POWER DIGRAPHS MODULO n

Brad Wilson
2030 State Street #5, Santa Barbara, CA 93105
(Submitted August 1996-Final Revision October 1996)

1. INTRODUCTION

A directed graph, or digraph, is a finite set of vertices together with directed edges. A closed trail of a digraph in which no vertices are repeated is a cycle. A tree is an acyclic connected digraph and a forest is an acyclic graph (thus a forest is made up of trees) [1].

Starting with the elements of $\mathbb{Z}_n$ as our set of vertices, we can create a digraph associated to any function f modulo n by having an edge from vertex b_1 to vertex b_2 if $f(b_1) \equiv b_2 \pmod{n}$. This digraph reflects properties of $\mathbb{Z}_n$ and f.

Digraphs arising when $f(x) = x^2$ have been studied in [2] and [5]. More recently, digraphs arising from $f(x) = x^k$ and n a prime have been studied in [4]. In this article we study digraphs arising from $f(x) = x^k$ and arbitrary $n \in \mathbb{N}$.

If $n = 2^a \prod_{i=1}^{m} p_i^{a_i}$ with $a_i \geq 1$, $a \geq 0$, define

$$\delta_1 = \begin{cases} 0 & \text{if } a = 0, 1, \\ 1 & \text{if } a \geq 2, \end{cases} \qquad \delta_2 = \begin{cases} 0 & \text{if } a < 3, \\ 1 & \text{if } a \geq 3, \end{cases}$$

and

$$L = \operatorname{lcm}(2^{\delta_1}, 2^{\delta_2(a-2)}, p_1^{a_1-1}(p_1 - 1), \ldots, p_m^{a_m-1}(p_m - 1)).$$

We use L to determine when two digraphs are equal (Theorem 1). Define G_n^k (resp. $G_n^{k^*}$) as the graph whose vertices are elements of $\mathbb{Z}_n$ (resp. $\mathbb{Z}_n^*$) with an edge from b_1 to b_2 if $b_1^k \equiv b_2 \pmod{n}$.

Our principal results on $G_n^{k^*}$ are:

(1) Determine when $G_n^{k_1^*} = G_n^{k_2^*}$ (Theorem 1).

(2) Show that elements in a cycle have the same order, d, and determine the cycle length, $\ell(d)$, based on that order (Theorem 2).

(3) Derive a formula for the number of cycles of order d (Theorem 3).

(4) Show that the trees of all cycle vertices are isomorphic (Theorem 4) and derive a formula for the height of these trees (Theorem 5).

We handle $G_n^k - G_n^{k^*}$ by showing that well-defined parts of this graph are isomorphic to corresponding $G_{n'}^{k}$'s (Theorem 6). Finally, we use these well-defined parts and a result about the number of solutions to congruences (Theorem 7) to fill in the whole of G_n^k.

2. BACKGROUND RESULTS

The following facts will be used in Sections 3 and 4. Facts 1, 2, and 3 are from [3].

Fact 1 (Chinese Remainder Theorem). If $(m_i, m_j) = 1$ $(1 \leq i < j \leq n)$, then the simultaneous congruences $x \equiv a_i \pmod{m_i}$, $1 \leq i \leq n$, have a unique solution mod $m_1 m_2 \ldots m_n$.

Fact 2. A necessary and sufficient condition for m to have a primitive root is that $m = 2$, 4, p^ℓ, or $2p^\ell$, where p is an odd prime.

Fact 3. Let $\ell > 2$. Then the order of 5 with respect to the modulus 2^ℓ is $2^{\ell-2}$.

Fact 4. For p an odd prime either the congruence $x^k \equiv b \pmod{p^m}$, $p \nmid b$ has 0 or $(k, p^{m-1}(p-1))$ solutions. The number of solutions of $x^k \equiv b \pmod{2^a}$ is 0 or $(2, k)^{\delta_1}(2^{a-2}, k)^{\delta_2}$.

Proof: If p is an odd prime, Fact 2 says $\mathbb{Z}^*_{p^m} \cong \mathbb{Z}_{p^{m-1}(p-1)}$. Multiplication in $\mathbb{Z}^*_{p^m}$ corresponds to addition in $\mathbb{Z}_{p^{m-1}(p-1)}$, so x^k corresponds to kx. The map

$$\lambda_k : \mathbb{Z}_{p^{m-1}(p-1)} \to \mathbb{Z}_{p^{m-1}(p-1)} \text{ such that } \lambda_k(x) = kx$$

is a $(k, p^{m-1}(p-1))$-to-one map, so an element in $\mathbb{Z}_{p^{m-1}(p-1)}$ is either the image of $(k, p^{m-1}(p-1))$ elements or none.

For modulus 2^a, Fact 3 says $\mathbb{Z}^*_{2^a} \cong \mathbb{Z}_2^{\delta_1} \times \mathbb{Z}_{2^{a-2}}^{\delta_2}$. In $\mathbb{Z}_2^{\delta_1} \times \mathbb{Z}_{2^{a-2}}^{\delta_2}$, the multiplication by k map is $(2, k)^{\delta_1}(2^{a-2}, k)^{\delta_2}$-to-one, giving our result. □

Fact 5. In $\mathbb{Z}_m$, the cyclic group of order m, there exists an element of order ℓ if and only if $\ell | m$. Further, if there exists an element of order ℓ, then there exist exactly $\phi(\ell)$ of them.

Proof: If $\ell \nmid m$, then Lagrange's Theorem says there is no element of order ℓ.

If $\ell | m$, then $m = \ell u$. For b an element of order m, we have $\ell(ub) = (\ell u)b = mb = \overline{0}$. Further, if $\ell' < \ell$ such that $\ell'(ub) = \overline{0}$, then $m | (\ell' u)$, but $\ell' u < m$, a contradiction, so ub is of order ℓ.

Finally, we need to count the number of elements of order ℓ if there is at least one. For b of order m, we know $\text{ord}(vb) = m/(v, m)$, so we get an element of order ℓ if and only if $u = (v, m)$. Since $u | m$, we know v must be a multiple of u, but $u = (v'u, m)$ if and only if $1 = (v', \ell)$. There are $\phi(\ell)$ such values of v'. □

Fact 6. For $(m_1, m_2) = 1$, we have

$$\mathbb{Z}^*_{m_1 m_2} \cong \mathbb{Z}^*_{m_1} \times \mathbb{Z}^*_{m_2}.$$

Proof: The map $\rho : \mathbb{Z}^*_{m_1 m_2} \to \mathbb{Z}^*_{m_1} \times \mathbb{Z}^*_{m_2}$ defined by $\rho(x) = (x \pmod{m_1},\ x \pmod{m_2})$ is easily shown to be a homomorphism. It is an isomorphism since Fact 1 allows us to define a map which is the inverse:

$$\rho^{-1} : \mathbb{Z}^*_{m_1} \times \mathbb{Z}^*_{m_2} \to \mathbb{Z}^*_{m_1 m_2} \text{ such that } \rho^{-1}(x, y) = z,$$

where $z \equiv x \pmod{m_1}$, $z \equiv y \pmod{m_2}$. □

Facts 2 and 3 tell us the structure of $\mathbb{Z}^*_{p^\ell}$:

$$\mathbb{Z}^*_{p^\ell} \cong \begin{cases} \{\overline{1}\}, & \text{for } p = 2,\ \ell = 1, \\ \mathbb{Z}_2, & \text{for } p = 2,\ \ell = 2, \\ \mathbb{Z}_2 \times \mathbb{Z}_{2^{\ell-2}}, & \text{for } p = 2,\ \ell \geq 3, \\ \mathbb{Z}_{p^{\ell-1}(p-1)}, & \text{for } p \text{ an odd prime.} \end{cases} \tag{1}$$

From the structure of $\mathbb{Z}^*_{p^\ell}$ and Fact 6 follows the structure for $\mathbb{Z}^*_n$. If $n = 2^a \prod_{i=0}^{m} p_i^{a_i}$, then

$$\mathbb{Z}^*_n \cong \mathbb{Z}^*_{2^a} \times \mathbb{Z}^*_{p_1^{a_1}} \times \cdots\cdots \mathbb{Z}_{p_m^{a_m}} \cong \mathbb{Z}_2^{\delta_1} \times \mathbb{Z}_{2^{a-2}}^{\delta_2} \times \mathbb{Z}_{p_1^{a_1-1}(p_1-1)} \times \cdots \times \mathbb{Z}_{p_m^{a_m-1}(p_m-1)}. \tag{2}$$

Fact 7. In the group $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$, there are $(m_1, d)(m_2, d) \ldots (m_r, d)$ elements of order dividing d.

Proof: Since the order of $(x_1, x_2, \ldots, x_r)$ is the least common multiple of the orders of the x_i's, it is sufficient to show there are (m_i, d) elements of order dividing d in $\mathbb{Z}_{m_i}$. $\mathbb{Z}_{m_i}$ is cyclic of order m_i, so if $b \mid m_i$, there are $\phi(b)$ elements of order exactly b. If $b \nmid m_i$, there are no elements of order b. The number of elements of order dividing d is thus

$$\sum_{b \mid d,\, b \mid m_i} \phi(b) = \sum_{b \mid (d, m_i)} \phi(b) = (d, m_i)$$

by a famous property of the Euler-ϕ function (e.g., [3], Exercise 1, Section 2.5). □

3. STRUCTURE OF $G_n^{k^*}$

G_n^k is, by definition, the digraph whose vertices are the elements of $\mathbb{Z}_n$ and with an edge from b_1 to b_2 if $b_1^k \equiv b_2 \pmod{n}$. Since $b_1^k \pmod{n}$ is well defined for any given b_1, k and n, the outdegree of any vertex in our digraph is one. Since the outdegree from any vertex is one, we know that each component of G_n^k contains at most one cycle. Since there are only finitely many vertices, it is clear that from any starting point iteration of the k^{th} power map eventually leads to a cycle, so each component contains exactly one cycle. The vertices in a component outside the unique cycle are thus acyclic and form a forest.

If $p \mid n$ is a prime and $p \mid b$, then $p \mid b^k$, so $p \mid (b^k \pmod{n})$. If $p \nmid b$, then $p \nmid b^k$, so $p \nmid (b^k \pmod{n})$. This says, if $n = 2^a p_1^{a_1} p_2^{a_2} \ldots p_m^{a_m}$, there are at least 2^m components, at least 2^{m+1} if $a \neq 0$. In particular, we will examine the components with vertices relatively prime to n separately from those with vertices not relatively prime to n.

Recall that $G_n^{k^*}$ was defined to be the digraph with the elements of $\mathbb{Z}_n^*$ as vertices and an edge from b_1 to b_2 if $b_1^k \equiv b_2 \pmod{n}$. By the last paragraph, we can study this graph independently of the vertices not relatively prime to n. We start our study with a lemma on $\psi(d)$, the number of elements in $\mathbb{Z}_n^*$ of order d.

Lemma 1: If $n = 2^a \prod_{i=1}^m p_i^{a_i}$ and $\psi(d)$ denotes the number of elements of order d in $\mathbb{Z}_n^*$, then

$$\psi(d) = (2, d)^{\delta_1} (2^{a-2}, d)^{\delta_2} \prod_{i=1}^{m} (d, p_i^{a_i - 1}(p_i - 1)) - \sum_{\delta \mid d,\, \delta \neq d} \psi(\delta).$$

Proof: From Fact 7 and (2), we know the number of elements of order dividing d is $(2, d)^{\delta_1} (2^{a-2}, d)^{\delta_2} \prod_{i=1}^m (d, p_i^{a_i - 1}(p_i - 1))$, i.e.,

$$\sum_{\delta \mid d} \psi(\delta) = (2, d)^{\delta_1} (2^{a-2}, d)^{\delta_2} \prod_{i=1}^{m} (d, p_i^{a_i - 1}(p_i - 1)).$$

Solving this for $\psi(d)$ gives the result. □

The following results are analogs of results 11 through 14 of [4].

Lemma 2: The indegree of any vertex in $G_n^{k^*}$ is 0 or $(2, k)^{\delta_1} (2^{a-2}, k)^{\delta_2} \prod_{i=1}^m (k, p_i^{a_i - 1}(p_i - 1))$.

Proof: $\mathbb{Z}_n^* \cong \mathbb{Z}_2^{\delta_1} \times \mathbb{Z}_{2^{a-2}}^{\delta_2} \times \mathbb{Z}_{p_1^{a_1-1}(p_1-1)} \times \cdots \times \mathbb{Z}_{p_m^{a_m-1}(p_m-1)}$. For $b \in \mathbb{Z}_n^*$, $x^k \equiv b \pmod{n}$ is equivalent to

$$\begin{aligned} x^k &\equiv b \pmod{2^a}, \\ x^k &\equiv b \pmod{p_1^{a_1}}, \\ &\vdots \\ x^k &\equiv b \pmod{p_m^{a_m}}. \end{aligned} \tag{3}$$

By Fact 4 we know that, for p odd, $x^k \equiv b \pmod{p_i^{a_i}}$ has 0 or $(k, p_i^{a_i-1}(p_i-1))$ solutions and, for modulus 2^a, there are 0 or $(2,k)^{\delta_1}(2^{a-2},k)^{\delta_2}$ solutions. Taken together, the system (3) thus has 0 or $(2,k)^{\delta_1}(2^{a-2},k)^{\delta_2}\prod_{i=1}^{m}(k, p_i^{a_i-1}(p_i-1))$ solutions. □

Corollary 1: Every component of $G_n^{k^*}$ is cyclic if and only if $(2,k)^{\delta_1}(2^{a-2},k)^{\delta_2}=1$ and $(k, p_i^{a_i-1}(p_i-1))=1$ for all i.

Proof: If a component of $G_n^{k^*}$ is cyclic, then every indegree must be 1. By Lemma 2, this says $(2,k)^{\delta_1}(2^{a-2},k)^{\delta_2}\prod_{i=1}^{m}(k, p_i^{a_i-1}(p_i-1))=1$, so each factor must be 1.

Conversely, if $(2,k)^{\delta_1}(2^{a-2},k)^{\delta_2}=1$ and $(k, p_i^{a_i-1}(p_i-1))=1$ for each i, then Lemma 2 says the indegree of any vertex must be 0 or 1. Since each outdegree is 1 and the sum of the indegrees and outdegrees must be equal, this forces each indegree to be 1, so every component is cyclic. □

Corollary 2: Any cycle vertex has $(2,k)^{\delta_1}(2^{a-2},k)^{\delta_2}\left(\prod_{i=1}^{m}(k, p_i^{a_i-1}(p_i-1))\right)-1$ noncycle parents.

Proof: If b is a cycle vertex, the indegree is at least one because it has a cycle vertex parent. By Lemma 2, the indegree of b is $(2,k)^{\delta_1}(2^{a-2},k)^{\delta_2}\prod_{i=1}^{m}(k, p_i^{a_i-1}(p_i-1))$. Since exactly one of b's parents is a cycle vertex, there are

$$(2,k)^{\delta_1}(2^{a-2},k)^{\delta_2}\left(\prod_{i=1}^{m}(k, p_i^{a_i-1}(p_i-1))\right)-1$$

noncycle parents. □

Theorem 1: $k_1 \equiv k_2 \pmod{L}$ if and only if $G_n^{k_1^*} = G_n^{k_2^*}$.

Proof: Since $\mathbb{Z}_n^* \cong \mathbb{Z}_2^{\delta_1} \times \mathbb{Z}_{2^{a-2}}^{\delta_2} \times \mathbb{Z}_{p_1^{a_1-1}(p_1-1)} \times \cdots \times \mathbb{Z}_{p_m^{a_m-1}(p_m-1)}$, all elements have orders dividing L and we know that there exists an element of this order, namely, $(\overline{1}, \overline{1}, \ldots, \overline{1})$.

If $k_1 \equiv k_2 \pmod{L}$, then for any $b \in \mathbb{Z}_n^*$, $b^{k_1} \equiv b^{k_2+d\cdot L} \equiv b^{k_2} \pmod{n}$.

Conversely, if $G_n^{k_1^*} = G_n^{k_2^*}$, then $b^{k_1} \equiv b^{k_2} \pmod{n}$ for all $b \in \mathbb{Z}_n^*$. This means $\mathrm{ord}_n b \mid (k_1 - k_2)$. Since there is an element of order L, we get $k_1 \equiv k_2 \pmod{L}$. □

We now classify whether an element of a given order will be in a tree or cycle. First, we fix notation: factor $L = tw$ for t the largest factor relatively prime to k.

Lemma 3: The vertex b is a cycle vertex if and only if $(\mathrm{ord}_n b) \mid t$.

Proof: If b is a cycle vertex, then there is some ℓ such that $b^{k^\ell} \equiv b \pmod{n}$. We assume ℓ is the minimal natural number with this property. Since $b^{k^\ell - 1} \equiv 1 \pmod{n}$, we know that

$(\text{ord}_n b)|(k^\ell - 1)$, so $(\text{ord}_n b, k) = 1$ and $(\text{ord}_n b, w) = 1$. Since $(\text{ord}_n b)|L$, we have $(\text{ord}_n b)|tw$, so $(\text{ord}_n b)|t$.

Conversely, if $(\text{ord}_n b)|t$, then $b^t \equiv 1 \pmod n$, so $(t, k) = 1$ implies there exists $\ell > 0$ so that $k^\ell \equiv 1 \pmod t$. This means $b^{k^\ell - 1} \equiv 1 \pmod n$, so $b^{k^\ell} \equiv b \pmod n$, so b is a cycle vertex. □

An immediate corollary of this classification is a count of the number of cycle vertices in $G_n^{k^*}$.

Corollary 3: There are $(2, t)^{\delta_1}(2^{a-2}, t)^{\delta_2} \prod_{i=1}^{m}(t, p_i^{a_i-1}(p_i - 1))$ cycle vertices.

Proof: By Lemma 3, we are counting the number of elements of $\mathbb{Z}_n^*$ of order dividing t. By (2) and Fact 7, there are $(2, t)^{\delta_1}(2^{a-2}, t)^{\delta_2} \prod_{i=1}^{m}(t, p_i^{a_i-1}(p_i - 1))$ elements of order dividing t. □

The following result gives a connection between cycle vertices in the same cycle.

Lemma 4: Vertices in the same cycle have the same order modulo n.

Proof: It is enough to show that consecutive vertices in a cycle have the same order. Suppose $b_2 \equiv b_1^k \pmod n$. If $\text{ord}_n b_1 = \ell_1$ and $\text{ord}_n b_2 = \ell_2$, then $b_2^{\ell_1} \equiv (b_1^k)^{\ell_1} \equiv (b_1^{\ell_1})^k \equiv 1^k \equiv 1 \pmod n$. This means $\ell_2 | \ell_1$, so

$$\text{ord}_n b_1 \geq \text{ord}_n b_2 = \text{ord}_n(b_1^k) \geq \text{ord}_n(b_1^{(k^2)}) \geq \cdots \geq \text{ord}_n(b_1^{(k^\ell)}) = \text{ord}_n b_1.$$

This forces all the inequalities to be equalities, so the orders of all elements in the same cycle are equal. □

By Lemma 4, it makes sense to speak of the order of a cycle. The next result relates the order and length of a cycle.

Theorem 2: The length $\ell(d)$ of a cycle of order d is the smallest natural number ℓ such that $d|(k^\ell - 1)$, i.e., $\ell(d) = \text{ord}_d k$.

Proof: If $\ell(d)$ denotes the cycle length and b is a cycle vertex, then $b \not\equiv b^{(k^i)} \pmod n$ for any $i < \ell(d)$, but $b \equiv b^{(k^{\ell(d)})} \pmod n$. Stated differently, $b^{(k^i - 1)} \not\equiv 1 \pmod n$ for any $i < \ell(d)$, but $b^{(k^{\ell(d)} - 1)} \equiv 1 \pmod n$. Since $\text{ord}_n b = d$, this says $d \nmid (k^i - 1)$ for any $i < \ell(d)$ but $d|(k^{\ell(d)-1})$. □

We can use Theorem 2 to get the length of the longest cycle in $G_n^{k^*}$.

Corollary 4: The longest cycle in $G_n^{k^*}$ has length $\ell(t) = \text{ord}_t k$.

Proof: By Lemma 3, the order modulo n of every cycle vertex divides t. Further, there exists a cycle vertex of order t. Since, for any $d|t$, we have $k^{\ell(t)} \equiv 1 \pmod t$ implies $k^{\ell(t)} \equiv 1 \pmod d$, Theorem 2 says $\ell(t) = \text{ord}_t k \geq \text{ord}_d k = \ell(d)$. Therefore, the greatest cycle length is $\ell(t) = \text{ord}_t k$. □

The following theorem gives the number of cycles in $G_n^{k^*}$ of a given order.

Theorem 3: The number of cycles of order d in $G_n^{k^*}$ is $\psi(d) / \ell(d)$.

Proof: There are, by definition, $\psi(d)$ elements in $\mathbb{Z}_n^*$ of order d. Each is in a cycle of length $\ell(d)$ containing only elements of order d, so

$$\frac{\psi(d)}{\ell(d)} = \frac{\text{number of vertices of order } d}{\text{number of vertices of order } d \text{ per cycle of order } d}$$

$$= \text{number of cycles of order } d. \ \square$$

Finally, we give a few results about the tree structure. These results parallel those for prime modulus [4]. If b is a noncycle vertex in $G_n^{k^*}$, the height of b is defined to be the minimal natural number h such that b^{k^h} is a cycle vertex. For c a cycle vertex, define F_c^h as all noncycle vertices b of height h such that $b^{k^h} = c$. We define the tree above c as $F_c = \bigcup_h F_c^h$.

Lemma 5: If $b, c \in G_n^{k^*}$, $b \in F_1^h$, and c is a cycle vertex, then $bc \in F_{c^{k^h}}^h$.

Proof: By Lemma 3, $(\text{ord}_n b) \nmid t$ while $(\text{ord}_n c) | t$. Since $\mathbb{Z}_n^*$ is abelian, $(bc)^t \equiv b^t c^t \equiv b^t \not\equiv 1 \pmod{n}$, so the order of bc does not divide t. By Lemma 3, this says bc is not a cycle vertex, so the product of a cycle and noncycle vertex is a noncycle vertex.

Since $(bc)^{k^h} \equiv b^{k^h} c^{k^h} \equiv c^{k^h} \pmod{n}$, we see bc is in the forest above the cycle containing the vertex c. If $i < h$, then $(bc)^{k^i} \equiv b^{k^i} c^{k^i} \pmod{n}$, which is a cycle times a noncycle, thus a noncycle vertex. This means that bc first meets a cycle after h iterations of the k^{th} power map, i.e.,

$$bc \in F_{c^{k^h}}^h. \ \square$$

We can use Lemma 5 to show that any two trees in $G_n^{k^*}$ are isomorphic.

Theorem 4: If c is a cycle vertex, then $F_1 \cong F_c$.

Proof: For each h, we wish to construct a map from F_1^h to F_c^h that is one-to-one, onto, and preserves edges. As in [4], we define c_h as the cycle vertex such that $c_h^{k^h} \equiv c \pmod{n}$. This means c_h is the cycle vertex h cycle vertices before the cycle vertex c and therefore exists and is well defined. Following [4], define $f_h : F_1^h \to F_c^h$ such that $f_h(b) \equiv bc_h \pmod{n}$.

If $b_1, b_2 \in F_1^h$ and $f_h(b_1) \equiv f_h(b_2) \pmod{n}$, then $b_1 c_h \equiv b_2 c_h \pmod{n}$. Since $c_h \in \mathbb{Z}_n^*$, this implies $(b_1 - b_2)c_h \equiv 0 \pmod{n}$, so $b_1 \equiv b_2 \pmod{n}$.

If $b \in F_c^h$, then $(bc_h^{-1})^{k^h} \equiv b^{k^h} (c_h^{k^h})^{-1} \equiv cc^{-1} \equiv 1 \pmod{n}$. Since $(bc_h^{-1})^{k^{h-1}} \equiv b^{k^{h-1}} (c_h^{k^{h-1}})^{-1} \pmod{n}$ is a noncycle times a cycle vertex, we get a noncycle vertex. Therefore, $bc_h^{-1} \in F_1^h$ and $f_h(bc_h^{-1}) \equiv bc_h^{-1} c_h \equiv b \pmod{n}$.

Having shown f_h is one-to-one and onto for vertices, we must show it preserves edges. Specifically, if $b_1 \in F_1^{h+1}$ and $b_2 \in F_1^h$ such that $b_1^k \equiv b_2 \pmod{n}$, then $f_{h+1}(b_1)^k \equiv b_1^k c_{h+1}^k \equiv b_2 c_h \equiv f_h(b_2) \pmod{n}$, where we have used $c_{h+1}^k \equiv c_h \pmod{n}$, since c_{h+1} is $h+1$ vertices before c in the cycle and c_h is h vertices before c in the cycle. Similarly, if $b_1 \in F_c^{h+1}$ and $b_2 \in F_c^h$ such that $b_1^k \equiv b_2 \pmod{n}$, then $(b_1 c_{h+1})^k \equiv b_1^k c_{h+1}^k \equiv b_2 c^k \pmod{n}$. $\square$

Finally, we give two results to help determine the height of the tree, i.e., the maximum height of a noncycle element of $G_n^{k^*}$. Both of these are direct analogs of the prime modulus case [4].

Lemma 6: If $b \in F_c$ and $d = \text{ord}_n c$, then $(\text{ord}_n b) | k^h d$ if and only if $b \in F_c^x$ for some $x \le h$.

Proof: If $(\text{ord}_n b)|k^h d$, then $\text{ord}_n(b^{k^h})|d$ so $\text{ord}_n(b^{k^h})|t$ since $d|t$ as c is a cycle vertex. This means b^{k^h} is a cycle vertex in the same cycle as c, so $b \in F_c^x$ for some $x \le h$.

Conversely, if $b \in F_c^x$ for some $x \le h$, then $b^{k^x} \equiv c \pmod n$ so $\text{ord}_n(b^{k^x}) = d$. Therefore, $\text{ord}_n(b^{k^h}) = \text{ord}_n((b^{k^x})^{k^{h-x}}) = \text{ord}_n c^{k^{h-x}} = d$ by Lemma 4. □

Theorem 5: The height of the trees in $G_n^{k^*}$ is the minimal h such that $L|k^h t$.

Proof: If $(k, L) = 1$, then $t = L$ so Lemma 3 says that all vertices are cycles; thus, the height is 0 and $L|k^0 t$ since $t = L$.

If $(k, L) \ne 1$, then $h > 0$. Take b a vertex of maximal order, $\text{ord}_n b = L$. By Lemma 6, b is of height h since $(\text{ord}_n b)|k^h t$ but $(\text{ord}_n b) \nmid k^{h-1} t$. □

4. STRUCTURE OF $G_n^k - G_n^{k^*}$

Let $\wp$ be the set of all prime divisors of n and consider a partition of this set: $\wp = \wp_1 \cup \wp_2$. Let $G_{n,\wp_1}^k$ be the graph whose vertices are the multiples of $\prod_{p\in\wp_1} p$ relatively prime to all $p \in \wp_2$ and with an edge from b_1 to b_2 if $b_1^k \equiv b_2 \pmod n$. If a_p is such that $p^{a_p}|n$ but $p^{a_p+1} \nmid n$, define $n_1 = \prod_{p\in\wp_1} p^{a_p}$ and $n_2 = \prod_{p\in\wp_2} p^{a_p}$. Define $G_{n,\wp_1,\max}^k$ to be the graph whose vertices are the multiples of n_1 relatively prime to all $p \in \wp_2$ and where there is an edge from b_1 to b_2 if $b_1^k \equiv b_2 \pmod n$. We give a few results to help determine the structure of $G_{n,\wp_1}^k$.

Theorem 6: $G_{n,\wp_1,\max}^k \cong G_{n_2}^{k^*}$.

Proof: Let b_0 be the solution to $n_1 b_0 \equiv 1 \pmod{n_2}$. Define

$$\mu: G_{n_2}^{k^*} \to G_{n,\wp_1,\max}^k \text{ such that } \mu(b) \equiv b b_0 n_1 \pmod n.$$

For $q \in \wp_2$, $q \nmid b_0$, $q \nmid n_1$ so $b \in G_{n_2}^{k^*}$ implies $b b_0 n_1 \pmod n$ is in $G_{n,\wp_1,\max}^k$. Having shown our map is well defined on the set of vertices, we must show it is one-to-one onto, and preserves edges.

If $\mu(b_1) \equiv \mu(b_2) \pmod n$, then $(b_1 - b_2) b_0 n_1 \equiv 0 \pmod n$. This means $(b_1 - b_2) b_0 \equiv 0 \pmod{n_2}$. Since b_0 is invertible modulo n_2, $b_1 - b_2 \equiv 0 \pmod{n_2}$ so $b_1 = b_2$ in $G_{n_2}^{k^*}$.

If $c \in G_{n,\wp_1,\max}^k$, then $c = n_1 c_0$, so we want to show that there exists $b \in G_{n_2}^{k^*}$ such that $\mu(b) \equiv c \pmod n$. This is equivalent to

$$b b_0 n_1 \equiv c_0 n_1 \pmod n,$$

which is equivalent to

$$b b_0 \equiv c_0 \pmod{n_2}.$$

Since b_0 is invertible modulo n_2 and c_0 is relatively prime to all primes in $\wp_2$, $b \equiv b_0^{-1} c_0 \pmod{n_2}$ is an element of $G_{n_2}^{k^*}$ sent to c via μ.

If $b_1, b_2 \in G_{n_2}^{k^*}$ such that $b_1^k \equiv b_2 \pmod{n_2}$, then

$$\mu(b_1)^k \equiv b_1^k b_0^k n_1^k \equiv b_1^k b_0 n_1 \equiv b_2 b_0 n_1 \equiv \mu(b_2) \pmod n.$$

Finally, we deal with those vertices divisible by $\prod_{p\in\wp_1} p$ but not by n_1.

Theorem 7: $\left(\prod_{p\in\wp_1} p^{b_p}\right)b$ with $(b, p) = 1$ for all $p \in \wp$ has zero or

$$\left(\prod_{p\in\wp_2,\, p\neq 2} (k, p^{a_p-1}(p-1))\right)\cdot\left(\prod_{p\in\wp_1,\, p\neq 2,\, b_p\geq a_p,\, kc_p\geq a_p} p^{a_p-c_p-1}(p-1)\right)\cdot$$

$$\left(\prod_{p\in\wp_1,\, p\neq 2,\, a_p>c_pk,\, b_p=c_pk} p^{(k-1)c_p}(k, p^{a_p-b_p-1}(p-1))\right).$$

$$\begin{Bmatrix} (2,k)^{\delta_1}(2^{a-2},k)^{\delta_2} & \text{if } 2\in\wp_2 \\ 2^{a-c_2-1} & \text{if } 2\in\wp_1,\, b_2\geq a,\, c_2k\geq a \\ 2^{(k-1)c_2}(2,k)^{\delta_3}(2^{a-b_2-2},k)^{\delta_4} & \text{if } 2\in\wp_1, a>c_2k,\, b_2=c_2k \end{Bmatrix}$$

parent vertices of the form $\left(\prod_{p\in\wp_1} p^{c_p}\right)c$ with $(c, p) = 1$ for all $p \in \wp$, where

$$\delta_3 = \begin{cases} 0 & \text{if } a-b_2<2, \\ 1 & \text{if } a-b_2\geq 2, \end{cases} \quad \text{and} \quad \delta_4 = \begin{cases} 0 & \text{if } a-b_2<3, \\ 1 & \text{if } a-b_2\geq 3. \end{cases}$$

Proof: We want to find the number of distinct solutions, $\left(\prod_{p\in\wp_1} p^{c_p}\right)c$, to

$$\left(\left(\prod_{p\in\wp_1} p^{c_p}\right)c\right)^k \equiv \left(\prod_{p\in\wp_1} p^{b_p}\right)b \pmod{n},$$

where $(cb, p) = 1$ for all $p \in \wp$.

This is equivalent to counting the number of solutions to the system

$$\left(\left(\prod_{p\in\wp_1} p^{c_p}\right)c\right)^k \equiv \left(\prod_{p\in\wp_1} p^{b_p}\right)b \pmod{2^a},$$

$$\left(\left(\prod_{p\in\wp_1} p^{c_p}\right)c\right)^k \equiv \left(\prod_{p\in\wp_1} p^{b_p}\right)b \pmod{p_1^{a_1}}$$

$$\vdots$$

$$\left(\left(\prod_{p\in\wp_1} p^{c_p}\right)c\right)^k \equiv \left(\prod_{p\in\wp_1} p^{b_p}\right)b \pmod{p_m^{a_m}}.$$

Fact 1 allows us to work with each of these congruences separately and then multiply the number of solutions to each congruence to get the number of solutions to the system.

If $q \in \wp_2$, then all $p \in \wp_1$ are invertible, so the number of solutions to

$$\left(\left(\prod_{p\in\wp_1} p^{c_p}\right)c\right)^k \equiv \left(\prod_{p\in\wp_1} p^{b_p}\right)b \pmod{q^{a_q}}$$

equals the number of solutions to $c^k \equiv b' \pmod{q^{a_q}}$ for some b'. By Fact 4 the number of solutions is zero or $(k, q^{a_q-1}(q-1))$ if q is an odd prime, and zero or $(2,k)^{\delta_1}(2^{a-2},k)^{\delta_2}$ if $q=2$.

If $q \in \wp_1$, then all $p \in \wp_1 - \{q\}$ are invertible, so the number of solutions to

$$\left(\left(\prod_{p\in\wp_1} p^{c_p}\right)c\right)^k \equiv \left(\prod_{p\in\wp_1} p^{b_p}\right)b \pmod{q^{a_q}}$$

is equal to the number of solutions to $(q^{c_q}c)^k \equiv q^{b_q}b' \pmod{q^{a_q}}$ for some b'. If $c_qk \neq b_q$ and either $b_q < a_q$ or $c_qk < a_q$, then there are no solutions for $(cb', q) = 1$ since the powers of q dividing the left- and right-hand sides of the congruence will be unequal for all k.

If $b_q, c_qk \geq a_q$, then we are trying to solve $0 \cdot c^k \equiv 0 \pmod{q^{a_q}}$. This has $q^{a_q-c_q-1}(q-1)$ solutions c for which $(c,q)=1$ and $q^{c_q}c$ are distinct modulo q^{a_q}. For $q=2$, this reduces to 2^{a-c_2-1}.

Finally, if $a_q > c_qk = b_q$, then; the number of solutions $q^{c_q}c$ to $(q^{c_q}c)^k \equiv q^{b_q}b' \pmod{q^{a_q}}$ is $q^{(k-1)c_q}$ times the number of solutions to $c^k \equiv b' \pmod{q^{a_q-b_q}}$. By Fact 4 this is zero or

$$q^{(k-1)c_q}(k, q^{a_q-b_q-1}(q-1))$$

if q is an odd prime, and zero or

$$2^{(k-1)c_2}(2,k)^{\delta_3}(2^{a-b_2-2},k)^{\delta_4}$$

if $q=2$.

The product of the numbers of solutions to each of these congruences gives the number of solutions to the system, proving the result. □

Remark: Similar results may be developed where the hypothesis $(c,p)=1$ is dropped. For example, if $p \in \wp_1$ is an odd prime and $(b,p)=1$, then the number of solutions to $(p^{c_p}c)^k \equiv p^{b_p}b \pmod{p^{a_p}}$ is zero or $p^{a_p-c_p}$ if $c_pk, b_p \geq a_p$. Other cases for a_p, b_p, c_pk may be worked out as in the proof of the last theorem.

5. AN EXAMPLE

Example 1: We will determine the structure of G_{56}^2. Note that $n=56$, $k=2$, $L=6$, $t=3$, and $w=2$. We start with the components with vertices that are not multiples of 2 or 7. $\mathbb{Z}_{56}^* \cong \mathbb{Z}_7^* \times \mathbb{Z}_8^* \cong \mathbb{Z}_6 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. This means the orders of all elements divide $\text{lcm}(6,2,2)=6$. We get the number of elements of each order using Lemma 1.

$$\begin{aligned}
\psi(1) &= (1,6)(1,2)(1,2) = 1,\\
\psi(2) &= (2,6)(2,2)(2,2) - \psi(1) = 7,\\
\psi(3) &= (3,6)(3,2)(3,2) - \psi(1) = 2,\\
\psi(6) &= (6,6)(6,2)(6,2) - \psi(3) - \psi(2) - \psi(1) = 14.
\end{aligned}$$

The one element of order 1 goes to itself since $2^1 \equiv 1 \pmod 1$; the seven elements of order 2 each go to the element of order 1 when squares; the two elements of order 3 are, by Theorem 2, in a cycle of length 2 since $2^1 \not\equiv 1 \pmod 3$, but $2^2 \equiv 1 \pmod 3$; and the fourteen elements of order 6 go to elements of order 3. If b is an element of order 3, we know that $x^2 \equiv b \pmod{56}$ has at

least one solution (the other element of order 3). Solving $x^2 \equiv b \pmod{56}$ is equivalent to solving the system

$$\begin{aligned} x^2 &\equiv b \pmod 7 \\ x^2 &\equiv b \pmod 8. \end{aligned} \tag{4}$$

Since $\mathbb{Z}_7^* \cong \mathbb{Z}_2 \times \mathbb{Z}_3$, the first congruence in our system has 0 or 2 solutions. Since $\mathbb{Z}_8^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, the second congruence in our system has 0 or 4 solutions. This means the system (4) has 0 or 8 solutions. Since there is at least one solution, this forces each element of order 3 to have indegree 8, i.e., seven elements of order 6 and one of order 2. This completely classifies the structure of $G_{56}^{2^*}$ (see Fig. 1).

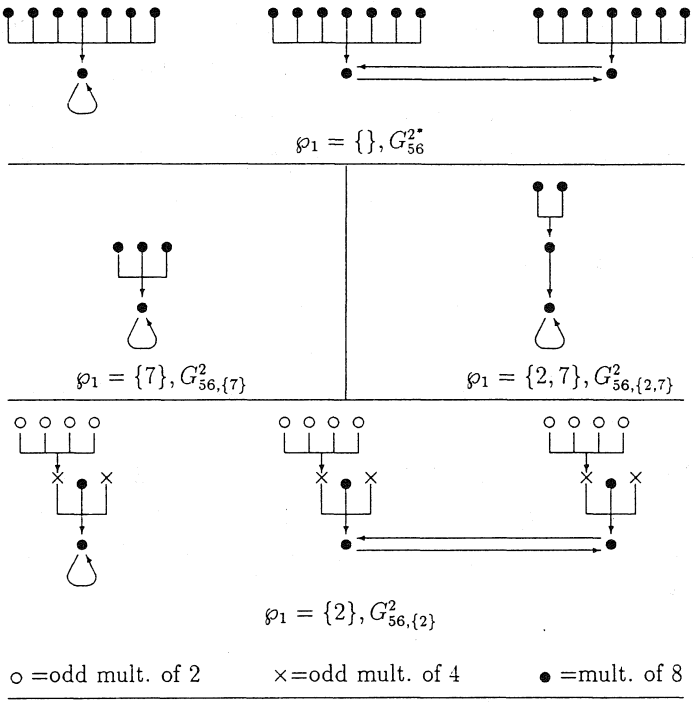

FIGURE 1. G_{56}^{2}

Next, consider the components which are multiples of 7 but relatively prime to 2. By Theorem 6 this will have a digraph structure isomorphic to $G_8^{2^*}$. $\mathbb{Z}_8^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, so there is one element of order 1 and three elements of order 2. Each element of order 2, when squared goes to the element or order 1.

The trickiest part is classifying the components that have vertices which are multiples of 2 but relatively prime to 7. By Theorem 6, $G_{56,\{2\},\max}^{2} \cong G_7^{2^*}$. $\mathbb{Z}_7^* \cong \mathbb{Z}_6$, so there is one element of order 1, one of order 2, two of order 3, and two of order 6. Upon squaring, the element of order 1 goes to itself, the element of order 2 goes to the element of order 1, the elements of order 3 go to each other, by Theorem 2, since $2^1 \not\equiv 1 \pmod 3$, $2^2 \equiv 1 \pmod 3$, and the elements of order 6 go to the elements of order 3. By Fact 4, $x^2 \equiv b \pmod 7$ has 0 or 2 solutions (since $\mathbb{Z}_7^* \cong \mathbb{Z}_2 \times \mathbb{Z}_3$) and

each element of order 3 has the other element of order 3 coming to it, we know the indegree must be 2, so each element of order 6 goes to a different element of order 3 (see Fig. 1).

We now add vertices for the multiples of 4 and of 2 that are prime to 7. Theorem 7, with $n = 56, k = 2, \wp_1 = \{2\}, \wp_2 = \{7\}, c_2 = 2$, and $b_2 \geq 3$, says the indegree for vertices that are multiples of 8 from those that are multiples of 4, relatively prime to 7, is zero or $(2, 7^{1-1}(7-1))2^{3-2-1} = 2$. Using the remark after Theorem 7, considering the graph of multiples of 4 relatively prime to 7, each vertex has indegree 0 or 4. There are $56 \cdot \frac{1}{8} \cdot \frac{6}{7} = 6$ odd multiples of 4, so each of the three cycle vertices of $G^2_{56,\{2\},\max}$ has two odd multiples of 4 parents (see Fig. 1).

To add the odd multiples of 2 prime to 7, we note that these will be parents of odd multiples of 4. Using Theorem 7, with $n = 56, k = 2, \wp_1 = \{2\}, \wp_2 = \{7\}, c_2 = 1$, and $b_2 = 2$, says the indegree for vertices that are odd multiples of 4 from those that are odd multiples of 2, relatively prime to 7, is zero or $(2, 7^{1-1}(7-1))2^{(2-1)1}(2,2)^0(2^0,2)^0 = 4$. Using Theorem 7, with $n = 56$, $k = 4 = 2^2$, $\wp_1 = \{2\}$, $\wp_2 = \{7\}$, $c_2 = 1$, and $b_2 \geq 3$, says the number of odd multiples of 2 in each tree in $G^2_{56,\{2\}}$ is zero or $(4, 7^{1-1}(7-1))2^{3-1-1} = 4$. Since there are $56 \cdot \frac{1}{4} \cdot \frac{6}{7} = 12$ odd multiples of 2 relatively prime to 7, we have three sets of four odd multiples of 2 going to one of each pair of odd multiples of 4 over each cycle vertex in $G^2_{56,\{2\},\max}$ (Fig. 1). This completes the structure of $G^2_{56,\{2\}}$.

Finally, $G^2_{56,\{2\},\max} \cong G_1^{2^*}$, which is a single element with edge from and to itself. To map directly onto a multiple of $2^3 \cdot 7$, the power on 2 must be at least 2, so the only parent of our single cycle vertex is the odd multiple of $2^2 \cdot 7$ (mod 56). Odd multiples of $2 \cdot 7$ map to the odd multiple of $2^2 \cdot 7$ when squared. This completes the description of G^2_{56} (see Fig. 1).

REFERENCES

1. M. Behzad & G. Chartrand. *Introduction to the Theory of Graphs.* Boston: Allyn and Bacon, 1971.
2. E. Blanton, Jr., S. Hurd, & J. McCranie. "On a Digraph Defined by Squaring Modulo n." *The Fibonacci Quarterly* **30.4** (1992):322-34.
3. L. K. Hua. *Introduction to Number Theory.* New York: Springer-Verlag, 1982.
4. C. Lucheta, E. Miller, & C. Reiter. "Digraphs from Powers Modulo p." *The Fibonacci Quarterly* **34.3** (1996):226-39.
5. T. D. Rogers. "The Graph of the Square Mapping on the Prime Fields." *Discrete Math.* **148** (1996):317-24.

AMS Classification Numbers: 05C20, 11B50

❖❖❖