The College of Wooster Libraries
Open Works

Senior Independent Study Theses

2012

Iteration Digraphs

Hannah Roberts
The College of Wooster, hjroberts3141@gmail.com

Iteration Digraphs

Independent Study Thesis

Presented in Partial Fulfillment of the Requirements for
the Degree Bachelor of Arts in the
Department of Mathematics at The College of Wooster

by
Hannah Roberts

The College of Wooster
2012

Advised by:

Dr. Jennifer Bowen (Mathematics)

THE COLLEGE OF
WOOSTER

Abstract

An iteration digraph, $G(n)$, generated by the function $f(x) \pmod{n}$ is a digraph on the set of vertices $V = \{0, 1, \ldots n-1\}$ with the directed edge set $E = \{(v, f(v)), | \, v \in V\}$. Focusing specifically on the function $f(x) = 10x(modn)$, we consider the structure of these graphs as it relates to the factors of n. The levels, cycle lengths, and number of cycles are determined for any integer relatively prime to 10. Isomorphic subgraphs arising from multiples of 3 and 9, and tree structures specific to powers of 2 and 5 are also described.

Contents

List of Figures

CHAPTER 1

Introduction

Tanya Khovanova's Math Blog [Wilson, 2009] contains a variety of math related posts, from stories and jokes to puzzles and questions. Some of the puzzles and questions include solutions, while others are left open for readers to explore for themselves, and many leave comments having done so. A post contributed by David Wilson briefly presents a graphically based algorithm for determining if an integer is divisible by 7. He simply describes the method, without any explanation for how it was created, how it works, or if a similar method could be applied to integers other than 7. In fact, the vertices of his graph are not even numbered, as he does not suggest that it can be used to find remainders of dividing by 7.

Wilson does note that the graph is planar, which seems to be the main focus for most readers, based on the comments made. There is even some consideration in the comments (mostly by Wilson himself) of divisibility graphs for integers represented in a base other than decimal, and which of these may be planar. Clearly those moving into different bases understand how the graph was produced and why it works, but do not explain it, and almost nobody discusses it at all. Also, the discussion of structure for these graphs is limited entirely to the matter of planarity.

This project began with a curiosity to understand how and why the divisibility graph works. Thus, we will also begin here by presenting the divisibility graph and algorithm.

1.1 The Algorithm

The digraph in Figure 1.1, adapted from Khovanova's blog [Wilson, 2009], provides an algorithm for determining the remainder of any positive integer, N, when divided by 7 without the need to perform actual calculations. As an example of this method, consider $N = 375$. Starting at 0, follow 3 black edges, ending on 3. Then follow one red edge to 2. Next follow 7 black edges, ending back on 2, and 1 red edge to land on 6. Finally, follow 5 more black edges to end on 4. This means that 375 has remainder $4 \mod 7$.

Generalized for any $N = d_0 d_1 d_2 \ldots d_k$, where d_i is the i^{th} digit of N, we start at 0 and follow d_0 black edges. Then follow one red edge and d_1 more black edges. We continue to alternate between one red edge and d_i black edges. After following the last d_k black edges, the vertex we end on is the remainder of N divided by 7.

A similar graph can be constructed for any integer n, which will determine the remainder of $N \mod n$ by the same process. We will consider why this works and how to construct such a graph for any integer in Section 1.3, but we first need to establish some definitions and properties from graph theory, number theory, and for iteration digraphs.

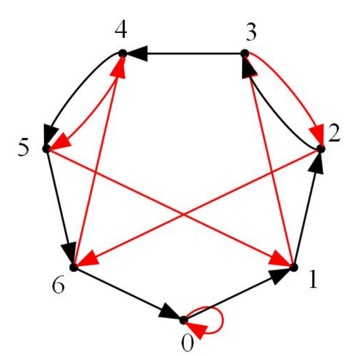
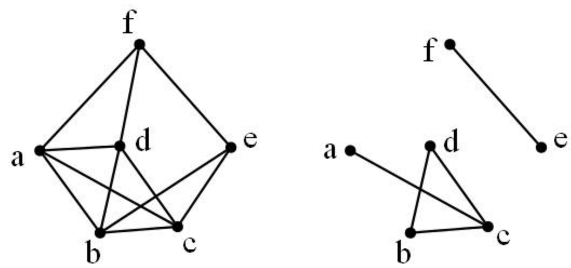


Figure 1.1: The digraph $G(7)$ for determining remainders $\mod 7$.

1.2 Background

1.2.1 Graph Theory

A **graph**, G, is defined by two sets: the set of **vertices**, $V(G)$, and the set of **edges**, $E(G)$. Each edge in $E(G)$ is a pair of vertices, (a, b) where a and b are elements of $V(G)$. These vertices are the endpoints of the edge when the graph is drawn. For the graph G_1 shown in Figure 1.2(a), $V = \{a, b, c, d, e, f\}$ and some of the edges in E are $(a, b), (a, c), (a, d), (b, c), (b, d)$.



(a) Graph G_1 (b) Subgraph G_2

Figure 1.2: Example graph and subgraph

A directed graph, or **digraph**, is a graph whose edges have a specified direction. Edges of a digraph are represented by ordered pairs of vertices, and drawings have arrows on the edges. If (a, b) is an edge in a digraph, then the arrow on the edge points from a to b and we say a is **adjacent** to b. Note that for a digraph, edges are ordered pairs with (a, b) and (b, a) representing different edges, whereas order is unimportant for edges in an undirected graphs. Shown in Figure 1.3, the digraph D_1 has the same vertex set as G_1, but here the edge set includes $(a, b), (b, c), (e, b)$. If (b, a) was also an edge in D_1, there would be an additional edge with the arrow pointing from b to a. Since e is both the head and tail of the edge (e, e), the edge is called a **loop** and e is called a **fixed point**.

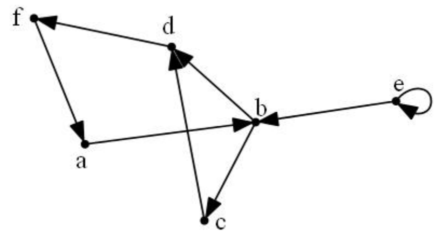


Figure 1.3: D_1 is a basic digraph

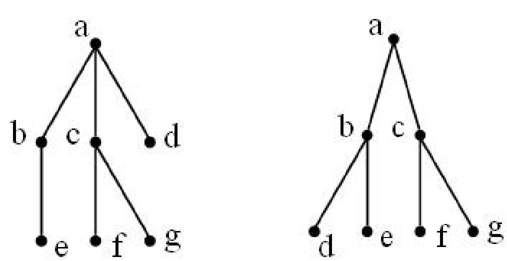
Given a graph $G = (V, E)$, $H = (W, F)$ is a subgraph of G if the vertex and edge sets of H are subsets of G's vertex and edge sets. That is, if $W \subset V$ and $F \subset E$. If F contains exactly all of the edges of G that join vertices of W, then H is called the **subgraph generated by** W. In Figure 1.2(b), G_2 is a subgraph of G_1 because all of the vertices and edges in G_2 are also in G_1. It is not, however, a generated subgraph, because several edges are not included, such as $(a, d), (a, b), (e, c)$.

There are many different structural aspects to graphs and digraphs. A graph is **connected** if, for every pair of vertices u and v, there is a path between u and v. In Figure 1.2, G_1 is a connected graph, but G_2 is not because there are no paths from e or f to any of the other vertices. A **component**, C, of a graph is a connected generated subgraph where there is no larger connected generated subgraph that includes all of the vertices in C. For example, G_2 has two components. They are the subgraphs generated by the vertex sets $\{a, b, c, d\}$ and $\{e, f\}$. The generated subgraph for the set $\{a, b, c\}$, however, is not a component.

The **degree** of a vertex v is the number of edges for which v is an endpoint. In a digraph, the **indegree** and **outdegree** of v, $indeg(v)$ and $outdeg(v)$, are the number of edges with v at the head and tail, respectively. In D_1, $indeg(e) = 1$ and $outdeg(e) = 2$. A digraph is **regular** if all its vertices have the same indegree. Similarly, a digraph is **semiregular** if the indegree of every vertex is either 0 or d, where d is a positive integer.

A **path** is a sequence of either vertices or edges that can be followed through the graph, obeying all directional restrictions. For example, e, e, b, d, f is a path in D_1. A **cycle** is a path whose first and last vertex are the same and no vertex in between is visited more than once. More specifically, a t**-cycle** is a cycle of length t. In D_1, one example of a 4-cycle is b, d, f, a, b. The loop (e, e) is a 1-cycle. We call a vertex or edge **cyclical** if it is part of a cycle and **noncyclical** otherwise.

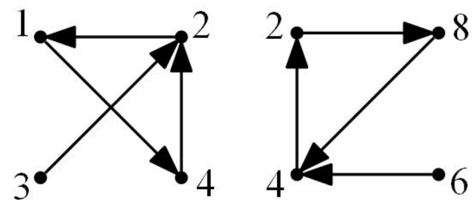
A **tree** is a graph which is connected and has no cycles. The **level** of a vertex, v, is a distance measurement between v and a vertex designated as the **root**. The vertex v is at level i if there is a path between v and the root of i that is edges long. The root is the only vertex at level 0. The **height** of a tree with levels $0, 1, 2, \ldots k$ is k. The trees shown in Figure 1.4 have root a and height 2. In T_1, $b, c,$ and, d are all at level 1, and $e, f,$ and, g are at level 2. For a vertex v, all vertices adjacent to v and at the level below v are called the **children** of v. If every vertex in a tree has m or fewer children, it is called m**-ary**. If every vertex has exactly m or 0 children, it is called a **complete** m-ary tree. Thus, T_1 is a 3-ary tree and T_2 is a complete 2-ary (or binary) tree.



(a) Tree T_1 (b) Binary tree T_2

Figure 1.4

Finally two graphs, G and H, are **isomorphic** if their exists a one-to-one and onto function $f : V(G) \to V(H)$ such that $(a, b) \in E(G)$ if and only if $(f(a), f(b)) \in E(H)$. The function f is called an **isomorphism**. In Figure 1.5, digraphs G and H are isomorphic with an isomorphism of $f(x) = 2x$. The edge $(1, 4)$ in G becomes $(2, 8)$ in H, $(2, 1)$ becomes $(4, 2)$, $(3, 2)$ goes to $(6, 4)$, and $(4, 2)$ to $(8, 4)$. On the other hand, the graph F in Figure 1.6 is not isomorphic to either G or H because the edge $(2, 3)$ has the wrong direction and also because F has the extra edge $(3, 4)$.



(a) G (b) H

Figure 1.5: G and H are isomorphic graphs

1.2.2 Number Theory

Two integers a, b are said to be **congruent modulo** $m \in \mathbb{Z}^+$ if $m|a - b$, otherwise, they are called **incongruent**. Congruence is written $a \equiv b \mod m$. If $0 \leq b \leq m - 1$, then a has a remainder of b when divided by m. For example, $15 \equiv 3 \mod 6$ because $6|(15 - 3) = 12$.

Several properties of traditional arithmetic also hold for modular arithmetic.

Theorem 1.1.

Modular arithmetic is an equivalence relation, so it satisfies the properties

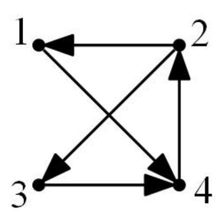


Figure 1.6: F is not isomorphic to either G or H

(i) $a \equiv a \mod m$

(ii) *if* $a \equiv b \mod m$*, then* $b \equiv a \mod m$

(iii) *if* $a \equiv b \mod m$ *and* $b \equiv c \mod m$*, then* $a \equiv c \mod m$

Proof. For part (*i*), $a - a = 0 = 0m$, so $a \equiv a \mod m$. For (*ii*), since $a \equiv b \mod m$, we have $a - b = m \cdot n$ for some integer n. Then, $b - a = m \cdot (-n)$, so $b \equiv a \mod m$. Finally, for part (*iii*), we have $a - b = m \cdot n$ and $b - c = m \cdot p$ where n and p are integers. Adding these gives $a - c = m \cdot n + m \cdot p = m(n + p)$, so $a \equiv c \mod m$. □

Theorem 1.2.

If a, b, c, d*, and* m *are integers with* $m > 0$*,* $a \equiv b \mod m$ *and* $c \equiv d \mod m$*, then*

(i) $a + c \equiv b + d \mod m$

(ii) $a - c \equiv b - d \mod m$

(iii) $ac \equiv bd \mod m$

Proof. From the given congruences, we get $a - b = m \cdot n$ and $c - d = m \cdot p$. Thus, $a - b + (c - d) = m \cdot n + m \cdot p$ or $a + c - (b + d) = m(n + p)$, so $a + c \equiv b + d \mod m$. Also, $a - b - (c - d) = m \cdot n - m \cdot p$ or $a - c - (b - d) = m(n - p)$, so $a - c \equiv b - d \mod m$. Finally, for part (*iii*), rewrite the equations as $a = m \cdot n + b$ and $c = m \cdot p + d$. Then,

$$
\begin{aligned}
a \cdot c &= (m \cdot n + b)(m \cdot p + d) \\
a \cdot c &= m^2 np + mnd + mpb + bd \\
a \cdot c - b \cdot d &= m(mnp + nd + pb)
\end{aligned}
$$

so $ac \equiv bd \mod m$. □

It is important to note that $a/c \equiv a/d \mod m$ is not necessarily true for all integers. For example, we said $15 \equiv 3 \mod 6$ above, but $15/3 = 5 \not\equiv 1 = 3/3 \mod 6$.

By definition, $a \equiv r \mod m$ means that $a = bm + r$, where b is an integer. If we have additionally that $0 \leq r \leq m-1$, then r is the **least residue** of a modulo m. The set of all $0 \leq r \leq m-1$ is the **set of least residues** modulo m. A set of m integers which are incongruent modulo m is called a **complete system of residues** modulo m and reduces to the set $\{0, 1, 2, \ldots m-1\}$. For $m = 6$, $\{12, 7, -4, 63, 10, -1\}$ is a complete system of residues, because the numbers reduce to $\{0, 1, 2, 3, 4, 5\}$, the least residues modulo 6.

Another important piece of notation for Number Theory is **greatest common divisor**. For two integers a and b, not both 0, their greatest common divisor is the largest integer d that divides both a and b. We write $\gcd(a, b) = d$, so $\gcd(15, 6) = 3$. If $\gcd(a, b) = 1$, then a and b are called **relatively prime**. One common property of greatest common divisors, known as Bezout's identity, says that if $\gcd(a, b) = d$, then there exist integers m and n such that $ma + nb = d$. In fact, d is the smallest positive integer for which there is such a linear combination of a and b.

Two other common functions will also be necessary. The **order** of an integer x modulo m is the smallest power k such that $x^k \equiv 1 \mod m$. This is written $ord_m(x) = k$. For example, $ord_7(10) = 6$ because $10^6 \equiv 1 \mod 7$, but $10^k \not\equiv 1 \mod 7$ for all $k < 6$. Finally, the **Euler Phi Function**, $\phi(n)$, is the number of positive integers, $a < n$ for which $\gcd(a, n) = 1$. For example, $\phi(12) = 4$ because there are 4 integers less than and relatively prime to 12: 1, 5, 7, 11. Note that for any prime, p, every integer less than p is relatively prime, so $\phi(p) = p - 1$.

1.2.3 Iteration Digraphs

An **iteration digraph** is generated by a function $f : \mathbb{Z}_n \to \mathbb{Z}_n$. The directed graph G_n is formed on the vertex set $V = \mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ with exactly one edge from v to $f(v)$ for all $v \in V$. Thus, the edge set of G_n is $E = \{(v, f(v)) | v \in V\}$. In Figure 1.7, D_{11} is the iteration digraph produced by the function $f(x) \equiv x^2 \mod 11$.

Thus, $V(D_{11}) = \{0, 1, 2, \ldots 10\}$ and $E(D_{11})$ includes $(9, 4), (4, 5)$ and so on, because $9^2 = 81 \equiv 4 \mod 11$ and $4^2 = 16 \equiv 5 \mod 11$.

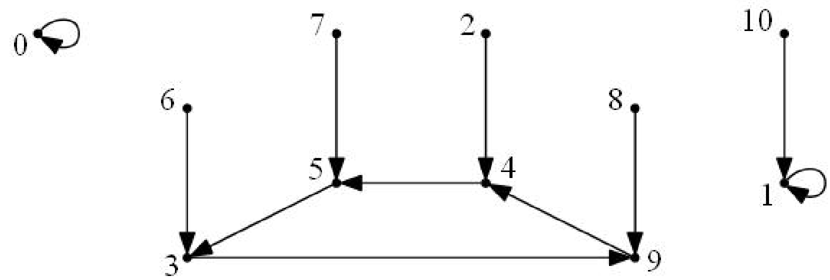


Figure 1.7: D_{11} generated by $f(x) = x^2 \mod 11$

Let $\{x_j\}$ be a sequence of vertices in an iteration digraph with initial vertex x_0. Since each vertex, x_k, is at the tail of exactly one edge with the head at $f(x_k)$, the sequence is defined recursively by $x_{k+1} = f(x_k)$. Also, since there exists an x_{k+1} for every x_k, we can create a sequence of any length on a digraph with any number of vertices. Suppose $\{x_j\}$ is a sequence of $n + 1$ vertices on a graph with n vertices, then there must be two elements of the sequence such that $x_i = x_k$, so the graph has a cycle. The above is really a proof for a basic iteration digraph theorem.

Theorem 1.3.

Every iteration digraph contains at least one cycle. Moreover, every component of an iteration digraph must contain a cycle.

The graph D_{11} includes one 4-cycle, $4, 5, 3, 9$, and two 1-cycles, or fixed points, at 0 and 1. More specifically, 0 is called an **isolated fixed point**, because there is no vertex other than itself that is adjacent to 0. On the other hand, 1 is not isolated because 10 is adjacent to 1.

A level was defined for a tree in Section 1.2.1, but a different definition for the **level** of an iteration digraph is given in [Somer and Křížek, 2004] and will be the primary definition used in this work. A vertex v in graph D is at level i if the longest directed path that ends at v and does not contain any cyclical edges has length i. For instance, graph D_{11} (Fig. 1.7) has 2 levels with $0, 2, 6, 7, 8$, and 10 at level 0 and the rest of the vertices are at level 1. In Figure 1.8, the levels used for a tree put a at level 0, e at 1, c, d at 2, and b, f at 3. However, the levels just defined for iteration digraphs put b, f, and d at level 0, c at 1, e at 2, and a at 3. For the rest of this paper, the iteration digraph definition for level will be used unless otherwise stated.

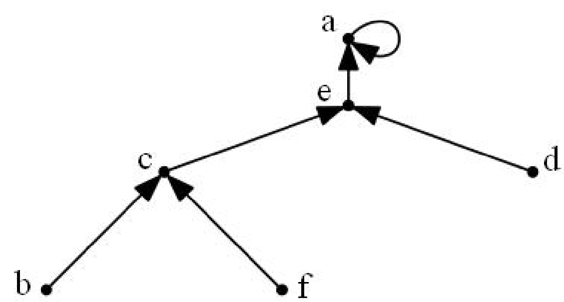


Figure 1.8: Different definitions assign vertices to different levels.

1.3 Algorithm Proof

Based on the definitions from Sections 1.2.1-1.2.3, we can see that Figure 1.1 is actually two iteration digraphs drawn on the same set of vertices. The black edges are easily seen to be the digraph generated by $g(x) = x+1 \mod 7$. Closer inspection also shows that the red edges are the digraph generated by $f(x) = 10x \mod 7$. Thus, for any integer n, let $D(n)$ be the union if the iteration digraphs generated by $g(x) = x + 1 \mod n$ and $f(x) = 10x \mod n$. If the $g(x)$ edges are black and the $f(x)$ edges are red, then we can use the algorithm given in Section 1.1 to find the remainder when N is divided by n, or $N \mod n$.

Theorem 1.4.

Let $D(n)$ be the iteration digraph generated by both $g(x) = x + 1 \mod n$ and $f(x) = 10x$

mod *n on the same set of vertices, and let* $N = a_0a_1a_2 \ldots a_k$ *where* a_i *is the* i^{th} *digit of N. Begin at the 0 vertex and follow* a_0 $g(x)$ *(black) edges. Continue to iterate through i first following 1* $f(x)$ *(red) edge and then* d_i $g(x)$ *edges for* $i = 1, 2, \ldots k$*. Let v be the vertex after the final* a_k $g(x)$ *edges. Then* $N \equiv v \mod n$*.*

Proof. Let N be a positive k-digit integer with decimal expansion

$$N = 10^k a_k + 10^{k-1} a_{k-1} + \cdots + 10a_1 + a_0$$

where $0 \leq a_i \leq 9$. Define $r_0 \equiv 0 \mod n$ and $r_i \equiv 10b_i \pmod{n} = f(b_i)$ for $i \geq 1$. Thus, r_i is the vertex after following one red edge from b_i. Also define $b_i \equiv r_{i-1} + a_{k+1-i}$ for $i \geq 1$. Thus, b_i is the vertex after following a_{k+1-i} black edges from r_{i-1}. The values of b_i and r_i correspond to the vertices which are landed on throughout the algorithm. Thus, we have

$$\begin{aligned}
r_0 &\equiv 0 \\
b_1 &\equiv r_0 + a_k \equiv a_k \\
r_1 &\equiv 10b_1 \equiv 10a_k \\
b_2 &\equiv r_1 + a_{k-1} \equiv 10a_k + a_{k-1} \\
r_2 &\equiv 10(10a_k + a_{k-1}) \equiv 10^2 a_k + 10a_{k-1} \\
&\vdots \\
b_p &\equiv 10^{p-1} a_k + 10^{p-2} a_{k-1} + \cdots + 10a_{k+2-p} + a_{k+1-p} \\
r_p &\equiv 10^p a_k + 10^{p-1} a_{k-1} + \cdots + 10^2 a_{k+2-p} + 10a_{k+1-p} \\
&\vdots \\
b_k &\equiv 10^{k-1} a_k + 10^{k-2} a_{k-1} + \cdots + 10a_2 + a_1 \\
r_k &\equiv 10^k a_k + 10^{k-1} a_{k-1} + \cdots + 10^2 a_2 + 10a_1 \\
b_{k+1} &\equiv 10^k a_k + 10^{k-1} a_{k-1} + \cdots + 10^2 a_2 + 10a_1 + a_0
\end{aligned}$$

Thus, $b_{k+1} \equiv N \mod n$. □

In the above iterations, each b_i corresponded to following the black edges for the digit a_{k+1-i} and each r_i was the single red edge followed between digits. Thus, following the edges in the graphical algorithm is really just building N according to its decimal expansion while reducing mod n at every step.

Returning to the example of $N = 375$ for $n = 7$, we have $k = 2$ and the algebraic algorithm is as follows:

$$r_0 \equiv 0$$

$$b_1 \equiv r_0 + a_2 \equiv 0 + 3 \equiv 3$$

$$r_1 \equiv 10b_1 \equiv 30 \equiv 2$$

$$b_2 \equiv r_1 + a_1 \equiv 2 + 7 \equiv 2$$

$$r_2 \equiv 10b_2 \equiv 20 \equiv 6$$

$$b_3 \equiv r_2 + a_0 \equiv 6 + 5 \equiv 4$$

Note that the sequence produced here—0,3,2,2,6,4—is the same as the path of vertices taken when using the graph.

For another example, let $N = 5046$, still with $n = 7$. Then $k = 3$ and

$$r_0 \equiv 0$$

$$b_1 \equiv 5$$

$$r_1 \equiv 1$$

$$b_2 \equiv 1$$

$$r_2 \equiv 3$$

$$b_3 \equiv 0$$

$$r_3 \equiv 0$$

$$b_4 \equiv 6$$

so $5046 \equiv 6 \mod 7$.

Notice that the above proof was generalized for any positive integer n, not just for 7. Thus, we can draw a divisibility graph for any integer n and follow the same algorithm to determine remainders modulo n.

Understanding how the algorithm works, was clearly a short process. From here I began to wonder about different patterns which appear visually, and specifically, how the graph of a number is related to its factors and their graphs. Since the function $g(x) = x + 1 \mod n$ will always produce a simple cycle through the consecutive vertices, it is uninteresting. Thus, the remainder of this paper focuses on the structure of the iteration digraph $G(n)$ generated by the function $f(x) = 10x \mod n$.

CHAPTER 2

Graphs for n

Because the function $f(x) = 10x \mod n$ is dependent on 10, integers divisible by 2 or 5 have graphs with a different structure. Their structure will, however, be based on that of integers relatively prime to 10. Thus, before looking at the graph of any given integer, we first need to consider the structure of $G(n)$ where n is relatively prime to 10.

First, a theorem about complete systems of residues adapted from [Rosen, 2011] will help determine the indegrees and levels in a graph.

Theorem 2.1.

If $r_1, r_2, r_3, \ldots r_m$ is a complete system of residues modulo m, and if a is a positive integer where $\gcd(a, m) = 1$, then $ar_1 + b, ar_2 + b, ar_3 + b, \ldots ar_m + b$ is also a complete system of residues modulo m for any integer b.

Proof. First, pick any r_i and r_j where $i \neq j$. Then $r_i \not\equiv r_j \mod m$, so $m \nmid (r_i - r_j)$. Since $\gcd(a, m) = 1$, m also does not divide $a(r_i - r_j)$. Hence, $ar_i \not\equiv ar_j \mod m$. Now, because $(ar_i + b) - (ar_j + b) = ar_i - ar_j$, we have that m does not divide $(ar_i + b) - (ar_j + b)$, so $ar_i + b \not\equiv ar_j + b \mod m$. Therefore, we have m incongruent integers, and $ar_1 + b, ar_2 + b, ar_3 + b, \ldots ar_m + b$ is also a complete system of residues modulo m. □

Now, we use this theorem to consider the degrees of vertices in $G(n)$. Note that

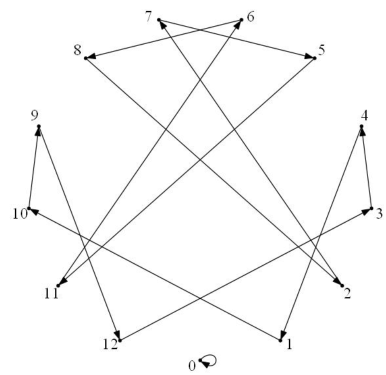


Figure 2.1: Every vertex in $G(13)$ is part of one of 3 cycles.

by definition, every vertex of an iteration digraph has an outdegree of 1, for any $n \in \mathbb{Z}$, so we only need to look at indegree here.

Theorem 2.2.

If n is not divisible by 2 or 5, then $indeg(v) = 1$ for every $v \in V(G(n))$.

Proof. By definition, $V(G(n)) = \{0, 1, 2, \ldots n - 1\}$ is a complete system of residues modulo n. From Theorem 2.1, since $\gcd(10, n) = 1$, the set $\{f(v) \mid v \in V(G(n))\} = \{10v \mid v \in V(G(n))\}$ is also a complete system of residues. Hence, $\{10v \mid v \in V(G(n))\} \equiv V(G(n)) \mod n$ and f is a bijection from $V(G(n))$ to itself. Therefore, exactly one edge leeads into each element of $V(G(n))$, so $indeg(v) = 1$ for all $v \in V(G(n))$. □

In Figure 2.1, we see that $G(13)$ is a regular graph with $indeg(v) = 1$ for every vertex. In fact, Theorem 2.2 tells us that $G(n)$ is regular for every n relatively prime to 10, because each vertex has the same indegree. Furthermore, its also means that every vertex of $G(n)$ is part of a cycle, which leads to the following theorem about levels.

Theorem 2.3.

$G(n)$ has 1 level for all n where $\gcd(10, n) = 1$.

Proof. Let $\gcd(10, n) = 1$ and assume $v \in V(G(n))$ is at level $i > 0$. Then there must be a path of i edges leading to v which are not part of a cycle. The first vertex in this non-cyclic path, must have an indegree of 0. This a contradiction to Theorem 2.2, which said that $indeg(v) = 1$. Therefore, v must be at level 0, so $G(n)$ has 1 level. □

The above theorem could be restated to say every vertex in $G(n)$ is at level 0. From this fact, it is clear that every graph $G(n)$ where $\gcd(10, n) = 1$ is simply a set of isolated cycles. That is, $G(n)$ is a set of cycles without any adjacent non-cyclic vertices. We next consider the lengths of these cycles.

Theorem 2.4.

For all integers n where $\gcd(3, n) = 1$, the only fixed point in $G(n)$ is 0. Additionally, fixed points are isolated if $\gcd(10, n) = 1$.

Proof. First, $10 \cdot 0 \equiv 0 \mod n$ for any integer n, so $(0, 0)$ is a 1-cycle.

From Theorem 2.2, $indeg(v) = 1$ for n relatively prime to 10, so a fixed point v is an isolated fixed point whenever $\gcd(10, n) = 1$.

Now, let $\gcd(10, n) = 1$ and let v be a nonzero fixed point, so $10v \equiv v \mod n$, or $n \mid (10v - v) = 9v$. Since $v < n$, we know that $n \nmid v$ and $gcd(n, 9) > 1$. Hence, 3 must divide n for v to be a fixed point. Thus, if $\gcd(3, n) = 1$, then the only fixed point in $G(n)$ is 0. □

Looking again at Figure 2.1, we see that the only isolated fixed point is 0, while in Figure 2.2, $G(33)$ has isolated fixed points at 0, 11, and 22. The length of the rest of the cycles in $G(n)$ is dependent on the prime factors of n, so we will start with the cycle lengths of primes not equal to 2 or 5. First, we need a theorem concerning the cycles on vertices relatively prime to n.

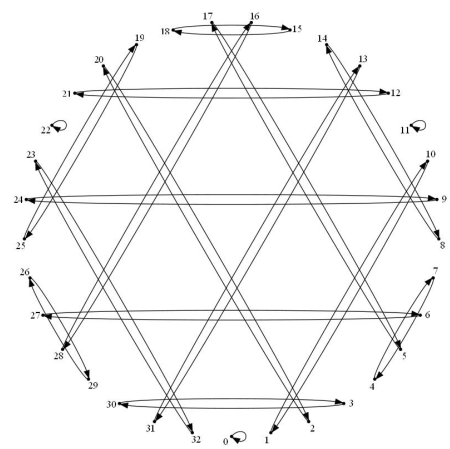


Figure 2.2: G(33) has 3 isolated fixed points.

Theorem 2.5.
In $G(n)$, if V_1 is the subset of vertices relatively prime to n, then there are $\frac{\phi(n)}{ord_n(10)}$ cycles each with length $ord_n(10)$ in the subgraph generated by V_1 .

Proof. First, let (a, b) be an edge in $G(n)$. Since, $\gcd(10, n) = 1$, if $\gcd(a, n) = 1$ then $10a \equiv b \mod n$ and b is also relatively prime to n. Thus, if a cycle contains one vertex that is relatively prime to n, then all vertices in the cycle must also be relatively prime to n.

Now, let $r = ord_n(10)$, so r is the least integer for which $10^r \equiv 1 \mod n$, or equivalently $10^r v \equiv v \mod n$ for every $v \in V(G(n))$. In the sequence $\{v_0, v_1, v_2, \ldots v_r\}$ of vertices from $G(n)$, $v_t \equiv 10^t v_0$. Thus, $v_r \equiv 10^r v_0 \equiv v_0$ and the sequence is an r-cycle.

Consider $s > r$. We can write $s = mr + t$ where m, t, and s are integers such that

$0 \leq t < r$. Hence,

$$\begin{aligned} 10^s v_0 &\equiv 10^{mr+t} v_0 \mod n \\ &\equiv 10^t (10^{mr} v_0) \mod n \\ &\equiv 10^t (1^m v_0) \mod n \\ &\equiv 10^t v_0 \mod n \\ &\equiv v_t \mod n \end{aligned}$$

and $10^s v_0 \equiv v_0 \mod n$ if and only if $t = 0$, or equivalently $r|s$. If $10^s v_0 \equiv v_0 \mod n$, this suggests a cycle of length s, but the r-cycle has really just been cycled through m times. Thus, the longest possible cycle in $G(n)$ has length r.

Now, let $v \in G(n)$ such that $\gcd(v, n) = 1$ and assume v is part of an s-cycle where $s < r = ord_n(10)$. Then $10^s v \equiv v \mod n$, but $10^s \not\equiv 1 \mod n$ because by definition, r is the smallest positive integer for which $10^r \equiv 1 \mod n$. This means $10^s - 1 = np + r$ for some integers p and $0 < r < n$. Also, $10^s v - v = nm$ for some integer m, so

$$\begin{aligned} v(10^s - 1) &= nm \\ v(np + r) &= nm \\ vr &= nm - vnp \\ vr &= n(m - vp). \end{aligned}$$

This means that $n|(vr)$, but $n \nmid r$ because $0 < r < n$. Hence, $\gcd(n, v) > 1$, which is a contradiction since $\gcd(n, v) = 1$. Therefore, all cycles on vertices relatively prime to n have length $r = ord_n(10)$. Also, there are $\phi(n)$ vertices relatively prime to n, so there are $\dfrac{\phi(n)}{ord_n(10)}$ such cycles. □

We now define C_n to be the number of cycles in $G(n)$ and find the following for primes. Note that from [Somer and Křížek, 2004] the number of cycles in an

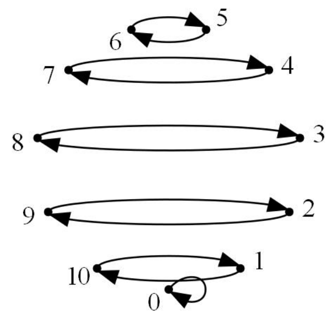


Figure 2.3: $G(11)$ has six 2-cycles and one 1-cycle

iteration digraph is the same as the number of components. Also, define L_n to be the set of all cycle lengths in $G(n)$. For primes $p \neq 2, 5$, C_p and L_p are now a corollary to the previous theorem.

Corollary 2.1.
If p is a prime not equal to 2 or 5, $G(p)$ has $\frac{p-1}{ord_p(10)} + 1$ cycles each with length 1 or $ord_p(10)$.

Proof. From Theorem 2.4, we know that $(0, 0)$ is a 1-cycle for every p. All nonzero vertices in $G(p)$ are relatively prime to p, so $\phi(p) = p - 1$ and by Theorem 2.5, the nonzero vertices form $\frac{p-1}{ord_p(10)}$ cycles with length $ord_p(10)$. Therefore, including the fixed point at 0, $G(p)$ has

$$\frac{p-1}{ord_p(10)} + 1 \tag{2.1}$$

cycles each with length 1 or $ord_p(10)$. □

When $n = 3$, we have a special case of Corollary 2.1 because $ord_3(10) = 1$, so every vertex in $G(3)$ is an isolated fixed point,as seen in Figure 3.1.

We now want to determine C_n and L_n for any n relatively prime to 10. However, we first need the following theorem on an important relation between the edges in $G(n)$ and the edges of $G(nm)$.

Theorem 2.6.

For any integers n and m, $(a, b) \in E(G(n))$ *if and only if* $(ma, mb) \in E(G(mn))$.

Proof. Let (a, b) be an edge in $G(n)$. Then $10a \equiv b \mod n$, so

$$10a - b = np$$
$$10(ma) - mb = (mn)p.$$

Thus, $10(ma) \equiv mb \mod mn$, and (ma, mb) is an edge in $G(mn)$. Therefore, $(a, b) \in E(G(n))$ if and only if $(ma, mb) \in E(G(n))$ □

From the above theorem, we begin to see how the cycles in a graph $G(n)$ will also be contained in the graph of $G(mn)$.

Corollary 2.2.

If $G(n)$ *has t cycles of length r, then* $G(mn)$ *also has at least t r-cycles.*

Proof. Let $G(n)$ have t cycles of length r and let $v_1, v_2, v_3, \ldots v_r, v_1$ be one r-cycle in $G(n)$. Then from Theorem 2.6, $mv_1, mv_2, mv_3, \ldots mv_r, mv_1$ is an r-cycle in $G(mn)$. Thus, $G(mn)$ has at least t r-cycles. □

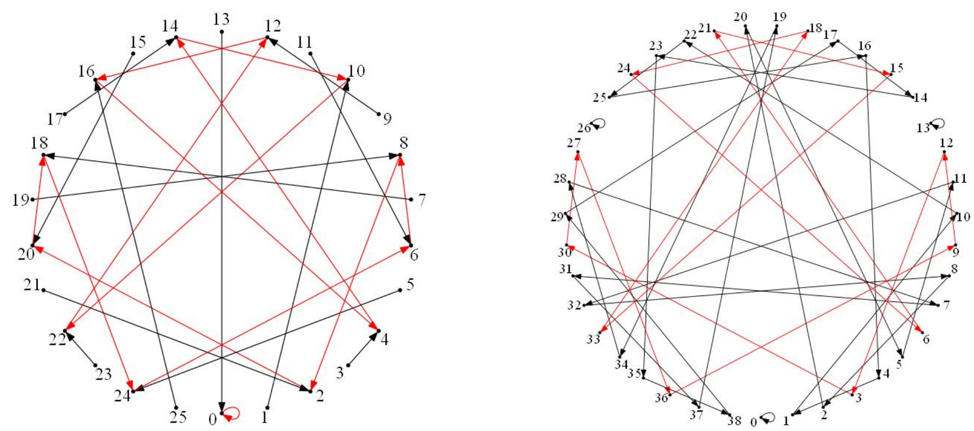
We have seen in Figure 2.1 that $G(13)$ has one 1-cycle and two 6-cycles. Now, in Figure 2.4, $G(26)$ has the same number of cycles of each length as $G(13)$, whereas $G(39)$ has three 1-cycles and six 6-cycles.

Now, if p and q are prime, we can determine exactly the number and lengths of cycles of $G(pq)$.

Theorem 2.7.

If p and q are distinct prime integers not equal to 2 or 5, then $G(pq)$ *has cycles of lengths 1,* $ord_p(10)$, $ord_q(10)$, *and* $ord_{pq}(10)$. *Also,*

$$C_{pq} = \frac{pq - p - q + 1}{ord_{pq}(10)} + C_p + C_q - 1$$



(a) $G(26)$ (b) $G(39)$

Figure 2.4: $G(26)$ and $G(39)$ both have at least one 1-cycle and two 6-cycles.

Proof. The nonzero vertices in both $G(p)$ and $G(q)$ form $C_p - 1$ and $C_q - 1$ cycles respectively. From Corollary 2.2, this means that $C_{pq} \geq C_p - 1$ and $C_{pq} \geq C_q - 1$. Let $P = \{(qa, qb) \mid (a, b) \neq (0, 0) \in E(G(p))\}$ and let $Q = \{(pc, pd) \mid (c, d) \neq (0, 0) \in E(G(q))\}$. By Theorem 2.6, both P and Q are subsets of $E(G(pq))$ and contain the cycles from $G(p)$ and $G(q)$, respectively. If $P \bigcap Q = \emptyset$, then we have $C_{pq} \geq (C_p - 1) + (C_q - 1)$. Since $a, b \in \{0, 1, 2 \ldots (p-1)\}$, every vertex in an edge of P is divisible by q, but not by p. Similarly, every vertex in an edge of Q is divisible by p. Hence, there are no common vertices between the edges in P and those in Q, so $P \bigcap Q = \emptyset$ and $C_{pq} \geq (C_p - 1) + (C_q - 1)$. Additionally, these cycles will all have length $ord_p(10)$ or $ord_q(10)$.

Now the loop $(0, 0)$ is the only remaining cycle in both $G(p)$ and $G(q)$. Since $(p \cdot 0, p \cdot 0) = (0, 0) = (q \cdot 0, q \cdot 0)$, this loop in both $G(p)$ and $G(q)$ produces only one loop in $G(pq)$. Thus, $C_{pq} \geq (C_p - 1) + (C_q - 1) + 1 = C_p + C_q - 1$.

These cycles include all of the vertices in $G(pq)$ that are divisible by p or q. Since 0 is divisible by both, $(p - 1) + (q - 1) + 1 = p + q - 1$ vertices are already in a cycle.

The remaining $pq-(p+q-1)$ vertices are relatively prime to pq, so by Theorem 2.5, these vertices form $\frac{pq-(p+q-1)}{ord_{pq}(10)}$ more cycles with length $ord_{pq}(10)$ Thus,

$$C_{pq} = \frac{pq-p-q+1}{ord_{pq}(10)} + C_p + C_q - 1 \tag{2.2}$$

and the cycles all have length 1, $ord_p(10)$, $ord_q(10)$, or $ord_{pq}(10)$. □

Figure 2.4(b) shows in red the two 6-cycles on the vertices that are multiples of 3. Also, $(13,13)$ and $(26,26)$ are the two nonzero 1-cycles formed by the multiples of 13. The remaining nonzero vertices are divided into four cycles with length $ord_{39}(10) = 6$. Thus, C_{39} should be 9, and in fact, has

$$\begin{aligned} C_{39} &= \frac{39-13-3+1}{ord_{39}(10)} + C_{13} + C_3 - 1 \\ &= \frac{24}{6} + 3 + 3 - 1 \\ &= 9. \end{aligned}$$

We now look to generalize this to all $G(n)$ where n is relatively prime to 10.

Theorem 2.8.

Let $\gcd(10,n) = 1$, *then*

$$C_n = \sum_{d|n} \frac{\phi(d)}{ord_d(10)}$$

and the set of cycle lengths is $L_n = \{ord_d(10) \mid d|n\}$.

Proof. First, define the set $V_d = \{v \in V(G(n)) \mid \gcd(v,n) = d\}$ for all $d|n$. Every v in $G(n)$ will be in exactly one set V_d, so these sets form a partition of $V(G(n))$. Also, define $G_d(n)$ to be the subgraph of $G(n)$ generated by the vertex set V_d.

Let $a \in V_d$ and $(a,b) \in E(G(n))$. Then $d|a$, so $a = dt$ where $(\frac{n}{d}, t) = 1$ and $b \equiv 10a \equiv 10dt$. Now, consider $\gcd(b,n) = \gcd(10dt, n)$. We know that $\gcd(b,n) \geq d$ since $d|10dt$. Assume $\gcd(b,n) = \gcd(10dt,n) > d$, so $\gcd(10t, \frac{n}{d}) > 1$. Then since

$\gcd(10, n) = 1$, we have $\gcd(\frac{n}{d}, t) > 1$. This is a contradiction to the fact that $(\frac{n}{d}, t) = 1$. Hence, $\gcd(b, n) = d$ and $b \in V_d$. Thus, every cycle in $G(n)$ contains vertices from exactly one set V_d and we can determine C_n by adding the number of cycles in $G_d(n)$ for every $d|n$, or

$$C_n = \sum_{d|n} (\text{number of cycles in } G_d(n)) \tag{2.3}$$

We now need to find the number of cycles in each subgraph $G_d(n)$. Let (a, b) be an edge in $G_d(n)$. We already have $a = dt$ where $\gcd(\frac{n}{d}, t) = 1$, and similarly, $b = ds$ where $\gcd(\frac{n}{d}, s) = 1$. Thus, $(a, b) = (dt, ds)$. By Theorem 2.6, if $(dt, ds) \in E(G(n))$, then $(t, s) \in E(G(\frac{n}{d}))$. Since t and s are relatively prime to $\frac{n}{d}$, it is now equivalent to find the number of cycles on the vertices of $G(\frac{n}{d})$ relatively prime to $\frac{n}{d}$. In other words, the number of cycles in $G_d(n)$ is the same as the number of cycles in $G_1(\frac{n}{d})$. From Theorem 2.5, we know that $G_1(\frac{n}{d})$ contains $\dfrac{\phi(\frac{n}{d})}{ord_{\frac{n}{d}}(10)}$ cycles with length $ord_{\frac{n}{d}}(10)$.

Thus, there are also $\dfrac{\phi(\frac{n}{d})}{ord_{\frac{n}{d}}(10)}$ cycles in $G_d(n)$ with length $ord_{\frac{n}{d}}(10)$. Therefore,

$$C_n = \sum_{d|n} \frac{\phi(\frac{n}{d})}{ord_{\frac{n}{d}}(10)}.$$

Every divisor d_1 can be written as $d_1 = \frac{n}{d_2}$ for some other divisor, d_2. Hence, as we sum over every divisor d we are also summing over $\frac{n}{d}$ for every d, so we can rewrite C_n as

$$C_n = \sum_{d|n} \frac{\phi(d)}{ord_d(10)} \tag{2.4}$$

□

One example of the previous theorem is $G(77)$ (Fig. 2.5). To make it easier to see the various cycles of $G(77)$, Figures 2.6 and 2.7 show the subgraphs of $G(77)$ generated by V_d for $d = 1, 7, 11, 77$. Figure 2.6(a) shows the entire subgraph $G_1(77)$,

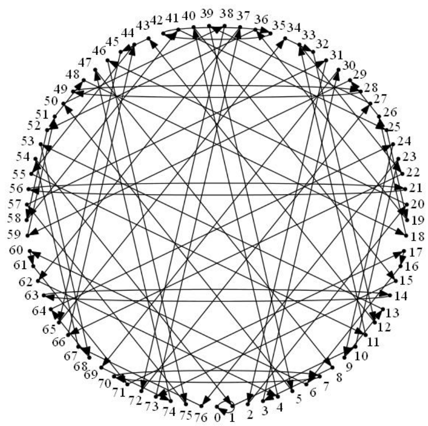


Figure 2.5: $G(77)$ is built from subgraphs isomorphic to graphs of its factors

or on all the vertices relatively prime to 77. This subgraph contains ten 6-cycles, which have been pulled apart further in the rest of Figure 2.6.

Looking at $G_7(77)$ in Figure 2.7(a), the vertices all have $\gcd(v, 77) = 7$. If we compare this subgraph to $G(11)$ in Figure 2.3, we see that $G_7(77)$ is isomorphic to $G_1(11)$ by the isomorphism $h(v) = 7v$. This isomorphism comes directly from Theorem 2.6 on the relation of edges in $G(n)$ and in $G(mn)$. Similarly, $G_{11}(77)$ in Figure 2.7(b) is isomorphic to $G_1(7)$. Finally, $G_{77}(77)$ in Figure 2.7(c) is simply the isolated fixed point isomorphic to $G(1)$ that appears in every $G(n)$ where $(10, n) = 1$.

From both the above theorem and example as well as Theorem 2.6, we can now see how graphs of divisors of n will appear in the graph $G(n)$. For $d|n$, the subgraph $G_d(n)$ is isomorphic to the subgraph $G_1(\frac{n}{d})$. Thus, much of $G(n)$ is built from the graphs of $G(d)$. The subgraph $G_1(n)$, on the vertices that are relatively prime to n, is the only portion of the total graph $G(n)$ that can not be built directly from a graph $G(d)$ for some $d|n$.

Theorem 2.8 also allows us to reconsider Corollary 2.1 and Theorem 2.7. Since $\phi(p) = p - 1$ for any prime p, Equation 2.1 becomes $C_p = \dfrac{\phi(p)}{ord_p(10)} + 1$. Then, by their

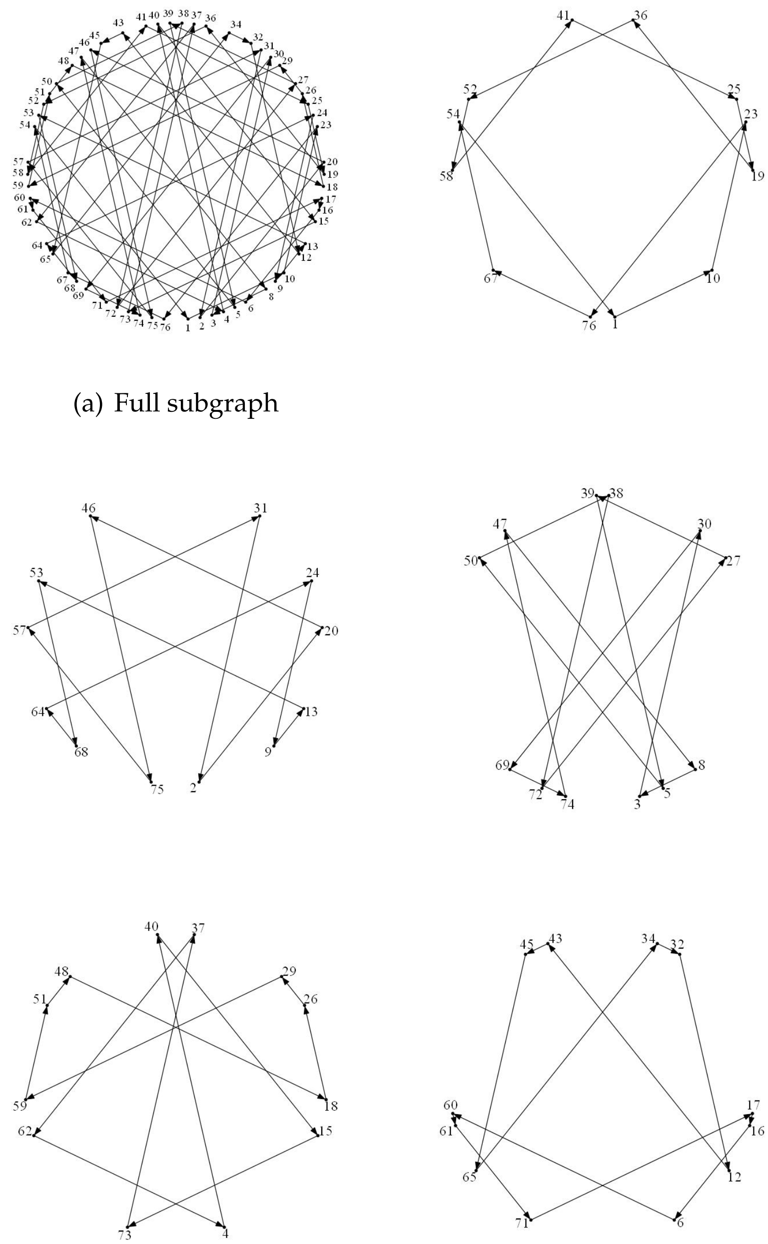
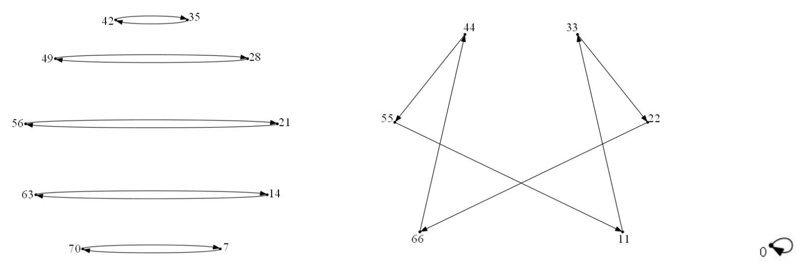


Figure 2.6: The full subgraph of $G(77)$ generated by V_1, and then separated into pairs of 6-cycles.



(a) V_7 (b) V_{11} (c) V_{77}

Figure 2.7: The subgraphs of $G(77)$ generated by V_7, V_{11}, and V_{77}.

definitions, $\phi(1) = ord_1(10) = 1$. Thus

$$C_p = \frac{\phi(p)}{ord_p(10)} + \frac{\phi(1)}{ord_1(10)} = \sum_{d|p} \frac{\phi(d)}{ord_d(10)}.$$

In the proof of Theorem 2.7, we determined the number of vertices relatively prime to pq to be $pq - p - q + 1$, but by definition, this is just $\phi(pq)$. Then Equation 2.2 becomes

$$C_{pq} = \frac{\phi(pq)}{ord_{pq}(10)} + C_p + C_q - 1$$
$$C_{pq} = \frac{\phi(pq)}{ord_{pq}(10)} + \left(\frac{\phi(p)}{ord_p(10)} + 1\right) + \left(\frac{\phi(q)}{ord_q(10)} + 1\right) - 1$$
$$C_{pq} = \frac{\phi(pq)}{ord_{pq}(10)} + \frac{\phi(p)}{ord_p(10)} + \frac{\phi(q)}{ord_q(10)} + 1$$
$$C_{pq} = \frac{\phi(pq)}{ord_{pq}(10)} + \frac{\phi(p)}{ord_p(10)} + \frac{\phi(q)}{ord_q(10)} + \frac{\phi(1)}{ord_1(10)}$$
$$C_{pq} = \sum_{d|pq} \frac{\phi(d)}{ord_d(10)}.$$

Thus, Theorem 2.8 is a generalization of both Corollary 2.1 and Theorem 2.7.

We now have the basic structure of the graph for any n relatively prime to 10 and can consider which integers produce a more specific structure. The next section, explores how multiples of 3 affect the structure of a graph to produce a set of isomorphic subgraphs.

CHAPTER 3

Multiples of 3

In looking at the graphs of integers relatively prime to 10, we saw that 3 was the exception to some of the previous theorems. This is because of the unique relationship between 3 and 10. We see that because $10 \equiv 1 \mod 3$, for every vertex, v, in $G(3)$, $10v \equiv v \mod 3$, or (v, v) is an edge. This is shown in Figure 3.1. This property of $G(3)$ leads to a highly predictable structure for $G(3n)$ where $\gcd(3, n) = 1$.

We first need to establish some notation for the vertices of $G(n)$ and $G(3n)$. Define V to be the vertex set of $G(n)$, so $V = V(G(n)) = \{0, 1, 2, \ldots n - 1\}$. Also define

$$V_t = \{3v + tn \mod 3n \mid v \in V\} \text{ for } t = 0, 1, 2.$$

If $v \in V$, then $v_t = (3v + tn \mod 3n) \in V_t$. For $n = 2$, we have $G(2)$ with $V = \{0, 1\}$ and $G(3n) = G(6)$ with $V_0 = \{0, 3\}$, $V_1 = \{2, 5\}$, and $V_2 = \{1, 4\}$ in Figure 3.2.

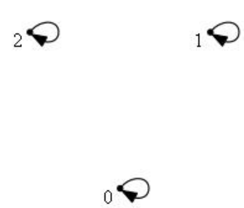


Figure 3.1: Every vertex in $G(3)$ is an isolated fixed point

The following theorem uses these vertex sets to relate the edge sets of $G(n)$ and $G(3n)$.

Theorem 3.1.

If $3 \nmid n$ and $E(G(n) = \{(a, b) \mid b = f(a), a \in V\}$, then $E(G(3n)) = \{(a_t, b_t) \mid (a, b) \in E(G(n)), t = 0, 1, 2\}$

Proof. Let (a, b) be an edge in $G(n)$. Then $10a \equiv b \mod n$, so

$$10a - b = nk$$
$$30a - 3b = 3nk.$$

Thus, $10(3a) \equiv 3b \mod 3n$, and $(3a, 3b) = (a_0, b_0)$ is an edge in $G(3n)$. Now, consider

$$\begin{aligned} 10(3a + n) &\equiv 30a + 10n \mod 3n \\ &\equiv 3b + n + 3(3n) \mod 3n \\ &\equiv 3b + n \mod 3n \end{aligned}$$

and

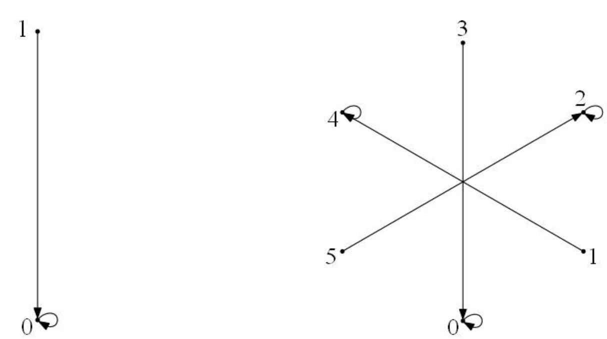
$$\begin{aligned} 10(3a + 2n) &\equiv 30a + 20n \mod 3n \\ &\equiv 3b + 2n + 6(3n) \mod 3n \\ &\equiv 3b + 2n \mod 3n. \end{aligned}$$

Therefore, (a_1, b_1) and (a_2, b_2) are also edges in $G(3n)$. We now have the set of edges $S = \{(a_t, b_t) \mid (a, b) \in E(G(n)), t = 0, 1, 2\}$ which is a subset of $E(G(3n))$. By definition of an iteration digraph, we know that $G(3n)$ has $3n$ distinct edges. The set S has $3n$ edges, which we now need to show are distinct.

From Theorem 2.1, since V is a complete system of residues modulo and $\gcd(3, n) = 1$, we know that V_0, V_1, and V_2 each contain n incongruent integers.

Then, if $a \in V$, we have $a_0 \equiv 0 \mod 3$, $a_1 \equiv n \mod 3$, and $a_2 \equiv 2n \mod 3$. Hence, for any $b, c, d \in V$, not necessarily distinct, b_0, c_1, and d_2 are incongruent modulo 3. Now, assume $b_0 \equiv c_1 \mod 3n$, so $b_0 - c_1 = 3n(p)$ for some integer p. Then $b_0 - c_1 = 3(np)$ and $b_0 \equiv c_1 \mod 3$. This is a contradiction since b_0 and c_1 are incongruent mod 3. Hence, $b_0 \not\equiv c_1 \mod 3n$. Similarly, $b_0 \not\equiv d_2 \mod 3n$ and $c_1 \not\equiv d_2 \mod 3n$. Thus, for any $b, c, d \in V$, b_0, c_1, and d_2 are incongruent modulo $3n$. Furthermore, $a_t \not\equiv b_r \mod 3n$ whenever either $a \not\equiv b \mod n$ or $r \neq t$. Therefore, the $3n$ edges in S are distinct, so $E(G(3n)) = S = \{(a_t, b_t) \mid (a, b) \in E(G(n)), t = 0, 1, 2\}$. □

The graph for $n = 6$ in Figure 3.2(b) has three components on the sets of vertices $\{0, 3\}$, $\{1, 4\}$, and $\{2, 5\}$. Comparing these to $G(2)$, each component is isomorphic to $G(2)$. Thus, the relation from Theorem 3.1 between any $G(n)$ and $G(3n)$ can also be expressed in terms of isomorphisms between the graphs.



(a) $G(2)$ (b) $G(6)$

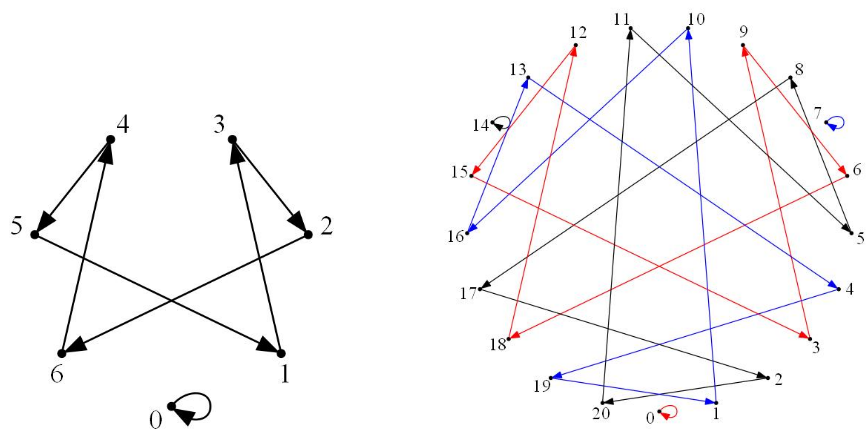
Figure 3.2: The components of $G(6)$ are all isomorphic to $G(2)$.

Corollary 3.1.

$G(3n)$ is the union of three subgraphs, each of which is isomorphic to $G(n)$.

Proof. Let $G_t(3n)$ be the subgraph of $G(3n)$ generated by the set V_t. Then, from Theorem 3.1, we know that $E(G_t(3n)) = \{(a_t, b_t) \mid (a, b) \in E(G(n))\}$ contains n distinct edges. These edges are related to those of $G(n)$ by the isomorphism $h : V \to V_t$ where $h(v) = 3v + tn$, because $(a, b) \in E(G(n))$ if and only if $(h(a), h(b))$ is an edge in the subgraph on V_t. Therefore, $G(n)$ is isomorphic to $G_t(3n)$ for $t = 0, 1, 2$. □

Another example, for $n = 7$ is given in Figure 3.3. The isomorphic subgraph $G_0(21)$ is shown in red, $G_1(21)$ is in blue, and $G_2(21)$ is black.



(a) $G(7)$ (b) $G(21)$

Figure 3.3: $G(7)$ is isomorphic to three subgraphs of $G(21)$.

3.1 Multiples of 9

The structural elements of $G(3n)$ resulting from the fact that $10 \equiv 1 \mod 3$ are also seen in the graphs of $9n$ when $3 \nmid n$. This is again because $10 \equiv 1 \mod 9$, so every vertex in $G(9)$ is an isolated fixed point.

Again, we need the same type of sets used before, so $V = V(G(n))$ and

$$V_t = \{9v + tn \mod 9n | v \in V\} \text{ for } t = 0, 1, 2 \ldots 8.$$

Also, if $v \in V$, then $v_t = (9v + tn \mod 9n) \in V_t$. These sets help to describe the sets of corresponding edges in $G(n)$ and $G(9n)$ in the following theorem.

Theorem 3.2.

If $3 \nmid n$ *and* $E(G(n) = \{(a, b) \mid b = f(a), a \in V\}$, *then*

$$E(G(9n)) = \{(a_t, b_t) \mid (a, b) \in E(G(n)), t = 0, 1, 2 \ldots 8\}.$$

Proof. Let (a, b) be an edge in $G(n)$. Then $10a \equiv b \mod n$ and by Theorem 2.6, we know $10(9a) \equiv 9b \mod 9n$. Now, considering $a_t = 9a + tn$, we get

$$\begin{aligned} 10(9a + tn) &\equiv 90a + 10tn \mod 9n \quad (3.1) \\ &\equiv 9b + tn + 9tn \mod 9n \\ &\equiv 9b + tn \mod 9n. \end{aligned}$$

Therefore, (a_t, b_t) is also an edge in $G(9n)$ for all $t = 0, 1, 2 \ldots 8$. We now have the set of edges $S = \{(a_t, b_t) \mid (a, b) \in E(G(n)), t = 0, 1, 2 \ldots 8\}$ which is a subset of $E(G(9n))$. As in Theorem 3.1, we now need to show that the $9n$ edges in S are distinct.

Again, since V is a complete system of residues modulo 9 and $\gcd(3, n) = 1$, V_t has n incongruent integers for all $t = 0, 1, 2, \ldots 8$.

For all $a \in V_t$, we have $a_t \equiv 9a + tn \equiv tn \mod 9$ since $t < 9$. Thus, for any $b, c \in V$, not necessarily distinct, if $t \neq s$, then $b_t \not\equiv c_s \mod 9$.

Now, suppose $b_t \equiv c_s \mod 9n$. Then $b_t - c_s = 9n(p)$ for some integer p and $b_t - c_s = 9(np)$, so $b_t \equiv c_s \mod 9$. This is a contradiction, so $b_t \not\equiv c_s \mod 9n$ whenever $t \neq s$. We now have $b_t \not\equiv c_s \mod 9n$ whenever either $b \not\equiv c \mod n$ or

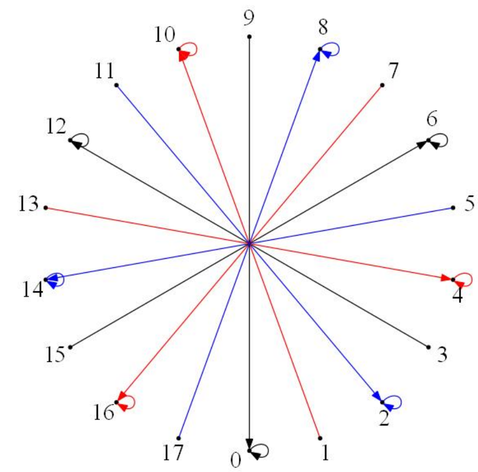


Figure 3.4: $G(18)$ is comprised of 9 subgraphs isomorphic to $G(2)$

$t \neq s$. Therefore, the $9n$ edges in S are distinct, so $E(G(3n)) = S = \{(a_t, b_t) \mid (a, b) \in E(G(n)), t = 0, 1, 2, \ldots 8\}$. □

As with the $G(3n)$ case, the edges produced from Theorem 3.2 indicate subgraphs of $G(9n)$ that are isomorphic to $G(n)$.

Corollary 3.2.

$G(9n)$ is the union of nine subgraphs, each of which is isomorphic to $G(n)$.

Proof. Let $G_t(9n)$ be the subgraph of $G(9n)$ generated by the set V_t. Since $(9a + tn, 9b + tn)$ is a distinct edge in $G(9n)$ for every (a, b) in $G(n)$, the function $h(v) = 9v + tn$ is an isomorphism from V to V_t for $t = 0, 1, 2, \ldots 8$. Therefore, $G(n)$ is isomorphic to $G_t(9n)$. □

The 9 subgraphs in $G(9n)$ that are isomorphic to $G(n)$ can also be viewed as 3 subgraphs, each isomorphic to $G(3n)$.

Theorem 3.3.

If 3 does not divide n, then $E(G(9n)) = \{(3a_t + sn, 3b_t + sn) \mid (a_t, b_t) \in E(G(3n))$ and $s = 0, 1, 2\}$.

Proof. Let $\gcd(3, n) = 1$ and $(a_t, b_t) \in E(G(3n))$. Then consider $(3a_t + sn, 3b_t + sn)$. From Theorem 3.1, we know that $a_t = 3a + tn$ and $b_t = 3b + tn$ where $(a, b) \in E(G(n))$ and $t = 0, 1, 2$. Hence,

$$\begin{aligned}(3a_t + sn, 3b_t + sn) &= (3(3a + tn) + sn, 3(3b + tn) + sn) \\ &= (9a + 3tn + sn, 9b + 3tn + sn) \\ &= (9a + (3t + s)n, 9b + (3t + s)n).\end{aligned}$$

Let $q = 3t + s$. Since $t, s \in \{0, 1, 2\}$, we have $q = 0, 1, 2, \ldots 8$. Thus, $(3a_t + sn, 3b_t + sn) = (3a + qn, 3b + qn)$ and by Theorem 3.2, $(3a_t + sn, 3b_t + sn) \in E(G(9n))$. Therefore,

$$S = \{(3a_t + sn, 3b_t + sn) \mid (a_t, b_t) \in E(G(3n)) \text{ and } s = 0, 1, 2\}.$$

□

If we reconsider $G(18)$ by the above theorem, the subgraph generated by $V_1 = \{2, 5, 8, 11, 14, 17\}$ is isomorphic to $G(6)$, as are the subgraphs from V_0 and V_2. The three isomorphic graphs are highlighted in Figure 3.4.

From Theorems 3.1 and 3.2 we get a corollary for $C_{3^k n}$ and $L_{3^k n}$ where $k = 1, 2$.

Corollary 3.3.
If $\gcd(3, n) = 1$ *and* $k = 1, 2$*, then* $C_{3^k n} = 3^k C_n$ *and* $L_{3^k n} = L_n$*.*

Proof. The graph of $G(3^k n)$ is comprised of 3^k subgraphs that are isomorphic to $G(n)$ whenever $\gcd(3, n) = 1$. Each subgraph has C_n cycles with the set of lengths L_n. Thus, $C_{3^k n} = 3^k C_n$ and $L_{3^k n} = L_n$. □

Theorems 3.1 and 3.2 also indicate that perhaps this type of edge relation will exist for higher powers of 3. If we have 3^k with $k > 2$ and $(a, b) \in E(G(n))$

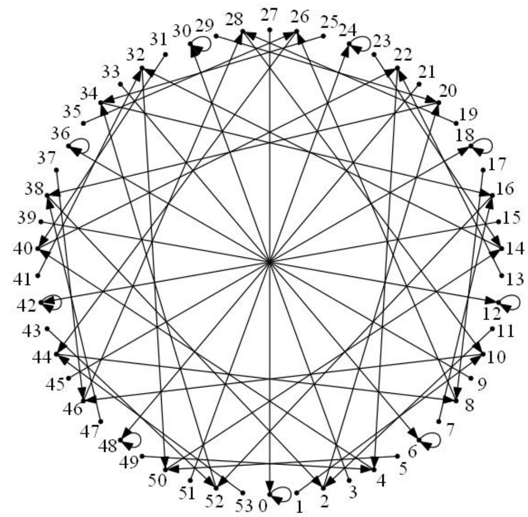


Figure 3.5: $G(54)$ is not comprised entirely of subgraphs that are isomorphic to $G(2)$

where $(3, n) = 1$, then by Theorem 2.6, $(a_0, b_0) = (3^k a, 3^k b) \in E(G(3^n))$. However, for $(a_t, b_t) = (3^k a + tn, 3^k b + tn)$ where $t > 0$, we get

$$10(3^k a + tn) \equiv 10 \cdot 3^k a + 10tn \mod 3^k n$$
$$10(3^k a + tn) \equiv 3^k b + tn + 9tn \mod 3^k n, \tag{3.2}$$

so $10(3^k a + tn) \equiv 3^k b + tn \mod 3^k n$ is true if and only if $9tn \equiv 0 \mod 3^k n$. This means that 3^{k-2} must divide t. Thus, (a_t, b_t) is not a edge of $G(3^k n)$ for every $t = 0, 1, 2, \ldots 3^k - 1$.

For example, in Figure 3.5, $G(54)$ contains some edges of the form $(3^3 a + t \cdot 2, 3^3 b + t \cdot 2)$, such as $(3^3 \cdot 0 + 21 \cdot 2, 3^3 \cdot 0 + 21 \cdot 2) = (42, 42)$ and $(3^k \cdot 1 + 21 \cdot 2, 3^k 0 + 21 \cdot 2) = (15, 42)$. The subgraph of just those two edges is isomorphic to $G(2)$. However, edges such as $(2, 20)$ and $(20, 38)$ cannot be written in the form $(3^3 a + t \cdot 2, 3^3 b + t \cdot 2)$.

This can also be understood visually. Theorems 3.1 and 3.2 were dependent on the fact that Equation 3.2 holds for all values of t. More specifically, this is because

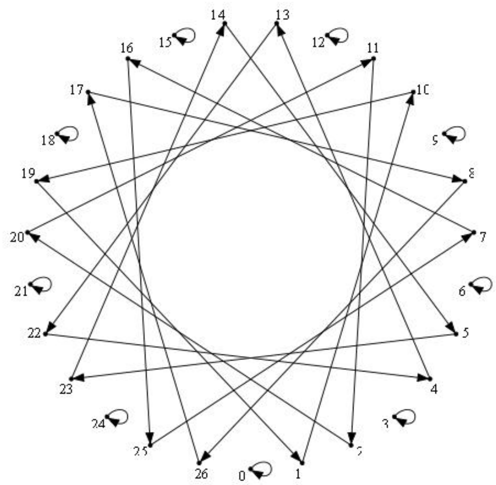


Figure 3.6: 27 is the first power of 3 for which not every vertex in $G(3^k)$ is a fixed point.

$10 \equiv 1 \mod 3$ and $\mod 9$, which is seen graphically in the isolated fixed points at every vertex of $G(3)$ and $G(9)$. Looking at $G(27)$ in Figure 3.6, we see that 27 is the first power of 3 for with $G(3^k)$ has non-fixed points.

While the results in this section do not require that n be relatively prime to 10, we have mostly ignored integers divisible by 2 or 5 to this point. In the next section, we consider the how the graph structure is affected when $(10, n) > 1$.

CHAPTER 4

Powers of 2

One class of integers for which $G(n)$ has a distinctive and relatively predictable digraph is the powers of 2. When $n = 2^k$ for some integer $k > 0$, $G(2^k)$ takes the form of a binary tree with all edges heading towards the root. In this section, congruences should all be considered modulo 2^k unless otherwise specified.

The unique form of $G(2^k)$ is resultant from the fact that 2 is a factor of 10. Suppose $G(2^k)$ contains an r-cycle, so $10^r a \equiv a$ for every vertex in the cycle. Then $10^r a - a = 2^k b$ for some integer b and $(10^r - 1)a = 2^k b$, so $2^k | (10^r - 1)a$. Because $2|10$, 2 does not divide $(10^r - 1)$ and neither can 2^k. Hence, $2^k | a$, but 0 is the only vertex in $G(2^k)$ which is divisible by 2^k. Thus, all nonzero vertices in $G(2^k)$ are also noncyclic.

Given the tree structure of digraphs for powers of 2, which will be proved in Theorem 4.1, each vertex will be referenced by its level and its position within that level. Number the vertices in level $i < k$ left to right from 0 to $2^s - 1$ where $s = k - i - 1$. Then $v_{i,t}$ is the the vertex in level $0 \leq i \leq k$ at position $0 \leq t \leq 2^s - 1$. In Figure 4.1, for example, $v_{0,0} = 1$, $v_{0,1} = 5$, and $v_{1,0} = 2$. Additionally, for each pair of vertices $v_{i,t}$ and $v_{i,t+1}$ where both are adjacent to the same vertex at level $i + 1$, we will draw the graph such that $v_{i,t} < v_{i,t+1}$.

For the first theorem, we need to define notation for **exactly divides**. We say that a^k exactly divides b if k is the largest power a that divides b. We write $a||b$. Thus, $2^3||24$ because $8|24$, but $16 \nmid 24$.

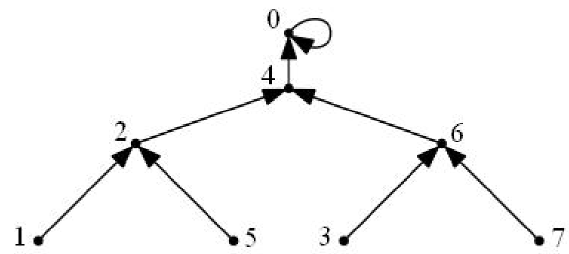


Figure 4.1: $G(8)$

We can now develop the basic structure of the 2^k iteration digraph.

Theorem 4.1.

If $G(n)$ is the iteration digraph of $f(x) \equiv 10x \mod 2^k$ where $n = 2^k$ for $k = 1, 2, 3, \ldots,$ then

1. *$G(n)$ has $k + 1$ levels*
2. *The non-zero vertices form a complete binary tree with height k and with 2^{k-1} as the root*
3. *0 and 2^{k-1} are adjacent to 0*
4. *exactly 2 vertices at level $i < k - 1$ are adjacent to each vertex at level $i + 1$*
5. *for each vertex, $v_{i,t}$, at level $i < k$, $2^i \| v_{i,t}$*
6. *the number of vertices in level $i < k$ is 2^{k-i-1}*
7. *for any vertex v at level 0, the shortest path from v to the 0 vertex has length k*

Proof. Part 3 is easily seen since $f(2^k) = 10 \cdot 2^k \equiv 0$ and $f(2^{k-1}) = 10 \cdot 2^{k-1} = 5 \cdot 2^k \equiv 0$.

For part 1, we know that for any vertex, v, $10^k v = 2^k(5^k v) \equiv 0 \mod 2^k$. Thus, the longest possible path from v to 0 has length k. Now suppose the longest path that exists is only $k-1$ edges long. Then $10^{k-1}v = 2^{k-1}(5^{k-1}v) \equiv 0$ for all v. This means that

$$2^{k-1}(5^{k-1}v) = 2^k p$$
$$5^{k-1}v = 2p$$

and v must be divisible by 2. This is a contradiction for all odd vertices, so there must exist a path from v to 0 with length k. Thus, $G(2^k)$ has $k+1$ levels.

Considering part 5, at level $k-1$, we have $2^{k-1} \| 2^{k-1}$. Now, assume that $2^i \| v_{i,t}$ for all vertices at some level $i < k-1$ and let $v_{i-1,r}$ be adjacent to $v_{i,t} = 2^i c$ where c is an odd integer. Hence, $v_{i-1,r}$ is at level $i-1$ and

$$10v_{i-1,r} - v_{i,t} = 2^k b$$
$$10v_{i-1,r} - 2^i c = 2^k b$$
$$10v_{i-1,r} = 2^i(2^{k-i}b + c)$$

Thus, 2^i divides $10v_{i-1,r}$, so 2^{i-1} divides $v_{i-1,r}$.

We now need to show that $2^{i-1} \| v_{i-1,r}$. Assume that $2^i | v_{i-1,r}$, then $10v_{i-1,r} \equiv v_{i,t}$ is divisible by 2^{i+1}. This is a contradiction to the initial assumption that $2^i \| v_{i,t}$. Therefore, 2^i does not divide $v_{i-1,r}$, so $2^{i-1} \| v_{i-1,r}$, and for every vertex, $v_{i,t}$, at a level $i < k$, $2^i \| v_{i,t}$

For part 6, we know from part 5 that level i will contain all of the vertices exactly divisible by 2^i. For any $i \leq k$, 2^i will divide $1/2^i$ of the vertices, or $2^k/2^i = 2^{k-i}$ vertices. Then, the number of vertices that 2^i exactly divides will be all of those not divisible by 2^{i+1}, or $2^{k-i} - 2^{k-(i+1)} = 2^{k-i-1}$. Thus, the number of vertices at level i is 2^{k-i-1}.

For part 4, let a and b be vertices such that $f(a) = b$ and b is at level i where

$0 < i \le k-1$. Then consider $a + 2^{k-1}$.

$$\begin{aligned} f(a + 2^{k-1}) &= 10a + 10 \cdot 2^{k-1} \\ &\equiv b + 5 \cdot 2^k \\ &\equiv b + 0 \mod 2^k. \end{aligned} \tag{4.1}$$

Since $2^{k-1} < 2^k$, then $a \not\equiv a + 2^{k-1} \mod 2^k$. Thus, at least two distinct vertices are adjacent to b. From part 5, there are 2^{k-i-1} vertices at level i and 2^{k-i} at level $i+1$, so there are exactly twice as many vertices at level i as at level $i+1$. Thus, exactly two vertices are adjacent to each vertex at level $0 < i < k$.

Part 2 also follows directly from parts 4 and 5 and the definition of a tree, so the non-zero vertices form a complete binary tree with height k and with 2^{k-1} as the root.

Finally, for part 7, suppose there is a vertex v at level 0 such that the path from v to 0 has length $j < k$. Then $10^j v \equiv 0$, so

$$\begin{aligned} 10^j v &= 2^k p \\ 2^j 5^j v &= 2^k p \\ 5^j v &= 2^{k-j} p. \end{aligned}$$

Thus, 2^{k-j} divides v. This contradicts part 5, where $2^0 | v$ since v is at level 0. Therefore, the shortest path from v to 0 has length k. □

Note that part 7 of the above theorem means that there is no branch of the tree which stops shorter or longer than the others.

Using the results of Theorem 4.1, the basic structure of $G(2^k)$ can now be constructed for any nonnegative k. The next step is to label the vertices with the correct values modulo 2^k. Unfortunately, this turns out to be a much more complex task. However, given the label of one vertex, several other vertices can also be determined.

Corollary 4.1.

If $i \leq k-2$ and t is an even integer, then $v_{i,t+1} = v_{i,t} + 2^{k-1}$

Proof. Since t is even, if $v_{i,t}$ is adjacent to $v_{i+1,r}$, then $v_{i,t+1}$ is also adjacent to the same vertex. From Equation (4.1), we see that $v_{i,t+1} = v_{i,t} + 2^{k-1}$ will be adjacent to $v_{i+1,r}$. □

There is clearly a symmetry to the tree structure of $G(2^k)$, but there is also a symmetry to the vertex labels, which is illustrated in the following theorem.

Theorem 4.2.

For the digraph $G(2^k)$, $v_{i,2^s-1-t} = 2^k - v_{i,t}$ for all $i \in \{0, 1, 2, \ldots k\}$ and $t \in \{0, 1, 2, \ldots 2^s - 1\}$

Before proving the above theorem, we need to consider a more basic form of symmetry for all $G(n)$.

Lemma 4.1.

If (a, b) is an edge in $G(n)$, then $(-a, -b)$ is also an edge in $G(n)$.

Proof. In $G(n)$ pick distinct edges (a_1, b_1) and (a_2, b_2) such that $a_2 \equiv -a_1 \mod n$. Then

$$\begin{aligned} a_1 + a_2 &\equiv 0 \mod n \\ 10a_1 + 10a_2 &\equiv 0 \mod n \\ b_1 + b_2 &\equiv 0 \mod n \end{aligned}$$

Thus, $b_2 \equiv -b_1 \mod n$, so $(a_2, b_2) = (-a_1, -b_1)$. □

Note that Lemma 4.1 applies to the graphs of all integers, not just the powers of 2. The next lemma gives intervals for the label of every vertex.

Lemma 4.2.

If $i < k-1$, then t is even if and only if $0 < v_{i,t} < 2^{k-1}$

Proof. Recall that for two vertices, a and b, at level $i < k-1$ both adjacent to the same vertex, if $a < b$, then we label the left vertex a and the right vertex b. Thus, $v_{i,m} = a$ and $v_{i,m+1} = b$ means m must be an even index. From Corollary 4.1 recall also, that $a = b + 2^{k-1}$. Then, since $a, b < 2^k$ and $a < b$. we have that $0 < a < 2^{k-1}$ and, hence, $2^{k-1} < b < 2^k$. □

We are now ready to prove Theorem 4.2.

Proof. At levels k and $k-1$, there is only one vertex, so it is trivial to see that $v_{k,0} = 0 \equiv -v_{k,0}$ and $v_{k,0} = 2^{k-1} \equiv -v_{k,0}$. For induction on i, in the base case at level $k-2$, there are two vertices, $v_{k-2,0}$ and $v_{k-2,1} = v_{k-2,2^1-1-0}$. Both vertices are exactly divisible by 2^{k-2} and are less than $2^k = 4 \cdot 2^{k-2}$, so we have $v_{k-2,0} = 2^{k-2}$ and $v_{k-2,1} = 3 \cdot 2^{k-2}$. Thus,

$$\begin{aligned} v_{k-2,1} &= 4 \cdot 2^{k-2} - v_{k-2,0} \\ &= 2^k - v_{k-2,0} \end{aligned}$$

Now, let $i < k-2$ and assume

$$v_{i+1,2^q-1-r} \equiv -v_{i+1,r} \tag{4.2}$$

for all $r \in \{0, 1, 2, \ldots 2^q - 1\}$ where $q = k - (i+1) - 1$, so 2^q is the number of vertices in level $i+1$. Let $(v_{i,t}, v_{i+1,r})$ be an edge of $G(2^k)$. We want to show that $v_{i,2^s-1-t} \equiv -v_{i,t}$.

By Lemma 4.1, $(-v_{i,t}, -v_{i+1,r})$ is also an edge in $G(2^k)$ and by the assumption of Equation 4.2, $(-v_{i,t}, -v_{i+1,r}) = (-v_{i,t}, v_{i+1,2^q-1-r})$. Thus, we know that $-v_{i,t}$ must be congruent to one of the two vertices adjacent to $v_{i+1,2^q-1-r}$. From here, there are two cases if t is odd or if t is even.

Case 1 If t is even, then $2^s - 1 - t$ is odd, so $-v_{i,t}$ is congruent to either $v_{i,2^s-1-t}$ or $v_{i,2^s-2-t}$. This is illustrated in Figure 4.2. By Lemma 4.2, $0 < v_{i,t} < 2^{k-1}$. Then

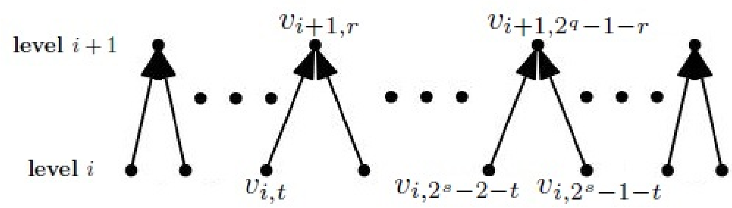


Figure 4.2: Relative positions of vertices in $G(2^k)$ when t is even.

$-v_{i,t} \equiv 2^k - v_{i,t}$, so $2^{k-1} < -v_{i,t} < 2^k$. Therefore, $-v_{i,t} \equiv v_{i,2^s-1-t}$ because $2^s - 1 - t$ is odd.

Case 2 If t is odd, then $2^s - 1 - t$ is even, so $-v_{i,t}$ is congruent to either $v_{i,2^s-1-t}$ or $v_{i,2^s-t}$. Again, by Lemma 4.2, $2^{k-1} < v_{i,t} < 2^k$. Then $-v_{i,t} \equiv 2^k - v_{i,t}$, so $0 < -v_{i,t} < 2^{k-1}$. Therefore, $-v_{i,t}$ must be congruent to a vertex in an even position, so $-v_{i,t} \equiv v_{i,2^s-1-t}$.

Therefore, $v_{i,2^s-1-t} \equiv -v_{i,t}$ for all vertices $v_{i,t} \in V(G(2^k))$. Additionally, since $v_{i,t} < 2^k$, we know that $(2^k - v_{i,t}) < 2^k$ and we can rewrite the equivalence as $v_{i,2^s-1-t} = 2^k - v_{i,t}$. □

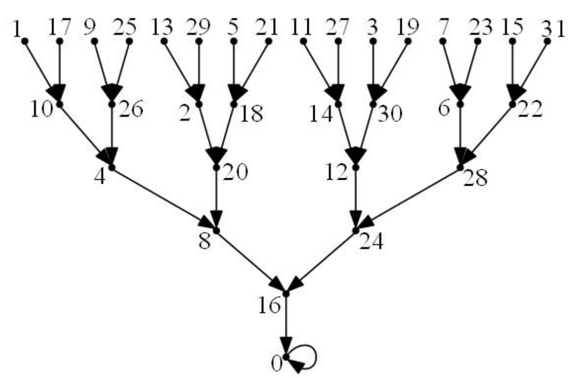


Figure 4.3: $G(32)$ shows the reflective relationship of Theorem 4.2.

For example, consider $v_{1,2} = 2$ of $G(32)$ in Figure 4.3. The corresponding vertex

$$v_{1,2^3-3} = v_{1,5} = 2^k - 2 = 30.$$

Similarly, $v_{0,9} = 27$ and $v_{0,15-9} = v_{0,6} = 5$.

The next theorem shows the isomorphism between $G(2^k)$ and $G(2^m)$ where $m > k$.

Theorem 4.3.

Let $v_{i,t} \in G(2^k)$ and $u_{i,t} \in G(2^m)$ where $m > k$. If $u_{m-j,r} = 2^{m-k}v_{k-i,t}$, then $i = j$ and $t = r$.

Proof. Pick $v_{k-i,t} \in V(G(2^k))$ and $u_{j,r} \in V(G(2^m))$ such that $2^{m-k}v_{k-i,t} = u_{m-j,r}$. Then $2^{k-i} \| v_{k-i,t}$ and multiplying by 2^{m-k}, we get

$$2^{m-k}2^{k-i} \| 2^{m-k}v_{k-i,t}$$
$$2^{m-i} \| u_{m-j,r},$$

so $j = i$.

Now, we need to show that $r = t$. There is only one vertex each at levels k and $k-1$, so we must have $r = t$. For some level $k-i$, with $i > 1$, assume $r = t$ for all $v_{k-i,t}$ and $u_{m-i,r}$ where $2^{m-k}v_{k-i,t} = u_{m-i,r}$. Then, in level $k-i-1$, both $v_{k-i-1,2t}$ and $v_{k-i-1,2t+1}$ are adjacent to $v_{k-i,t}$. Let $2^{m-k}v_{k-i-1,2t} = u_{m-i-1,a}$ and $2^{m-k}v_{k-i-1,2t+1} = u_{m-i-1,b}$. Then

$$\begin{aligned} 10u_{m-i-1,a} &\equiv 10(2^{m-k}v_{k-i-1,2t}) \\ &\equiv 2^{m-k}(10v_{k-i-1,2t}) \\ &\equiv 2^{m-k}(v_{k-i,t}) \\ &\equiv u_{m-i,r} \end{aligned}$$

and similarly $10u_{m-i-1,b} \equiv u_{m-i,r}$. Hence, both $u_{m-i-1,a}$ and $u_{m-i-1,b}$ are adjacent to $u_{m-i,r}$, so either $a = 2r$ and $b = 2r + 1$ or vice versa.

Again making use of Lemma 4.2, $0 < v_{k-i-1,2t} < 2^{k-1}$, so $0 < u_{m-i-1,a} < 2^{m-1}$. Thus, a is even, so $a = 2r$ and $b = 2r + 1$. Then, $2^{m-k}v_{k-i-1,2t} = u_{m-i-1,2r}$ and $2^{m-k}v_{k-i-1,2t+1} =$

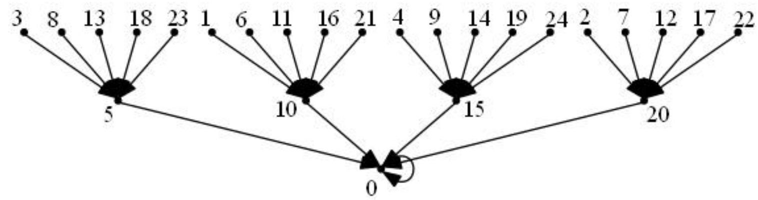


Figure 4.4: $G(25)$

$u_{m-i-1,2r+1}$, so $r = t$ for all $2^{m-k}v_{k-i-1,t} = u_{m-i-1,r}$. Therefore, if $u_{m-j,r} = 2^{m-k}v_{m-i,t}$, then $i - j$ and $r = t$. □

For example, consider $G(8)$ (Fig. 4.1) and $G(32)$ (Fig. 4.3), where $k = 3$ and $m = 5$. We see that $G(8)$ is isomorphic to the subgraph of $G(32)$ generated by the vertex set $V = \{v_{i,t} \mid 2 \leq i \leq 5\}$. The isomorphism is $h(v) = 2^{5-3}v = 4v$.

4.1 Powers of 5

Similar to how $G(3n)$ and $G(9n)$ shared similar properties, the fact that both 2 and 5 are factors of 10 means that powers of 5 have much the same structure as was seen in the 2^k graphs. Additionally, the proofs will be very similar to those for the 2^k graphs. The following discussion of $G(5^k)$ could have been combined with Section 4, however they have been kept separate for the sake of the clarity of the proofs. Generalizing to $G(p^k)$ where $p = 2, 5$ would have made the proofs much more difficult to follow.

With a tree structure of the digraphs similar to those for powers of 2, we will use the same notation for referencing the vertices of $G(5^k)$. We number the vertices in level $i < k - 1$ left to right from 0 to $(4 \cdot 5^s - 1)$ where $s = k - i - 1$. Then $v_{i,t}$ is the the vertex in level i at position t.

Additionally, if $v_{i,t} < v_{i,r}$ and both vertices are adjacent to the same vertex at level $i + 1$, we will draw the graph such that $t < r$. As with $G(2^k)$, we begin with the basic structure of the 5^k graph. In this section, congruences should all be considered modulo 5^k unless otherwise specified.

Theorem 4.4.

If $G(5^k)$ is the iteration digraph of $f(x) \equiv 10x \mod 5^k$ for $k = 1, 2, 3, \ldots$, then

1. *$G(5^k)$ has $k + 1$ levels*
2. *The non-cyclic edges form a 5-ary tree with height k and with $5^k \equiv 0$ as the root*
3. *$5^{k-1}c$ for $c = 0, 1, 2, 3, 4$ are all adjacent to 0*
4. *exactly 5 vertices at level $i < k - 1$ are adjacent to each vertex at level $i + 1$*
5. *for each vertex, $v_{i,t}$, at level $i < k$, $5^i \| v_{i,t}$*
6. *at level $i < k$, there are $4 \cdot 5^s$ vertices where $s = k - i - 1$.*
7. *for any vertex v at level 0, the shortest path from v to the 0 vertex has length k*

Proof. Part 3 is easily seen since $f(5^{k-1}c) = 10 \cdot 5^{k-1}c = 2 \cdot 5^k c \equiv 0$.

For part 1, we know that $10^k v = 5^k(2^k v) \equiv 0$ for all v in $G(5^k)$, so the longest possible, noncyclical path has length k. Assume, that the longest noncyclical path that exists in $G(5^k)$ only has length $(k - 1)$. Then $10^{k-1}v \equiv 0 \mod 5^k$ for all $v \in V(G(5^k))$. Thus,

$$10^{k-1}v = 5^k n$$

$$2^{k-1}5^{k-1}v = 5^k n$$

$$2^{k-1}v = 5n,$$

so 5 divides all v. This is clearly a contradiction, so there must exist at least one path with length k. Therefore, there are $k + 1$ levels in $G(5^k)$.

For part 5, at level $k-1$, we have $5^{k-1} \| 5^{k-1}c$ for $c = 1, 2, 3, 4$. Now, assume that $5^i \| v_{i,t}$ for all vertices at some level $i < k-1$ and let $v_{i-1,r}$ be adjacent to $v_{i,t} = 5^i a$ where $5 \nmid a$. Hence, $v_{i-1,r}$ is at level $i-1$ and

$$\begin{aligned} 10v_{i-1,r} - v_{i,t} &= 5^k b \\ 10v_{i-1,r} - 5^i a &= 5^k b \\ 10v_{i-1,r} &= 5^i(5^{k-i}b + a) \end{aligned}$$

Thus, 5^i divides $10v_{i-1,r}$, so 5^{i-1} divides $v_{i-1,r}$. If we now assume that $5^i | v_{i-1,r}$, then $10v_{i-1,r} = v_{i,t}$ is divisible by 5^{i+1}. This is a contradiction, hence, 5^i does not divide $v_{i-1,r}$, and $5^{i-1} \| v_{i-1,r}$. Therefore, for every vertex, $v_{i,t}$, at a level i, $5^i \| v_{i,t}$.

For part 6, we know from part 5 that level i will contain all of the vertices exactly divisible by 5^k. For any $i \leq k$, 5^i will divide $1/5^i$ of the vertices, or $5^k/5^i = 5^{k-i}$ vertices. Then, the number of vertices that 5^i exactly divides will be all of those not divisible by 5^{i+1}, or $5^{k-i} - 5^{k-(i+1)} = 4 \cdot 5^{k-i-1}$. Thus, the number of vertices at level i is $(4 \cdot 5^{k-i-1})$.

For part 4, let a and b be vertices such that $f(a) = b$ and b is at level i where $0 < i \leq k-1$. Then consider $a + 5^{k-1}c$ for $c = 0, 1, 2, 3, 4$.

$$\begin{aligned} f(a + 5^{k-1}c) &= 10a + 10 \cdot 5^{k-1}c \\ f(a + 5^{k-1}c) &\equiv b + 2 \cdot 5^k c \\ f(a + 5^{k-1}c) &\equiv b + 0. \end{aligned} \tag{4.3}$$

Since $5^{k-1}c < 5^k$, then $a \not\equiv a + 5^{k-1}c \mod 5^k$. Thus, at least five distinct vertices are adjacent to b. From part 5, there are $4 \cdot 5^{k-i-1}$ vertices at level i and $4 \cdot 5^{k-i}$ at level $i+1$, so there are five times as many vertices at level i as at level $i+1$. Thus, exactly five vertices are adjacent to each vertex at level $0 < i < k$.

Part 2 also follows directly from parts 4 and 5 and the definition of a tree, so the non-zero vertices form a 5-ary tree with height k and with 5^{k-1} as the root.

Finally, for part 7, suppose there is a vertex v at level 0 such that the path from v to 0 has length $j < k$. Then $10^j v \equiv 0$, so

$$\begin{aligned} 10^j v &= 5^k p \\ 2^j 5^j v &= 5^k p \\ 2^j v &= 5^{k-j} p. \end{aligned}$$

Because 5 does not divide 2^j, 5^{k-j} must divide v. Since v is at level 0, this contradicts part 5 which says that v must be at least at level $k - j > 0$. Therefore, the shortest path from v to 0 has length k. □

Just as with $G(2^k)$, we now want to label the vertices through their relations to each other.

Corollary 4.2.
If $i \leq k-2$ and $t \equiv 0 \mod 5$, then $v_{i,t+c} = v_{i,t} + 5^{k-1}c \mod 5^k$ for $c = 0, 1, 2, 3, 4$.

Proof. Since $t \equiv 0 \mod 5$, if $v_{i,t}$ is adjacent to $v_{i+1,r}$, then $v_{i,t+c}$ is adjacent to the same vertex for $c = 0, 1, 2, 3, 4$. From Equation (4.3), we see that $v_{i,t+c} = v_{i,t} + 5^{k-1}c$ will be adjacent to $v_{i+1,r}$. □

In Figure 4.4, $G(25)$ is an example of this relationship between the 5 vertices adjacent to a common vertex. In a position equivalent to $0 \mod 5$, $v_{0,10} = 4$. Then,

$$v_{0,10+1} = 4 + 5^{2-1} \cdot 1 = 9,$$

$$v_{0,12} = 4 + 5 \cdot 2 = 14,$$

$v_{0,13} = 19$ and $v_{0,14} = 24$. Similarly, starting with $v_{0,15} = 2$, we have $v_{0,16} = 7$, $v_{0,17} = 12$, $v_{0,18} = 17$, and $v_{0,19} = 22$.

Next, we consider a relation between vertices that is based on a reflective symmetry of $G(5^k)$.

Theorem 4.5.

For the digraph $G(5^k)$, $v_{i,4\cdot 5^s-1-t} = 5^k - v_{i,t}$ for all $i \in \{0,1,2,\dots k\}$ and $t \in \{0,1,2,\dots 4\cdot 5^s - 1\}$

Because Lemma 4.1 applied to all integers n, we only need to consider a lemma corresponding to Lemma 4.2 before proving the theorem.

Lemma 4.3.

For $i < k-1$, $t \equiv c \mod 5$ if and only if $5^{k-1}c < v_{i,t} < 5^{k-1}(c+1)$.

Proof. Recall from both Theorem 4.44 and Corollary 4.2 that the five vertices $v_{i,t+c} = v_{i,t} + 5^{k-1}c$ where $t \equiv 0 \mod 5$ and $c = 0,1,2,3,4$ are all adjacent to the same vertex at level $i+1$. Now, assume that $5^{k-1}c < v_{i,t+a}, v_{i,t+b} < 5^{k-1}(c+1)$ where $a, b, c \in \{0,1,2,3,4\}$ such that $a \neq b$. This means that $v_{i,t+a} - v_{i,t+b} = 5^{k-1}(a-b) < 5^{k-1}$, but this is not possible since $a \neq b$. Thus, $5^{k-1}c < v_{i,t+a} < 5^{k-1}(c+1)$ for exactly one a. Recall now that for two vertices, $v_{i,t}$ and $v_{i,r}$, at level $i < k-1$ both adjacent to the same vertex, if $v_{i,t} < v_{i,r}$, then $t < r$. Thus, $v_{i,t+0} < v_{i,t+1} < v_{i,t+2} < v_{i,t+3} < v_{i,t+4}$, so we have $0 < v_{i,t} < 5^{k-1}$, $5^{k-1} < v_{i,t+1} < 5^{k-1}2$ and so forth. Therefore, $5^{k-1}c < v_{i,t} < 5^{k-1}(c+1)$ for $t \equiv c \mod 5$. □

We are now ready to prove Theorem 4.5.

Proof. At level k, there is only one vertex, $v_{k,0} = 0$, so it is trivial that $v_{k,0} \equiv -v_{k,0}$.

For induction on i, in the base case at level $k-1$, there are four vertices. These vertices are paired across the vertical symmetry of the tree: $v_{k-1,0}$ with $v_{k-1,4\cdot 5^0-1-0} = v_{k-1,3}$ and $v_{k-1,1}$ with $v_{k-1,4\cdot 5^0-1-1} = v_{k-1,2}$. All these vertices are exactly divisible by 5^{k-1} and are not congruent to $5^k = 5 \cdot 5^{k-1}$, so we have $v_{k-1,0} = 5^{k-1}$, $v_{k-1,1} = 2 \cdot 5^{k-5}$, $v_{k-1,2} = 3 \cdot 5^{k-5}$, and $v_{k-1,3} = 4 \cdot 5^{k-5}$. Thus,

$$\begin{aligned} v_{k-1,3} &= 5 \cdot 5^{k-1} - v_{k-1,0} \\ &= 5^k - v_{k-1,1} \end{aligned}$$

and

$$v_{k-1,2} = 5^k - v_{k-1,1}$$

Now, let $i < k-1$ and assume

$$v_{i+1,4\cdot 5^q-1-r} \equiv -v_{i+1,r} \mod 5^k \tag{4.4}$$

for all $r \in \{0, 1, 2, \ldots 4 \cdot 5^q - 1\}$ where $q = k - (i+1) - 1$, so $4 \cdot 5^q$ is the number of vertices in level $i + 1$. Let $(v_{i,t}, v_{i+1,r})$ be an edge of $G(5^k)$. We want to show that $v_{i,4\cdot 5^s-1-t} \equiv -v_{i,t}$.

By Lemma 4.1 and Equation 4.4, $(-v_{i,t}, -v_{i+1,r}) = (-v_{i,t}, v_{i+1,4\cdot 5^q-1-r})$ is also an edge. Thus, we know that $-v_{i,t}$ must be congruent to one of the five vertices adjacent to $v_{i+1,4\cdot 5^q-1-r}$.

Suppose $t \equiv c \mod 5$. From Lemma 4.3, we know that $5^{k-1}(c) < v_{i,t} < 5^{k-1}(c+1)$. Hence $5^{k-1}(5-c) > -v_{i,t} > 5^{k-1}(5-(c+1))$. Thus, if we let $-v_{i,t} = v_{i,a}$, then $a \equiv 5 - (c+1) \equiv -c - 1 \mod 5$.

Since $t \equiv c \mod 5$, we have $4 \cdot 5^s - 1 - t \equiv 0 - 1 - c \equiv -c - 1 \mod 5$. Since the five possible vertices all have incongruent positions, we now have $a = 4 \cdot 5^s - 1 - t$, so $-v_{i,t} \equiv v_{i,4\cdot 5^s-1-t}$ for all $v_{i,t} \in V(G(5^k))$. Therefore $v_{i,4\cdot 5^s-1-t} = 5^k - v_{i,t}$. □

For example, looking at $G(25)$ in Figure 4.4, we see that $v_{0,6} = 6$ and

$$v_{0,20-1-6} = v_{0,13} = 25 - 6 = 19.$$

The following theorem looks at the isomorphism between $G(5^k)$ and a subgraph of $G(5^m)$ when $m > k$.

Theorem 4.6.

Let $v_{i,t} \in G(5^k)$ and $u_{i,t} \in G(5^m)$ where $m > k$. If $u_{m-i,t} = 5^{m-k}v_{k-j,r}$, then $i = j$ and $r = t$.

Proof. Choose $v_{k-i,t} \in V(G(5^k))$ and $u_{j,r} \in V(G(5^m))$ such that $5^{m-k}v_{k-i,t} = u_{j,r}$. Then $5^{k-i} \| v_{k-i,t}$ and multiplying by 5^{m-k}, we get

$$5^{m-k}5^{k-i} \| 5^{m-k}v_{k-i,t}$$
$$5^{m-i} \| u_{j,r}$$

so, $j = i$.

Now, we need to show that $r = t$. There is only one vertex at level k, so we must have $r = t$. For some level $k - i$, with $i \geq 1$, assume $r = t$ for all $v_{k-i,t}$ and $u_{m-i,r}$ where $5^{m-k}v_{k-i,t} = u_{m-i,r}$. Then, in level $k-i-1$, let $5^{m-k}v_{k-i-1,s} = u_{m-i-1,q}$ and let $(v_{k-i-1,s}, v_{k-i,s})$ be an edge in $G(5^k)$. Thus,

$$10 \cdot v_{k-i-1,s} \equiv v_{k-i,t}$$
$$10 \cdot 5^{m-k}v_{k-i-1,s} \equiv 5^{m-k}v_{k-i,t}$$
$$10 \cdot u_{m-i-1,q} \equiv u_{m-i,r}.$$

We now have $u_{m-i-1,q}$ in one of five incongruent positions all adjacent to $u_{m-i,r}$.

Assume that $s \equiv c \mod 5$. Then

$$5^{k-i}c < v_{k-i-1,s} < 5^{k-i}(c+1)$$
$$5^{k-i}5^{m-k}c < 5^{m-k}v_{k-i-1,s} < 5^{k-i}5^{m-k}(c+1)$$
$$5^{m-i}c < u_{m-i-1,q} < 5^{m-i}(c+1).$$

Hence, $q \equiv c \mod 5$. Since the five possible vertices all have incongruent positions, we have $q = s$. Therefore, $u_{m-i,t} = 2^{m-k}v_{k-i,t}$ for all $u_{i,t} \in G(2^m)$. □

From Theorem 4.6, we get that for $k < m$, $G(5^k)$ is isomorphic to the subgraph of $G(5^m)$ generated by the vertex set $S = \{v_{i,t} \mid i \geq m-k\}$. The isomorphism from $G(5^k)$ to the subgraph of $G(5^m)$ is $h(v) = 5^{m-k}v$.

4.2 Multiples of 2^k

Now that we have the structure and some labeling of $G(2^k)$ and $G(5^k)$, we can consider how these graphs relate to the graphs of $2^k n$ and $5^k n$ where n is relatively prime to 10.

Recall that a graph, G, is semiregular if $indeg(v) = 0$ or d for every v in $V(G)$ with d a positive integer. The first theorem shows the semiregularity of $G(2^k n)$.

Theorem 4.7.

If n is not divisible by 2 or 5, then $G(2^k n)$ is semiregular with $d = 2$ and $indeg(v) = 2$ if and only if $2 \mid v$.

Proof. Let (a, b) be an edge in $G(2^k n)$. Then $10a \equiv a \mod 2^k n$, and also

$$10(a + 2^{k-1}n) \equiv 10a + 5 \cdot 2^k n \mod 2^k n$$
$$10(a + 2^{k-1}n) \equiv b + 0 \mod 2^k n. \tag{4.5}$$

Since $2^{k-1}n < 2^k n$, $a \not\equiv a + 2^{k-1}n$ and $(a + 2^{k-1}n, b)$ is also an edge in $G(2^k n)$. Thus, if $indeg(v) \geq 1$ for any $v \in V(G(2^k n))$, then $indeg(v) \geq 2$.

Now, assume there exists a third vertex, c, which is also adjacent to b and is incongruent to both a and $a + 2^{k-1}n$. Then

$$10c - b = 2^k ns \tag{4.6}$$

and

$$10a - b = 2^k np \tag{4.7}$$

where s and p are integers such that $s \neq p$.

From Equations 4.6 and 4.7 we get

$$\begin{aligned} 10(c - a) &= 2^k n(s - p) \\ 5(c - a) &= 2^{k-1} n(s - p). \end{aligned}$$

Since $5 \nmid 2^{k-1}n$, we know that 5 divides $(s - p)$, so $(s - p) = 5t$ for some integer t and

$$\begin{aligned} 5(c - a) &= 2^{k-1} n(5t) \\ (c - a) &= 2^{k-1} n(t) \\ c &= a + 2^{k-1} nt. \end{aligned} \tag{4.8}$$

If t is even, then $t = 2r$ and $c \equiv a + 2^{k-1}n(2r) \equiv a \mod 2^k n$. If t is odd, then $t = 2r + 1$ and

$$\begin{aligned} c &\equiv a + 2^{k-1} n(2r + 1) \\ &\equiv a + 2^k nr + 2^{k-1} n \\ &\equiv a + 2^{k-1} n \mod 2^k. \end{aligned}$$

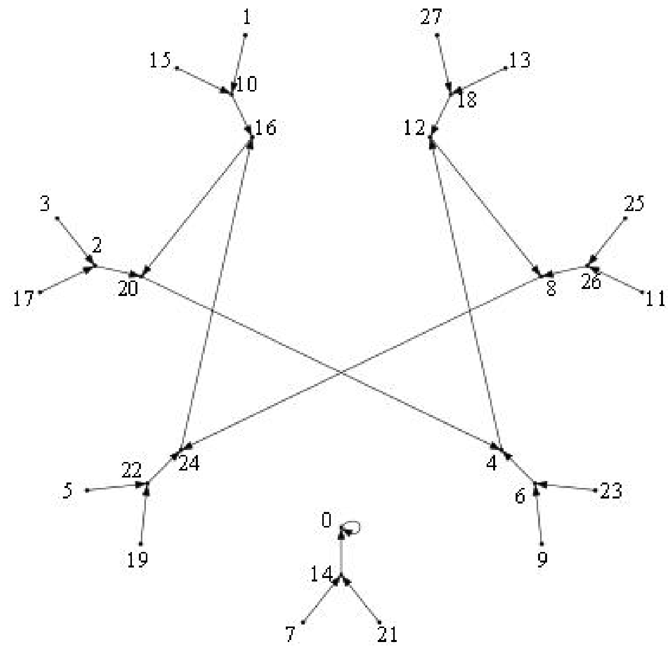


Figure 4.5: $G(28)$

Thus, c is congruent to either a or $a + 2^{k-1}n$, so the indegree of b is exactly 2 and the indegree of any vertex of $G(2^k n)$ is either 0 or 2. Therefore, $G(2^k n)$ is semiregular with $d = 2$.

Now, assume (a, b) is an edge where $2 \nmid b$. Then $10a \equiv b \mod 2^k n$, so

$$10a - b = 2^k np$$
$$10a - 2^k np = b$$
$$2(5a - 2^{k-1}np) = b.$$

Thus, $2 \mid b$, which is a contradiction, so when $2 \nmid v$, $indeg(v) = 0$. There are $2^{k-1}n$ vertices that are divisible by 2 and, hence, can have an indegree of 2. Since there are exactly twice as many edges as there are vertices divisible by 2, $indeg(v) = 2$ whenever $2 \mid v$. Therefore, $indeg(v) = 2$ if and only if $2 \mid v$. □

The graph $G(28)$ is seen to be semiregular with $d = 2$ in Figure 4.5. It also includes several subgraphs with a binary tree structure. These subgraphs are isomorphic to $G(2^k)$, as seen in the following theorem.

Theorem 4.8.

If n is not divisible by 2 or 5 and $k > 0$, then $G(2^k n)$ contains n generated subgraphs that are isomorphic to the subgraph of $G(2^k)$, excluding the loop $(0, 0)$. The root of each isomorphic subgraph is a vertex $v \in V(G(2^k n))$ where $2^k | v$.

Proof. From Theorem 2.6, we know that $S = \{(2^k a, 2^k b) \mid (a, b) \in E(G(n))\}$ is a subset of $E(G(2^k n))$. Also, since $G(n)$ is a set of isolated cycles, we have that the edges in S form a set of cycles, which are isomorphic to $G(n)$. Hence, for all $2^k v \in V(G(2^k n))$, $2^k v$ is part of a cycle, so $indeg(2^k v) \geq 1$. Then by Theorem 4.7, $indeg(2^k v) = 2$. Since exactly one vertex adjacent to $2^k v$ is part of the cycle, the other adjacent vertex must be noncyclical. Thus, there is a tree, with at least one vertex other than the root, whose root vertex is $2^k v$ where $v \in V(G(n))$.

We now need to show that each of these trees is isomorphic to $G(2^k)$ without the loop $(0, 0)$. Define $T_v(2^k n)$ to be the tree whose root is $r = 2^k v$. Adapted from Theorem 4.1, each tree needs to satisfy these three properties

1. $T_v(2^k n)$ has $k + 1$ levels

2. $T_v(2^k n)$ is a binary tree with exactly one vertex adjacent to r and $indeg(v) = 0$ or 2 for all $v \neq r$

3. for any vertex v at level 0, the shortest path from v to r has length k.

First, from Equation 4.5, we know that if a is the cyclical vertex adjacent to the root $r = 2^k m$, then $s = a + 2^{k-1} n$ is also adjacent to r and $2^{k-1} \| s$. Thus, we have 2 vertices adjacent to r, and by Theorem 4.7, s is the only vertex in $T_m(2^k n)$ that is adjacent to r. Thus, exactly one vertex in the tree is adjacent to r. The rest of part 2 follows by definition from Theorem 4.7, so $T_m(2^k n)$ is a binary tree and $indeg(v) = 0$ or 2 for all $v \neq r$.

Now, for part 1, for any $v \in V(T_m(2^k n))$ such that $v \neq r$, there exists an integer $j \geq 0$ such that $10^j v \equiv s = 2^{k-1}q \mod 2^k n$ for some integer q such that $2 \nmid q$. Suppose $j > k-1$, so

$$\begin{aligned} 10^j v - 2^{k-1}q &= 2^k np \\ 2^{k-1}(2^{j-k+1}5^j v - q) &= 2^k np \\ 2^{j-k+1}5^j v - q &= 2np. \end{aligned}$$

This says that 2 divides $(2^{j-k+1}5^j v - q)$. However, q is odd, so $(2^{j-k+1}5^j v - q)$ cannot be divisible by 2. Thus, $j \leq k-1$.

Now assume $j < k-1$ for all $v \in V(T_m(2^k n))$. Then,

$$\begin{aligned} 10^j v - 2^{k-1}q = 2^k np& \\ 2^j 5^j v &= 2^k np + 2^{k-1}q \\ 2^j 5^j v &= 2^{k-1}(2np + q) \\ 5^j v &= 2^{k-1-j}(2np + q). \end{aligned} \tag{4.9}$$

This means that $2|v$ for all $v \in V(T_m(2^k n))$. From Theorem 4.7, all vertices in the tree now have an indegree of 2, which makes an infinite tree. Thus, there exist vertices in $T_m(2^k n)$ such that $10^{k-1}v \equiv s$, or such that the path from v to s is $k-1$ edges long, and hence the path from v to r is k edges lone. Thus, $T_m(2^k n)$ has $k+1$ levels.

Finally, from Equation 4.9, we know that if the shortest path from v to s is less than $k-1$, then v must be even. Since all vertices at level 0 are odd, the shortest path from v at level 0 to s is $k-1$, and the shortest path from level 0 to r has length k.

Therefore, $T_v(2^k n)$ is isomorphic to the subgraph of $G(2^k)$ without the loop $(0,0)$. The root of each tree is $2^k v$, where $v \in V(G(n))$, so there are n of these trees. □

For vertices in the trees of $G(2^k n)$, we will use the same notation as with the 2^k

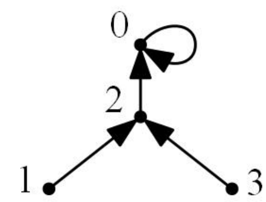


Figure 4.6: Each tree in $G(28)$ is isomorphic to the subgraph of $G(4)$ excluding the loop $(0,0)$

graphs. Thus, $v_{i,t} \in T_a(2^k n)$ indicates the vertex at level i in the t^{th} position. Also as before, if $v_{i,t} < v_{i,r}$ are adjacent to the same vertex, then $r < t$. In Figure 4.5, the tree $T_3(28)$ is the subgraph generated by the vertex set $\{12, 13, 18, 27\}$. Using the notation, $v_{k,0} = 12$ $v_{1,0} = 18$, $v_{0,0} = 13$, and $v_{0,1} = 27$. Comparing this tree to $G(4)$ in Figure 4.6, they are isomorphic through the function h, where $h(0) = 12$, $h(1) = 13$, $h(2) = 18$, and $h(3) = 27$.

Because of this isomorphism and by Theorem 4.1 part 6, we know that in $T_a(2^k n)$, the number of vertices at level $i < k$ is 2^{k-i-1}. There are several other results for $G(2^k)$ that which also appear in a modified form for $G(2^k n)$. First, Corollary 4.1 pertains to vertices which are adjacent to a common vertex.

Corollary 4.3.

Let $v \in T_a(2^k)$*. If* $i \leq k-2$ *and* t *is even, then* $v_{i,t+1} = v_{i,t} + 2^{k-1}n$*.*

Proof. Since t is even, $v_{i,t}$ and $v_{i,t+1}$ are adjacent to the same vertex. By Equation 4.5, $v_{i,t+1} = v_{i,t} + 2^{k-1}n$. □

Also from Theorem 4.8, we get a corollary on the number of cycles in $G(2^k n)$.

Corollary 4.4.

If $\gcd(n, 10) = 1$*, then* $C_{2^k n} = C_n$ *and* $L_{2^k n} = L_n$*.*

Proof. Since the root of each tree $T_v(2^k n)$ is part of a cycle, each cyclical vertex has the form $2^k v$ for $v \in V(G(n))$. Thus, by Theorem 2.6, $G(2^k n)$ has the same cycles as $G(n)$. Therefore $C_{2^k n} = C_n$ and $L_{2^k n} = L_n$. □

The vertices in $G(2^k n)$ are also sorted into levels according to their divisibility by 2 as with the vertices of $G(2^k)$.

Theorem 4.9.

For all $v \in V(G(2^k n))$, $2^i \| v$ if and only if v is at level $i < k$.

Proof. By Theorem 2.6, the vertices in $G(2^k n)$ that are part of a cycle are all of the form $2^k v$. From the proof of Theorem 4.8, these vertices are at level k and the noncyclical, adjacent vertex has the form $s = 2^{k-1}q$. Since s is not part of a cycle, it is not divisible by 2^k, so $2^{k-1}\|s$.

Now, for induction down the levels, assume 2^j exactly divides every vertex at level $j < k-1$. Let (a, b) be an edge in $G(2^k n)$ with b at level j, so $b = 2^j d$ where d is an odd integer. Then $10a \equiv b \mod 2^k n$ and

$$\begin{aligned}
10a - b &= 2^k np \\
10a - 2^j d &= 2^k np \\
10a &= 2^k np + 2^j d \\
10a &= 2^j(2^{k-j}np + 2) \\
5a &= 2^{j-1}(2^{k-j}np + d).
\end{aligned}$$

Hence, 2^{j-1} divides a.

Now, assume 2^j also divides a, or $a = 2^j t$. Then

$$\begin{aligned}
10a - b &= 2^k np \\
10(2^j t) - b &= 2^k np \\
2^{j+1}5t - b &= 2^k np \\
b &= 2^{j+1}(5t - 2^{k-(j+1)}np).
\end{aligned}$$

Thus, 2^{j+1} divides b, which is a contradiction. Therefore $2^{j-1} \| a$ and $2^i \| v$ if and only if v is at level $i < k$. □

The above theorem does not hold for level k. All the vertices at level k of $G(2^k n)$ are divisible by 2^k, but not all are exactly divisible. For example, in Figure 4.5, the vertices 8, 16, and 24 are all at level $k = 2$, but they are each divisible by at least $2^{k+1} = 8$.

A reflective relationship similar to that demonstrated in Theorem 4.2 relates vertices from different trees in $G(2^k n)$.

Theorem 4.10.

If $v_{i,t} \in T_a(2^k n)$ *and* $w_{i,2^s-1-t} \in T_{n-a}(2^k n)$*, then* $w_{i,2^s-1-t} = 2^k n - v_{i,t}$

Proof. Let $v_{i,t} \in T_a(2^k n)$ and $w_{i,t} \in T_{n-a}(2^k n)$. Then $r = 2^k a$ is the root of $T_a(2^k n)$, so $(v_{k-1,0}, 2^k a)$ is in $E(G(2^k n))$. By Lemma 4.1,

$$(-v_{k-1,0}, -2^k a) = (2^k n - v_{k-1,0}, 2^k n - 2^k a)$$

is also an edge. Now, $2^{k-1} \| v_{k-1,0}$, so 2^{k-1} also exactly divides $2^k n - v_{k-1,0}$. Hence, by Equation 4.5 this vertex must be adjacent to the root of a tree. Since it is adjacent to $2^k n - 2^k a = 2^k(n-a)$, it is in $T_{n-a}(2^k n)$ and $2^k n - v_{k-1,0} = w_{k-1,0}$.

Next, assume $w_{i,2^s-1-t} = 2^k n - v_{i,t}$ for some level $i < k-1$ and all $0 \le t \le 2^s - 1$, where 2^s is the number of vertices in level i. Let $v_{i-1,p}$ be adjacent to $v_{i,t}$. Using Lemma 4.1 again, $(-v_{i-1,p}, -v_{i,t}) = (-v_{i-1,p}, w_{i,2^s-1-t})$ is an edge in $T_{n-a}(2^k n)$.

Similar to Lemma 4.2, since vertices adjacent to the same vertex are arranged increasingly and by Corollary 4.3, t is even if and only if $0 < v_{i,t} < 2^{k-1} n$. Thus, we now have two cases.

Case 1 If $p \equiv 0 \mod 2$, then $-v_{i-1,p}$ is equivalent to either $w_{i-1,2^q-1-p}$ or $w_{i-1,2^q-2-p}$. Since p is even, $0 < v_{i-1,p} < 2^{k-1} n$ and $2^{k-1} n < -v_{i-1,p} < 2^k n$. Then $-v_{i-1,p}$ must be in an odd position. Thus, $-v_{i-1,p} \equiv w_{i-1,2^q-1-p}$.

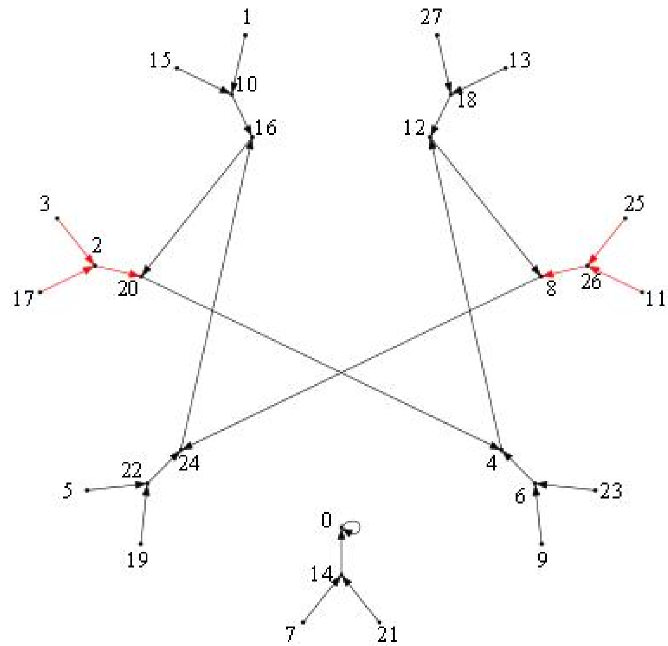


Figure 4.7: $G(28)$ with $T_2(28)$ and $T_5(28)$ highlighted in red.

Case 2 If $r \equiv 1 \mod 2$, then $-v_{i-1,p}$ is equivalent to either $w_{i-1,2^q-1-p}$ or $w_{i-1,2^q-p}$. Since p is odd, $2^{k-1}n < v_{i-1,p} < 2^k n$ and $0 < -v_{i-1,p} < 2^{k-1}n$. Then $-v_{i-1,p}$ must be in an even position. Thus, $-v_{i-1,p} \equiv w_{i-1,2^q-1-p}$.

Therefore, $w_{i,2^s-1-t} = 2^k n - v_{i,t}$ for all $v_{i,t} \in T_a(2^k n)$ and $w_{i,2^s-1-t} \in T_{n-a}(2^k n)$ □

Note that when $a = 0$, Theorem 4.10 is the same as Theorem 4.2, since $v_{i,t}$ and $w_{i,2^s-1-t}$ will both be in $T_0(2^k n)$. This is because $G(2^k)$ and $T_0(2^k n)$ are related through the isomorphism $h(v) = nv$.

Looking at $G(28)$ in Figure 4.7 for an example, consider $T_2(28)$ and $T_5(28)$, which have been highlighted in red. By our selection of trees, $2^k \cdot 2 + 2^k \cdot 5 = 8 + 20 = 28$. Then following the theorem, $26 + 2 = 28$, $11 + 17 = 28$, and $25 + 3 = 28$.

In addition to the above isomorphism, we also get a theorem showing how vertex labels of $T_v(2^k n)$ relate to those of $G(2^k)$. First, however, we need a better understanding of which numbers are in each tree.

Theorem 4.11.

If $\{2^k c_0, 2^k c_1, 2^k c_2, \ldots 2^k c_s\}$ *is a cycle in* $G(2^k n)$*, then* $v \in T_{c_j}(2^k n)$ *is at level* i *if and only if* $v \equiv 2^k c_{j-(k-i)} + nw$ *where* $w \in V(G(2^k))$ *and* w *is at level* i*.*

Proof. Let $v \in T_{c_j}(2^k n)$ such that $v = 2^k c_{j-(k-i)} + nw$ for some $w \in G(2^k)$ at level i. Then v is at level i if and only if the shortest path from v to $r = 2^k c_j$ is $(k-i)$ edges long , where r is the root of $T_{c_j}(2^k n)$. Thus, consider

$$10^{k-i} v = 10^{k-i}(2^k c_{j-(k-i)} + nw)$$
$$10^{k-i} v = 10^{k-i}(2^k c_{j-(k-i)}) + 10^{k-i} nw.$$

Since there are $(k-i)$ steps in the cycle from $2^k c_{j-(k-i)}$ to $2^k c_j$, we know that $10^{k-i} 2^k c_{j-(k-i)} \equiv 2^k c_j \mod 2^k n$. Hence, $10^{k-i} v \equiv 2^k c_j + 10^{k-i} nw \mod 2^k n$. Then, since w is at level i in $G(2^k)$, $10^{k-i} w \equiv 0 \mod 2^k$ or

$$10^{k-i} w = 2^k p$$
$$10^{k-i} wn = 2^k pn.$$

Thus, $10^{k-i} wn \equiv 0 \mod 2^k n$ and $10^{k-i} v \equiv 2^k c_j \mod 2^k n$. Also, there is no shorter path from w to 0 in $G(2^k)$. Therefore, the path from v to $2^k c_j$ is $(k-i)$ edges long, and v is in level i. □

Looking again at $G(28)$ in Figure 4.5, let $2^k c_0 = 4$. Then $20 = 2^k c_5$, so vertices at level 0 of $T_5(28)$ have the form $2^2 c_{5-2} + 7 \cdot w$ where $w = 1, 3$, because those are the two vertices at level 0 of $G(4)$. The level 0 vertices of this tree are then $2^2 6 + 7 \cdot 1 \equiv 3 \mod 28$ and $2^2 6 + 7 \cdot 3 \equiv 17 \mod 28$.

In the case of $T_0(2^k n)$, the tree whose root is 0, this theorem is a restatement of Theorem 2.6. This is because when $2^k c_j = 0$, we get $2^k c_{j-(k-i)} = 0$ for all values of k and i. Theorem 4.11 then says that vertices at level i take the form nw for $w \in V(G(2^k))$ at level i.

We can now use this theorem to see how the labels of the trees in $G(2^k n)$ relate to those in $G(2^k)$.

Theorem 4.12.

The vertex set $V(T_v(2^k n))$ forms a complete residue set modulo 2^k for itegers v, n, and k such that $v = 0, 1, 2, \ldots n-1$, $\gcd(10, n) = 1$ and $k > 0$.

Proof. First, the root of $T_v(2^k n)$, $r = 2^k v$, is the only vertex divisible by 2^k, so it is incongruent to the remaining vertices in the tree. Then, by Theorem 4.9, every vertex at some level $i < k$ is exactly divisible by 2^i, so any two vertices in different levels of $T_v(2^k n)$ are incongruent as well.

Finally, we need to compare vertices within the same level. Let both v_l and v_m in $T_v(2^k n)$ be at level i. By definition of the vertex set of $G(2^k n)$, we know that v_l and v_m are incongruent modulo $2^k n$. By Theorem 4.11, we can write these as $v_l \equiv 2^k c_{j-(k-i)} + nw_l$ and $v_m \equiv 2^k c_{j-(k-i)} + nw_m$. Then,

$$2^k c_{j-(k-i)} + nw_l \not\equiv 2^k c_{j-(k-i)} + nw_m \mod 2^k n$$
$$nw_l \not\equiv nw_m \mod 2^k n,$$

so $nw_l - nw_m \neq 2^k np$ and $w_l - w_m \neq 2^k p$. Thus, $w_l \not\equiv w_m \mod 2^k$, so if we assume $v_l \equiv v_m \mod 2^k$, we get

$$2^k c_{j-(k-i)} + nw_l \equiv 2^k c_{j-(k-i)} + nw_m \mod 2^k$$
$$nw_l \equiv nw_m \mod 2^k$$
$$w_l \equiv w_m \mod 2^k,$$

which is a contradiction. Therefore, $v_l \not\equiv v_m \mod 2^k$ and we have a set of 2^k incongruent vertices, so $V(T_v(2^k n))$ forms a complete residue set modulo 2^k. □

In $T_2(28)$ (part of Figure 4.7), the vertex set $\{8, 26, 11, 25\}$ reduces to $\{0, 2, 3, 1\}$

modulo 4. Note that position is not maintained between the two trees. If $w_{i,t} \in V(G(2^k))$ and $v_{j,r} \in V(T_c(2^k n))$ such that $v_{j,r} \equiv w_{i,t} \mod 2^k$, then we know $i = j$. This does not mean, however, that $t = r$. In $G(4)$, $w_{0,0} = 1$ and $w_{0,1} = 3$, but in $T_2(2)$, $v_{0,0} = 11 \equiv 3 \mod 4$ and $v_{0,1} = 25 \equiv 1 \mod 4$.

4.3 Multiples of 5^k

Despite containing the same results, the sections on $G(2^k)$ and $G(5^k)$ were kept separate so that the proofs might be easier to follow. However, comparing the proofs of corresponding theorems, we find that the proof for a $G(5^k)$ can be created by substituting a 5 for every 2 in the $G(2^k)$ proof. Not surprisingly, we can do the same for the $G(2^k n)$ theorems. Thus, the following results are presented without proof.

Theorem 4.13.

If n is not divisible by 2 or 5, then $G(5^k n)$ is semiregular with $d = 5$ and $indeg(v) = 5$ if and only if $5 \mid v$.

Looking at $G(55)$ (Fig. 4.8), we see that the cyclical vertices are the only vertices divisible by 5 and, thus, are the only an indgree of 5. The level 0 vertices are not divisible by 5.

Theorem 4.14.

If n is not divisible by 2 or 5 and $k > 0$, then $G(5^k n)$ contains n generated subgraphs that are isomorphic to the subgraph of $G(5^k)$ excluding the loop $(0, 0)$. The root of each isomorphic subgraph is a vertex $v \in V(G(5^k n))$ where $5^k | v$.

The subtrees $T_4(55)$ (with root $r = 20$) and $T_7(55)$ ($r = 35$) are highlighted in Figure 4.8. Comparing to $G(5)$ in Figure **??**, we see that every subtree in $G(55)$ is isomorphic to $G(5)$, excluding the $(0, 0)$ loop. The isomorphism $h : G(5) \to T_4(55)$ maps is defined such that $h(0) = 20$, $h(1) = 2$, $h(2) = 13$, $h(3) = 24$, and $h(4) = 46$.

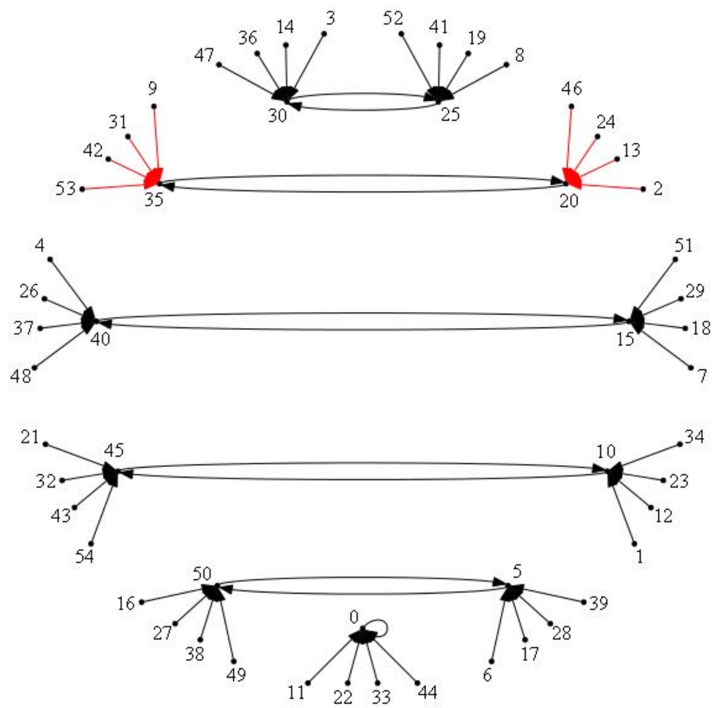


Figure 4.8: $G(55)$ with $T_4(55)$ and $T_7(55)$ highlighted.

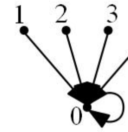


Figure 4.9: $G(5)$

Corollary 4.5.

Let $v \in T_a(5^k)$. If $i \leq k-2$ and $t \equiv 0 \mod 5$, then $v_{i,t+c} = v_{i,t} + 5^{k-1}nc$ for $c = 0,1,2,3,4$

Corollary 4.6.

If $\gcd(n,10) = 1$, then $C_{5^k n} = C_n$ and $L_{5^k n} = L_n$.

Theorem 4.15.

For all $v \in V(G(5^k n))$, $5^i \| v$ if and only if v is at level $i < k$.

In $G(55)$, all the level 0 vertices are relatively prime to 5. Since $k = 1$ and this theorem requires that $i < k$, it does not apply the vertices at level 1. They are all divisible by 5, but 25 and 50 are also divisible by 5^2, so 5 does not exactly divide every vertex at level 1.

Theorem 4.16.

If $v_{i,t} \in T_a(5^k n)$ and $w_{i,4\cdot 5^s-1-t} \in T_{n-a}(5^k n)$, then $w_{i,4\cdot 5^s-1-t} = 5^k n - v_{i,t}$

Looking again at $T_4(55)$ and $T_7(55)$, we have $7 = 11 - 4$, so the above theorem applies to these trees. For $v_{i,t} \in T_4(55)$ and $w_{i,t} \in T_7(55)$, we start with $v_{0,0} = 2$ and get $w_{0,4-0} = 55 - v_{0,0} = 53$. Similarly, $w_{0,3} = 42 = 55 - 13 = 55 - v_{0,1}$, $31 = 55 - 24$, and $9 = 55 - 46$.

Theorem 4.17.

If $\{5^k c_0, 5^k c_1, 5^k c_2, \ldots 5^k c_s\}$ is a cycle in $G(5^k n)$, then $v \in T_{c_j}(5^k n)$ is at level i if and only if $v \equiv 5^k c_{j-(k-i)} + nw$ where $w \in V(G(5^k))$ and w is at level i.

Let $c_1 = 4$, so the vertices at level 0 of $T_4(55)$ are $v \equiv 5^k c_{1-(1-0)} + 11w = 5^k \cdot 7 + 11w \mod 55$ where $w \in \{1,2,3,4\}$, the set of level 0 vertices in $G(5)$. Thus, the level 0 vertices of $T_4(55)$ are $35+11(1) \equiv 46$, $35+11(2) \equiv 2$, $35+11(3) \equiv 13$, and $35+11(4) \equiv 24$.

Theorem 4.18.

The vertex set $V(T_v(5^k n))$ forms a complete residue set modulo 5^k.

The vertex set $V(T_7(55)) = \{35, 9, 31, 42, 53\}$ reduces to $\{0,4,1,2,3\}$ modulo 5. Similarly, $V(T_4(55)) = \{20, 2, 13, 24, 46\}$ is $\{0,2,3,4,1\}$ modulo 5.

4.4 Graphs for 2^k5^j

With the structure of $G(2^kn)$ and $G(5^kn)$ classified, we now consider graphs for $n = 2^k5^j$ where $k, j > 0$. As before, we begin with the basic form of the $G(2^k5^j)$ tree. Unless otherwise specified, all numbers in this section are read modulo 2^k5^j.

Theorem 4.19.

If $G(2^k5^j)$ is the iteration digraph of $f(x) \equiv 10x \mod n$ for integers $k, j > 0$, then

1. *$G(2^k5^j)$ has $L = \max(k, j) + 1$ levels*
2. *The non-cyclic edges form a 10-ary tree with height $L - 1$ and with $2^k5^j \equiv 0$ as the root*
3. *exactly 10 vertices are adjacent to each vertex at level $i > 0$*
4. *v is at level 0 if and only if $2 \nmid v$ or $5 \nmid v$.*

Proof. For part 1, we have two cases. In the first case, assume $j \leq k$, so $10^kv \equiv 2^k5^j(5^{k-j}v) \equiv 0$ for all v in $V(G(2^k5^j))$. Suppose that $10^{k-1}v$ is also equivalent to 0 for all v, so $10^{k-1}v \equiv 0$, or

$$10^{k-1}v = 2^k5^jp$$
$$2^{k-1}5^{k-1}v = 2^k5^jp$$
$$5^{k-1}v = 2 \cdot 5^jp.$$

Hence, 2 must divide v. This is a contradiction when v is odd, so k is the smallest power of 10 for which $10^kv \equiv 0$ for all v. Thus, the longest path from a vertex at level 0 to the 0 vertex is k and $G(2^k5^j)$ has $k + 1$ levels.

For the second case, we assume $k < j$ and find similarly that the longest path to the 0 vertex is j, so $G(2^k5^j)$ has $j + 1$ levels. Therefore, $G(2^k5^j)$ has $L = \max(k, j) + 1$ levels.

In part 3, let $(a, b) \in E(G(2^k5^j))$, so $10a \equiv b \mod 2^k5^j$. Considering $a + 2^{k-1}5^{j-1}c$, we get

$$\begin{aligned} 10(a + 2^{k-1}5^{j-1}c) &\equiv 10a + 2^k5^jc \\ &\equiv b. \end{aligned} \tag{4.10}$$

Thus, $a + 2^{k-1}5^{j-1}c$ is adjacent to b for any value of c.

We now need to find how many values of c yield distinct values for $a + 2^{k-1}5^{j-1}c$. Assume $a + 2^{k-1}5^{j-1}c \not\equiv a + 2^{k-1}5^{j-1}d \mod 2^k5^j$. Then

$$\begin{aligned} a + 2^{k-1}5^{j-1}c - (a + 2^{k-1}5^{j-1}d) &\neq 2^k5^jp \\ 2^{k-1}5^{j-1}(c - d) &\neq 2^k5^jp \\ c - d &\neq 2 \cdot 5p, \end{aligned}$$

so $c \not\equiv d \mod 10$. There are 10 incongruent values of c modulo 10, so $a + 2^{k-1}5^{j-1}c$ for $c = 0, 1, 2, \ldots 9$ yields 10 distinct vertices all adjacent to b. Therefore, there are exactly 10 vertices adjacent to each vertex at level $i > 0$.

Parts 1 and 3 lead directly to part 2, so the non-cyclic edges $G(2^k5^j)$ form a 10-ary tree with height $L - 1$ and 0 as the root.

For part 4, assume b is a vertex at level $i > 0$. Then $10a \equiv b$ for some $a \in V(G(2^k5^j))$ and

$$\begin{aligned} 10a - b &= 2^k5^jp \\ b &= 10a - 2^k5^jp \\ b &= 2 \cdot 5(a - 2^{k-1}5^{j-1}p), \end{aligned}$$

Hence, $2|b$ and $5|b$.

Now, let b be a vertex such that $10|b$, so $b = 10t$. Assume b is at level 0.

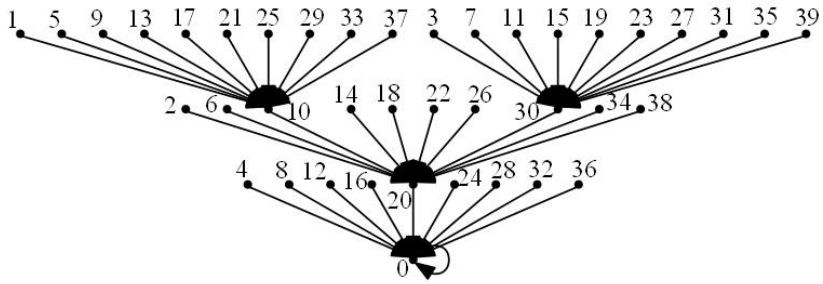


Figure 4.10: In $G(40)$, not all vertices at level 0 are the same distance from the 0 vertex

Then $10a \not\equiv b \mod 2^k5^j$ for all $a \in V(G(2^k5^j))$. However, consider $a = t$ and then $10a \equiv 10t = b$. Thus, we have a contradiction and b must not be at level 0 and v is at level $i > 0$ if and only if $10|v$. Therefore, v is at level 0 if and only if $2 \nmid v$ or $5 \nmid v$. □

Theorem 4.19 modifies several parts from Theorems 4.1 and 4.4, the basic structure theorems for $G(2^k)$ and $G(5^k)$. Recall that for powers of 2 and 5, these theorems included a statement that a vertex is at level $i < k$ if and only if $2^i||v$ or $5^i||v$, respectively. For $G(2^k5^j)$, we get have the following related claim, which we prove for certain cases.

Claim 1 *For each vertex, v, at level i of $G(2^k5^j)$, either $2^{\min(i,k)}||v$ or $5^{\min(i,j)}||v$.*

Let $b \in V(G(2^k5^j)$ at level $0 < i < L$. Thus, the longest path to b has length i. If a is the first vertex of the path to b, then a is at level 0. Hence, by Theorem 4.19 part 4, $a = 2^r5^sm$ where $\gcd(10, m) = 1$ and either $r = 0$ or $s = 0$. Then $10^ia \equiv b$, so

$$10^ia - b = 2^k5^jp$$

$$10^i2^r5^sm - b = 2^k5^jp$$

$$b = 2^k5^jp - 2^{r+i}5^{s+i}m \tag{4.11}$$

$$b = 2^{\min(k,r+i)}5^{\min(j,s+i)}(2^{k-\min(k,r+i)}5^{j-\min(j,s+i)}p - 2^{r+i-\min(k,r+i)}5^{s+i-\min(j,s+i)}m). \tag{4.12}$$

From the above equations, we now have four cases to consider.

Case 1 If $r+i \geq k$ and $s+i \geq j$, then by Equation 4.11, $2^i5^j | 2^{r+i}5^{s+i}m$, so b is divisible by 2^k5^j. The only vertex of $G(2^k5^j)$ for which this is true is the 0 vertex at level L. Thus, our claim does not apply to this case, because b is at level i where $0 < i < L$.

Case 2 If $r+i < k$ and $s+i < j$, then Equation 4.12 becomes

$$b = 2^{r+i}5^{s+i}(2^{k-(r+i)}5^{j-(s+i)}p - m).$$

Because m is relatively prime to 10, we now have that $2^{r+i} \| b$ and $5^{s+i} \| b$. We also know that either $r = 0$ or $s = 0$ since $a = 2^r5^sm$ is at level 0. Thus, either $2^i \| b$ or $5^i \| b$.

Case 3 If $r+i < k$ and $s+i \geq j$, then from Equation 4.12, we get

$$b = 2^{r+i}5^j(2^{k-(r+i)}p - 5^{s+i-j}m).$$

Now again, since $\gcd(10, m) = 1$, we have $2^{r+i} \| b$, and if $r = 0$, then $2^i \| b$. However, if $r > 0$, then we have $s = 0$ and we need to consider whether 5 divides p.

If $5 \nmid p$, then we will have $5^i \| b$. Unfortunately, we do not know enough about the composition of p. Thus, in this case, we cannot be certain that b is exactly divisible by 5^i.

Case 4 If $r+i \geq k$ and $s+i < j$, we have the same problem as in Case 3. Equation 4.12 becomes

$$b = 2^k5^{s+i}(5^{j-(s+i)}p - 2^{r+i-k}m)$$

and if $s = 0$, then $5^i \| b$. However, if $s > 0$, then $r = 0$ and we cannot know if b is exactly divisible by 2^i without knowing if 2 divides p.

Thus, our claim always holds for Cases 1 and 2. However, in Case 3, we must also have that $r = 0$, and in Case 4, we need $s = 0$. Since $\gcd(10, p)$ is potentially larger than 1, it is not determined what might happen with the divisibility of b in Cases 3 and 4 when $r > 0$ and $s > 0$, respectively. We have not found a counterexample to the claim, though it may be that this would require a 2^k5^j to be very large.

Notice that Theorem 4.19 part 3 is also different from part 4 in Theorems 4.1 and 4.4. In $G(2^k5^j)$, not all the vertices adjacent to a common vertex are in the same level. Recall that in $G(2^k)$ or $G(5^k)$, if v is in level i, not only is every vertex adjacent to v at the same level, but we know also they are all at level $i - 1$. In Figure 4.10, we see that 10 and 30 are at level 1 and adjacent to 20. Meanwhile, the rest of the vertices adjacent to 20 are at level 0. The level difference between adjacent vertices is not necessarily 1 as was the case for $G(2^k)$ and $G(5^k)$. There are vertices in $G(40)$ that are in level 0, but are adjacent to vertices in level 1 or 2, such as with the edges $(2, 20)$ and $(4, 0)$.

Another related difference is that part 7 for both $G(2^k)$ and $G(5^k)$ said that if a vertex v is at level 0, then the shortest path between v and 0 has length k. In $G(40)$ (Fig. 4.10), we can see that this is clearly not the case, because there vertices at level 0 that are adjacent to the 0 vertex, such as 4 and 8. The shortest path between these has a length of only 1. Other level 0 vertices are 2 or 3 steps away. This less predictable progression through the tree means that we cannot as easily determine the number of vertices in any given level like we did for $G(2^k)$ and $G(5^k)$. It is also more difficult to determine the divisibility by 2 or 5 of a vertex at level i.

The irregular movement through the levels of $G(2^k5^j)$ discussed above also makes notation for these graphs more difficult. Because vertex at level i of $G(2^k5^j)$ is not necessarily adjacent to a vertex at level $i + 1$, it is helpful to consider vertices based on what level they are adjacent to rather than which level they are actually in. We define $v_{i,t} \in G(2^k5^j)$ to be the vertex which is adjacent to level j in position t from the left. So in Figure 4.10, the vertices of $G(40)$ are arranged by adjacency rather than by level. We have $v_{2,0} = 2$, $v_{2,1} = 6$, and $v_{2,3} = 10$. These vertices all have the same first index, 2, even though they are not at the same level; 2 and 6 are at level 0, while 10 is at level 1. As before, if $v_{i,t} < v_{i,r}$ and both are adjacent to the same vertex at level i, then $t < r$. Also, 0 is adjacent to itself, but it does not have a position t relative to the rest of the vertices, so we will instead assign $r = 0$, since it is the root of $G(2^k 5^j)$.

Thus, we are set up with the notation to talk about the labeling of the vertices. However, the discussion of any such theorems is left to future work.

CHAPTER 5

Future Work

The problem of a less predictable progression through the graph of $G(2^k5^j)$ produces challenges in proving theorems about vertex labeling similar to those proved for both $G(2^k)$ and $G(5^k)$. Thus, it is left to future work to prove the following.

Proposition 5.1.

In the digraph $G(2^k5^j)$, let s be the number of vertices adjacent to level i. Then $v_{i,s-t} = 2^k5^j - v_{i,t}$ for $i \in \{1, 2, \ldots \max(k, j)\}$ and $t \in \{0, 1, \ldots s-1\}$.

Proposition 5.2.

Let $v_{i,t} \in G(2^k5^j)$ and $u_{i,t} \in G(2^m5^n)$ where $m \geq k$ and $j \geq n$, not both equal. If $u_{\max m,n-l,r} = 2^{m-k}5^{n-j}v_{\max(k,j)-i,t}$, then $i = l$ and $t = r$.

We would also expect that graphs for integers of the form 2^k5^jn will have a structure much like those of $G(2^kn)$ and $G(5^kn)$, with n subtrees isomorphic to $G(2^k5^j)$.

There is more to be done with the labeling theorems for the powers of 2 and 5, as well. We have presented results (Theorems 4.2 and 4.5 and Corollaries 4.1 and 4.2) from which, given a single vertex label, one can easily produce the labels for 3 or 9 other vertices within the level of a 2^k or 5^k graph, respectively. However, it remains to be determined if all of the labels in a level could be similarly generated based on knowledge of just one label.

Since many proofs presented throughout were not strictly dependent on the function $f(x) = 10x \mod n$, we may also expect that many results would generalize to iteration digraphs generated by the function $g(x) = ax \mod n$ where a is any integer. More specifically, the structures arising in the graphs for the divisors of both 10 and 9 may be expected to appear for the divisors of a and $(a - 1)$, as well.

Finally, we have focused on graphs generated by one function with various moduli. It would also be interesting to consider the graphs for a constant modulus n generated by $g(x) = ax \mod n$. For example, looking at how the graphs generated by $g(x) = ax \mod 7$ might compare as we consider various integers a.

There are a number of directions to continue forward with investigations of the structure of iteration digraphs and the relations between these structures for various integers.

APPENDIX A

Graph Code

I wrote the following Java code to create the *.txt* files which were then used to create the graphs in GVEdit. The first was used to create the circular graphs and the second was used to create trees. Some adjustments to the graphs were made within GVEdit itself.

Listing A.1: Circular graph code

```
import java.util.Scanner;
import java.io.FileNotFoundException;
import java.io.FileOutputStream;
import java.io.PrintStream;
import java.util.Vector;
/*import java.lang;

/**
 * Write a description of class Writer here.
 *
 * @author (your name)
 * @version (a version number or a date)
 */
public class IterationCircleGraph
{
    public static void main(String filename, int n, double size)
    {
      double PI = Math.PI;

      try {
      PrintStream out = new PrintStream(new FileOutputStream(
          filename));

```

```java
      out.println("digraph G{");
      out.println("size = \"" + 2*size + "!\";");
      out.println("viewport = \"" + 175*size + "," + 175*size + "\";");
      out.println();

      for (int i = 0; i < n; i++)
        out.println( i + "[shape=point, pos=\" " + size*72*Math.cos(i*(2*PI/n)-PI/2)+ "," + size*72*Math.sin(i*(2*PI/n)-PI/2) + "!\"];");

      out.println();

      for (int i = 0; i < n; i++)
        out.println( i + "->" + (10*i)%n + " [taillabel = " + i + ", labelangle = 180, labeldistance = 1.25];");

      out.println("}");

      out.close();

    } catch (FileNotFoundException e) {
      e.printStackTrace();
    }
    }


}
```

Listing A.2: Tree code

```
import java.util.Scanner;
import java.io.FileNotFoundException;
import java.io.FileOutputStream;
import java.io.PrintStream;
import java.util.Vector;
/*import java.lang;

/**
 * Creates graph for f(x)=10x mod n without constraining position of vertices
 *
 * @author (your name)
 * @version (a version number or a date)
 */
public class IterationGraph
{
    public static void main(String filename, int n, double size)
    {
      /**double PI = Math.PI;
        */
      try {
      PrintStream out = new PrintStream(new FileOutputStream(
          filename));

      out.println("digraph G{");
      out.println("size = \"" + 2*size + "!\";");
      out.println("viewport = \"" + 175*size + "," + 175*size + "\";");
      out.println("node [shape=point]");

      out.println();

      for (int i = 0; i < n; i++)
        out.println( i + ";");

      out.println(" ");


      for (int i = 0; i < n; i++)
        out.println( i + "->" + (10*i)%n + " [taillabel = " + i + " labelangle = 240];");

      out.println("}");

```

```
            out.close();

        } catch (FileNotFoundException e) {
            e.printStackTrace();
        }
        }


}
```

References

Fred S. Roberts and Barry Tesman. *Applied Combinatorics*. Chapman & Hall/CRC, Boca Raton, 2009.

Kenneth H. Rosen. *Elementary Number Theory and Its Applications*. Addison-Wesley, Boston, 2011. 14

Lawrence Somer and Michal Křížek. On a connection of number theory with graph theory. *Czechoslovak Mathematical Journal*, 54(2):465–485, 2004. 9, 18

David Wilson. Divisibility by 7 is a walk on a graph. World Wide Web, 2009. URL http://blog.tanyakhovanova.com/?p=159. Accessed on 05/01/2011. 1, 2