On Digraphs Associated to Two Quadratic Forms Modulo n

Hamza Daoub [(*)]

Dept. of Mathematics, Faculty of Sciences

Abstract

If $n < \infty$ *is a positive integer,* $R = \mathbb{Z}_n$ *is the ring of integers modulo* n*, with the assumption that on one hand* $G(\mathbb{Z}_n)$ *is a directed graph of the quadratic polynomial,* $x^2 + ax + b = 0 \ mod(n)$*, presented by the mapping* $\varphi_1 : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n \times \mathbb{Z}_n$*, defined as* $\varphi_1(v_1, v_2) = (v_1 + v_2, v_1 v_2)$*. On the other hand,* $\Gamma(\mathbb{Z}_n)$ *is a directed graph of the quadratic congruence* $x^2 + c = 0 \ mod(n)$*, presented by the mapping* $\varphi_2 : \mathbb{Z}_n \to \mathbb{Z}_n$ *given by* $\varphi_2(v) = v^2$*. We investigate the*

(∗) Email: h.daoub@zu.edu.ly

relationship between G and Γ, supporting the study with computer computations using Wolfram Mathematica software.

***Keywords**: Digraphs, Commutative Ring, Cycle Length, Quadratic Congruence, Quadratic Polynomial.*

1. Introduction

The study of associations between directed graphs and finite commutative rings has been growing interest for the last few decades. In 1996 Rogers' published paper [7] concerned the graph of the square mapping on the prime fields, which was a topic appended as a kind of postscript to his talks on discrete dynamical systems. In 1967, Bryant [13] employed quadratic digraphs and enumerated isomorphic subgroups of a finite group. Incidentally, Lipkovski investigated properties of a digraph representing quadratic polynomials with coefficients modulo n. Later, Christopher Ang and Alex Schulte published a paper [3] concerned the structure of the sources in directed graphs of commutative rings with identity, with special concentration in the finite and reduced cases. However, the association between the ring $\mathbb{Z}_n$ and digraphs is related to elementary number theory. For algebraic and number-theoretic notions used here, see [2], [8], [9]).

Specifically, our study highlights the relationship between the theoretic properties of the Quadratic forms $x^2 + c = 0\ (mod\ n)$ and $x^2 + ax + b = 0\ \ (mod\ n)$ with coefficients from finite ring $\mathbb{Z}_n$.

We denote cycles of length greater than one in both digraphs by $\overrightarrow{C_k}$, and cycles of length 1 are considered as loops. Furthermore, we will refer to $\mathbb{Z}_n$, $\mathbb{Z}_p$ and $\mathbb{Z}_q$ as sets of natural numbers, for some primes p and q.

2. Basic Concepts

In number theory, an integer α is called a quadratic residue of n, if the congruence $x^2 \equiv \alpha \ (mod \ n)$ has a solution. If there is no solution, then a is called a quadratic nonresidue of n.

To decide whether a number α is a square $mod \ n$, it suffices to decide it is mod powers of primes dividing n.

Theorem 2.1. Let $n = p_1^{e^1} p_2^{e^2} \dots p_r^{e^r}$. Then the number α is a square $mod \ n$ iff there are numbers $x_1, x_2, \dots, x_r$ such that

$$x_1^2 \equiv \alpha \,(mod \ \ p_1^{e^1})$$
$$x_2^2 \equiv \alpha \,(mod \ \ p_2^{e^2})$$
$$\vdots$$
$$x_r^2 \equiv \alpha \,(mod \ \ p_r^{e^r})$$

Proof: See Reference [10]. ■

Theorem 2.2. If n is an odd prime, $(\alpha, p) = 1$ and α is a quadratic residue of n, then the congruence $x^2 \equiv \alpha \ (mod \ n)$ has exactly two roots.

Proof: See Reference [12]. ■

Corollary 2.1. Let n be prime, the congruence

$$x^2 \equiv 1 \ (mod \ n)$$

has only the solutions $x = \pm 1 \ (mod \ n)$.

Proof: See Reference [5]. ■

Corollary 2.2. The equation $x^2 \equiv \alpha \ (mod \ n)$ has no solution if and only if $\alpha^{\frac{(n-1)}{2}} \equiv -1 \ (mod \ n)$.

The ***Euler*** $\phi(n)$ of a positive integer n is the number of all nonnegative integers b less than n which are prime to n. It is clear to see that $\phi(1) = 1$ and $\phi(n) = n - 1$, for any prime n.

Euler's function ϕ has the property that $\phi(n)$ is the order of the group $U(n)$ of units of $\mathbb{Z}_n$.

Proposition 2.1. (Fermat's Little Theorem). Let n be a prime. Any integer α satisfies $\alpha^n \equiv \alpha \, mod \, n$, and any integer α not divisible by n satisfies $\alpha^{n-1} \equiv 1 \, mod \; n$.

Proof: See Reference [4].

Proposition 2.2. Let n be any odd prime number, if $d|(n-1)$, then $x^d \equiv 1 \; mod \; n$ has exactly d solutions.

Proof: See Reference [11]. ■

In ring theory it is well known that, an element x of R is called ***nilpotent*** if there exists an integer $m \geq 0$ such that $x^m = 0$. An ***idempotent*** element of a ring is an element x such that $x^2 = x$.

Proposition 2.3. If x is an idempotent, then $y = 1 - x$ is also idempotent.

In graph theory, ***a walk*** of length k in G is a sequence of vertices $v_0, v_1, \ldots, v_{k-1}$ of G such that for each $i = 1, 2, \ldots, k-1$, the edge e_i has tail v_{i-1} and head v_i. A walk is closed if $v_0 = v_{k-1}$. ***A path*** in G is a walk in which all the vertices are distinct.

A ***cycle*** is a closed walk, where $v_0 = v_{k-1}$ and the vertices $v_0, v_1, \ldots, v_{k-1}$ are distinct from each other, thus the definition of length is still applicable.

The outgoing (incoming) degree of a vertex v is the number of arrows going out (coming in) this vertex.

A homomorphism of G to H, is a mapping $f: V(G) \rightarrow V(H)$ from G to H, such that it preserves edges, that is, if for any edge (u, v) of G, $(f(u), f(v))$ is an edge of H. We write simply $G \rightarrow H$.

If f is homomorphism of G to H, then the digraph with vertices $f(v)$, $v \in V(G)$, and edges $f(v)f(w), vw \in E(G)$ is a homomorphic image of G. Note that $f(G)$ is a subgraph of H, and that $f: G \to f(G)$ is a surjective homomorphism.

In particular, homomorphisms of G to H map paths in G to walks in H, and hence do not increase distances (the minimum length of the paths connecting two vertices).

Corollary 2.3 A mapping $f: V\left(\overrightarrow{C_k}\right) \to V(G)$ is a homomorphism of $\overrightarrow{C_k}$ to G if and only if $f(1), f(2), \ldots, f(k)$ is a cycle in G.

3. Digraphs associated to $x^2 + ax + b = 0 \mod(n)$

This kind of association between digraphs and finite rings has been studied and proposed previously [1], [6]. However, further properties and results are presented here using only the finite commutative ring $R = \mathbb{Z}_n \times \mathbb{Z}_n$. Some results are quoted from [6], [2] for the sake of completeness.

Let $n < \infty$ be a natural number. Define the mapping $\varphi_1: \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n \times \mathbb{Z}_n$ by $\varphi_1(a, b) = (a + b, a.b)$. Since $\mathbb{Z}_n$ is finite, so φ_1 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_1.

Since φ_1 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 solution of this polynomial is associated to the characteristic of $\mathbb{Z}_n$, which 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 more than a solution.

Since $\mathbb{Z}_n$ is a field for a prime number n, a polynomial of the form $x^2 - ax + b \in \mathbb{Z}_n[x]$ is reducible if and only if there exist $c, d \in \mathbb{Z}_n$ so that, $x^2 - ax + b = (x - c)(x - d)$. There are $\binom{n}{2}$ such polynomials for which $c \neq d$, and n for which $c = d$. Therefore, there are exactly

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

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

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

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

In $G(\mathbb{Z}_n)$, the starting vertices (a, b) (with incoming degree 0) correspond to irreducible quadratic polynomials $x^2 - ax + b$ in $\mathbb{Z}_n[x]$. This gives us a rough upper estimate for the number of components of graph $G(\mathbb{Z}_n)$, that is $c_n \leq \frac{n(n-1)}{2}$.

Proposition 3.1. The incoming degree of the vertex $(a, b) \in G$ equals the number of distinct roots of the quadratic polynomial $x^2 - ax + b \in \mathbb{Z}_n[x\ ]$.

***Proof**: See reference* [6]. ■

In the case of G_n for prime n, the incoming degree of a vertex (a, b) can be either 0 (if $x^2 - ax + b$ is irreducible, i.e., $0 = 4b - a^2 \in \mathbb{Z}_n$ is a quadratic nonresidue modulo n), or 1 (if $4b - a^2 = 0$), or 2 (if $4b - a^2 = 0$ is a quadratic residue modulo n).

In the case of G_n for nonprime n, the incoming degree of a vertex (a, b) can be greater than 2, which depends on the different factorizations of $x^2 - ax\ + b$.

Let $\mathrm{N}(n)$ denote the number of solutions of $x^2 - ax + b = 0 \ mod\, n$. If $n = p^{n_1}p^{n_2}\ldots p_k^{n_k}$ is the prime decomposition of n, then $\mathrm{N}(n) = \mathrm{N}(p^{n_1})\mathrm{N}(p^{n_2})\ldots\mathrm{N}(p_k^{n_k})$. Since the incoming degree of a vertex (a, b) is the number of roots of the quadratic polynomial $x^2 - ax + b = 0 \ \ mod\, n$, then we have the following.

Theorem 3.1. *Let $p_1, p_2, \ldots, p_k$ be the prime component of the number n. Then the highest degree of a vertex (a, b) in the graph $G(\mathbb{Z}_n)$ is less than or equal to 2^k.*

Proof. Let $x^2 - ax + b = 0$ be a reducible quadratic polynomial over $\mathbb{Z}_n$. From Theorem 2.2, we have

$$deg(a, b) = 2 \times 2 \times\ldots\times 2 \ (k \ \ times) = 2^k. \ ■$$

Consider closed paths, or cycles, in G. Up to cyclic permutations, the loops are described by the corresponding arrow sequences:

The sequence

$$(a_1 , b_1) \ \rightarrow \ (a_2 , b_2) \ \rightarrow \cdot\cdot\cdot \rightarrow \ (a_k , b_k) \qquad (3.1)$$

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 $(a_i + b_i , a_i\, b_i) = (a_j , b_j)$ for all $j \leq \ i \ < \ k$.

Note that there may exist loops as well as $k - cycles$. The definition also implies that if $k > 1$, then every $b_i \neq 0$.

Proposition 3.2. i) There are exactly $n \ = \ \# \, \mathbb{Z}_n$ loops in G, and they correspond to the vertices $(a, 0)$.

ii) Each connected component of G contains exactly one cycle, and the number of connected components is $n + \#\{k - cycles\}$.

Proof: *See reference* [6]. ■

In Figure 1 we note that loops correspond to the vertices $(a, 0)$.

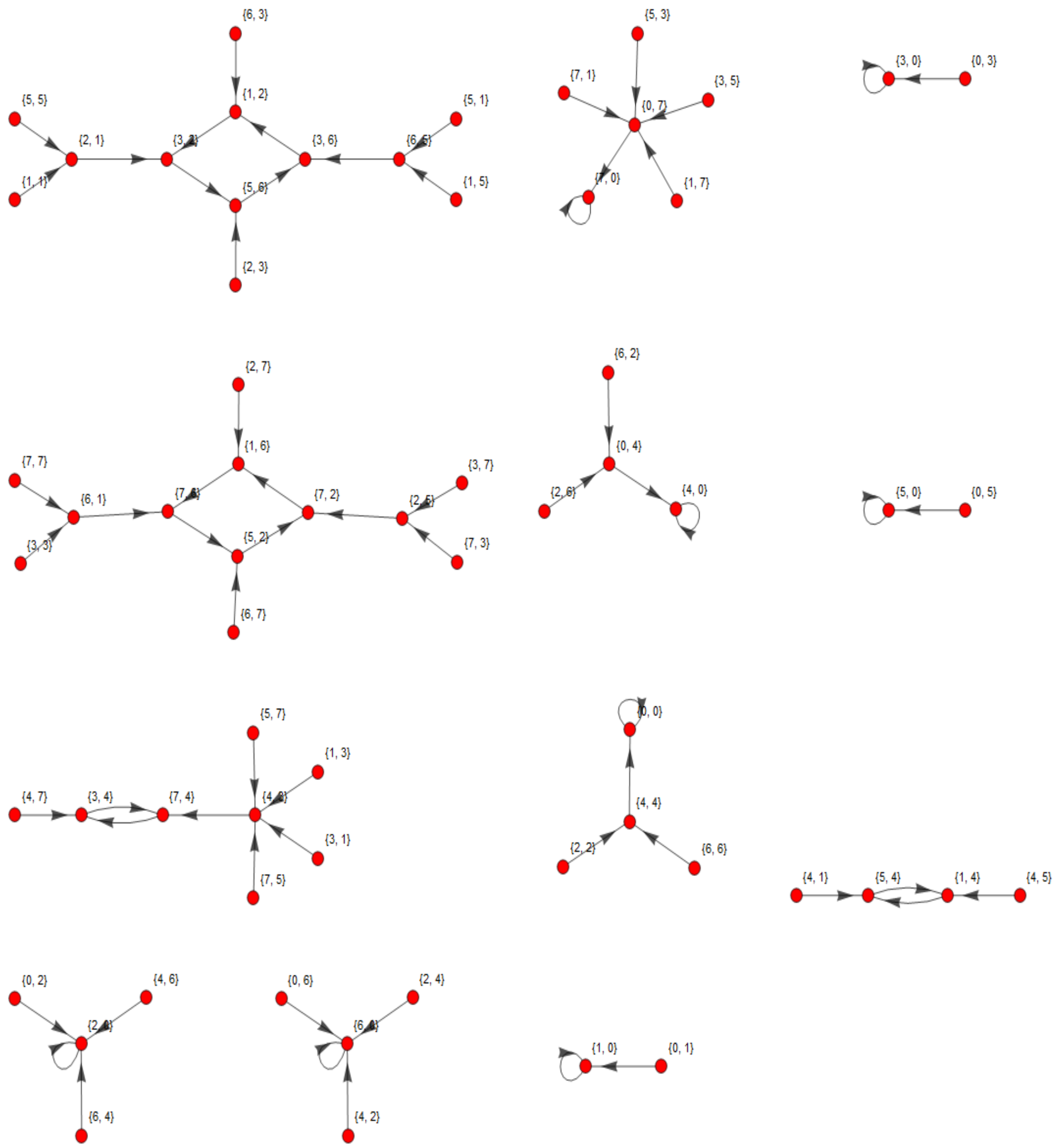

Figure 1: Shown is $G(\mathbb{Z}_8)$

4. Digraphs associated to $\boldsymbol{x^2 + \mathrm{c} = 0 \mod(n)}$

For an integer number $n < \infty$, define a mapping $\varphi_2 : \mathbb{Z}_n \to \mathbb{Z}_n$ by $a \mapsto a^2$. This mapping can be interpreted as directed graph $\Gamma(\mathbb{Z}_n)$, whose vertex set is $\mathbb{Z}_n$ and arrows defined by φ_2 .

Let p and q be relatively prime numbers, such that $n = pq,\ p < q$. Define a map $f_1 : \mathbb{Z}_n \to \mathbb{Z}_p$ that maps representatives $0 \leq a < n$ in $\mathbb{Z}_n$ to $(a \ mod \ p)$ in $\mathbb{Z}_p$. Since p divides n, then f_1 is a homomorphism. Similarly, the same holds for $f_2 : \mathbb{Z}_n \to \mathbb{Z}_q$.

Observe that mappings f_1 and f_2 induce mappings of corresponding graphs, which will be denoted again by f_1 and f_2.

Since φ_2 is a function, so it is clear that the outgoing degree of each vertex is one. The question here is what the incoming degree of the vertex v is.

The digraphs structure related to the quadratic form $x^2 + \mathrm{c} = 0 \mod(n)$ were investigated, and proposed in [12].

Proposition 4.1. The incoming degree of the vertex $v \in \Gamma$ equals the number of distinct roots of the quadratic polynomial $x^2 - v \in \mathbb{Z}_n[x]$.

Proof: *See reference* [12]. ■

In the case of $\Gamma(\mathbb{Z}_n)$ for nonprime n, the incoming degree of a vertex v can be greater than 2, which depends on the different factorizations of $x^2 - v$.

Theorem 4.1. Let $p_1, p_2, \ldots, p_k$ be the composition of the number n, then the highest degree of a vertex v in the graph $\Gamma(\mathbb{Z}_n)$ is less than or equal to 2^k.

Proof: Let $x^2 - v = 0$ be a reducible quadratic polynomial over $\mathbb{Z}_n$. From Theorem 2.2, we have

$$deg(v) = 2 \times\ 2 \times \ldots \times 2 \quad (k - times) = 2^k ■$$

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

Consider closed paths, or cycles, in Γ. The cycles are described by the corresponding arrow sequences.

The sequence

$$v \to v^2 \to \cdots \to v^{2^k} \qquad (4.1)$$

of arrows in Γ defines a cycle of length k (or a *k-cycle*) if $\varphi_2(v^{2^k}) = v$ and $\varphi_2\left(v^{2^i}\right) \neq v^{2^j}$ for all $j \leq i < k$.

In Figure 2, there may exist loops and longer cycles. Also, some graphs Γ_n do contain a loop with incoming degree one as a (weakly) connected component and some do not.

The following Proposition shows the essential loops in $\Gamma(\mathbb{Z}_n)$.

Proposition 4.2. i) If $\mathbb{Z}_n$ is a domain, then there are exactly $n = 2$ loops in Γ, and they correspond to the vertices 0, 1.

ii) If $\mathbb{Z}_n$ is not a domain, then there are $n = \#\ \{x \in \mathbb{Z}_n : x = x^2\}$ cycles of length 1 in Γ.

iii) Each connected component of Γ contains exactly one cycle or loop, and the number of connected components is $\#\ \{x \in \mathbb{Z}_n : x\ is\ an\ idempotent\} + \#\{$cycles of length greater than one$\}$.

Proof: i) It is clear that if $\mathbb{Z}_n$ is a domain, then the solution of the congruence $x^2 \equiv x\ mod\ n\, is\ 0, 1$. Therefore, there are exactly $n = 2$ cycles of length 1 in Γ.

ii) if $\mathbb{Z}_n$ is not a domain, then the solution of the congruence $x^2 \equiv x\ mod\ n$ is $S = \{x \in \mathbb{Z}_n :\ x\ is\ an\, idempotent\}$. Note that the set S is not empty, because $\{0, 1\} \subseteq S$.

iii) According to definition 4.1 every component must end with a cycle(loop). Thus (3) follows. ■

In Figure 2 we note that 2, 4, 6 are zero-divisors, while 3, 5, 7 are multiplicative inverse of their selves.

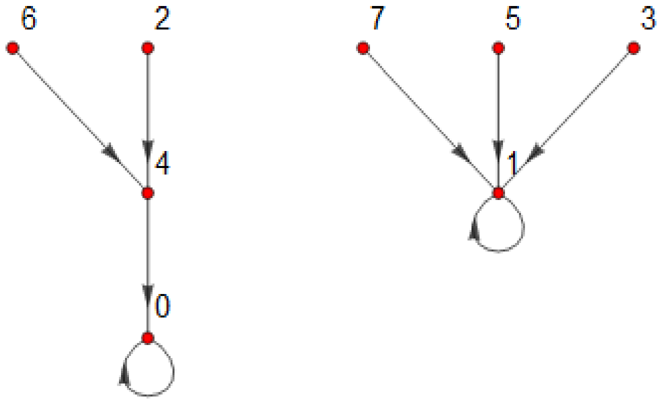

Figure 2: $\Gamma(\mathbb{Z}_8)$

Since a closed walk might be a cycle, so according to the structure of f_1, f_2, sequence 4.1, and Corollary 2.3 we conclude that a closed walk, which is mapped by f_1 (f_2) is a cycle.

The following Proposition presents a relation between cycles in commutative rings $\mathbb{Z}_n$, and $\mathbb{Z}_p$ as long as $p|n$.

Proposition 4.3. Let $\overrightarrow{C_\alpha}$ and $\overrightarrow{C_\beta}$ be two directed cycles in $G(\mathbb{Z}_n)$ and $G(\mathbb{Z}_p)$ respectively. If $\overrightarrow{C_\alpha} \mapsto \overrightarrow{C_\beta}$, then β divides α.

Proof: See reference [12]. ■

5. The relation between the two quadratic forms

When we consider the solution of a reducible quadratic polynomial $x^2 + ax + b \equiv 0 \ (mod \ n)$, we have then $x^2 + ax + b = (x + v_1)(x + v_2)$, where $a = v_1 + v_2, b = v_1 v_2$. The formula uses the two arithmetic operations, addition and multiplication, and also a square root. The new operation here is the square root of the discriminate. This quadratic polynomial has at least two roots, which are not related in many cases. Therefore, the vertices in $G(\mathbb{Z}_n)$ are defined to be the Cartesian product of the ring $\mathbb{Z}_n$.

To solve a congruence $x^2 + c \equiv 0\ (mod\ \ n)$, we need to realize whether c is a quadratic residue. If c is a quadratic residue, then the quadratic congruence has two related roots. Hence, the vertices in $\Gamma(\mathbb{Z}_n)$ are defined to be the set $\mathbb{Z}_n$.

In the graph $G(\mathbb{Z}_n)$, if (v_1, v_2) is a starting vertex (a vertex with zero-indegree) such that v_1 is additive inverse to v_2, then a must equal to zero, thus $x^2 + ax + b = x^2 + b = 0\ \ (mod\, n)$. Therefore, $x^2 \equiv n - b\ (mod\ \ n)$. This quadratic polynomial is solvable and its solution is $x = n - v_1, x = n - v_2$, where $b = v_1 v_2$, and $v_1 + v_2 = 0$. If we map components which have starting vertex (v_1, v_2) with the property $v_1 + v_2 = 0$ by the second projection mapping $\pi_2 \colon \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ defined by $\pi_2(x, y) = y$, we get a component in $\Gamma(\mathbb{Z}_n)$ with $n - b$ vertices. When we replace the vertices by their complements, we get the graph $\Gamma(\mathbb{Z}_n)$.

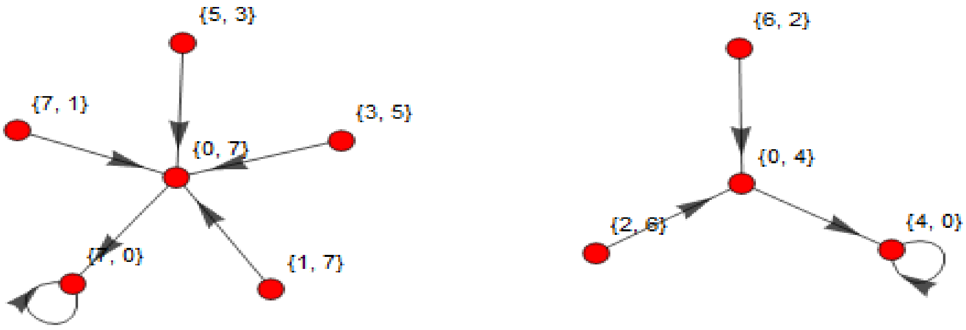

Figure 3: Part of $\mathbf{G}(\mathbb{Z}_8)$

For instance, in Figure 3 if we use the second projection mapping π_2 for these two components we get digraphs shown in Figure 4:

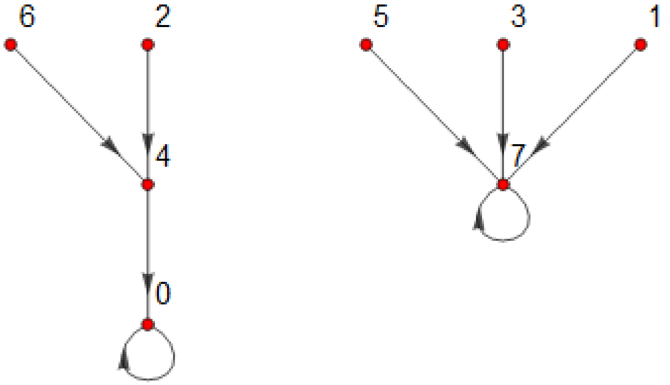

Figure 4: Part of $\mathbf{G}(\mathbb{Z}_8)$ mapped by $\boldsymbol{\pi_2}$

Replace vertices with their complements to get digraphs shown in Figure 5:

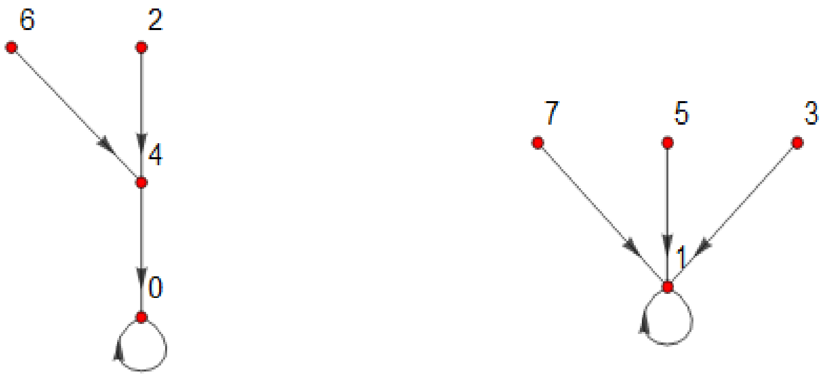

Figure 5: $\boldsymbol{\Gamma}(\mathbb{Z}_8)$

<u>References</u>

[1] Wei, Yangjiang, and Gaohua Tang. "The iteration digraphs of finite commutative rings." Turkish Journal of Mathematics 39.6 (2015): 872-883.

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

[3] Ang, Christopher, and Alex Shulte. "Directed Graphs of Commutative Rings with Identity." Rose-Hulman Undergraduate Mathematics Journal 14.1 (2013).

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

[5] Kraft, James S., and Lawrence 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.

[7] Rogers, Thomas D. "The graph of the square mapping on the prime fields." Discrete Mathematics 148.1-3 (1996): 317-324.

[8] Niven, Ivan, Herbert S. Zuckerman, and Hugh L. Montgomery. An introduction to the theory of numbers. John Wiley & Sons, 2008.

[9] Bell, E. T. "GH Hardy and EM Wright, An Introduction to the Theory of Numbers." Bulletin of the American Mathematical Society 45.7 (1939): 507-509.

[10] Childs, Lindsay N. A concrete introduction to higher algebra. New York: Springer, 2009.

[11] Ireland, Kenneth, and Michael Rosen. A classical introduction to modern number theory. Vol. 84. Springer Science & Business Media, 2013.

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

[13] S. Bryant, Groups, graphs, and Fermat's last theorem, Am. Math. Monthly, 74 (1967), 152–155.