On Digraphs Related to Cubic Mapping Modulo n

Dr.Hamza Daoub, Dr.Fathi Bribesh
Dept. of Mathematics, Faculty of Sciences
Zawia University

Abstract:

Let η be a map on the commutative ring $A = \mathbb{Z}_n$ into itself. For each $a \in A$, let $\eta(a)$ be the remainder of a^3 $modulo$ n, i.e., $\eta(a) = a^3 \ mod \ n$. The iteration digraph $G_n = G(\mathbb{Z}_n)$ of η is a directed graph whose vertices are elements of A and exactly one directed edge from a to $\eta(a)$ for all $a \in A$. We investigate the properties of this digraph using Mathematica notebook to calculate and display the corresponding associated digraph of certain ring.

Keywords:*digraphs,cycle,cubic congruence,primitive,Commutative ring.*

I. Introduction:

Graph theory considered one of the prime objects of study in discrete mathematics and used widely in solving majority of computational problems where every system is based on some discrete relation such as, traffic organization, social relations, artificial intelligence, problems in number theory and abstract algebra and so on.

One of a very wide area of study is associating a graph with an algebraic structure. Commonly, the aim of such studies is exposing the relationship between algebra and graph theory where an intricate algebraic structure can be visualized in a graph. The idea of associating a graph to a commutative ring, where all elements of the ring are vertices of a graph, appeared widely in literature such as [1, 2].

Over the past two decades, many researchers have been worked on associating graphs with polynomial roots modulo n on commutative ring see for instance references [3, 4, 5].

For each positive integer n, and any $a \in V$, let $\eta(a)$ be the remainder of a^3 modulo n, i.e., $\eta(a) \in V$ and $a^3 = \eta(a)\, mod\ n$. We define a digraph G_n whose set of vertices is the set $V = \mathbb{Z}_n$ and for which there is a directed edge from $a \in V$ to $b \in V$ if $a^3 \equiv b\ mod\, n$.

In this work, we introduce the number of fixed points in the digraph G_n, and present simple conditions for the number of components and cycle length. Also, we study the in-degree, out-degree and the isolated fixed points. Furthermore, we look at the Carmichael Lambda-function, Euler Totient function, and some concepts related to number theory in the framework of graph language.

II. Background:

Throughout this section, we summarize some well-known theories and properties of congruence modulo n that are considered as basics of our work. We start with following definitions:

Definition 1.1: the Euler's phi function $\phi(m)$ that denotes the number of positive integers less than or equal to m and relatively prime to m, where m is a positive integer.

Also, the Carmichael function of a positive integer n, denoted by $\lambda(n)$, is the smallest positive integer m such that $a^m \equiv 1 \mod n$ for every integer a that is coprime to n.

Definition 1.2: A fixed point of a function is an element of the function's domain that is mapped to itself by the function, i.e., a is fixed point of η if $\eta(a) = a$ for any $a \in \mathbb{Z}_n$.

Definition 1.3: Let m and a be any positive integers such that $(a, m) = 1$. Then the least positive exponent e such that $a^e \equiv 1 \mod m$ is the order of a modulo m and denoted by $ord_m a$.

Definition 1.4: Let a, n be positive integers and suppose that $gcd(a, n) = 1$. Then a is called a cubic residue of n if there is an integer x such that $x^3 \equiv a \mod n$. If the congruence has no solution, then a is called cubic nonresidue of n.

The following theorem helps to determine several positive integers k such that $k \leq \phi(m)$ as possible candidates for $ord_m a$.

Theorem 1.1: Let a be a positive integer such that $(a, m) = 1$ and $ord_m a = e$. Then $a^n \equiv 1 \mod m$ if and only if $e|n$.

Proof: See ref [6]. ■

Corollary 1.1: Let a be a positive integer such that $(a,m) = 1$. Then $ord_m a \,|\phi(m)$. In particular, if p is a prime and $p \nmid a$, then $ord_p a \mid (p-1)$.

Proof*:* See ref [6]. ■

The following corollary shows the relation between two powers of a number a satisfies the congruence $a^i \equiv a^j \ mod\ n$.

Corollary 1.2: Let $ord_m a = e$. Then $a^i \equiv a^j \ mod\ m$ if and only if $i \equiv j \ mod\ e$.

Proof: See ref [6]. ■

Let α be a positive integer such that $(\alpha, m) = 1$. Then α is a primitive root modulo m if $ord_m \alpha = \phi(m)$. Note that, if x is primitive root of unity modulo a prime number p, then $ord_m x = p-1$.

Theorem 1.2: Let p be a prime and d is a positive factor of $p-1$. Then there are exactly $\phi(d)$ incongruent integers of order d modulo p.

This theorem is proved by the French mathematician Adrien-Marie Legendre in 1785.

For sake of completeness, we introduce the Carmichael's theorem which states.

Theorem 1.3: Let m be a positive integer and a any integer with $(a,m) = 1$. Then $a^{\lambda(m)} \equiv 1 \ mod\ m$.

If we consider the problem of solving modulo prime powers, then by using the Chinese remainder theorem algorithm, we can give the total number of solutions of $f(x) = 0 \ mod\ m$. In this regard, we introduce the following theorem.

Theorem 1.4: If $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ is the prime decomposition of n, then $N(n) = N(p_1^{e_1}) N(p_2^{e_2}) \dots N(p_k^{e_k})$, where $N(n)$ denote the number of solutions of $f(x) \equiv 0 \mod m$.

The simplest case of solving modulo a prime power p^{α} is when $\alpha = 1$. Since p is a prime, then $\mathbb{Z}_n$ is a field. This means we can use the normal properties of equations over fields to simplify the problem using the following theorem.

Theorem 1.5: The polynomial congruence $f(x) \equiv 0 \mod p$, p is prime has at most k solutions if the degree of $f(x)$ is k.

The coming theorem is the special case of the k^{th} power theorem, which proved in reference [7].

Theorem 1.6: Let n be a positive integer having a primitive root and suppose $(a, n) = 1$. Then the congruence $x^3 \equiv a \mod n$ has a solution if and only if

$$a^{\frac{\phi(n)}{gcd(3,\phi(n))}} = 1 \mod n.$$

This theorem determines whether a is a residue or not. However, the following theorem specifies exactly the number of roots of the congruence equation $x^3 \equiv a \mod n$.

Theorem 1.7: If p is a prime and $(n, p-1) = 1$, then the congruence $x^n \equiv a \mod p$ has $(n, p-1)$ solutions or no solutions if a is non residue modulo p.

Proof: See ref [8]. ■

Corollary 1.3: Let p is a prime and, $p \equiv 1 \mod 3$. Then the congruence $x^3 \equiv a \mod p$ has exactly three solutions.

Corollary 1.4: Let p is a prime and, $p \equiv 2 \mod 3$. Then the congruence $x^3 \equiv a \mod p$ has exactly one solution.

Corollary 1.5: Let p be a prime number, then there exists a primitive cube root of unity in $\mathbb{Z}_p$ if and only if $p \equiv 1 \; mod \; 3$.

Theorem 1.8: Let p be a prime number, If $x^a \equiv 1 \mod p$ and $x^b \equiv 1 \mod p$, then $x^{gcd(a,b)} \equiv 1 \mod p$.

We now present some facts in graph theory that used to describe the related digraph of commutative ring $\mathbb{Z}_n$.

The in-degree of a vertex $a \in A$ of G_n denoted by $indeg(a)$, is the number of directed edges going into a.The out-degree of each vertex $a \in A$ of G_n is the number of directed edges coming out of a. It is obvious that G_n has exactly n directed edges. Thus, if $(v_i, \; i = 1, 2, 3, \dots, q)$ denote all the vertices of G_n having positive in-degree, then $\sum_1^q v_i = n$.

A strongly connected component of a directed graph G_n is a subgraph that is strongly connected, and is maximal with this property: no additional edges or vertices from G_n can be included in the subgraph without breaking its property of being strongly connected. The collection of strongly connected components forms a partition of the set of vertices of *G*.

It is clear that each component of our graph has a unique cycle, since each vertex of the component has out-degree 1 and the component has only a finite number of vertices. See for instance, Figures 1, 2, 3.

III. Main results:

In this section, we study the properties of the graph G_n referring to the number theoretic properties of $\mathbb{Z}_n$that mentioned in the previous section. We will refer to $\mathbb{Z}_n$ as set of natural numbers. First, we introduce the following theorem that shows a simple criterion for deciding whether an integer a is a cubic residue modulo a prime number p.

Theorem 2.1: Let p be a prime such that $(a,p)=1$ and $p \equiv 1 \ mod\ 3$. Then a is a cubic residue modulo p if $a^{\frac{p-1}{3}} \equiv 1 \ mod\ p$.

Proof: Using Fermat's Little Theorem, we find that

$$\left(a^{\frac{p-1}{3}}-1\right)\left(a^{\frac{p-1}{3}}+1\right)\left(a^{\frac{p-1}{3}}+1\right) \equiv$$
$$\left(a^{2\left(\frac{p-1}{3}\right)}-1\right)\left(a^{\frac{p-1}{3}}+1\right) \equiv$$
$$a^{p-1}-1 \ \equiv 0 \ mod \ p.$$

Thus,

$$a^{\frac{p-1}{3}} \equiv 1 \ \ mod\ p.$$

If a is a cubic residue modulo p, then there exists an integer x_0 such tha $x_0^3 \equiv a \ mod\ p$. By Fermat's little theorem, we have

$a^{\frac{p-1}{3}} \equiv (x_0^3)^{\frac{p-1}{3}} \equiv x_0^{p-1} \equiv 1 \ \ mod\ p.$ ■

Theorem 2.2: The in-coming degree of a vertex $a \in G$ equals the number of distinct roots of the cubic polynomial $(x^3-a) \in \mathbb{Z}_n[x]$.

Proof: The directed edge $x \to a$, means that $\eta(x) = x^3 = a$, and by Theorem 1.7, we deduce that the solutions are roots of this polynomial. Conversely, if x is a root of this polynomial, then there is a directed edge $x \to a$, and for distinct roots such edges are also distinct. In fact, if $x_1, \ldots, x_k$ are all the distinct roots of the polynomial, then $x_i^3 = a$. ■

Let $\mathrm{N}(n,a)$ denote the number of incongruent solutions of the congruence

$x^3 \equiv a \ mod\ n$,

then by theorem 2.2. $\mathrm{N}(n,a) = indeg_n(a)$. It follows from Theorem 1.5 that $indeg_n(a) = \mathrm{N}(n,a) = \Pi_{i=1}^{k}\mathrm{N}(p_i^{\alpha_i},a) = \Pi_{\mathrm{i}=1}^{k} indeg_{q_i}(a)$, where $q_i = p_i^{\alpha_i}$.

Definition 2.1: The sequence

$$a \longrightarrow a^3 \longrightarrow a^9 \longrightarrow \cdots \longrightarrow a^{3^k} \longrightarrow a, \qquad (1)$$

of arrows in G, define a cycle of length k. if $\eta\left(a^{3^k}\right) = a$ and $\eta(a^{3^i}) \neq a^{3^j}$ for all $1 < j \leq i < k$.

It is clear that each component has a unique cycle, since each vertex of the component has out-degree 1 and the component has only a finite number of vertices. It is also obvious that cycle vertices have positive in-degree. Cycles of length 1 are called *loops*.

Theorem 2.3: Let $p_1, p_2, \ldots, p_k$, be different prime factors of the number n such that $p_i \equiv 1 \, mod \, 3$ for all $1 \leq i \leq k$, then the highest in-degree of a vertex v in the graph G_n is 3^k.

Proof: Suppose that $x^3 - \alpha = 0$, be a reducible cubic polynomial over $\mathbb{Z}_n$. Then by theorem1.5 and corollary 1.3, we have

$N(n, a) = 3 \times 3 \times \ldots \times 3(ktimes) = 3^k$. ■

Note that, our observations in the graph under investigation show that if $n = p_1 p_2 \ldots p_k$ such that $p_i \equiv 2 \ mod \, 3$, then the in-degree of a vertex v is much smaller than 3^k. For example: If $n = 3 \times 5 \times 7$, then the largest $indeg_n v$ is 3 (see figure 1). However, if $n = 7 \times 13$, then the largest $indeg_n v$ is 9 (see figure 2).

There is an interesting relation between the quadratic congruence and the cubic congruence modulo n that can be given by the following proposition.

Proposition 2.1: The roots of the equation $x^2 \equiv 1 \ mod \, n$ are fixed points of η.

Proof: if a is a root of $x^2 \equiv 1 \ mod\, n$, then we have $a^2 \equiv 1\, mod\, n$, this implies

$\eta(a) = a^3 = a^2a = 1.a = a.$

Thus, a is a fixed point. ■

Proposition 2.2: Let $b \neq 1$ is an idempotent, then b and the roots of the congruence $x^2 \equiv b \ mod\, n$, are fixed points of η.

Proof: Suppose that b is an idempotent not equal to 1, then $b^2 = b$, this implies that $\eta(b) = b^3 = b^2b = b^2 = b$ which means b is a fixed point.

On the other hand, suppose that c is a root of $x^2 \equiv b \ mod\, n$, then $c^2 \equiv b \ mod\, n$.Thus, $\eta(c) = c^3 = c^2c = bc$ this implies $bc^3 = b^2c = bc$, applying cancelation low, we get $c^3 = c$ this means $\eta(c) = c$. Therefore, c is a fixed point.■

Recall that, if n is not a prime then there could be a nilpotent different from 0 and an idempotent different from 1.

The following theorem is already studied in reference [3]. We implement this theorem in different manner to classify loops in G_n.

Theorem 2.4: If $n = p$ is a prime, then the loops in G_n correspond to vertices $0, 1, p-1$.

Proof: Since 0 and 1 are fixed points so both of them are loops. Now suppose that p is prime, then $\mathbb{Z}_p$ is a field, since $p-1$ is a root of $x^2 \equiv 1\, mod\, p$, then by Proposition 2.1 we have $p-1$ is a fixed point. Hence $(p-1)$ is a loop. On the other hand, since $\mathbb{Z}_n$ is a field, so there is no idempotent different from 1 nor nilpotent different from 0, and since 1 and $p-1$ are the only roots of the congruence $x^2 \equiv 1 \ mod\, p$, this yields the loops are only $0, 1, p-1$.■

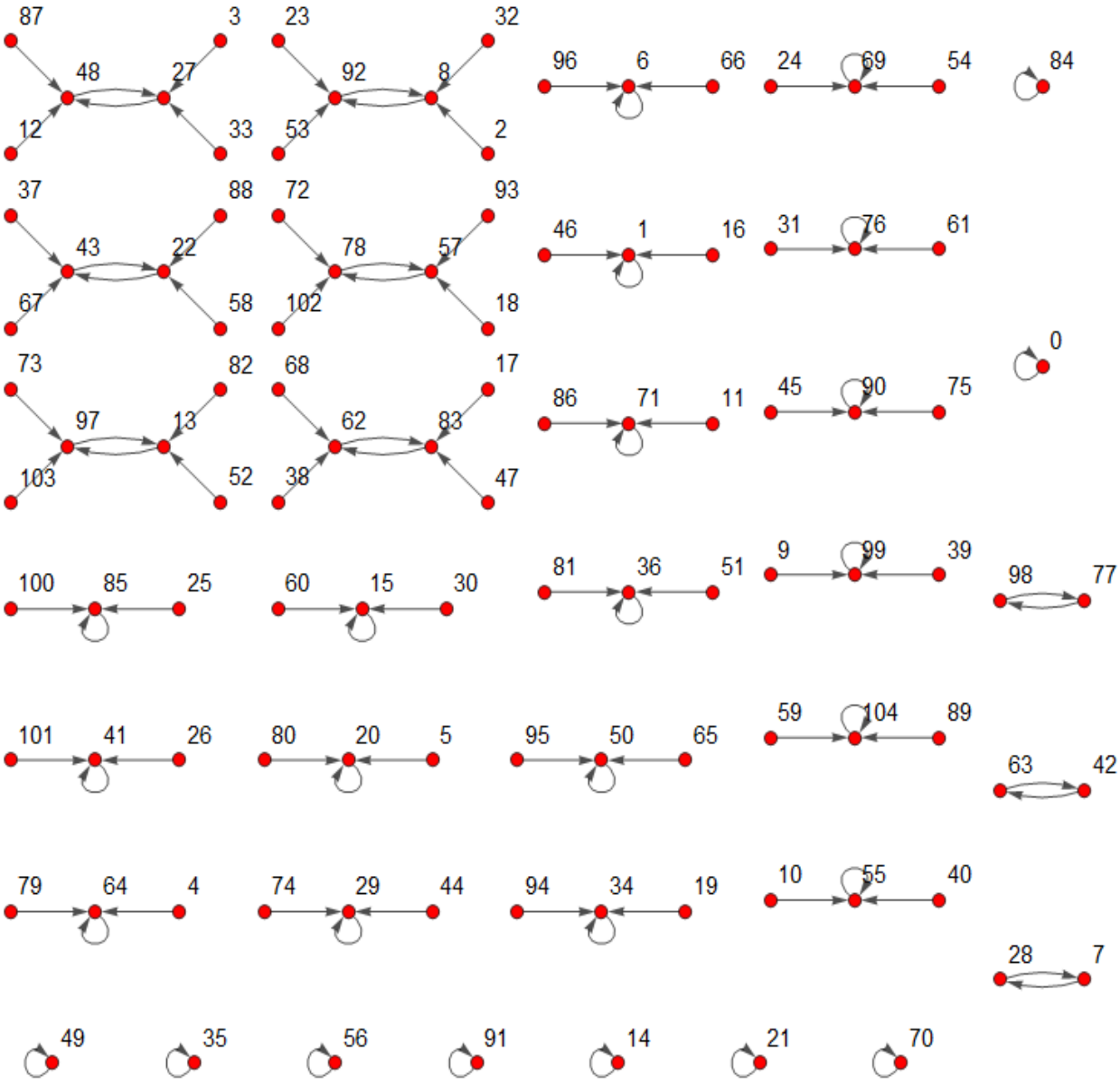

Figure 1: Shown are all the components of $G_{3\times 5\times 7}$.

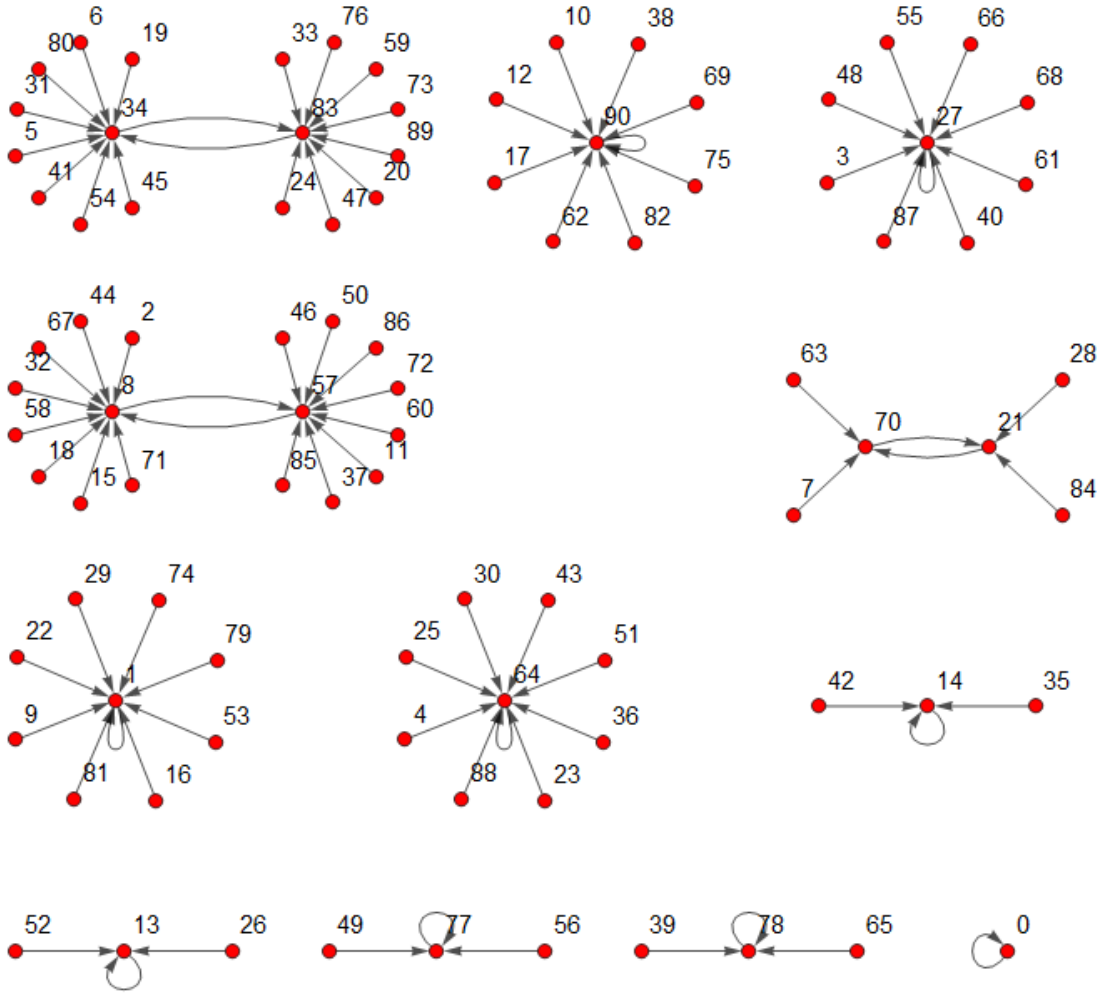

Figure 2: Shown are all the components of $G_{7\times13}$.

Theorem 2.5: If n is not a prime, then the loops in G_n are the idempotent elements and their quadratic roots in addition to $0, 1, p-1$.

Proof: We have proved in Theorem 2.4, that loops are $0, 1, p-1$. Now, suppose that α is an idempotent different from 1, so by Proposition

2.2, the roots of the quadratic $x^2 \equiv \alpha \ mod\, n$ are fixed points. Therefore, they correspond to loops in G_n. ■

Corollary 2.1: If $n = p$ is a prime, then there are no cycles of length $p - 1$.

Proof: From Theorem 2.5, we note that 0, 1, and $p - 1$ represent loops, so the number of the remained elements in $\mathbb{Z}_n$ is $p - 3$, which can not contain a cycle of length $p - 1$. ■

Let p is a prime number, in the digraph G_n, every vertex in a *k-cycle* must satisfy the congruence

$$x^{3^k} \equiv x mod n,$$

$$x^{3^k} - x \equiv 0 mod n,$$

$$x(x^{3^k-1} - 1) \equiv 0 mod n.$$

Since $x \neq 0$, then $x^{3^k-1} - 1 \equiv 0 \ mod\, p$, this equivalent to

$$x^{3^k-1} \equiv 1 \ mod\, p. \qquad (2)$$

Equation (2) motivates us to study the relation between primitive roots and k-cycles. First, we try to classify cycles according to primitive and non-primitive vertices.

Suppose that there is a *k-cycle* contains a vertex which is a primitive root of unity, then

$$x^{\lambda(n)} = x^{p-1} \equiv 1 \ mod p.$$

By sequence (2), $x^{3^k-1} \equiv 1 \ \ mod\, p$. We know that $3^k - 1 \neq p - 1$, and by the definition of primitive roots $3^k - 1 \not< p - 1$. Therefore, $3^k - 1 > p - 1$. Since $t = GCD(p - 1, 3^k - 1)$ must satisfy $x^t \equiv 1 \ mod\, p$ (by Theorem1.9). Since $p - 1$ and $3^k - 1$ are always even, then both of them are divisible by 2 (sometimes multiple of 2). But t cannot be

smaller than $p-1$, (since x is primitive). Therefore, t must equal $p-1$. Thus, $3^k - 1 = m(p-1)$ for some positive integer m, which means

$$3^k = m(p-1) + 1,$$

$$k = \log_3(m(p-1)+1). \qquad (3)$$

Note that, m must be positive integer makes $\log_3(m(p-1)+1)$ positive integer as well. Also, Corollary 1.2 shows that $3^k - 1 \equiv p - 1 \ mod\ p$, this means $3^k - 1 = \beta p + p - 1$. Therefore,

$$3^k = \beta p + p,$$

$$3^k = p(\beta + 1),$$

$$k = \log_3 p(\beta+1), \qquad (4)$$

where β is an integer.

Now, suppose that there is r-cycle contain a vertex that is not a primitive root of unity, then

$x^{\alpha} \equiv 1 \ \ mod\ p,$

where $\alpha = ord_p\ x$. Sequence (2) shows that $x^{3^r-1} \equiv 1 \ \ mod\ p$.

It is obvious that $3^r - 1 \neq p - 1$, so we have

$3^r - 1 < p - 1$ or $3^r - 1 > p - 1$,

For both cases $t = gcd(3^r - 1, p-1)$, this satisfies $x^t \equiv 1\ mod\ p$. Since $\alpha | 3^r - 1$ and $\alpha | p-1$, then $t = \alpha$. By Corollary 1.2, if $p - 1 > 3^r - 1$, we have

$p - 1 \equiv 3^r - 1\ mod\ \alpha.$

Therefore,

$p - 1 = q\alpha + 3^r - 1,$

for some positive integer q. Thus,

$$3^r = p - q\alpha,$$

$$r = \log_3(p - q\alpha).$$

If $p - 1 < 3^r - 1$, then we have

$$3^r - 1 \equiv p - 1 \ mod\ \alpha.$$

Therefore,

$$3^r - 1 = q\alpha + p - 1,$$

for some positive integer q. Hence,

$$3^r = q\alpha + p,$$

$$r = \log_3(q\alpha + p). \qquad (5)$$

Note that, when we say a component is a cycle, we mean that there is no vertex v in this component with $indeg\ v$ =0, i.e., situations similar to the example shown in Figure 3.

For the sake of argument, we introduce the following theorem.

Theorem 2.6: Let p be a prime number such that $p \equiv 2\ mod\ 3$, then all components in G_p are cycles.

Proof: Suppose that there is a component with zero in-degree vertex v**,** so by the definition of G_p, this vertex is mapped into its cubic modulo p, i.e., $v \to v^3 \to \cdots \to v^{3^j}$ for some j. Since every path ends with a cycle, this means there is a vertex u on the cycle with $indeg = 2$. A contradiction, because the congruence $x^3 \equiv a\ mod\ p$ has a unique solution when $p \equiv 2\ mod\ 3$. ■

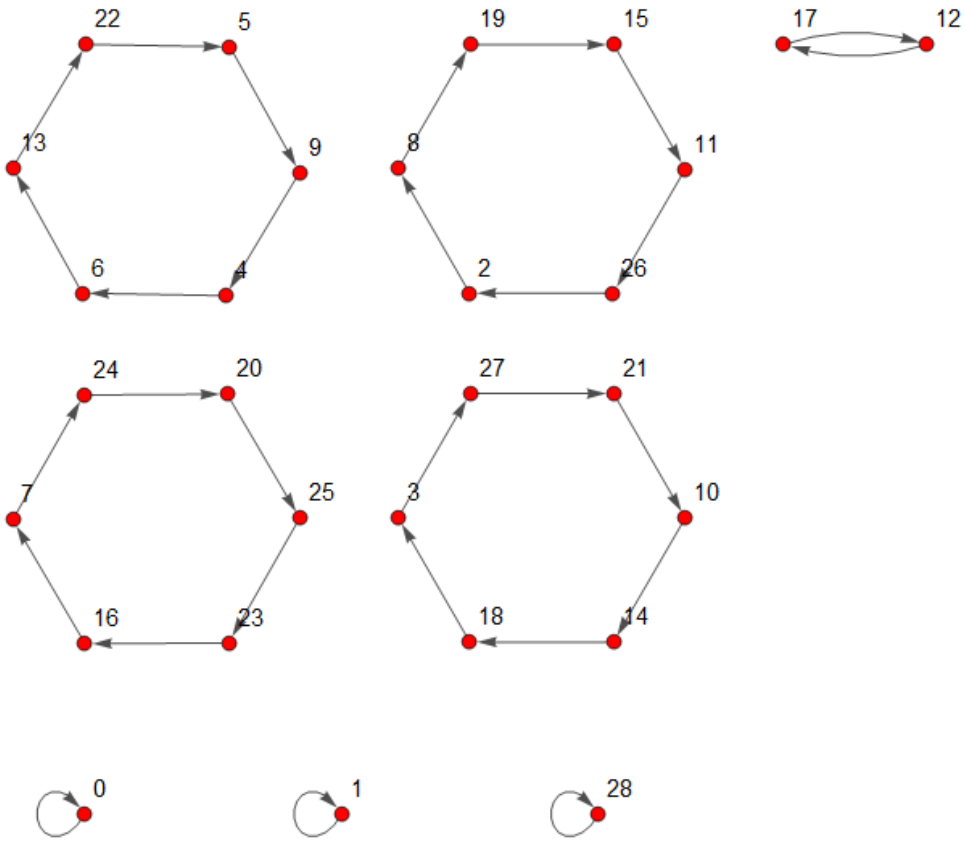

Figure 3: Shown are all the components of G_{29}.

IV. Mathematica Calculations

In this section, we introduce calculations regarding to components of the graphs G_n, $n = 2, 3, \ldots, 90$. The computations accomplished using Mathematica note book and introduced in Table 1. Corresponding to every graph G_n, we refer to the number of components by c_n, the length of longest cycle by l_c and the number of longest cycles by nl_c.

n	c_n	l_c	nl_c
2	2	1	2
3	3	1	3
4	3	1	3
5	4	2	1
6	6	1	6
7	3	1	3
8	5	1	5
9	3	1	3
10	8	2	2
11	5	4	2
12	9	1	9
13	4	2	1
14	6	1	6
15	12	2	3
16	7	2	2
17	8	4	2
18	6	1	6
19	3	1	3
20	12	2	3
21	9	1	9
22	10	4	4
23	7	5	4
24	15	1	15
25	8	4	4
26	8	2	2
27	3	1	3
28	9	1	9
29	8	6	4
30	24	2	6

n	c_n	l_c	nl_c
47	7	11	4
48	21	2	6
49	5	6	2
50	16	4	8
51	24	4	6
52	12	2	3
53	16	6	4
54	6	1	6
55	22	4	10
56	15	1	15
57	9	1	9
58	16	6	8
59	5	28	2
60	36	2	9
61	8	4	4
62	10	4	4
63	9	1	9
64	15	4	4
65	17	2	8
66	30	4	12
67	7	5	4
68	24	4	6
69	21	5	12
70	24	2	6
71	11	12	4
72	15	1	15
73	6	2	3
74	8	2	2
75	24	4	12

31	5	4	2
32	11	2	6
33	15	4	6
34	16	4	4
35	12	2	3
36	9	1	9
37	4	2	1
38	6	1	6
39	12	2	3
40	20	2	5
41	14	4	8
42	18	1	18
43	5	6	2
44	15	4	6
45	12	2	3
46	14	5	8

76	9	1	9
77	15	4	6
78	24	2	6
79	11	3	8
80	30	2	15
81	3	1	3
82	28	4	16
83	13	8	10
84	27	1	27
85	37	4	10
86	10	6	4
87	24	6	12
88	25	4	10
89	16	10	6
90	24	2	6

Table1: Mathematica calculations for $2 \leq n \leq 90$. c_n is number of components, l_c is the length of longest cycle and nl_c is the number of longest cycles, for the graph G_n.

V. Conclusion:

In this work, we proved interesting properties related to the diagraph associated to remainder of cubic mapping modulo n. Our contribution focus on the properties of fixed points and cycles of the digraph G_n. Also, we introduced cycle properties with relations belonging to primitive roots of unity.

References:

[1] Barati Z, Khashyarmanesh K, Mohammadi F, Nafar K. On the associated graphs to a commutative ring. Journal of Algebra and Its Applications. 2012 Apr;11(02):1250037.

[2] Pucanović Z, Petrović Z. On the radius and the relation between the total graph of a commutative ring and its extensions. Publications de l'InstitutMathematique. 2011;89(103):1-9.

[3] J. Skowronek-Kaziów, Zielona Gora, Properties of Digraphs Connected with Some Congruence Relations, Czechoslovak Mathematical Journal, 59 (134) (2009), 39–49.

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

[5] Hamza Daoub, On Digraphs Associated to Quadratic Congruence Modulo n,University Bulletin – ISSUE No.19- Vol. (3) – July – 2017.

[6] Thomas Koshy, Elementary Number Theory with Applications, Elsevier,2nd edition,USA.

[7] Song Y. Yan, Number Theory for Computing, Springer-Verlag Berlin Heidelberg New York, 2nd edition, 2002.

[8] I. Niven, H.S. Zuckerman, H.L. Montgomery, An Introduction to the Theory of Numbers, fifth ed., John Wiley & Sons, New York, 1991.