a cycle of length $n = LCM(\alpha, \beta)$, where α is the length of the longest cycle in $G(\mathbb{Z}_p)$ and β is the length of the longest cycle in $G(\mathbb{Z}_q)$.

Proof.

The projection map $\varphi_1: \mathbb{Z}_p \times \mathbb{Z}_q \to \mathbb{Z}_p$, where $\varphi_1((a, b)) = [a]_p$ is a homomorphism.

Also the map $\varphi_2: \mathbb{Z}_p \times \mathbb{Z}_q \to \mathbb{Z}_q$, where $\varphi_2((a, b)) = [b]_q$ is a homomorphism.

Suppose that $(a_1, b_1) \to (a_2, b_2) \to \ldots \to (a_n, b_n)$ is the longest cycle in the graph $G(\mathbb{Z}_p \times \mathbb{Z}_q)$, where $a_i, b_i \in Z_p \times \mathbb{Z}_q$.

Since φ_1 is a homomorphism then,

$$\begin{aligned} &\varphi_1((a_1, b_1)) = (\varphi_1(a_1), \varphi_1(b_1)) \\ &= (\varphi_1(a_n + b_n), \varphi_1(a_n . b_n)) \\ &= (\varphi_1(a_n) + \varphi_1(b_n), \varphi_1(a_n) . \varphi_1(b_n)) \end{aligned} \tag{6}$$

From the definition of φ_1, we observe that $\varphi_1(a_i)$ is the first coordinate of a_i . Similarly, $\varphi_1(b_i)$ is the first coordinate of b_i. In addition, $\varphi_2(a_i)$ is the second coordinate of a_i. Similarly, $\varphi_2(b_i)$ is the second coordinate of b_i, we will refer to it by b_{i2}.

Thus, from (1) we get

$$(a_{11}, b_{11}) = (a_{n1} + b_{n1}, a_{n1} . b_{n1}). \tag{7}$$

It is clear that $\varphi_1(\overrightarrow{C_n})$ is a cycle in $G(\mathbb{Z}_p)$, also it satisfies (2). That shows us $\varphi_1(\overrightarrow{C_n})$ divides $\overrightarrow{C_n}$.

If we repeat the same procedure on φ_2, we get

$$\varphi_2((a_1, b_1)) = (\varphi_2(a_1), \varphi_2(b_1))$$

$$= (\varphi_2(a_n + b_n), \varphi_2(a_n.b_n))$$
$$= (\varphi_2(a_1) + \varphi_2(b_n), \varphi_2(a_n).\varphi_2(b_n)) \qquad (8)$$

Therefore:

$$(a_{12}, b_{12}) = (a_{n2} + b_{n2}, a_{n2}.b_{n2}). \qquad (9)$$

It is clear that $\varphi_2(\overrightarrow{C_n})$ is a cycle in $G(\mathbb{Z}_q)$, also it satisfies (4). That shows us $\varphi_2(\overrightarrow{C_n})$ divides $\overrightarrow{C_n}$.

That means $\overleftarrow{C_n}$ is a multiple of $\varphi_1(\overrightarrow{C_n})$ and $\varphi_2(\overrightarrow{C_n})$. Observe that α and β are the lengths of the longest cycles in the graphs $G(\mathbb{Z}_p)$ and $G(\mathbb{Z}_q)$ respectively. Furthermore, the maps φ_1 and φ_2 are onto and the multiple of these two cycles is longer than any other two cycles. Therefore, By using Chinese Reminder Theorem, we find that the length of $\overrightarrow{C_n}$ is the Least Common Multiple of $\varphi_1(\overrightarrow{C_n})$ and $\varphi_2(\overrightarrow{C_n})$. □

Let p and q be any two prime numbers. Then the longest cycle in the graph $G(\mathbb{Z}_p \times \mathbb{Z}_q)$ has a length $l_{pq} = l_{qp}$, where l_{qp} is the length of the longest cycle in $G(\mathbb{Z}_q \times \mathbb{Z}_p)$. That can be seen from the isomorphism; $\mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_q \times \mathbb{Z}_p$.

The following two theorems can be proved immediately from theorem 5 by induction and using Chinese Reminder Theorem.

Theorem 6:

Let p_1, p_2, ..., p_n are distinct prime numbers. Then the longest cycle in the graph $G(\mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \ldots \times \mathbb{Z}_{p_n})$ is a cycle of length $l_p = LCM(l_{p_1}, l_{p_2}, \ldots, l_{p_n})$, where $l_{p_1}, l_{p_2}, \ldots, l_{p_n}$ are the length of the longest cycles in $G(\mathbb{Z}_{p_1})$, $G(\mathbb{Z}_{p_2})$, ..., $G(\mathbb{Z}_{p_n})$.

Theorem 7:

Let $p_1^{\alpha}, p_2^{\beta}, \ldots, p_r^{n_r}$ are relatively primes. Then the longest cycle in the graph $G(\mathbb{Z}_{p_1^{\alpha}} \times \mathbb{Z}_{p_2^{\beta}} \times \ldots \times \mathbb{Z}_{p_r^{n_r}})$ is a cycle of length $l_p = LCM(l_{p_1^{\alpha}}, l_{p_2^{\beta}}, \ldots, l_{p_r^{n_r}})$, where $l_{p_1^{\alpha}}, l_{p_2^{\beta}}, \ldots, l_{p_r^{n_r}}$ are the length of the longest cycles in $G(\mathbb{Z}_{p_1^{\alpha}})$, $G(\mathbb{Z}_{p_2^{\beta}})$, ..., $G(\mathbb{Z}_{p_r^{n_r}})$.

Theorem 8:

Consider that $n \cong 1 \,(\mathrm{mod} \quad m\,)$. The function $f: \mathbb{Z}_m \to \mathbb{Z}_{mn}$ given by $f([x]_m) = [nx]_{mn}$ is an injective homomorphism .

Proof.

Let $[a]_m, [b]_m \in \mathbb{Z}_m$. Then

$f([a]_m + [b]_m) = f([a+b]_m) = [n(a+b)]_{mn} = [na]_{mn} + [nb]_{mn} = f([a]_m) + f([b]_m)$.

Furthermore, we note that

$f([a]_m) f([b]_m) = [na]_{mn}[nb]_{mn} = [n^2ab]_{mn}$.

We have given that $n \cong 1 \ (mod \ \ m)$, hence $n = mq + 1$ for some $q \in \mathbb{Z}$. By multiplying both sides of this equation by n we get $n^2 = mnq + n$, so $n^2 \cong n \ (mod \ \ mn)$. Therefore, we get

$f([a]_m) f([b]_m) = [n^2ab]_{mn} = [nab]_{mn} = f([ab]_m) = f([a]_m[b]_m)$.

Hence f is a homomorphism. To show f is injective, we can compute the kernel of f. Let $x \in ker(f)$. Then $[0]_{mn} = f([x]_m) = [nx]_{mn}$ so $mn|nx \Rightarrow m|nx$. But $n \cong 1 \,(\, mod \quad m\,)$ tells us that $(m, n) = 1$. So we have $m|nx \Rightarrow m|x$. Therefore $[x]_m = [0]_m$ and so $ker(f) = \{[0]_m\}$. Hence f is injective. □

Theorem 9:

Suppose that $n \cong 1(mod \ \ m)$. There is a cycle of length $r, r \geq 1$ in the graph $G(\mathbb{Z}_{mn})$(and not neccessary the longest one) if and only if the longest cycle in $G(\mathbb{Z}_m)$ is of length r.

Proof:

assume that $\overrightarrow{C_{l_r}}$ is the longest cycle in the graph $G(\mathbb{Z}_m)$, that is

$(a_1, b_1) \to (a_2, b_2) \to \ldots \to (a_r, b_r)$

Since f is a homomorphism. Then $f(\overrightarrow{C_{l_r}})$ is a cycle in the graph $G(\mathbb{Z}_{mn})$. Since every element in Imf is of the form $[na]_{mn}, a \in \mathbb{Z}_m$

, therefore, we notice that

$$f((a_1,b_1)) = (f(a_1),f(b_1)) = (na_1,nb_1) = (n(a_n + b_n, n(a_n.b_n)$$

Since f is injective. Then $f(\overrightarrow{C_{l_r}})$ is a cycle of length r.

($\Rightarrow$) This direction can be proved easily by taking a map $g: \mathbb{Z}_{mn} \to \mathbb{Z}_m$, where $g(a) = [a]_m$. □

Computer Caculations:

A computer program has been written and run on a PC to calculate some properties of the graph G_n. Some notations are used, such as c_n (number of components), l_c (length of the longest cycle), $N.l_c$ (number of lengest cycles), and p_n (the longest path). The ring of integers modulo n is a field if and only if n is a prime number. Otherwise, it is not even a domain. However, the direct product of the rings R_i, for i in some index set I has zero divisors. For instance, in the ring $\mathbb{Z}_p \times \mathbb{Z}_q$, the elements (1,0) and (0,1) satisfy that $(1,0).(0,1) = 0$. That means $\mathbb{Z}_p \times \mathbb{Z}_q$ can't be domain, so that can't be field.

Similar observations can be seen in the Table 1 and Table 2 such as;

In the case, when $n_1 = n_2$; the construction of the digraphs $G(\mathbb{Z}_{n_1 n_2})$ and $G(\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2})$ is completley different.

2. In the construction of the digraphs $G(\mathbb{Z}_{pq})$ and $G(\mathbb{Z}_p \times \mathbb{Z}_q)$, we have that both have the same number of component, number of longest cycles, length of longest cycle, and length of longest path, which has been partly proved.

In the digraph $G(\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2})$, where n_1 is prime and $n_2 =$ 2,3,7; the number of components $c_{n_1 n_2} = c_{n_1} \times c_{n_2}$; the longest cycle $l_{n_1 n_2} = l_{n_1}$; the number of cycles $\mathrm{N}.l_{n_1 n_2} = n_2$ the length of the longest path $p_{n_1 n_2} = p_{n_1}$.

Table 1: Results for $1 \leq n \leq 20$

n	c_n	l_c	$N.l_c$	p_n
1	1	1	1	1
2	4	1	4	3
3	9	1	9	5
4	26	2	10	4
5	39	4	14	8
6	36	1	36	5
7	49	1	49	9
8	168	4	64	8
9	213	6	12	10
10	156	4	56	8
11	149	6	28	19
12	234	2	90	6
13	199	4	30	22
14	196	1	196	9
15	351	4	126	8
16	1232	8	448	10
17	375	20	4	34
18	852	6	48	10
19	704	8	46	34
20	1154	4	504	8

Table 2: Results for $1 \leq n_1, n_2 \leq 20$

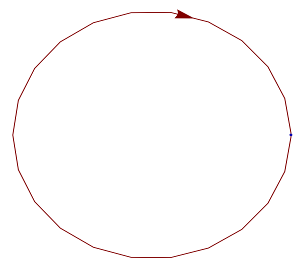
n_1	n_2	c_n	l_c	$N.l_c$	p_n	n_1	n_2	c_n	l_c	$N.l_c$	p_n
2	3	6	1	6	5	4	13	71	4	6	22
2	4	10	2	2	4	4	14	70	2	14	9
2	5	12	4	2	6	4	15	93	4	18	8
2	6	12	1	12	5	4	16	164	8	24	10
2	7	14	1	14	9	4	17	97	10	6	18
2	8	24	4	4	6	4	18	146	6	4	6
2	9	28	3	4	6	4	19	101	8	6	34
2	10	24	4	4	6	4	20	166	4	36	6
2	11	24	6	2	14	5	6	36	4	6	8
2	12	30	2	6	6	5	7	42	4	7	12
2	13	28	4	2	22	5	8	80	4	30	8
2	14	28	1	28	9	5	9	87	12	2	14
2	15	36	4	6	8	5	10	78	4	28	8
2	16	60	8	8	10	5	11	73	12	2	18
2	17	38	10	2	18	5	12	93	4	18	8
2	18	56	3	8	6	5	13	87	4	22	22
2	19	40	8	2	34	5	14	84	4	14	12
2	20	62	4	12	6	5	15	117	4	42	8
3	4	15	2	3	6	5	16	206	8	36	12
3	5	18	4	3	8	5	17	118	20	2	24
3	6	18	1	18	5	5	18	174	12	4	14
3	7	21	1	21	9	5	19	132	8	9	34
3	8	36	4	6	8	5	20	209	4	84	8
3	9	42	3	6	7	6	7	42	1	42	9
3	10	36	4	6	8	6	8	72	4	12	8
3	11	36	6	3	14	6	9	84	3	12	7
3	12	45	2	9	6	6	10	72	4	12	8
3	13	42	4	3	22	6	11	72	6	6	14
3	14	42	1	42	9	6	12	90	2	18	6
3	15	54	4	9	8	6	13	84	4	6	22
3	16	90	8	12	12	6	14	84	1	84	9
3	17	57	10	3	18	6	15	108	4	18	8
3	18	84	3	12	7	6	16	180	8	24	12
3	19	60	8	3	34	6	17	114	10	6	18
3	20	93	4	18	8	6	18	168	3	24	7
4	5	31	4	6	6	6	19	120	8	6	34
4	6	30	2	6	6	6	20	186	4	36	8
4	7	35	2	7	10	7	8	84	4	14	12
4	8	64	4	12	6	7	9	98	3	14	11
4	9	73	6	2	8	7	10	84	4	14	12
4	10	62	4	12	6	7	11	84	6	7	14
4	11	61	6	6	15	7	12	105	2	21	10
4	12	78	2	30	6	7	13	98	4	7	22

Table 3: Results for $1 \leq n_1, n_2 \leq 20$

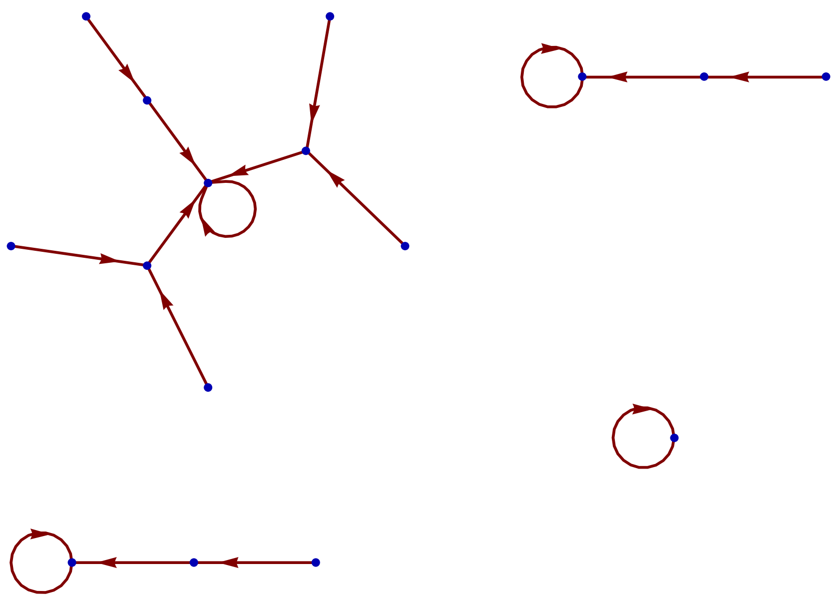
n_1	n_2	c_n	l_c	$N.l_c$	p_n	n_1	n_2	c_n	l_c	$N.l_c$	p_n
7	14	98	1	98	9	11	15	219	12	6	18
7	15	126	4	21	12	11	16	374	24	8	30
7	16	210	8	28	16	11	17	230	30	2	36
7	17	133	10	7	18	11	18	350	6	42	16
7	18	196	3	28	11	11	19	241	24	2	50
7	19	140	8	7	34	11	20	383	12	12	18
7	20	217	4	42	12	12	13	213	4	18	22
8	9	180	12	4	14	12	14	210	2	42	10
8	10	160	4	60	8	12	15	279	4	54	8
8	11	148	12	4	18	12	16	492	8	72	12
8	12	192	4	36	8	12	17	291	10	18	18
8	13	176	4	46	22	12	18	438	6	12	10
8	14	168	4	28	12	12	19	303	8	18	34
8	15	240	4	90	8	12	20	498	4	108	8
8	16	440	8	80	10	13	14	196	4	14	22
8	17	240	20	4	24	13	15	261	4	66	22
8	18	360	12	8	14	13	16	446	8	68	26
8	19	248	8	20	34	13	17	270	20	2	38
8	20	440	4	180	8	13	18	398	12	4	30
9	10	174	12	4	14	13	19	283	8	17	34
9	11	175	6	21	16	13	20	457	4	132	22
9	12	219	6	6	10	14	15	252	4	42	12
9	13	199	12	2	30	14	16	420	8	56	16
9	14	196	3	28	11	14	17	266	10	14	18
9	15	261	12	6	16	14	18	392	3	56	11
9	16	462	24	8	26	14	19	280	8	14	34
9	17	272	30	2	34	14	20	434	4	84	12
9	18	426	6	24	10	15	16	618	8	108	12
9	19	283	24	2	50	15	17	354	20	6	24
9	20	467	12	12	14	15	18	522	12	12	16
10	11	146	12	4	18	15	19	369	8	27	34
10	12	186	4	36	8	15	20	627	4	252	8
10	13	174	4	44	22	16	17	610	40	8	34
10	14	168	4	28	12	16	18	924	24	16	66
10	15	234	4	84	8	16	19	642	8	148	34
10	16	412	8	72	12	16	20	1156	8	216	12
10	17	236	20	4	24	17	18	544	30	4	34
10	18	348	12	8	14	17	19	384	40	2	66
10	19	246	8	18	34	17	20	623	20	12	24
10	20	418	4	168	8	18	19	566	24	4	50
11	12	183	6	18	15	18	20	934	12	24	14
11	13	169	12	2	30	19	20	643	8	54	34
11	14	168	6	14	14	-	-	-	-	-	-

Digraphs for $1 \leq n \leq 5$

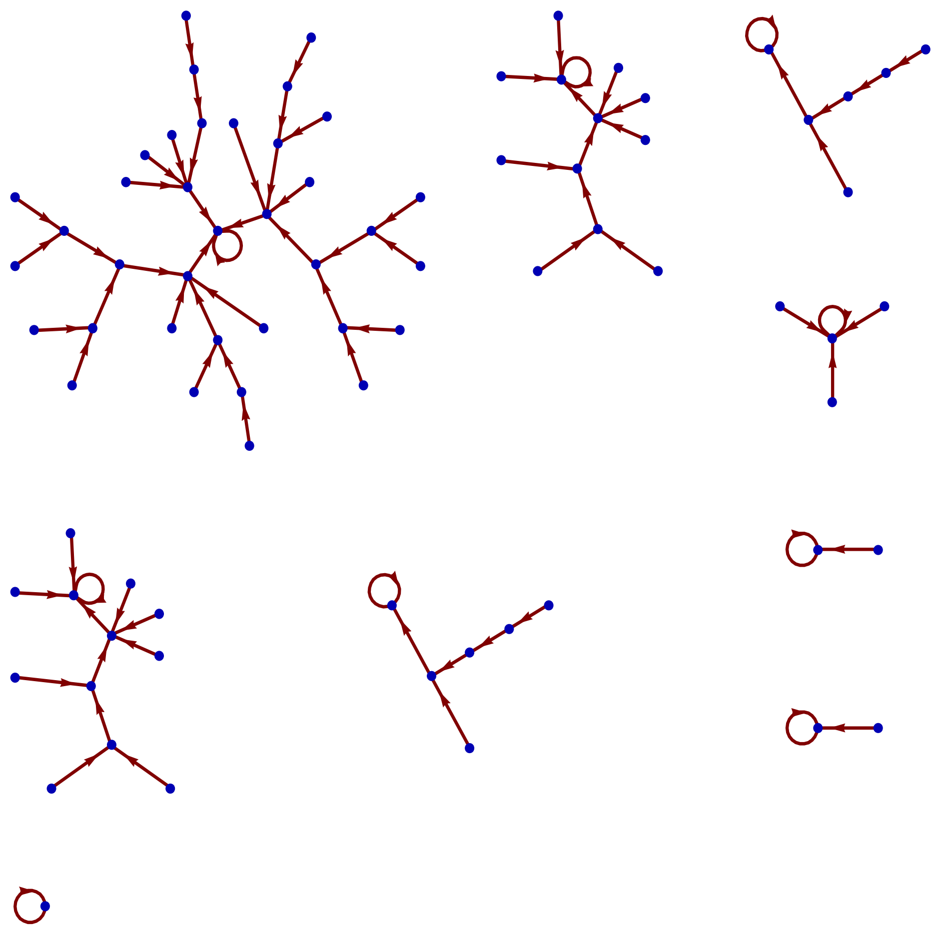
Here are the first five digraphs of $\mathbb{Z}_n \times \mathbb{Z}_n$



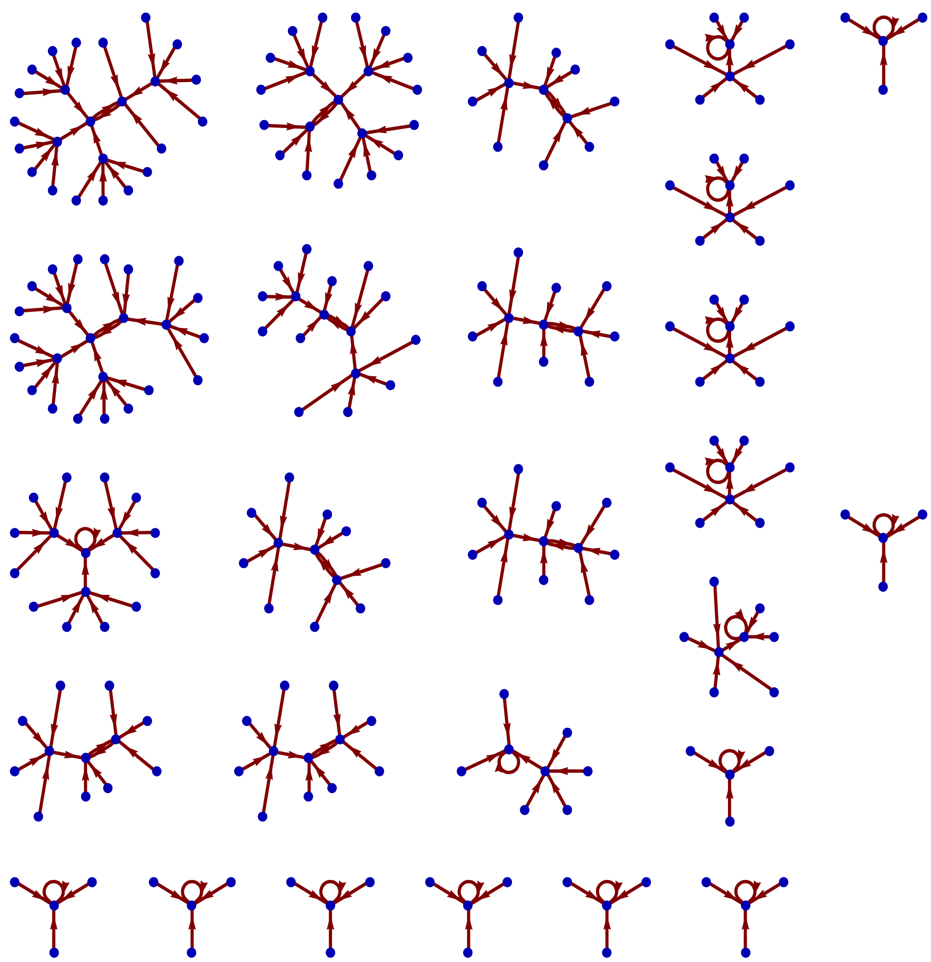
The Directed graph of $\mathbb{Z}_1 \times \mathbb{Z}_1$



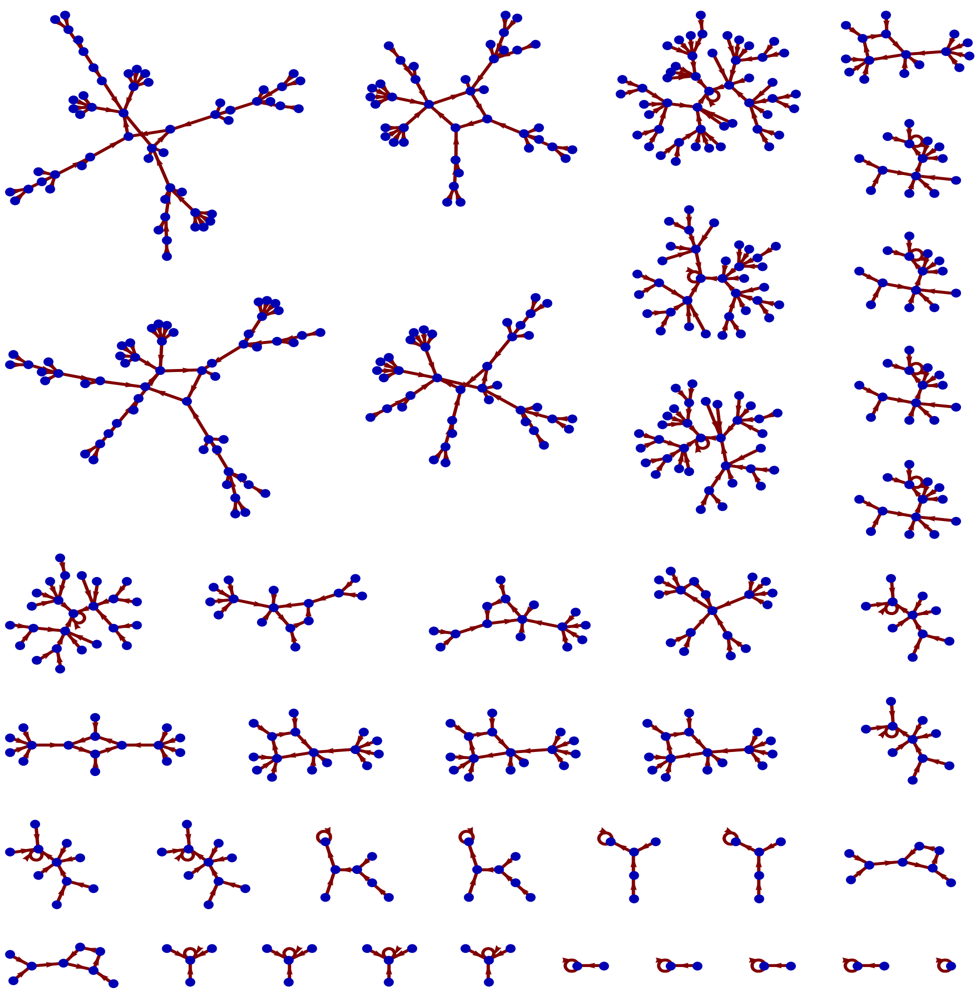
The Directed graph of $\mathbb{Z}_2 \times \mathbb{Z}_2$



The Directed graph of $\mathbb{Z}_3 \times \mathbb{Z}_3$



The Directed graph of $\mathbb{Z}_4 \times \mathbb{Z}_4$



The Directed graph of $\mathbb{Z}_5 \times \mathbb{Z}_5$

البيانات الموجهة المرتبطة بالحدوديات التربيعية ذات معاملات بمقياس *n*

حمـزة الهـادي داعـــو *
أسامة عبدالسلام الشفح *

المستخلص:

لتكن A حلقة ابدالية منتهية ذات عنصر محايد، البيان الموجه لهذه الحلقة هو عبارة عن تمثيل بياني لعمليتي الجمع والضرب المعرفتين عليها. باستخدام الراسم $\varphi: A^2 \to A^2$ المعرف بالصيغة $(a,b) \to (a+b, ab)$، فإن البيان الموجه ذي الرؤوس A^2 والحواف المعرفة بواسطة φ يمكن تعيينه لكل حلقة.

في هذا العمل سوف نعرض العديد من الخواص لهذا النوع من البيانات الموجهة كذلك سنستخدم برنامج Mathematica لتحسين الخوارزمية التي استخدمت من قبل لحساب البيان الموجه للحلقة A.

* قسم الرياضيات – جامعة الزاوية.

References:

1. Lipkovski, Digraphs associated with rings and some integer functions, IX Congress of Mathematicians in Yugoslavia, Petrovac, May 22-27, 1995, Book of abstracts p. 32.
2. A. Lipkovski, O. Shafah, H. Daoub, Vychislenie grafov konechnyh kolec. International Conference "Mathematical and informational technologies", Report 177, Vrnjacka Banja Serbia - Budva Montenegro, August 27-September 5, 2011.
3. Benjamin Fine, Gerhard Rosenberger, Number Theory: An Introduction via the Distribution of Primes, Birkhauser Boston, 2007.