On Digraphs Associated to Quadratic Congruence Modulo n

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

Abstract:

For a finite commutative ring A, the mapping $\varphi: A \to A$ defined by $a \mapsto a^2$ could be interpreted as directed graph $G = G(A)$, whose vertex set is A and arrows defined by φ. We invistigate the graph properties of G from the ring $\mathbb{Z}_n$of integers modulo n. Mathematica notebook is used to calculate and display the associated graph of certain rings.

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

1.Introduction.

In recent years, there has been growing interest in the digraphs associated with the ring $\mathbb{Z}_n$, More specificaly (e.g [6], [1]). 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. Subsequently, Yangjiang WEI and Gaohua TANG generalized some previous results of the iteration digraphs from the ring $\mathbb{Z}_n$ to finite commutative rings. Incidentally, Lipkovski investigated properties of a digraph representing quadratic polynomials with coefficients modulo n. Later, Christopher Ang and Alex Schulte published 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. In the present paper, however, a related connection between finite rings and digraphs is studied. This also has connections to elementary number theory. For an algebraic and number-theoretic notions used here, see [2], [8], [9]).

Let A be a finite commutative ring with unity (ring for short). Define a mapping $\varphi : A \rightarrow A$ by $a \mapsto a^2$. One can interpret this mapping as directed graph $G = G(A)$, whose vertex set is A and arrows defined by φ . The main idea is to deduce, if possible, ring properties of A from graph properties of G (e.g., the number of components, the lengths of longest paths and longest loops, the maximal degree of vertices, etc.).

When we consider the solution of a quadratic congruence $ax^2 + bx + c \equiv 0 \ (mod \ n)$. The quadratic formula gives two roots. It uses the four arithmetic operations, addition, subtraction, multiplication and division, and also a square root. The new operation here is the square root of the discriminate.

To solve a congruence $x^2 \equiv r\ (mod\ n)$, one solves the same congruence modulo each prime power factor of n and combines the solutions using the Chinese Remainder Theorem. The real difficulty concerning with solving $x^2 \equiv r\ (mod\ p)$ when p is prime.

Specifically, our study offers the chance to study the interplay between the theoretic properties of the Quadratic congruence $x^2 \equiv r\ (mod\ n)$ in the finite commutative ring of integers $\mathbb{Z}_n$ and the theoretic properties of the related $G = G(\mathbb{Z}_n)$.

2. Background:

It is well known in number theory that, For any a, b in $\mathbb{Z}_n$, 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 2.1. 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.

Definition 2.2. Suppose that $(a, m) = 1$. Then a is called a quadratic residue of m, if the congruence $x^2 \equiv a\ (mod\ m)$ has a solution. If there is no solution, then a is called a quadratic nonresidue of m.

Since the derivative of x^2 is $2x$, and $2x \equiv 0\ (mod\ 2)$ we have to distinguish between the cases $p = 2$ and p odd prime.

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

Theorem 2.1. Let p be an odd prime, and $(a,p) = 1$. Then there is a solution of $x^2 = a\ (mod\ p^e)$, $e > 1$, if and only if there is a solution of $x^2 = a\ (mod\ p)$.

Proof: See Reference [10]

Theorem 2.2. Let $m = p_1^{e^1} p_2^{e^2} \dots p_r^{e^r}$. Then the number a is a square $mod\ m$ iff there are numbers $x_1, x_2, \dots, x_r$ such that

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

Proof: See Reference [10].

Theorem 2.3. If p is an odd prime, $(a,p) = 1$ and a is a quadratic residue of p, then the congruence $x^2 \equiv a\ (mod\ p)$ has exactly two roots.

Proof: This quadratic congruence has at least one root c. Therefore, $-c$ is a root too, and $c \not\equiv -c\ (mod\ p)$. We know that a congruence $f(x) \equiv 0\ (mod\ p)$ of degree n has at most n solutions. Thus, there can not be more than two roots.

Corollary 2.1. Let p be prime. The congruence

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

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

Proof: See Reference [5].

Theorem 2.4. Let p be an odd prime. Then there are exactly $(p - 1)/2$ incongruent quadratic residues of p and exactly $(p-1)/2$ quadratic nonresidues of p.

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

Definition 2.3. An element x of R is called nilpotent if there exists an integer $m \geq 0$ such that $x^m = 0$.

Definition 2.4. An idempotent element of a ring is an element x such that $x^2 = x$.

One can also conclude that idempotent elements satisfy $x = x^2 = x^3 = x^4 = \ldots = x^n$ for any positive integer n. However, 0 and 1 are the only idempotents in a domain.

Proposition 2.1. If x is an idempotent, then $y = 1 - x$ is also idempotent.

Proof: Observe that, $y^2 = (1-x)^2 = 1 - 2x + x^2 = 1 - x = y$.

Definition 2.5. Let n be a positive integer. The Euler $\phi(n)$ 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 $\phi(p) = p - 1$, for any prime p.

Proposition 2.2.(*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 Reference [4].

Proposition 2.3. If $g.c.d(a, m) = 1$, then $a^{\phi(m)} = 1 \ (mod\ m)$.

Proof: See Reference [4]..

Proposition 2.4. lf $d|(p-1)$, then $x^d \equiv 1\ (mod\ p)$ has exactly d solutions.

Proof: See Reference [12].

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

Definition 2.6. The Carmichael function of a positive integer n, denoted $\lambda(n)$, is the smallest positive integer m such that $a^m \equiv 1 \ (mod\ n)$ for every integer a that is coprime to n.

We introduce some properties of Carmichael lambda function for the sake of completeness.

Proposition 2.3. (a) If $n = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$ where $p_1, p_2, \ldots, p_r$ are distinct primes and $a_1, a_2, \ldots, a_r > 0$, then $\lambda(n) = lcm(\lambda(p_1^{a_1}), \lambda(p_2^{a_2}), \ldots, \lambda(p_r^{a_r})$.

(b) If p is an odd prime and $a > 0$, then $\lambda(p^a) = \phi(p^a) = p^{a-1}(p-1)$.

(c) $\lambda(2) = 1, \lambda(4) = 2$, and for $a \geq 3$, we have $\lambda(2^a) = 2^{a-2} = \frac{\phi(2^a)}{2}$.

It immediately follows from Proposition 2.5 that

$$\lambda(n) | \ \phi(n)$$

for all n and that $\lambda(n) \ = \phi(n)$ if and only if $n \in \{1,2,4, q^k, 2q^k\}$, where q is an odd prime and $k \geq \ 1$.

Theorem 2.5.(***Chinese Remainder Theorem***). Assume that $m_1, \ m_2, \ldots, m_r$ are positive integers that are pairwise relatively prime (that is, $gcd(m_i, m_j) \ = \ 1$if $i \neq \ j$). Then the system of congruences

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

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

Proof: See Reference [5].

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.

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

A homomorphism of G to H, is a mapping $f: V(G) \to V(H)$ 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 $G \to H$.

If f is any 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).

3. Main Results:

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 $(a \bmod p)$ 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.

We will denote to cycles in $G(\mathbb{Z}_n)$ by $\overrightarrow{C_k}$. Furthermore, we will refer to $\mathbb{Z}_n$, $\mathbb{Z}_p$ and $\mathbb{Z}_q$ as sets of natural numbers.

3.1 Degrees of Vertices. In this work, we consider the degrees of vertices in $G(\mathbb{Z}_n)$. As usual, the outgoing (incoming) degree of a vertex v is the number of arrows going out (coming in) this vertex. Since φ 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.

Proposition 3.1. The incoming degree of the vertex $a \in G$ equals the number of distinct roots of the quadratic polynomial $x^2 - a \in A[X]$.

Proof: If there is an arrow $x \to a$, then $x^2 = a$, and by Theorem 2.3 we deduce that the solutions are roots of this polynomial. Conversely, if x is a root of this polynomial, then there is an arrow $x \to a$, and for distinct roots such arrows are also distinct. In fact, if $x_1, \ldots, x_k$ are all the distinct roots of the polynomial, then $x_i^2 = a$.

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

Theorem 3.1. 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 $G(\mathbb{Z}_n)$ is less than or equal to 2^k.

Proof: Let $x^2 - a = 0$ be an reducible quadratic polynomial over $\mathbb{Z}_n$. From Theorem 2.3, we have

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

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

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

Definition 3.1. The sequence

(3.1)
$$a \to a^2 \to \cdots \to a^{2^k}$$

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

We see from figures in Section 5 that there may exist loops (In this work, loops are cycles of length 1) as well as longer cycles. Also, some graphs G_n do contain loop with incoming degree one as a (weakly) connected component and some do not.

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

Proposition 3.2. 1) If $\mathbb{Z}_n$ is a domain, then there are exactly $n = 2$ loops in G_n, and they correspond to the vertices 0, 1.

2) If $\mathbb{Z}_n$ is not a domain, then there are $n = \#\ \{x \in \mathbb{Z}_n : x\ is\ idempotent\}$ loops in G.

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

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

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

3) According to definition 3.1 every component must end with a cycle(loop). Thus (3) follows.

According to Proposition 2.1, we can say that the number of loops in a graph $G(\mathbb{Z}_n)$ is even. However, Definition 3.1 shows that *k-cycles* follow the rule of solving the congruence $x^{2^k} \equiv x \bmod n$, which means

$$x^{2^k} - x \equiv 0 \ (mod\ n)$$

$$x\left(x^{2^k-1} - 1\right) \equiv 0 \ (mod\ n).$$

When n is a prime number, then $\mathbb{Z}_n$is a field, which means there are no zero divisors. Therefore, $x \equiv 0 \ (mod\ n)$ or $(x^{2^k-1} - 1) \equiv 0 \ (mod\ n)$. Since $x = 0$ is an idempotent, so it can not be in a *k-cycle*. If $\left(x^{2^k-1} - 1\right) \equiv 0 \ (mod\ n)$, then $x^{2^k-1} \equiv 1 \ (mod\ n)$. Referring to ***Fermat Little Theorem*** we have

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

But 2^k can not be a prime number. Thus we have two cases:

Case I. If $2^{k-1} < \lambda(n)$ then $2^{k-1} \mid \lambda(n)$. That is, the orders of primitive roots of unity in the ring of integers modulo n are divisors of $\lambda(n)$.

Case II. If $2^{k-1} > \lambda(n)$ then, $x^{2^k-1-\lambda(n)} \equiv 1 \ (mod\ n)$. Furthermore, $x^{2^k-1-2\lambda(n)} \equiv 1 \ (mod\ n)$ and so on. In fact $t = GCD(x^{2^k-1}, \lambda(n))$ satisfies $x^t \equiv 1 \ (mod\ n)$. So, $x^{t+1} \equiv x \ (mod\ n)$.

Proposition 2.4 shows us that the cycles in $G(\mathbb{Z}_n)$ can be determined, the number d presents the number of vertices satisfy $x^d \equiv 1 \ (mod\ n)$. Therfore we have d distinct vertices consist a cycle in this graph. However, we know that $x = 1$ is hold. Thus there is a cycle of length $d - 1$in $G(\mathbb{Z}_n)$. Therefore, cycles in $G(\mathbb{Z}_n)$ can be determined that way.

A closed walk might be a cycle, so according to the structure of f_1, f_2 and the sequence 3.1, we have the following:

Corollary 3.1. A mapping $f: V(\overrightarrow{C_k}) \to V(G)$ 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.

From last Corollary we conclude, a closed walk, which is mapped by $f_1(f_2)$ is a cycle. This consequence will be used in this work from now on.

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

Proposition 3.3. 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 we have β divides α.

Proof: Suppose that $\overrightarrow{C_\alpha}$ is a $\alpha - cycle$; that is, $a_1 \to a_2 \to \ldots \to a_\alpha$. Since f_1 is a homomorphism, then

$$f_1(a_1), \to f_1(a_2) \to \ldots \to f_1(a_\alpha)$$

is a cycle in $G(\mathbb{Z}_p)$, and

$$\begin{aligned} f_1(a_1) &= f_1(a_\alpha^2), \\ &= f_1(a_\alpha) f_1(a_\alpha), \\ &= \left(f_1(a_\alpha)\right)^2 \end{aligned}$$

Since f_1 connects q elements in $\mathbb{Z}_n$ into every element $a \in \mathbb{Z}_p$, so that gives us two cases:

Case I. If $f_1(a_1) = f_1(a_2)$. Then by sequence 3.1, this process will be repeated for all $f_1(a_i), i = 2, \ldots, \alpha$. Hence α is divisible by .

Case II. If $f_1(a_1) = f_1(a_j)$, for some $2 < j < \alpha$. Then $f_1(a_i)$, $i < j$ are all different. So according to sequence 3.1 $\alpha = t.\beta$, for $1 \leq t < \alpha$. Hence α is divisible by .

4. Computer Calculation:

Mathematica notebook is used to calculate the graph properties of $G(\mathbb{Z}_n)$ for $2 \leq n \leq 100$ such as, number of components, number of longest cycles, and length of longest cycle. Furthermore, basic number theoritic functions are computed to support the study. However, the case $n = 1$ is omitted, because it is trivial.

From the results in Table 1 and Table 2 one can note the following:

I. The smallest number of components is 2, because 0 and 1 are idempotents included in $\mathbb{Z}_n$.

II. In the digraph $G(\mathbb{Z}_n)$which has unique longest cycle $\lambda(n) = \phi(n)$.

Table 1. Table of results for $2 \leq n \leq 50$

n	Number of Cycles	Length of Longest Cycle	Number of Longest Cycles	$\lambda(n)$	$\phi(n)$
2	2	1	2	1	1
3	2	1	2	2	2
4	2	1	2	2	2
5	2	1	2	4	4
6	4	1	4	2	2
7	3	2	1	6	6
8	2	1	2	2	4
9	3	2	1	6	6
10	4	1	4	4	4
11	3	4	1	10	10
12	4	1	4	2	4
13	3	2	1	12	12
14	6	2	2	6	6
15	4	1	4	4	8
16	2	1	2	4	8
17	2	1	2	16	16
18	6	2	2	6	6
19	4	6	1	18	18

n	Number of Cycles	Length of Longest Cycle	Number of Longest Cycles	$\lambda(n)$	$\phi(n)$
20	4	1	4	4	8
21	6	2	2	6	12
22	6	4	2	10	10
23	3	10	1	22	22
24	4	1	4	2	8
25	3	4	1	20	20
26	6	2	2	12	12
27	4	6	1	18	18
28	6	2	2	6	12
29	4	3	2	28	28
30	8	1	8	4	8
31	6	4	3	30	30
32	2	1	2	8	16
33	6	4	2	10	20
34	4	1	4	16	16
35	6	2	2	12	24
36	6	2	2	6	12
37	4	6	1	36	36
38	8	6	2	18	18
39	6	2	2	12	24
40	4	1	4	4	16
41	3	4	1	40	40
42	12	2	4	6	12
43	7	6	2	42	42
44	6	4	2	10	20
45	6	2	2	12	24
46	6	10	2	22	22
47	4	11	2	46	46
48	4	1	4	4	16
49	7	6	2	42	42
50	6	4	2	20	20

Table 2. Table of results for $51 \leq n \leq 100$

n	Number of Cycles	Length of Longest Cycle	Number of Longest Cycle	$\lambda(n)$	$\phi(n)$
51	4	1	4	16	32
52	6	2	2	12	24
53	3	12	1	52	52
54	8	6	2	18	18
55	6	4	2	20	40
56	6	2	2	6	24
57	8	6	2	18	36
58	8	3	4	28	28
59	3	28	1	58	58
60	8	1	8	4	16
61	6	4	3	60	60
62	12	4	6	30	30
63	10	2	6	6	36
64	2	1	2	16	32
65	6	2	2	12	48
66	12	4	4	10	20
67	6	10	3	66	66
68	4	1	4	16	32
69	6	10	2	22	44
70	12	2	4	12	24
71	7	12	2	70	70
72	6	2	2	6	24
73	4	6	1	72	72
74	8	6	2	36	36
75	6	4	2	20	40
76	8	6	2	18	36
77	10	4	4	30	60
78	12	2	4	12	24
79	6	12	3	78	78
80	4	1	4	4	32
81	5	18	1	54	54
82	6	4	2	40	40
83	4	20	2	82	82

n	Number of Cycles	Length of Longest Cycle	Number of Longest Cycle	$\lambda(n)$	$\phi(n)$
84	12	2	4	6	24
85	4	1	4	16	64
86	14	6	4	42	42
87	8	3	4	28	56
88	6	4	2	10	40
89	3	10	1	88	88
90	12	2	4	12	24
91	10	2	6	12	72
92	6	10	2	22	44
93	12	4	6	30	60
94	8	11	4	46	46
95	8	6	2	36	72
96	4	1	4	8	32
97	3	2	1	96	96
98	14	6	4	42	42
99	10	4	4	30	60
100	6	4	2	20	40

1. Graphs for Some integers n

Here are digraphs $G(\mathbb{Z}_n)$ for the values $n = 2, 3, 4, 5, 6, 7, 19, 23, 29$.

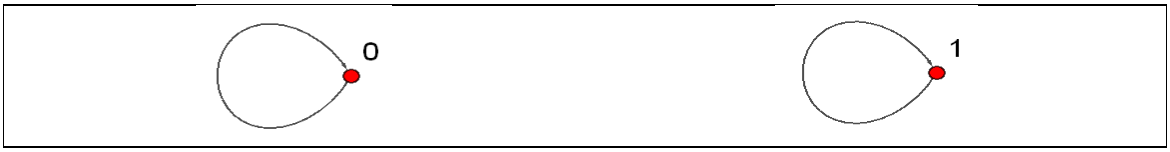

Figure 1. Shown is the graph $G(R)$ with vertices in the finite commutative ring $R = \mathbb{Z}_2$

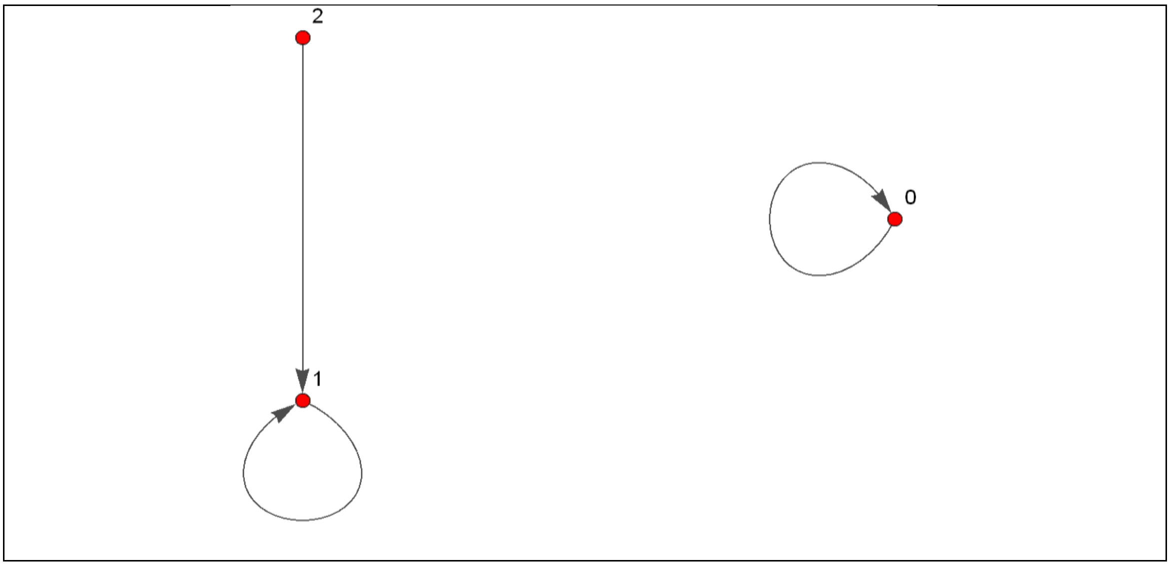

Figure 1. Shown is the graph $G(R)$ with vertices in the finite commutative ring $R = \mathbb{Z}_3$

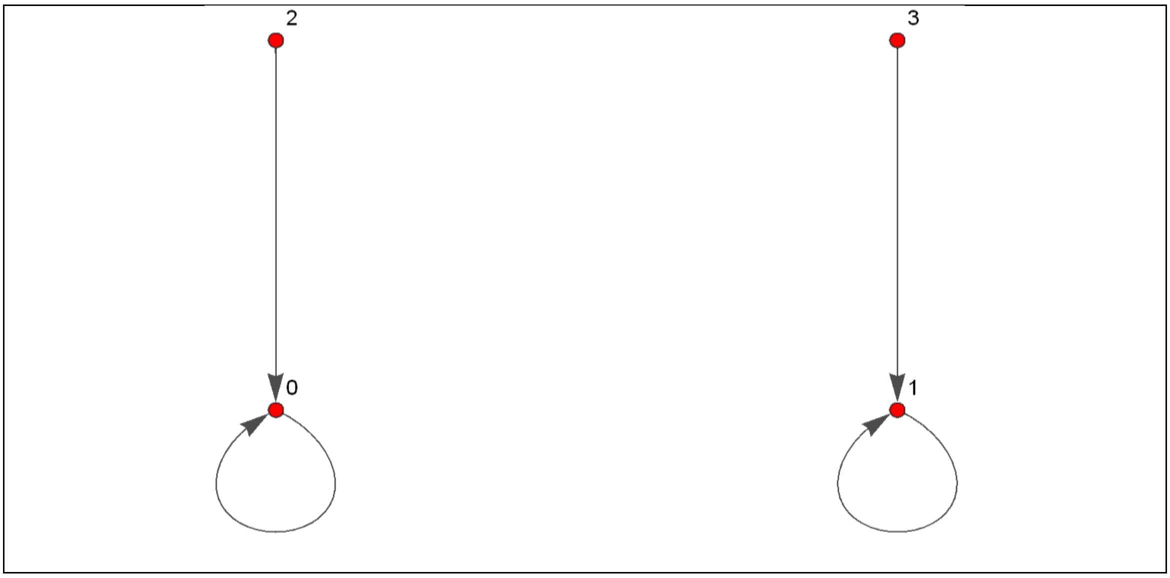

Figure 1. Shown is the graph $G(R)$ with vertices in the finite commutative ring $R = \mathbb{Z}_4$

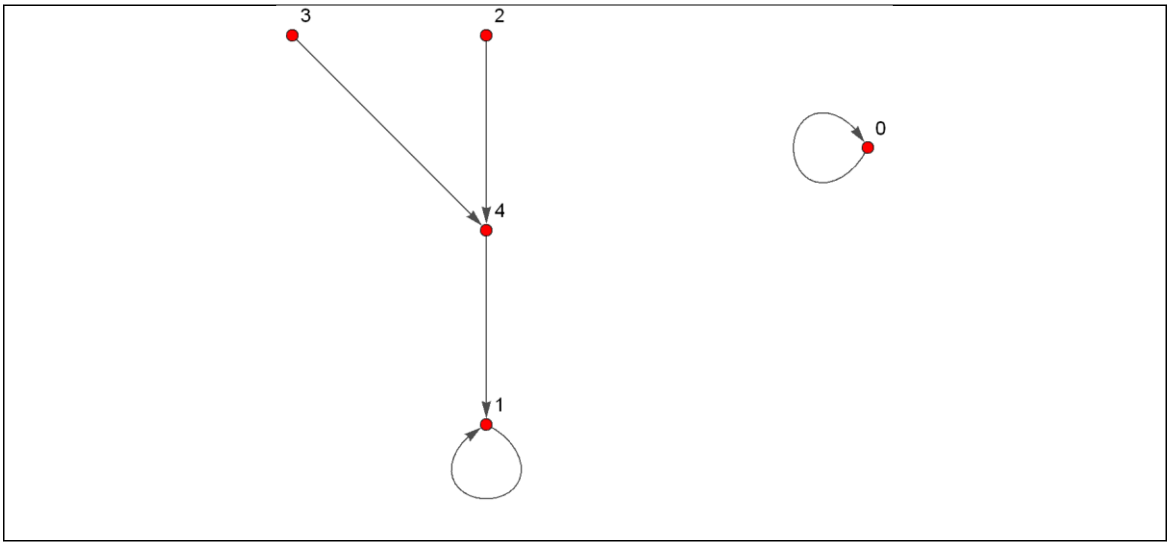

Figure 1. Shown is the graph $G(R)$ with vertices in the finite commutative ring $R = \mathbb{Z}_5$.

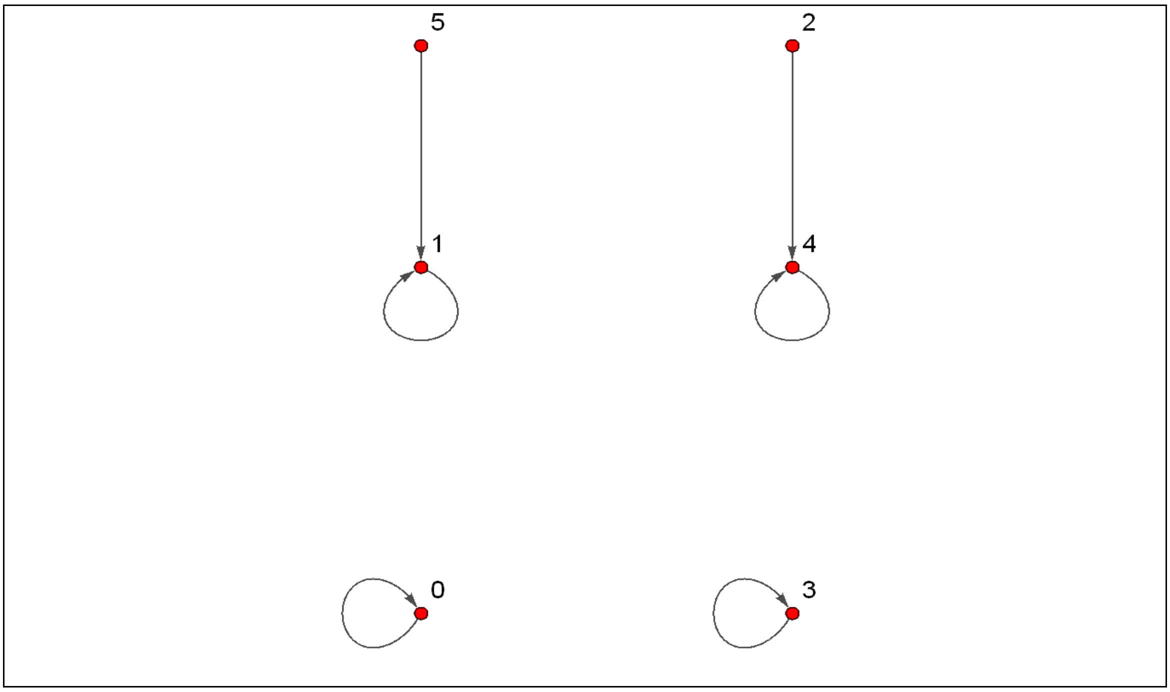

Figure 1. Shown is the graph $G(R)$ with vertices in the finite commutative ring $R = \mathbb{Z}_6$.

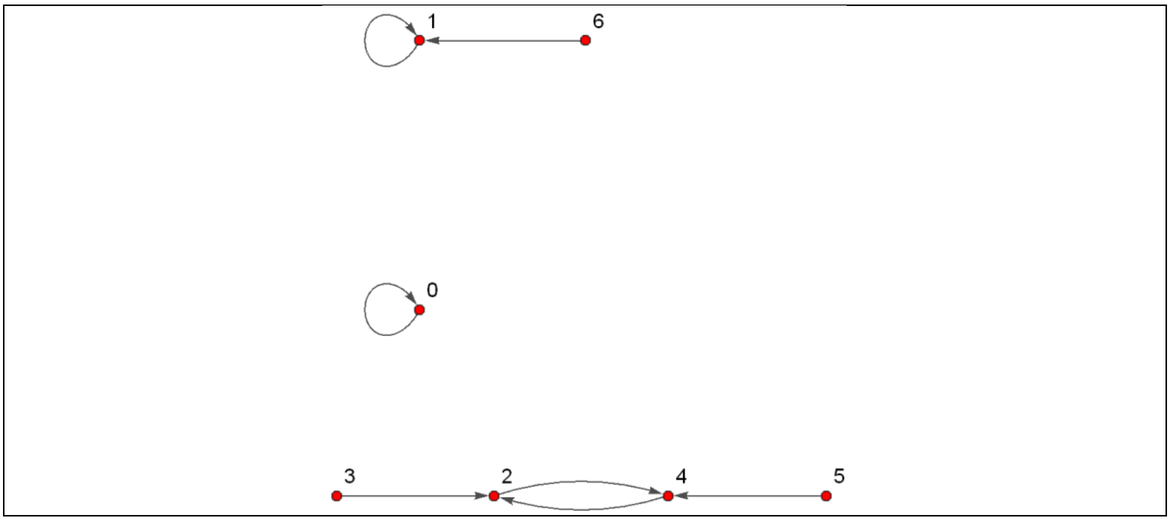

Figure 1. Shown is the graph $G(R)$with vertices in the finite commutative ring $R = \mathbb{Z}_7$.

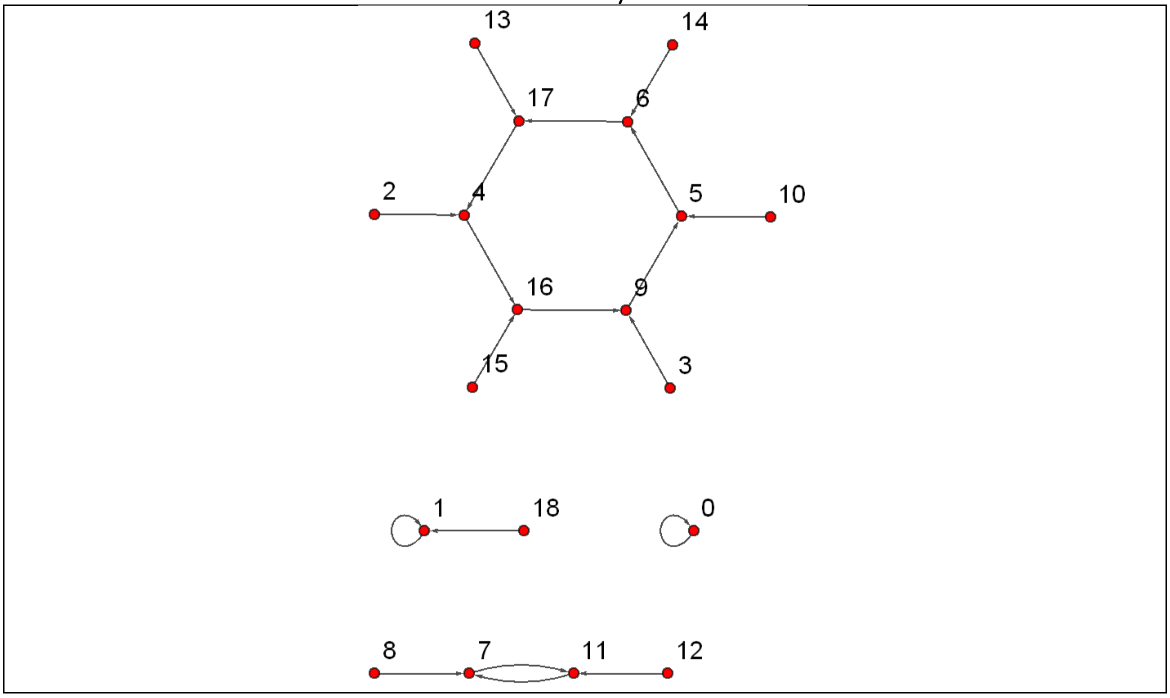

Figure 1. Shown is the graph $G(R)$with vertices in the finite commutative ring $R = \mathbb{Z}_{19}$.

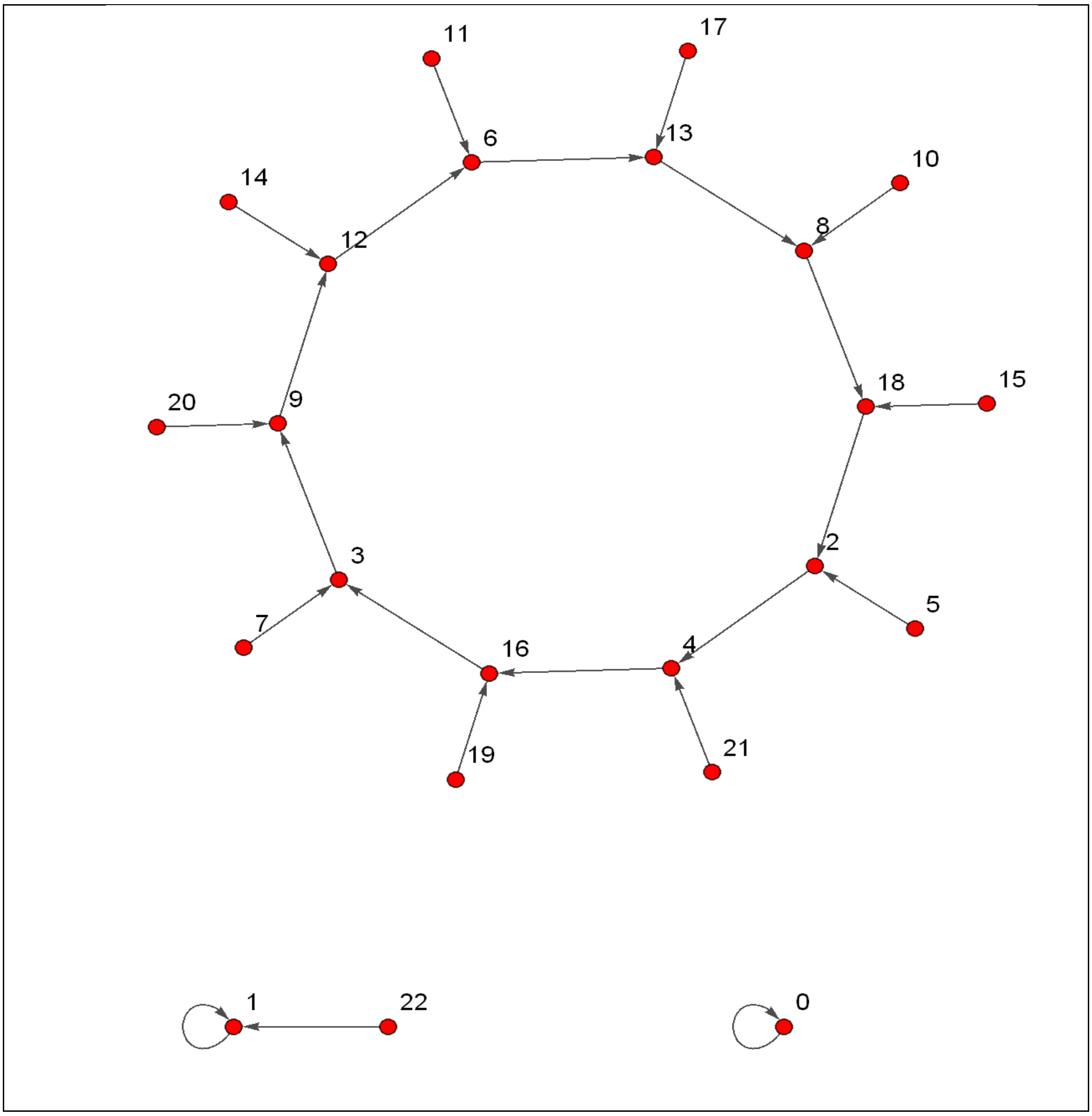

Figure 1. Shown is the graph $G(R)$ with vertices in the finite commutative ring $R = \mathbb{Z}_{23}$.

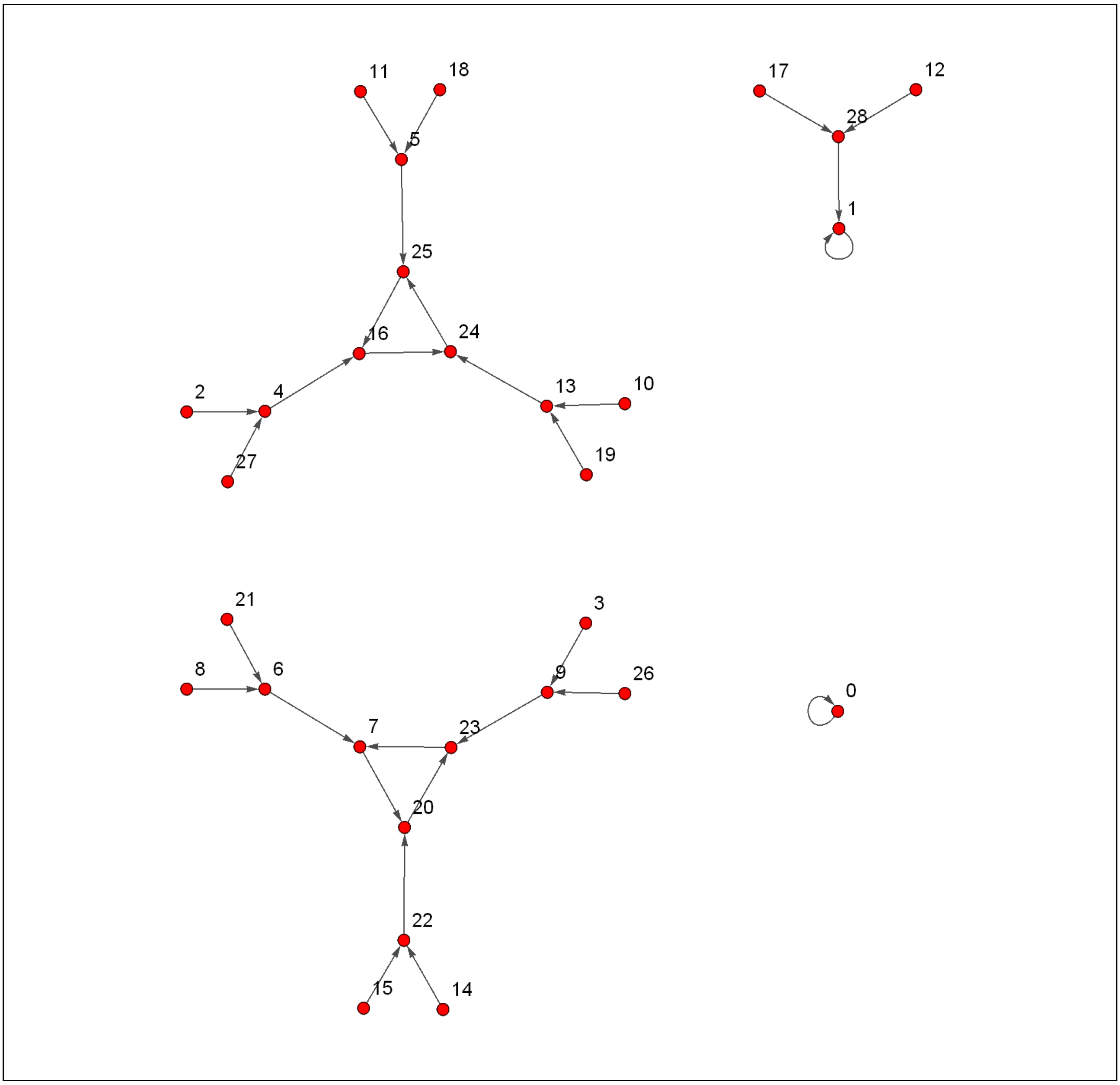

Figure 1. Shown is the graph $G(R)$ with vertices in the finite commutative ring $R = \mathbb{Z}_{29}$

References:

[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'InstitutMathematique 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.