DIGRAPHS FROM ENDOMORPHISMS OF FINITE CYCLIC GROUPS

MIN SHA

ABSTRACT. We associate each endomorphism of a finite cyclic group with a digraph and study many properties of this digraph, including its adjacency matrix and automorphism group.

1. INTRODUCTION

As we all know, we can construct Cayley graphs and Cayley digraphs from a group, and these graphs are vertex-transitive. In this article, we construct digraphs from a finite cyclic group by using its endomorphisms. In general, these digraphs are not vertex-transitive. But they have many good properties which may make them into beautiful graphs and may merit further researches.

Let H be a finite cyclic group with n elements, $n > 1$, we treat it as a multiplicative group. We denote its identity element by 1 without confusion. As we all know, H has n endomorphisms, every endomorphism has a unique form $f : H \to H, x \to x^k, k \in \mathbb{Z}, 1 \leq k \leq n$, and f is an isomorphism if and only if n and k are coprime. We can consider the digraph that has the elements of H as vertices and a directed edge from a to b if and only if $f(a) = b$. Since cyclic groups with the same order are isomorphic, this digraph only depends on n and k. So we can denote this digraph by $G(n, k)$. For example, see Figure 1 in section 4. [2] studied the digraph from any endomorphism of $\mathbb{Z}/n\mathbb{Z}$, especially the author studied the number of cycles. [1], [7] and [12] studied the digraph from the endomorphism $f(x) = x^2$ of $(\mathbb{Z}/p\mathbb{Z})^*$, p is a prime. In particular, the cycle and tree structures have been classified. [6] generalized those results in [1] to the digraph from any endomorphism of $(\mathbb{Z}/p\mathbb{Z})^*$. [8] studied some elementary properties of the digraph from any endomorphism of $(\mathbb{F}_q)^*$, $\mathbb{F}_q$ is a finite field with q elements.

In section 2 and section 3, we generalize those results in [6] to $G(n, k)$, and we consider many other properties of $G(n, k)$. In section 4 and section

2010 *Mathematics Subject Classification:* Primary 05C05, 05C20; Secondary 05C25, 05C50.

Key words: cyclic group, digraph, tree, adjacency matrix, automorphism group.

5, we consider its adjacency matrix and automorphism group respectively, furthermore we determine its characteristic polynomial and minimal polynomial.

Especially, the results here may have applications to monomial dynamical systems over finite fields, see [8].

2. Basic Properties of $G(n,k)$

Given two integers l and m, we denote their greatest common divisor and least common multiple by (l,m) and $[l,m]$ respectively.

First we factor n as tw where t is the largest factor of n relatively prime to k. So $(k,t)=1$ and $(w,t)=1$. For any $a \in H$, Let $\mathrm{ord}(a)$ denote its order.

For proceeding further, we need the following lemma.

Lemma 2.1. *Let $a \in H$, the equation $x^k = a$ has a solution if and only if $a^{\frac{n}{d}} = 1$, $d=(n,k)$. Moreover, if the equation has a solution, it has exactly d solutions.*

Proof. Applying the same argument as Proposition 7.1.2 in [5]. □

The following lemma is easy to prove but fundamental to the understanding of the structure of $G(n,k)$. We omit its proof and refer the readers to [6].

Lemma 2.2. *We have the following elementary properties of $G(n,k)$.*

(1) *The outdegree of any vertex in $G(n,k)$ is 1.*

(2) *The indegree of any vertex in $G(n,k)$ is 0 or (n,k). Moreover, the indegree of $a \in G$ is (n,k) if and only if $a^{\frac{n}{(n,k)}} = 1$.*

(3) *$G(n,k)$ has n vertices and n directed edges.*

(4) *Given $a,b \in H$, there exists a directed path from a to b if and only if there exists a positive integer m such that $a^{k^m} = b$.*

(5) *Given any element in $G(n,k)$, repeated iteration of f will eventually lead to a cycle.*

(6) *Every component of $G(n,k)$ contains exactly one cycle.*

(7) *The set of non-cycle vertices forms a forest.*

Proposition 2.3. *The number of the vertices with indegree 0 is $\frac{d-1}{d}n$, where $d=(n,k)$.*

Proof. By Lemma 2.1, a vertex a has non-zero indegree if and only if $a^{\frac{n}{d}} = 1$. Hence, the vertices with non-zero indegree form a subset $H_d = \{x \in H | x^{\frac{n}{d}} = 1\}$. It is well-known that H_d is a cyclic subgroup of H with $\frac{n}{d}$ elements. So we get the desired result. □

As follows, we want to study the cycle structures of $G(n,k)$.

Proposition 2.4. *The vertex a is a cycle vertex if and only if* $\mathrm{ord}(a) | t$.

Proof. Suppose a is a cycle vertex. Then there exists a positive integer m such that $a^{k^m} = a$. So $\mathrm{ord}(a)|(k^m - 1)$, which implies $(\mathrm{ord}(a), k) = 1$. So $(\mathrm{ord}(a), w) = 1$. Note that $\mathrm{ord}(a)|n$, then $\mathrm{ord}(a)|t$.

Conversely, suppose $\mathrm{ord}(a)|t$. Then $(\mathrm{ord}(a), k) = 1$. So there exists a positive integer m such that $\mathrm{ord}(a)|(k^m - 1)$, which implies $a^{k^m} = a$. So a is a cycle vertex. □

Corollary 2.5. *There are exactly t cycle vertices in $G(n, k)$.*

Proof. From Proposition 2.4, the total number of cycle vertices is $\sum_{d|t} \varphi(d) = t$, where φ is the Euler's φ-function, and $\varphi(d)$ is the number of elements with order d. □

Proposition 2.6. *Vertices in the same cycle have the same order.*

Proof. Assume a and b are in the same cycle. So there exists a m such that $a^{k^m} = b$, which implies $b^{\mathrm{ord}(a)} = 1$. So $\mathrm{ord}(b)|\mathrm{ord}(a)$. Similarly, we have $\mathrm{ord}(a)|\mathrm{ord}(b)$. So $\mathrm{ord}(a) = \mathrm{ord}(b)$. □

By Proposition 2.6, the notion of the order of a cycle is well-defined. Let $\ell(d)$ denote the length of a cycle with order d, where $d|t$. If two integers l and m are coprime, let $\mathrm{ord}_l m$ denote the exponent of m modulo l.

Proposition 2.7. *Let d and r be orders of cycles. Then:*

(1) $\ell(d) = \mathrm{ord}_d k$.

(2) *The longest cycle length in $G(n, k)$ is* $\ell(t) = \mathrm{ord}_t k$.

(3) *There are $\varphi(d)/\ell(d)$ cycles of order d.*

(4) *The total number of cycles in $G(n, k)$ is* $\sum_{d|t} \frac{\varphi(d)}{\ell(d)}$.

(5) $\ell([d, r]) = [\ell(d), \ell(r)]$.

Proof. (1) Let a be a vertex in a cycle of order d. It is obvious that $\ell(d)$ is the smallest positive integer such that $a^{k^{\ell(d)}} = a$, that is the smallest positive integer such that $d|(k^{\ell(d)} - 1)$. So $\ell(d) = \mathrm{ord}_d k$.

(2) By (1) and Proposition 2.4.

(3) Notice that the number of elements with order d is $\varphi(d)$.

(4) By (3) and Proposition 2.4.

(5) Since $d|[d, r]$, $\ell(d)|\ell([d, r])$. Similarly, we have $\ell(r)|\ell([d, r])$. So $[\ell(d), \ell(r)]|\ell([d, r])$. In addition, since $d|(k^{\ell(d)} - 1)$, $d|(k^{[\ell(d),\ell(r)]} - 1)$. Similarly, $r|(k^{[\ell(d),\ell(r)]} - 1)$. So $[d, r]|(k^{[\ell(d),\ell(r)]} - 1)$. Hence, $\ell([d, r])|[\ell(d), \ell(r)]$. So we have $\ell([d, r]) = [\ell(d), \ell(r)]$. □

But $\ell((d, r)) = (\ell(d), \ell(r))$ is not always true. For example, let $k = 2, d = 11$ and $r = 15$, we have $(11, 15) = 1$ and $\ell(1) = 1$, but $(\ell(11), \ell(15)) = (10, 4) = 2$.

Remark 2.8. Let μ be Möbius function. Similar as Proposition 2.5 in [8], the number of cycles with length r is $\frac{1}{r}\sum_{d|r}\mu(d)(k^{r/d}-1,n)$.

Corollary 2.9. *If a component has a generator of H, then its unique cycle has the longest length $\ell(t)$.*

Proof. Since if a component has a generator of H, the order of its unique cycle is t. □

Proposition 2.10. *Every generator of H has indegree 0 if and only if $(n,k) \neq 1$.*

Proof. Suppose $(n,k) \neq 1$. For any generator b of H, if the indegree of b is not 0, then there exists a vertex a such that $a^k = b$. Since $n = \mathrm{ord}(b) = \frac{\mathrm{ord}(a)}{(\mathrm{ord}(a),k)}$ and $\mathrm{ord}(a)|n$, $\mathrm{ord}(a) = n$ and $(n,k) = 1$. This leads to a contradiction.

Conversely, if every generator of H with indegree 0, then generators are not cycle vertices. By Proposition 2.4, $t \neq n$. So $(n,k) \neq 1$. □

Hence, if $(n,k) \neq 1$, since H has $\varphi(n)$ generators, by Proposition 2.3, we have $\varphi(n) \leq \frac{d-1}{d}n$, where $d = (n,k)$.

Now we would like to consider which kind of graphs $G(n,k)$ belongs to.

Proposition 2.11. *The following statements are equivalent.*

(1) *$G(n,k)$ is regular of degree 1.*

(2) *Every component of $G(n,k)$ is a cycle.*

(3) *f is an automorphism.*

Proof. Note that f is an automorphism if and only if $(n,k) = 1$, then applying Lemma 2.2 (2) and (7). □

Proposition 2.12. *$G(n,k)$ is connected if and only if there exists a positive integer m such that $n|k^m$.*

Proof. Suppose $n|k^m$. Then for any $a \in H$, $a^{k^m} = 1$. So $G(n,k)$ is connected.

Conversely, suppose $G(n,k)$ is connected. By Lemma 2.2 (7), there is only one cycle, that is $\{1\}$. By Lemma 2.2 (6), for any $a \in H$, there is a positive integer m such that $a^{k^m} = 1$. If a is a generator of H, then $n|k^m$. □

Notice that there exists a positive integer m such that $n|k^m$ if and only if $t = 1$. Hence, $G(n,k)$ is connected if and only if $G(n,k)$ has only one cycle vertex, that is the identity element.

Proposition 2.13. *The following statements are equivalent.*

(1) *$G(n,k)$ is arc-transitive.*

(2) $G(n,k)$ *is vertex-transitive.*
(3) f *is the identity.*

Proof. Note that there exist loops in $G(n,k)$. So $G(n,k)$ is arc-transitive if and only if there are no other edges except loops, that is for any $a \in G(n,k), f(a) = a$, that is for any $a \in G(n,k), a^{k-1} = 1$, that is $n|(k-1)$.

Applying the same argument as the above paragraph, we have $G(n,k)$ is vertex-transitive if and only if $n|k-1$.

Notice that $1 \leq k \leq n$, we get the desired result. □

Since the number of distinct endomorphisms of H is n, we attain n distinct digraphs by our manner. There is an interesting problem that whether there exist isomorphic digraphs among them. In [6], the authors gave an example $G(10,2) \cong G(10,8)$.

Proposition 2.14. *If n is a prime, for any $1 < k_1 < k_2 < n$, $G(n,k_1) \cong G(n,k_2)$ if and only if* $\mathrm{ord}_n k_1 = \mathrm{ord}_n k_2$.

Proof. Since $(n,k_1) = 1$, by Proposition 2.11, each component of $G(n,k_1)$ is a cycle. By Proposition 2.7 (1), there are only two kinds of cycles in $G(n,k_1)$, one with length 1, the other with length $\mathrm{ord}_n k_1$. Since $(n,k_1 - 1) = 1$, there is only one cycle with length 1. By Proposition 2.7 (3), there are $\frac{n-1}{\mathrm{ord}_n k_1}$ cycles with length $\mathrm{ord}_n k_1$.

We can get similar results for $G(n,k_2)$. Then we can get the desired result. □

3. Properties of Trees

Here we introduce some notations for the tree originating from any given cycle vertex.

For $m \geq 1$, we say a non-cycle vertex a has height m with respect to a cycle vertex c if m is the smallest positive integer such that $a^{k^m} = c$. For $m \geq 1$, let T_c^m denote the set of non-cycle vertices with height m with respect to the cycle vertex c. Similarly, T^m denotes the set of all vertices with height m. For convenience, we put $T_c^0 = \{c\}$ and say c has height 0, T^0 denotes the set of all cycle vertices. Let F_c be the induced subgraph of $G(n,k)$ with vertices $\bigcup_{m \geq 1} T_c^m$. In fact, F_c is a forest if it is not empty. We can get an induced subgraph of $G(n,k)$ with vertices $\bigcup_{m \geq 0} T_c^m$, and we delete the loop if it exists, then we get a tree and denote it by T_c.

All the vertices lie in the trees we define above. As follows, without special instructions, the concept of tree means what we define in the above.

We will show that for any cycle vertex c, $T_c \cong T_1$.

Lemma 3.1. *The product of a non-cycle vertex and a cycle vertex is a non-cycle vertex.*

Proof. Notice that by Proposition 2.4, the cycle vertices of $G(n,k)$ form a subgroup. □

Lemma 3.2. *If $a \in T_1^h, h \geq 1$ and c is a cycle vertex, then $ac \in T_{c^{k^h}}^h$.*

Proof. By Lemma 3.1, $ac \notin T^0$. Furthermore, $(ac)^{k^h} = c^{k^h}$ is a cycle vertex but $(ac)^{k^{h-1}}$ is a non-cycle vertex because $a^{k^{h-1}} \notin T^0$, which implies $ac \in T_{c^{k^h}}^h$. □

Theorem 3.3. *Let c be a cycle vertex, then $F_c \cong F_1$.*

Proof. First we show that there exists an one to one correspondence between the vertices of T_1^h and T_c^h for all heights $h \geq 1$, and hence between F_1 and F_c. Let h be fixed and let c_h denote the unique cycle vertex such that $c_h^{k^h} = c$. From Lemma 3.2, define $g_h : T_1^h \to T_c^h$ by $g_h(a) = ac_h$.

For any $b \in T_c^h$, $(b \cdot c_h^{-1})^{k^h} = b^{k^h} c^{-1} = 1$ and $(b \cdot c_h^{-1})^{k^{h-1}} \notin T^0$ because $b^{k^{h-1}} \notin T^0$. It follows that $b \cdot c_h^{-1} \in T_1^h$. Then $g_h(b \cdot c_h^{-1}) = b$. So g_h is surjective. It is obvious that g_h is injective. So g_h is one to one.

Combining these g_h, we get a bijective map g from F_1 to F_c.

It remain to show that g is indeed an isomorphism. For any directed edge of F_1, it is from some $a \in T_1^h$ to $a^k \in T_1^{h-1}$ for some h. We only need to show that there exists a directed edge from $g(a)$ to $g(a^k)$ in F_c, that is $(g(a))^k = g(a^k)$, that is $(g_h(a))^k = g_{h-1}(a^k)$. Now $c_h^{k^h} = c$ implies $(c_h^k)^{k^{h-1}} = c$, by the uniqueness of c_{h-1}, we have $c_h^k = c_{h-1}$. So $(g_h(a))^k = (ac_h)^k = a^k c_{h-1} = g_{h-1}(a^k)$. □

Corollary 3.4. *Let c be a cycle vertex, then $T_c \cong T_1$.*

Proof. Applying Theorem 3.3 and the relation between T_c and F_c. □

Hence, every tree has the same height, denote it by h_0, and different trees have the same number of vertices in each height.

Corollary 3.5. *For any two components G_1 and G_2 of $G(n,k)$, $G_1 \cong G_2$ if and only if the unique cycles in them have the same length.*

There is another property of the map g_h in Theorem 3.3, see the following proposition.

Proposition 3.6. *If $a \in T_1^h$ and $b \in T_c^h$ with c_h the cycle vertex such that $b = ac_h$, then* $\mathrm{ord}(b) = \mathrm{ord}(a) \cdot \mathrm{ord}(c)$.

Proof. Since $a^{k^h} = 1$, $\mathrm{ord}(a) | k^h$. By Proposition 2.6, $\mathrm{ord}(c_h) = \mathrm{ord}(c) | t$. So $(\mathrm{ord}(a), \mathrm{ord}(c_h)) = 1$. It follows that $\mathrm{ord}(b) = \mathrm{ord}(a) \cdot \mathrm{ord}(c)$. □

As follows, we would like to study the tree structures by using heights.

For any $a \in H$, denote its order $\mathrm{ord}(a)$ by n_a, and factor n_a by $t_a w_a$, where t_a is the largest factor of n_a relatively prime to k. So $n_a | n, t_a | t$ and

$w_a|w$. Similarly, we denote a's height by h_a. The next proposition shows that h_a only depends on w_a.

Proposition 3.7. *For any $a \in H$, h_a is the minimal h such that $w_a|k^h$. Especially, h_0 is the minimal h such that $w|k^h$.*

Proof. If $n_a \mid t$, then a is a cycle vertex. So $h_a = 0$. Note that $w_a = 1$, so the conclusion is correct in this case.

If $n_a \nmid t$. Since h_a is the minimal h such that a^{k^h} is a cycle vertex, that is the minimal h such that $\mathrm{ord}(a^{k^h}) = \frac{n_a}{(n_a, k^h)} \mid t$, then h_a is the minimal h such that $(n_a, k^h) = w_a$, that is the minimal h such that $w_a \mid k^h$. □

Corollary 3.8. *For any two vertices a and b,if $w_a = w_b$, then they have the same height. Especially, The vertices with the same order are at the same height.*

But if a and b have the same height, maybe $w_a \neq w_b$. For example, see Figure 3 in section 5, let $a = 9$ and $b = 40$, then a and b have the same height, but $w_a = 4$ and $w_b = 2$.

Corollary 3.9. *For any vertex a, if $w_a = w$, then a is at the largest height. Especially, the generators of H must be at the largest height.*

Proof. For any vertex a, $w_a \mid w$, then applying Proposition 3.7, we get the desired result. □

Corollary 3.10. *If k is a prime, then for any two vertices a and b, they have the same height if and only if $w_a = w_b$.*

Proof. Since $w_a = k^{h_a}$ and $w_b = k^{h_b}$ in this case. □

About the heights of the vertices we have the following proposition and corollary.

Proposition 3.11. *Let $a \in T_c$, $\mathrm{ord}(c) = d|t$ and $h \geq 0$. Then $\mathrm{ord}(a)|k^h d$ if and only if $a \in T_c^m$, for some $m \leq h$.*

Proof. Suppose $\mathrm{ord}(a)|k^h d$. Then $(a^{k^h})^d = 1$, which implies $\mathrm{ord}(a^{k^h})|d$. So a^{k^h} is a cycle vertex. Hence, there exists $m \leq h$ such that $a \in T_c^m$.

Conversely, suppose there exists $m \leq h$ such that $a \in T_c^m$. Then $a^{k^m} = c$. So $(a^{k^m})^d = c^d = 1$, which implies $\mathrm{ord}(a)|k^m d$. Hence, $\mathrm{ord}(a)|k^h d$. □

Corollary 3.12. *Let $a \in T_c$, $\mathrm{ord}(c) = d|t$ and $m \geq 1$. Then $a \in T_c^m$ if and only if $\mathrm{ord}(a)|k^m d$ and $\mathrm{ord}(a) \nmid k^{m-1} d$.*

For any $d \geq 1$, let H_d be the subgroup of H defined by $H_d = \{x \in H | x^d = 1\}$. It is well-known that H_d is cyclic with order (n, d). By Proposition 2.4, all cycle vertices of $G(n, k)$ form the subgroup H_t. By Lemma 2.1, all vertices with non-zero indegree form the subgroup $H_{\frac{n}{(k,n)}}$.

Corollary 3.13. *For any $d|t$ and $h \geq 0$, $\bigcup_{\substack{0\leq m\leq h \\ c\in T^0,\, \mathrm{ord}(c)|d}} T_c^m$ is exactly the subgroup $H_{k^h d}$.*

Proof. By Proposition 3.11 and the first part of its proof, this union consists of all $a \in H$ with $\mathrm{ord}(a)|k^h d$. So it is exactly the subgroup $H_{k^h d}$. □

Corollary 3.14. *For any $l \geq 1$ and $h \geq 0$, $\bigcup_{\substack{0\leq m\leq h \\ c\in T^0,\, \ell(c)|l}} T_c^m$ is exactly the subgroup $H_{k^h\cdot(t,k^l-1)}$.*

Proof. Since c is a cycle vertex, $\mathrm{ord}(c)|t$. Then $\ell(c)|l$ if and only if $c^{k^l} = c$, that is $\mathrm{ord}(c)|(k^l - 1)$, that is $\mathrm{ord}(c)|(t, k^l - 1)$, then applying Corollary 3.13. □

For any set X, denote the number of its elements by $|X|$.

Proposition 3.15. *For any cycle vertex c, we have:*

(1) $|T_c| = w$.

(2) *For $m \geq 1$, $|T^m| = (n, k^m t) - (n, k^{m-1}t)$ and $|T_c^m| = (w, k^m) - (w, k^{m-1})$.*

(3) *If $h_0 \geq 2$, for $1 \leq m \leq h_0 - 1$, the number of vertices in T_c^m with indegree 0 is $|T_c^m| - \frac{|T_c^{m+1}|}{(k,n)}$.*

Proof. (1) Note that there are t cycle vertices and $n = wt$, by Corollary 3.4, we have $|T_c| = w$.

(2) In Corollary 3.13, fix $d = t$, put $h = m$ and $h = m-1$ respectively, we have $T^m = \bigcup_{\mathrm{ord}(c)|t} T_c^m = H_{k^m t} \setminus H_{k^{m-1}t}$. So $|T^m| = (n, k^m t) - (n, k^{m-1}t)$. Since $|T_c^m| = \frac{1}{t}|T^m|$, we get the other formula.

(3) By Lemma 2.1, the number of vertices in T_c^m with non-zero indegree is $\frac{|T_c^{m+1}|}{(k,n)}$. □

Hence, if the unique cycle in a component of $G(n, k)$ has length r, then this component has rw vertices.

Corollary 3.16. $|T^{h_0}| \geq \frac{n}{2}$.

Proof. Recall that h_0 is the height of the trees.

If $h_0 = 0$, then all vertices are in cycles, so $|T^{h_0}| = n \geq \frac{n}{2}$.

If $h_0 \geq 1$, From Proposition 3.15 (2), we have $|T^{h_0}| = n - (n, k^{h_0-1}t) = n - t(w, k^{h_0-1})$. Since $n \nmid k^{h_0-1}t$, $w \nmid k^{h_0-1}$, which implies $(w, k^{h_0-1}) \leq \frac{w}{2}$. Hence, we have $|T^{h_0}| \geq \frac{n}{2}$. □

In fact, the lower bound in the above corollary is the best one. For example, let $k = 6$ and $n = 2^m$, where $m \geq 3$, then $t = 1$ and $h_0 = m$, so $|T^{h_0}| = n - (n, k^{h_0-1}t) = \frac{n}{2}$.

Proposition 3.17. *If $n \geq 5$ and n is even, then the length of the longest cycle in $G(n,k)$ is less than or equal to $\frac{n-2}{2}$.*

Proof. If $(n,k) \neq 1$, then $h_0 \geq 1$. By the above corollary, the number of non-cycle vertices is more than or equal to $\frac{n}{2}$, which implies the number of cycle vertices is less than or equal to $\frac{n}{2}$. Since the identity element of H is in a loop, the length of the longest cycle in $G(n,k)$ is less than or equal to $\frac{n}{2} - 1 = \frac{n-2}{2}$.

If $(n,k) = 1$, then all vertices are in cycles and $t = n$. Notice that the length of the longest cycle is $\ell(t) = \ell(n) = \mathrm{ord}_n k$. We factor n as $2^r s$, where $r \geq 1$ and $(2,s) = 1$. If $s \neq 1$, then $\ell(n) \leq \varphi(n) = 2^{r-1}\varphi(s) < 2^{r-1}s = \frac{n}{2}$. Since $\ell(n)$ is an integer, $\ell(n) \leq \frac{n}{2} - 1 = \frac{n-2}{2}$. If $s = 1$, that is $n = 2^r$, since $n \geq 5$, $r > 2$, which implies $(\mathbb{Z}/n\mathbb{Z})^*$ has no primitive roots, so $\ell(n) < \varphi(n) = 2^{r-1} = \frac{n}{2}$, then $\ell(n) \leq \frac{n-2}{2}$. □

Hence, the number of vertices in the largest component is less than or equal to $\frac{n-2}{2}w$. In fact, the upper bound in the above proposition is the best one. For example, let $k = 2$ and $n = 2p$, p is an odd prime, and 2 is the primitive root of $(\mathbb{Z}/p\mathbb{Z})^*$, then $t = p$ and $\ell(t) = \mathrm{ord}_p 2 = p - 1 = \frac{n-2}{2}$.

4. The adjacency matrix of $G(n,k)$

For any two vertices u and v of $G(n,k)$, if $u^k = v$, we call u a child of v.

If the vertex-set of $G(n,k)$ is $\{v_1, v_2, \cdots, v_n\}$, then the adjacency matrix of $G(n,k)$ is a $n \times n$ $(0,1)$-matrix with the (i,j)-entry equal to the number of directed edges from v_i to v_j, we denote it by $A(n,k)$.

We label the vertices of $G(n,k)$ as follows. First, we label the vertices component by component, so we can get a block diagonal matrix. Second, for each component, we label its vertices height by height according to the child relations. For example, see Fig. 2 in [12], let $H = (\mathbb{Z}/29\mathbb{Z})^*$ and $k = 2$, then there are three components, see Figure 1.

We label $G(28,2)$ by $v_1 = 1, v_2 = 28, v_3 = 12, v_4 = 17, v_5 = 7, v_6 = 20, v_7 = 23, v_8 = 6, v_9 = 22, v_{10} = 9, v_{11} = 8, v_{12} = 21, v_{13} = 14, v_{14} = 15, v_{15} = 3, v_{16} = 26, v_{17} = 16, v_{18} = 24, v_{19} = 25, v_{20} = 4, v_{21} = 13, v_{22} = 5, v_{23} = 2, v_{24} = 27, v_{25} = 10, v_{26} = 19, v_{27} = 11$ and $v_{28} = 18$. Then digraph $G(28,2)$ is given in Figure 2.

If we partition $A(28,2)$ according to the components, then we can get a block diagonal matrix and the main diagonal blocks are square matrixes.

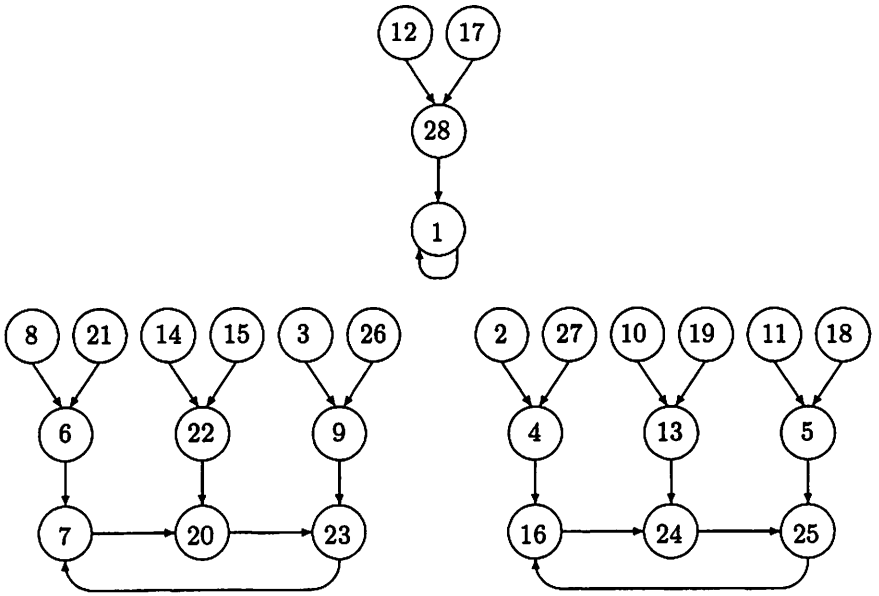

FIGURE 1. The digraph $G(28, 2)$

The main diagonal blocks are given as follows.

$$B_1 = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{cccc} v_1 & v_2 & v_3 & v_4 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \end{array}, \quad B_2 = \begin{array}{c} \\ v_5 \\ v_6 \\ v_7 \\ v_8 \\ v_9 \\ v_{10} \\ v_{11} \\ v_{12} \\ v_{13} \\ v_{14} \\ v_{15} \\ v_{16} \end{array} \begin{array}{c} \begin{array}{cccccccccccc} v_5 & v_6 & v_7 & v_8 & v_9 & v_{10} & v_{11} & v_{12} & v_{13} & v_{14} & v_{15} & v_{16} \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array},$$

$$B_3 = \begin{array}{c} \\ v_{17} \\ v_{18} \\ v_{19} \\ v_{20} \\ v_{21} \\ v_{22} \\ v_{23} \\ v_{24} \\ v_{25} \\ v_{26} \\ v_{27} \\ v_{28} \end{array} \begin{array}{c} \begin{array}{cccccccccccc} v_{17} & v_{18} & v_{19} & v_{20} & v_{21} & v_{22} & v_{23} & v_{24} & v_{25} & v_{26} & v_{27} & v_{28} \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array}.$$

Since B_2 and B_3 correspond to isomorphic components, $B_2 = B_3$. If we partition each main diagonal block according to the heights, then we can

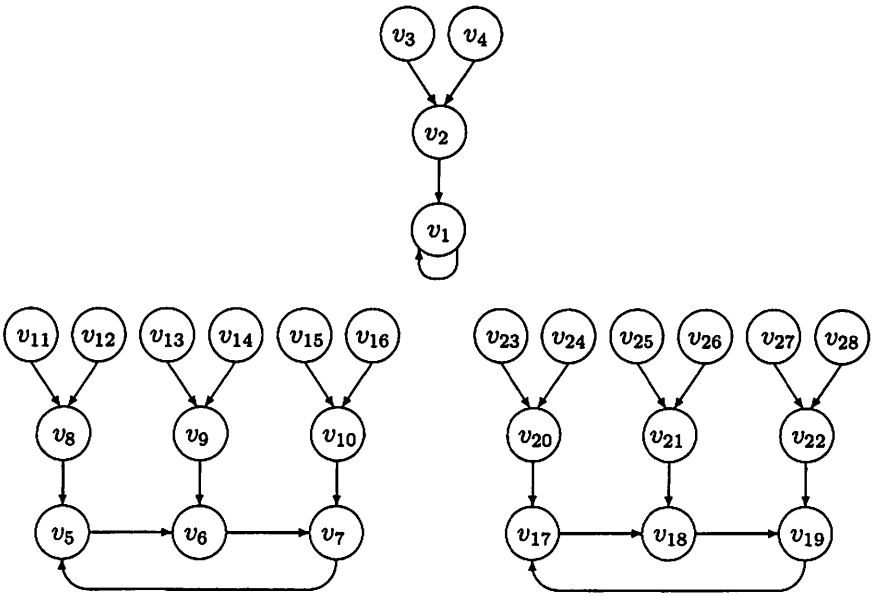

FIGURE 2. The digraph $G(28, 2)$

get a block lower triangular matrix and its main diagonal blocks are square matrixes, its main diagonal blocks are all equal to 0 except the $(1,1)$-block. After partitioning, B_1, B_2 and B_3 have the following form.

$$B_i = \begin{pmatrix} B_{i0} & 0 & 0 \\ B_{i1} & 0 & 0 \\ 0 & B_{i2} & 0 \end{pmatrix}, i = 1, 2, 3.$$

We denote the characteristic polynomial and minimal polynomial of a matrix A by $f_A(\lambda)$ and $m_A(\lambda)$ respectively. Notice that the characteristic polynomial and minimal polynomial of a $r \times r$ matrix with the following form

$$\begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 1 & & & 0 \end{pmatrix} \tag{4.1}$$

are both $\lambda^r - 1$. Hence, $f_{B_1}(\lambda) = \lambda^3(\lambda - 1)$ and $f_{B_2}(\lambda) = f_{B_3}(\lambda) = \lambda^9(\lambda^3 - 1)$.

Lemma 4.1. *If a partitioned matrix D has the following form*

$$D = \begin{pmatrix} D_0 & & & \\ D_1 & 0 & & \\ & \ddots & \ddots & \\ & & D_m & 0 \end{pmatrix},$$

where the main diagonal blocks are all square matrixes, D_0 is a $r \times r$ matrix with the form as (4.1), each D_i $(1 \leq i \leq m)$ is non-negative and its $(1,1)$-entry is positive. Then $m_D(\lambda) = \lambda^m(\lambda^r - 1)$.

Proof. It is obvious that $\lambda^r - 1 | m_D(\lambda)$ and the first row of the partitioned matrix $D^r - I$ is zero, where I is the identity matrix.

Since

$$D^m = \begin{pmatrix} D_0^m & 0 & \cdots & 0 \\ D_1 D_0^{m-1} & 0 & \cdots & 0 \\ D_2 D_1 D_0^{m-2} & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ D_m D_{m-1} \times \cdots \times D_1 & 0 & \cdots & 0 \end{pmatrix},$$

$D^m(D^r - I) = 0$.

Since

$$D^{m-1} = \begin{pmatrix} D_0^{m-1} & 0 & \cdots & 0 \\ D_1 D_0^{m-2} & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ D_{m-2} D_{m-3} \times \cdots \times D_0 & 0 & \cdots & 0 \\ D_{m-1} D_{m-2} \times \cdots \times D_1 & 0 & \cdots & 0 \\ 0 & D_m D_{m-1} \times \cdots \times D_2 & \cdots & 0 \end{pmatrix},$$

the $(m+1,1)$-entry of the partitioned matrix $D^{m-1}(D^r - I)$ is $D_m D_{m-1} \times \cdots \times D_2 \times D_1 D_0^{r-1}$. Since D_0^{r-1} is invertible and non-negative, there exists a positive entry in the first row of D_0^{r-1}. Notice that $D_m D_{m-1} \times \cdots \times D_2 D_1$ is non-negative and its $(1,1)$-entry is positive. Hence, $D_m D_{m-1} \times \cdots \times D_2 \times D_1 D_0^{r-1} \neq 0$. So $D^{m-1}(D^r - I) \neq 0$.

Hence, we have $m_D(\lambda) = \lambda^m(\lambda^r - 1)$. □

So by Lemma 4.1, $m_{B_1}(\lambda) = \lambda^2(\lambda - 1)$ and $m_{B_2}(\lambda) = m_{B_3}(\lambda) = \lambda^2(\lambda^3 - 1)$.

Recall that h_0 is the height of the trees. Let C be a component of $G(n,k)$ and the unique cycle in C has length r, then C has rw vertices, the characteristic polynomial and minimal polynomial of C is $\lambda^{rw-r}(\lambda^r - 1)$ and $\lambda^{h_0}(\lambda^r - 1)$ respectively.

Suppose the components of $G(n,k)$ consist of m_1 copies of G_1, m_2 copies of $G_2, \cdots$, m_s copies of G_s, where $G_1, G_2, \cdots, G_s$ are pairwise non-isomorphic, the unique cycle in each G_i $(1 \le i \le s)$ has length r_i. Then we get the following theorem.

Theorem 4.2. (1) *The characteristic polynomial of* $G(n,k)$ *is* $\prod_{i=1}^{s} [\lambda^{r_i w - r_i}(\lambda^{r_i} - 1)]^{m_i}$.

(2) *The minimal polynomial of* $G(n,k)$ *is* $\lambda^{h_0}(\lambda^{\ell(t)} - 1)$.

Proof. The result in (1) is obvious.

By Proposition 2.4 and Proposition 2.7 (1), the length of each cycle divides $\ell(t)$, this yields the result in (2). □

By the discussions in section 2 and section 3, if we specify the values of n and k, we can calculate explicitly these data $s, t, w, h_0, \ell(t), m_i$ and r_i $(1 \le i \le s)$.

Since we have determined the characteristic polynomial of $G(n,k)$, it is easy to get the eigenvalues and spectrum of $G(n,k)$.

5. The Automorphism Group of $G(n,k)$

For any graph G, we denote its automorphism group by $\mathrm{Aut}(G)$. For simplicity, we denote the automorphism group of $G(n,k)$ by $\mathrm{Aut}(n,k)$. Notice that $\mathrm{Aut}(G)$ is a permutation group on $\{1, 2, \cdots, |G|\}$.

Let S_m be the symmetric group on $\{1, 2, \cdots, m\}$. Let P_1 and P_2 be two permutation groups on $\{1, 2, \cdots, m\}$ and $\{1, 2, \cdots, r\}$ respectively. Recall that the wreath product $P_1 \wr P_2$ is generated by the direct product of r copies of P_1, together with the elements of P_2 acting on these r copies of P_1.

Using the notations in the above section, we get the following theorem.

Theorem 5.1. $\mathrm{Aut}(n,k) \cong (\mathrm{Aut}(G_1) \wr S_{m_1}) \times (\mathrm{Aut}(G_2) \wr S_{m_2}) \times \cdots \times (\mathrm{Aut}(G_s) \wr S_{m_s})$.

Proof. See Theorem 1.1 in [3]. □

For each component G_i $(1 \le i \le s)$, its unique cycle has length r_i, by Corollary 3.4, we have the following proposition.

Proposition 5.2. *For each* $1 \le i \le s$, $\mathrm{Aut}(G_i) \cong \mathrm{Aut}(T_1) \wr < \sigma_i >$, *where* σ_i *is a* r_i*-cycle,*

$$\sigma_i = \begin{pmatrix} 1 & 2 & 3 & \cdots & r_i \\ 2 & 3 & 4 & \cdots & 1 \end{pmatrix}.$$

Proof. Notice that the automorphism group of the cycle in G_i is exactly the permutation group generated by σ_i. □

Hence, we only need to determine $\mathrm{Aut}(T_1)$. If $(n,k)=1$, by Proposition 2.11, we have $\mathrm{Aut}(T_1)=\{1\}$. Then we get the following proposition.

Proposition 5.3. *If* $(n,k)=1$, *then* $\mathrm{Aut}(n,k)=(<\sigma_1>\wr S_{m_1})\times(<\sigma_2>\wr S_{m_2})\times\cdots\times(<\sigma_s>\wr S_{m_s})$.

Proposition 5.4. *If* $k=1$, *then* $\mathrm{Aut}(n,k)=S_n$.

Proposition 5.5. *If* $k=n$, *then* $\mathrm{Aut}(n,k)=S_{n-1}$.

But in general it is difficult to determine $\mathrm{Aut}(T_1)$. Since the vertices with the same height may have different number of children. For example, let $H=(\mathbb{Z}/41\mathbb{Z})^*$ and $k=4$, T_1 is given as follows.

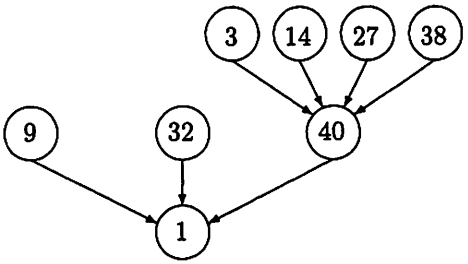

FIGURE 3. The tree T_1 for $n=40$ and $k=4$

Recall that if h_0 is the height of T_1, then the vertices of T_1 form the subgroup $H_{k^{h_0}}$, that is H_w. So $\mathrm{Aut}(H_w)\subseteq\mathrm{Aut}(T_1)$.

As follows we want to determine $\mathrm{Aut}(T_1)$ when k is a prime.

For any two vertices a and b, if there is a $g\in\mathrm{Aut}(n,k)$ such that $g(a)=b$, we say a is isomorphic to b, denote it by $a\cong b$. This is an equivalent relation in $G(n,k)$. We will show that if $\mathrm{ord}(a)=\mathrm{ord}(b)$, then $a\cong b$.

Suppose that M is a cyclic group with m elements. Given three positive integers r, r_1 and q such that $r|r_1|m$ and $r_1=rq$. For any $b\in M,\mathrm{ord}(b)=r$, put $M_b=\{a\in M|a^q=b,\mathrm{ord}(a)=r_1\}$. Then we have the following lemma.

Lemma 5.6. *For any* $b\in M$ *with* $\mathrm{ord}(b)=r$, $|M_b|=\frac{\varphi(r_1)}{\varphi(r)}$.

Proof. Fix a generator ζ of M such that $\zeta^{\frac{m}{r}}=b$. It is easy to see that $\zeta^{\frac{m}{r_1}}\in M_b$. So M_b is not empty.

Every element with order r_1 has a unique form $\zeta^{\frac{ml_1}{r_1}}, 1\le l_1\le r_1,(l_1,r_1)=1$. Then we have

$$\zeta^{(\frac{ml_1}{r_1})q}=b\Leftrightarrow m|(\frac{ml_1}{r}-\frac{m}{r})\Leftrightarrow r|l_1-1.$$

So $|M_b| = |\{l_1 | 1 \leq l_1 \leq r_1, (l_1, r_1) = 1, r | l_1 - 1\}|$, which implies that $|M_b|$ only depends on r and r_1 and it is independent of the specified value of b. Hence, given another $b' \in M, \text{ord}(b') = r$, we have $|M_{b'}| = |M_b|$.

Since there are $\varphi(r_1)$ elements with order r_1 and $\varphi(r)$ elements with order r, $|M_b| = \frac{\varphi(r_1)}{\varphi(r)}$. □

Corollary 5.7. *For any two elements $a, b \in M$, $\text{ord}(a) = \text{ord}(b), q \geq 1$, then for each positive integer r such that $\text{ord}(a) | r$, $M_1 = \{x | x^q = a\}$ and $M_2 = \{x | x^q = b\}$ have the same number of elements with order r.*

Proof. By Lemma 2.1, M_1 and M_2 have the same number of elements. Then we can get the desired result by applying Lemma 5.6. □

Theorem 5.8. *For any $a, b \in G(n, k)$, if $\text{ord}(a) = \text{ord}(b)$, then $a \cong b$.*

Proof. By Corollary 3.8, a and b are at the same height. Since for any positive integer h, $\text{ord}(a^h) = \text{ord}(b^h)$, then the cycles which they lead to have the same order. Then the desired result follows from Corollary 5.7. □

From now on we assume that k is a prime.

For any $a \in T_1$, there exists a h such that $a^{k^h} = 1$, which implies that $\text{ord}(a) | k^h$. So $w_a = \text{ord}(a)$. By Corollary 3.10, we get the following proposition.

Proposition 5.9. *If k is a prime, for any $a, b \in T_1$, a and b are at the same height if and only if $\text{ord}(a) = \text{ord}(b)$.*

Hence, all the vertices with indegree 0 of T_1 are at the largest height h_0.

Since k is a prime, $(n, k) = 1$ or k. We have discussed $\text{Aut}(n, k)$ on the case $(n, k) = 1$, see Proposition 5.3.

As follows we suppose that $(n, k) = k$. Then the largest height $h_0 \geq 1$. For $1 \leq h \leq h_0$, let T_{1h} be the tree originating from a vertex with height h in T_1. In particular, the vertex set of T_{1h_0} contains only one point. Proposition 5.9 and Theorem 5.8 tell us that T_{1h} is well-defined. Then we get the following proposition.

Proposition 5.10. *If k is a prime and $(n, k) = k$, then we have $\text{Aut}(T_1) \cong \text{Aut}(T_{11}) \wr S_{k-1}$, for any $1 \leq h < h_0$, $\text{Aut}(T_{1h}) = \text{Aut}(T_{1,h+1}) \wr S_k$, and $\text{Aut}(T_{1h_0}) = \{1\}$.*

6. Further Problems

We mention three further problems which may worth studying.

First, it may be interesting to consider other graphic problems for $G(n, k)$, such as the matching problem and the coloring problem.

Second, it may be interesting to study the asymptotic mean numbers of cycle vertices and cycles. [4], [8] and [12] will be helpful.

Third, what will happen if H is not cyclic? [1], [9], [10], [11] and [13] will be helpful.

7. Acknowledgment

We would like to thank Dr. Jingfen Lan for her valuable suggestions. We also thank the referee for the careful review and the valuable comments.

References

[1] E.L. Blanton Jr., S.P. Hurd, J.S. McCranie, On a digraph defined by squaring modulo n, Fibonacci Quart. 30 (1992) 322-333.

[2] E. Brown, Directed Graphs Defined by Arithmetic (mod n), Fibonacci Quart. 35 (1997) 346-351.

[3] P.J. Cameron, Automorphisms of graphs, Topics in Algebraic Graph Theory (eds. L.W. Beineke and R.J. Wilson), Cambridge Press, UK, 2004, 137-155.

[4] W.-S. Chou and I.E. Shparlinski, On the Cycle Structure of Repeated Exponentiation Modulo a Prime, J. Number Theory, 107 (2004) 345-356.

[5] K. Ireland, M. Rosen, A Classical Introduction to Mordern Number Theory, Second Edition, GTM84, Springer, New York, 2002.

[6] C. Lucheta, E. Miller, C. Reiter, Digraphs from powers modulo p, Fibonacci Quart. 34 (1996) 226-239.

[7] T.D. Rogers, The graph of the square mapping on the prime fields, Discrete Math. 148 (1996) 317-324.

[8] M. Sha, S. Hu, Monomial dynamical systems of dimension one over finite fields, Acta Arith.148 (2011) 309-331.

[9] L. Somer, M. Křížek, Structure of digraphs associated with quadratic congruences with composite moduli, Discrete Math. 306 (2006) 2174-2185.

[10] L. Somer, M. Křížek, On semiregular digraphs of the congruence $x^k \equiv y$ (mod n), Comment. Math. Univ. Carolin. 48 (2007) 41-58.

[11] L. Somer, M. Křížek, On symmetric digraphs of the congruence $x^k \equiv y$ (mod n), Discrete Math. 309 (2009) 1999-2009.

[12] T. Vasiga, J. Shallit, On the iteration of certain quadratic maps over $GF(p)$, Discrete Math. 277 (2004) 219-240.

[13] B. Wilson, Power digraphs modulo n, Fibonacci Quart. 36 (1998) 229-239.

Institut de Mathematiques de Bordeaux, Universite Bordeaux 1, 351, cours de la Liberation, 33405 Talence Cedex, France

E-mail address: shamin2010@gmail.com