involve
a journal of mathematics

Iteration digraphs of a linear function

Hannah Roberts

msp

2015 vol. 8, no. 2

INVOLVE 8:2 (2015)
dx.doi.org/10.2140/involve.2015.8.221

Iteration digraphs of a linear function

Hannah Roberts

(Communicated by Robert W. Robinson)

An iteration digraph $G(n)$ generated by the function $f(x) \bmod n$ is a digraph on the set of vertices $V = \{0, 1, \ldots, n-1\}$ with the directed edge set $E = \{(v, f(v)) \mid v \in V\}$. Focusing specifically on the function $f(x) = 10x \bmod n$, we consider the structure of these graphs as it relates to the factors of n. The cycle lengths and number of cycles are determined for various sets of integers including powers of 2 and multiples of 3.

1. Introduction

Using the graph D_7, shown in Figure 1, the remainder modulo 7 of any integer N can be determined based solely on the digits of the N [Wilson 2009]. For example, consider $N = 375$. Begin at the vertex labeled 0. First, follow three black edges. Then follow one red edge and seven black edges, ending on 2. Finally, follow one red edge and five black edges to end on 4. This indicates that $375 \equiv 4 \bmod 7$.

Generalizing this algorithm to any N where d_i is the i-th digit, we start at 0 and follow d_1 black edges. We then continue to follow d_i black edges for $i = 2, 3, \ldots, r$. Between each digit, we follow one red edge. The vertex where we end after the final d_r black edges is the remainder when N is divided by 7.

The graph D_7 is formed by two specific iteration digraphs, directed graphs each generated by a function $f : \mathbb{Z}_n \to \mathbb{Z}_n$. The 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 is $E = \{(v, f(v)) \mid v \in V\}$, where $(v, f(v))$ indicates the edge directed from vertex v to $f(v)$. The red edges in D_7 form the iteration digraph produced by the function $f(x) \equiv 10x \bmod 7$. Thus, $V(D_7) = \{0, 1, 2, \ldots, 6\}$, and $E(D_7)$ includes $(1, 3)$, $(3, 2)$, and so on, because $10 \equiv 3 \bmod 7$ and $30 \equiv 2 \bmod 7$. The black edges are generated by the function $g(x) \equiv x + 1 \bmod 7$.

Using these two functions, divisibility graphs can easily be drawn for any integer n, and the same algorithm will produce remainders modulo n. Given this, one may naturally question how the graph produced by $f(x) \bmod n$ changes for

MSC2010: 05C20, 11A07.
Keywords: digraph, cycle, congruence.

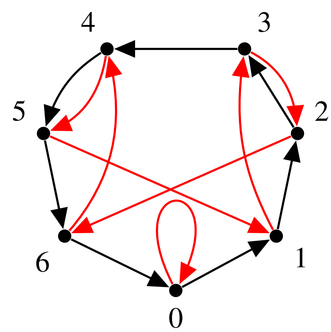


Figure 1. The graph D_7, used to determine divisibility by 7.

different integers n. This work considers the number and length of the cycles in the graph $G(n)$ generated by the function $f(x) = 10x \mod n$.

2. Relatively prime integers

To begin, we look at the common structures found in a broad subset, the set of all integers relatively prime to 10. The most basic feature of these graphs is given in Theorem 1 below.

A vertex v in $G(n)$ is said to be in level i if the longest path ending at v which does not contain any part of a cycle has length i [Somer and Křížek 2004]. If the highest level vertex in $G(n)$ is at level i, then $G(n)$ has $i+1$ levels. Thus, $G(28)$ (Figure 7) has 3 levels. Level 0 contains 7 and 9, level 1 contains 6, and level 2 contains 0. Also, the indegree of a vertex v, written $\operatorname{indeg}(v)$, is the number of edges directed towards v. In $G(28)$, $\operatorname{indeg}(7) = 0$ while $\operatorname{indeg}(6) = 2$.

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

Proof. Because $V(G(n))$ is the complete reduced residue set of n and $\gcd(10, n) = 1$, the set $S = \{10v \mid v \in V(G(n))\}$ is also a complete residue set [Rosen 2000]. Thus, $f : V(G(n)) \to V(G(n))$ is one-to-one and onto, so every vertex has indegree exactly 1.

Now assume $v \in V(G(n))$ is at level $i > 0$. Then there must be a path of i edges leading to v which is not part of a cycle. The first vertex in this noncyclic path must have an indegree of 0. This is a contradiction, so v must be at level 0 and $G(n)$ 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 $G(n)$ with $\gcd(10, n) = 1$ is simply a set of isolated cycles. That is, $G(n)$ is a set of cycles without any adjacent noncyclic vertices. We next consider the lengths of these cycles.

The length of the cycles in $G(n)$ is dependent on the prime factors of n, but before considering the total number of cycles, we first look at a subset of the vertices.

A graph H is called a subgraph of G if $V(H) \subset V(G)$ and $E(H) \subset E(G)$, where the edges in $E(H)$ must connect vertices in $V(H)$. We say H is generated by $V(H)$ if $E(H)$ contains every edge in G that connects vertices in $V(H)$.

Theorem 2. *In $G(n)$, if V_1 is the subset of vertices relatively prime to n, then there are $\phi(n)/\mathrm{ord}_n(10)$ cycles, each of length $\mathrm{ord}_n(10)$, 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 $10a \equiv b$ 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 $r = \mathrm{ord}_n(10)$, so r is the least integer for which $10^r \equiv 1 \bmod n$, or equivalently $10^r v \equiv v \bmod n$ for every $v \in V(G(n))$. In the sequence of vertices $\{v_0, v_1, v_2, \ldots, v_r\}$ 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 $0 \le t < r$. Since $10^s v_0 \equiv 10^t v_0 \equiv v_t$, a path longer than r will repeat through the cycle. 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 $s < r = \mathrm{ord}_n(10)$. Then $10^s v \equiv v \bmod n$, but $10^s \not\equiv 1 \bmod n$, because by definition r is the smallest positive integer for which $10^r \equiv 1 \bmod n$. This means $10^s - 1 = np + t$ for some integers p and $0 < t < n$. Also, $10^s v - v = nm$ for some integer m, so

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

Now we have $n \mid (vt)$, but $n \nmid t$ because $0 < t < n$. Hence, $\gcd(n, v) > 1$, which is a contradiction since we assumed $\gcd(n, v) = 1$. Therefore, all cycles on vertices relatively prime to n have length $r = \mathrm{ord}_n(10)$. Also, there are $\phi(n)$ vertices relatively prime to n, so there are $\phi(n)/\mathrm{ord}_n(10)$ such cycles. □

As an example of Theorem 2, consider $G(11)$ (Figure 2). There are 10 vertices relatively prime to 11, $V_1 = \{1, 2, 3 \ldots, 10\}$, and $\mathrm{ord}_{11}(10) = 2$. Thus, $G(11)$ contains $10/2 = 5$ cycles all of length 2.

Define C_n to be the number of cycles and L_n to be the set of all cycle lengths in $G(n)$. Now the above theorem is used to help determine C_n and L_n for any n relatively prime to 10.

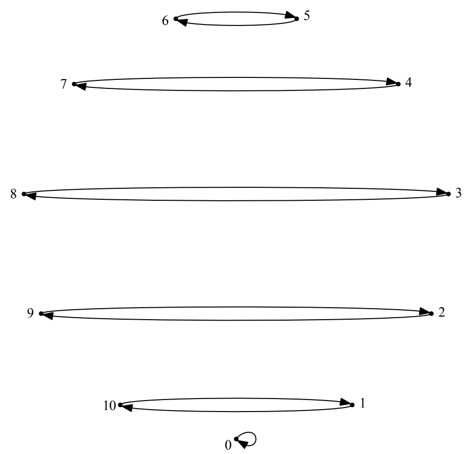


Figure 2. G_{11} contains five 2-cycles.

Theorem 3. *Let* $\gcd(10, n) = 1$. *Then*

$$C_n = \sum_{d|n} \frac{\phi(d)}{\text{ord}_d(10)},$$

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

Proof. First, define the set $V_d = \{v \in V(G(n)) \mid \gcd(v, n) = d\}$ for all $d \mid n$. 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 by reasoning similar to that used in the previous theorem, $b \in V_d$.

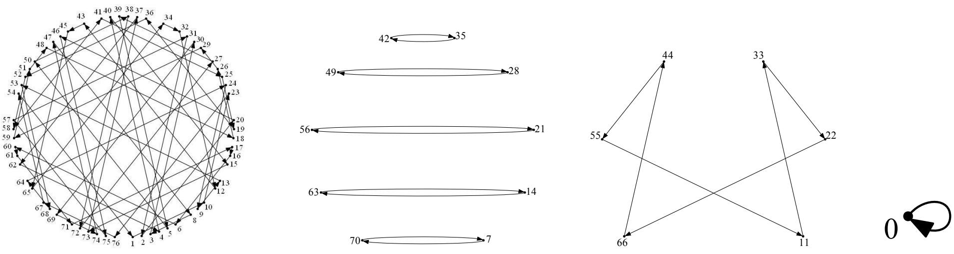
Thus, every cycle in $G(n)$ contains vertices from exactly one set V_d, and we can determine C_n by adding the number of cycles in $G_d(n)$ for every $d \mid n$, or

$$C_n = \sum_{d|n} (\text{number of cycles in } G_d(n)). \tag{1}$$

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 $\gcd(n/d, t) = 1$, and similarly, $b = ds$, where $\gcd(n/d, s) = 1$. Thus, $(a, b) = (dt, ds)$. Now,

$$\begin{aligned} 10a - b &= n(p) \\ 10(dt) - ds &= n(p) \\ 10t - s &= \frac{n}{d}(p), \end{aligned}$$

so (t, s) is an edge in $G(n/d)$. Since t and s are relatively prime to n/d, our problem is now equivalent to finding the number of cycles on the vertices of $G(n/d)$ relatively



(a) $G_1(77)$ (b) G_7 (c) G_{11} (d) G_{77}

Figure 3. The subgraphs of $G(77)$ generated by V_1, V_7, V_{11}, and V_{77}.

prime to n/d. In other words, the number of cycles in $G_d(n)$ is the same as the number of cycles in $G_1(n/d)$. From Theorem 2, we know that $G_1(n/d)$ contains $\phi(n/d)/\mathrm{ord}_{n/d}(10)$ cycles with length $\mathrm{ord}_{n/d}(10)$.

Thus, there are also $\phi(n/d)/\mathrm{ord}_{n/d}(10)$ cycles in $G_d(n)$ with length $\mathrm{ord}_{n/d}(10)$. Therefore,

$$C_n = \sum_{d \mid n} \frac{\phi(n/d)}{\mathrm{ord}_{n/d}(10)}.$$

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

$$C_n = \sum_{d \mid n} \frac{\phi(d)}{\mathrm{ord}_d(10)}. \qquad (2)$$

This concludes the proof. □

One example of the previous theorem is $G(77)$ (Figure 3). To make it easier to see the various cycles of $G(77)$, Figure 3 shows the subgraphs of $G(77)$ generated by V_d for $d = 1, 7, 11, 77$. Looking at $G_{11}(77)$ in Figure 3(c), the vertices all have $\gcd(v, 77) = 11$. If we compare this subgraph to $G(7)$ in Figure 1, we see that $G_{11}(77)$ is isomorphic to $G_1(7)$ by the isomorphism $h(v) = 11v$. This isomorphism illustrates the relation of edges in $G(n)$ and in $G(mn)$. Similarly, $G_7(77)$ is isomorphic to $G_1(11)$. Finally, $G_{77}(77)$ in Figure 3(d) is simply the isolated fixed point isomorphic to $G(1)$ that appears in every $G(n)$ where $(10, n) = 1$.

The isomorphisms seen in $G(77)$ can be generalized to other $G(n)$. For $d \mid n$, the subgraph $G_d(n)$ is isomorphic to the subgraph $G_1(n/d)$. 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 $d \mid n$.

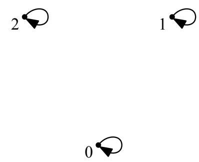


Figure 4. Every vertex in $G(3)$ is an isolated fixed point.

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.

3. Multiples of 3

Because $10 \equiv 1 \bmod 3$, for every vertex v in $G(3)$, (v, v) is an edge for all $v \in \{0, 1, 2\}$ (Figure 4). This property of $G(3)$ leads to a highly predictable structure for $G(3n)$ when $\gcd(3, n) = 1$.

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

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

If $v \in V$, then $v_t = 3v + tn \bmod 3n \in V_t$. 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 $V_2 = \{1, 4\}$, as in Figure 5.

The following theorem uses these vertex sets to relate the edge sets of $G(n)$ and $G(3n)$ for $\gcd(3, n) = 1$.

Theorem 4. *If* $3 \nmid n$ *and* $E(G(n)) = \{(a, b) \mid b = f(a), a \in V\}$, *then* $E(G(3n)) = \{(a_t, b_t) \mid (a, b) \in E(G(n)), t = 0, 1, 2\}$.

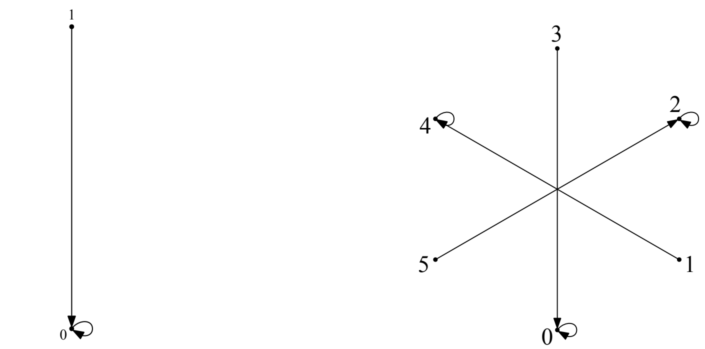
Proof. Let (a, b) be an edge in $G(n)$. Thus $10a \equiv b \bmod n$ and $3a \equiv 3b \bmod 3n$. Considering a_t,

$$\begin{aligned} 10(3a + tn) &\equiv 30a + 10tn \bmod 3n \\ &\equiv 3b + tn + 3n(3t) \bmod 3n \\ &\equiv 3b + tn \bmod 3n. \end{aligned}$$

Therefore, (a_t, b_t) is also an edge in $G(3n)$. We now have that

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

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.



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

Figure 5. The components of $G(6)$ are all isomorphic to $G(2)$.

For any $v, w \in V$, if $v \not\equiv w \bmod n$, then $v_t \not\equiv w_t \bmod 3n$. Hence, V_0, V_1, and V_2 each contain n incongruent integers.

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

An example of Theorem 4 is the graphs for $n = 6$ shown in Figure 5(b). The graph $G(6)$ 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 4 between any $G(n)$ and $G(3n)$ can also be expressed in terms of isomorphisms between the graphs.

Corollary 1. *$G(3n)$ is the union of three subgraphs, each of which is isomorphic to $G(n)$.*

A theorem similar to Theorem 4 can be proved for $G(9n)$ when $\gcd(3, n) = 1$. This indicates that perhaps this type of edge relation will exist for higher powers of 3 as well. However, for 3 and 9, the proofs are contingent on the fact that $10 \equiv 1$ modulo both 3 and 9. Theorem 4 cannot be generalized for $G(3^k n)$ where $k \geq 3$.

Based on Theorem 4, it is also clear that $G(3n)$ contains exactly 3 times as many cycles as $G(n)$ with all the same cycle lengths. Thus, while Theorem 3 holds for multiples of 3, we can now say $C_{3n} = 3C_n$ and $L_{3n} = L_n$ when $\gcd(3, n) = 1$. Similarly, $C_{9n} = 9C_n$ and $L_{9n} = L_n$.

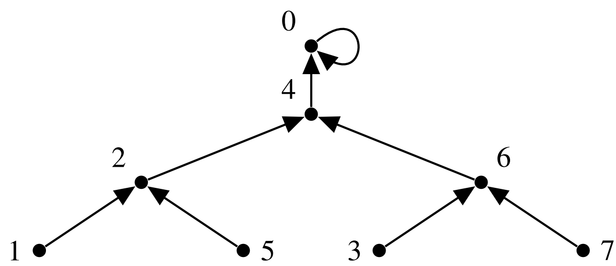


Figure 6. $G(8)$.

4. Powers of 2

Another class of integers for which $G(n)$ has a distinctive and 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. This unique form follows from the fact that 2 is a factor of 10. In this section, congruences should all be considered modulo 2^k unless otherwise specified.

Given this tree structure, which will be proved in Theorem 5, 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 vertex in level $0 \le i \le k$ at position $0 \le t \le 2^s - 1$. In Figure 6, 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 $v_{i,t} < v_{i,t+1}$.

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

Theorem 5. *If $G(n)$ is the iteration digraph of $f(x) \equiv 10x \bmod 2^k$, where $n = 2^k$ for $k = 1, 2, 3, \ldots$, then*:

(i) *$G(n)$ has $k + 1$ levels.*

(ii) *The nonzero vertices form a complete binary tree with height k.*

(iii) *Exactly 2 vertices at level $i < k - 1$ are adjacent to each vertex at level $i + 1$.*

(iv) *For each vertex $v_{i,t}$ at level $i < k$, $2^i \parallel v_{i,t}$.*

Proof. For part (i), we know for any vertex v that $10^k v = 2^k(5^k v) \equiv 0 \bmod 2^k$. 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 (iv), at level $k-1$, we have $2^{k-1} \parallel 2^{k-1}$. Now, for induction down the levels, assume that $2^i \parallel v_{i,t}$ for all vertices at some level $i \leq k-1$ 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

$$\begin{aligned} 10v_{i-1,r} - v_{i,t} &= 2^k b \\ 10v_{i-1,r} &= 2^i(2^{k-i}b + c). \end{aligned}$$

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

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

For part (iii), 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 $a + 2^{k-1}$.

$$10(a + 2^{k-1}) \equiv b + 5 \cdot 2^k \equiv b + 0 \bmod 2^k. \tag{3}$$

Since $2^{k-1} < 2^k$, $a \not\equiv a + 2^{k-1} \bmod 2^k$. Thus, at least two distinct vertices are adjacent to b. From part (iv), 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 (ii) also follows directly from parts (iii) and (i) and the definition of a tree, so the nonzero vertices form a complete binary tree with height k and with 2^{k-1} as the root. □

From the above theorem, $G(2^k)$ can be drawn for any $k \geq 1$ and we have some idea of the label placement within that graph. It is also clear that $G(2^k)$ always contains exactly one 1-cycle.

Since $G(2^k)$ is really just $G(2^k n)$ with $n = 1$, we now consider the more general $G(2^k n)$ with $\gcd(10, n) = 1$. First, we find that $G(2^k n)$ is semiregular; that is, each vertex in $G(2^k n)$ has an indegree of either 0 or d, for some positive integer d.

Theorem 6. *If n is not divisible by 2 or 5, then $G(2^k n)$ is semiregular with $d = 2$ and* $\operatorname{indeg}(v) = 2$ *if and only if* $2 \mid v$.

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

$$\begin{aligned} 10(a + 2^{k-1}n) &\equiv 10a + 5 \cdot 2^k n \bmod 2^k n \\ 10(a + 2^{k-1}n) &\equiv b + 0 \bmod 2^k n. \end{aligned} \tag{4}$$

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 $\operatorname{indeg}(v) \geq 1$ for any $v \in V(G(2^k n))$, then $\operatorname{indeg}(v) \geq 2$.

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

$$10c-b=2^k ns \quad \text{and} \quad 10a-b=2^k np, \tag{5}$$

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

From (5) we get

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

Then 5 divides $(s-p)$, so $(s-p)=5t$ for some nonzero integer t and

$$\begin{aligned} 5(c-a) &= 2^{k-1} n(5t) \\ c &= a+2^{k-1} nt. \end{aligned} \tag{6}$$

If t is even, then $t=2r$ and $c \equiv a+2^k nr \equiv a \bmod 2^k n$. If t is odd, then $t=2r+1$ and

$$c \equiv a+2^{k-1}n(2r+1) \equiv a+2^{k-1}n \bmod 2^k.$$

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 $10a \equiv b \bmod 2^k n$, so

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

Thus, $2 \mid b$, which is a contradiction, so when $2 \nmid v$, $\operatorname{indeg}(v)=0$. 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, $\operatorname{indeg}(v)=2$ whenever $2 \mid v$. Therefore, $\operatorname{indeg}(v)=2$ if and only if $2 \mid v$. $\square$

The graph $G(28)$ is seen to be semiregular with $d=2$ in Figure 7. It also includes several subgraphs with a binary tree structure. These subgraphs are isomorphic to $G(2^2)$. In the following theorem, these subgraphs isomorphic to $G(2^k)$ are shown to be present in $G(2^k n)$ for any $k \geq 1$ and n relatively prime to 10.

Theorem 7. *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 $2^k \mid v$.*

Proof. If $(a,b) \in E(G(n))$ then $(2^k a, 2^k b)$ is an edge in $G(2^k n)$, so we know that $S=\{(2^k a, 2^k b) \mid (a,b) \in E(G(n))\}$ is a subset of $E(G(2^k n))$. The edges in S form a set of cycles which are isomorphic to $G(n)$. Hence, for all $2^k v \in V(G(2^k n))$, $2^k v$

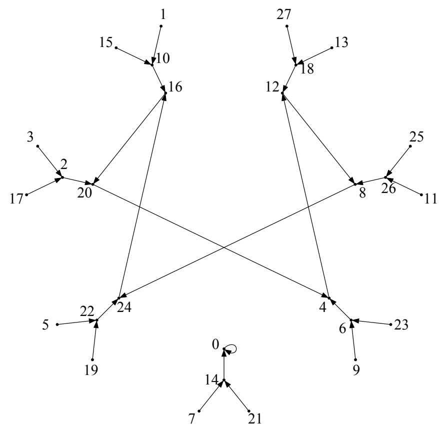


Figure 7. $G(28)$.

is part of a cycle, so $\operatorname{indeg}(2^k v) \geq 1$. Then by Theorem 6, $\operatorname{indeg}(2^k v) = 2$. Thus, $G(2^k n)$ contains a tree whose root vertex is $2^k v$ for every $v \in V(G(n))$.

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 5, each tree needs to satisfy the following three properties:

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

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

(iii) For any vertex v at level 0, the shortest path from v to r has length k.

First, Equation (4), 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 $2^{k-1} \parallel s$. Thus, we have two vertices adjacent to r, and by Theorem 6, 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 (ii) follows by definition from Theorem 6, so $T_m(2^k n)$ is a binary tree and $\operatorname{indeg}(v) = 0$ or 2 for all $v \neq r$.

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

$$10^j v - 2^{k-1} q = 2^k np$$
$$2^{j-k+1} 5^j v - q = 2np.$$

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,

$$\begin{aligned}10^j v - 2^{k-1} q &= 2^k np\\ 2^j 5^j v &= 2^k np + 2^{k-1} q\\ 5^j v &= 2^{k-1-j}(2np+q).\end{aligned} \tag{7}$$

This means that $2 \mid v$ for all $v \in V(T_m(2^k n))$. From Theorem 6, all vertices in the tree now have an indegree of 2, which cannot be true as this would mean there are no vertex with an indegree of 0 and would make the graph 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 long. Thus, $T_m(2^k n)$ has $k+1$ levels.

Finally, from (7), we know that if the shortest path from v to s has length 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. □

Theorem 7 is illustrated in $G(28)$ (Figure 7) which contains 7 subgraphs isomorphic to $G(4)$. From this theorem, we also know that $C_{2^k n} = C_n$ and $L_{2^k n} = L_n$.

Theorems 5 and 7 depended on the fact that 2 is a factor of 10. Thus, we can prove similar theorems for $G(5^k)$ and $G(5^k n)$ as well. From these, we can likewise determine that $C_{5^k n} = C_n$ and $L_{5^k n} = L_n$.

5. Conclusion

The function $f(x) = 10x \bmod n$ generates iteration digraphs whose cycles are greatly determined by the divisibility properties of n. With isomorphisms between $G(n)$ and $G(d)$, C_n is determined for any n relatively prime to 10. Then, 2 and 3 have specific relations to 10 which allow for simpler calculations for $C_{2^k n}$ and C_{3n}. Thus, we can now calculate the number and lengths of cycles in $G(n)$ for most integers n.

References

[Rosen 2000] K. H. Rosen, *Elementary number theory and its applications*, 4th ed., Addison-Wesley, Reading, MA, 2000. MR 2000i:11001 Zbl 0964.11002

[Somer and Křížek 2004] L. Somer and M. Křížek, "On a connection of number theory with graph theory", *Czechoslovak Math. J.* **54(129)**:2 (2004), 465–485. MR 2005b:05112 Zbl 1080.11004

[Wilson 2009] D. Wilson, "Divisibility by 7 is a walk on a graph", 2009, available at http://blog.tanyakhovanova.com/?p=159.

Received: 2012-11-05 Revised: 2013-03-04 Accepted: 2013-03-09

hjroberts3141@gmail.com College of Wooster, 91 Benton Street, Austintown, OH 44515, United States

involve

msp.org/involve

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2015 is US $140/year for the electronic version, and $190/year (+$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to MSP.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

involve

2015 vol. 8 no. 2

1944-4176(2015)8:2;1-5