Czechoslovak Mathematical Journal

Lawrence Somer; Michal Křížek
The structure of digraphs associated with the congruence $x^k \equiv y \pmod n$

Czechoslovak Mathematical Journal, Vol. 61 (2011), No. 2, 337–358

Persistent URL: http://dml.cz/dmlcz/141538

Czechoslovak Mathematical Journal, 61 (136) (2011), 337–358

THE STRUCTURE OF DIGRAPHS ASSOCIATED WITH THE CONGRUENCE $x^k \equiv y \pmod{n}$

Lawrence Somer, Washington, Michal Křížek, Praha

(Received December 3, 2009)

Abstract. We assign to each pair of positive integers n and $k \geqslant 2$ a digraph $G(n,k)$ whose set of vertices is $H = \{0, 1, \ldots, n-1\}$ and for which there is a directed edge from $a \in H$ to $b \in H$ if $a^k \equiv b \pmod{n}$. We investigate the structure of $G(n,k)$. In particular, upper bounds are given for the longest cycle in $G(n,k)$. We find subdigraphs of $G(n,k)$, called fundamental constituents of $G(n,k)$, for which all trees attached to cycle vertices are isomorphic.

Keywords: Sophie Germain primes, Fermat primes, primitive roots, Chinese Remainder Theorem, congruence, digraphs

MSC 2010: 11A07, 11A15, 05C20, 20K01

1. Introduction

In this paper, we construct a digraph associated with the congruence $x^k \equiv y \pmod{n}$. We will see that each component of this digraph contains a unique cycle. Our main result given in Theorem 6.1 is to partition this digraph into sets of components, called fundamental constituents, so that all trees attached to cycle vertices of a particular fundamental constituent of the digraph are isomorphic. In Theorem 9.2 we obtain new results on the length of the longest cycle in this digraph extending the results given in [7]. In Theorem 8.1, we obtain lower bounds for the number of cycles of length one, while in Theorem 8.2, we count the number of isolated cycles of length one. A major technique used in this paper is to decompose a digraph into a product of digraphs.

This paper was supported by Institutional Research Plan nr. AV0Z 10190503 and Grant nr. IAA 100190803 of the Academy of Sciences of the Czech Republic.

The paper extends results given in the works [7], [10], [14], and [16], which provide an interesting connection between number theory, graph theory, and group theory. In the papers [10]–[13], we investigated properties of the iteration digraph representing a dynamical system occurring in number theory. For related results also see [1].

For $n \geqslant 1$ let

$$H = \{0, 1, \ldots, n-1\}$$

and let f be a map of H into itself. The *iteration digraph* of f is a directed graph whose vertices are elements of H and such that there exists exactly one directed edge from x to $f(x)$ for all $x \in H$. For a fixed integer $k \geqslant 2$ and for each $x \in H$ let $f(x)$ be the remainder of x^k modulo n, i.e.,

$$f(x) \in H \quad \text{and} \quad x^k \equiv f(x) \pmod{n}. \tag{1.1}$$

From here on, whenever we refer to the iteration digraph of f, we assume that the mapping f is as given in (1.1). Each pair of natural numbers n and $k \geqslant 2$ has a specific iteration digraph corresponding to it.

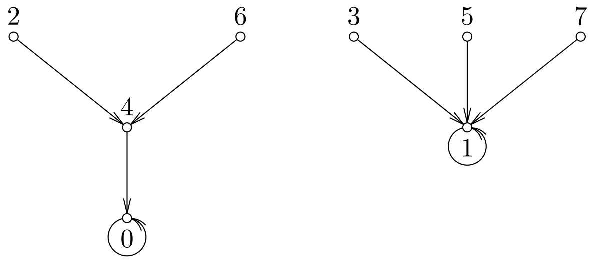

Figure 1. The iteration digraph $G(8, 2)$.

We identify the vertex a of H with its residue modulo n. We will also sometimes identify the vertex 0 with the integer n. For brevity we will make statements such as $\gcd(a, n) = 1$, treating the vertex a as a number. Moreover, when we refer, for instance, to the vertex a^k, we identify it with the remainder $f(a) \in H$ given by (1.1). For particular values of n and k, we denote the iteration digraph of f by $G(n, k)$, see Figures 1–3.

Let $\omega(n)$ denote the number of distinct primes dividing $n \geqslant 2$ and let the prime power factorization of n be given by

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}, \tag{1.2}$$

where $p_1 < p_2 < \ldots < p_r$ are primes and $\alpha_i > 0$, i.e., $r = \omega(n)$. For $n = 1$, we set $\omega(1) = 0$.

A *component* of the iteration digraph is a subdigraph which is a maximal connected subdigraph of the associated nondirected graph.

The *indegree* of a vertex $a \in H$ of $G(n,k)$, denoted by $\operatorname{indeg}_n(a)$, is the number of directed edges coming into a, and the *outdegree* of a is the number of directed edges leaving the vertex a. We will frequently simply write $\operatorname{indeg}(a)$ when it is understood that a is a vertex in $G(n,k)$. By the definition of f, the outdegree of each vertex of $G(n,k)$ is equal to 1. It is obvious that $G(n,k)$ with n vertices also has exactly n directed edges. Thus, if b_i, $i = 1, 2, \ldots, q$, denote the indegrees of all the vertices of $G(n,k)$ having positive indegree, then

$$\sum_{i=1}^{q} b_i = n.$$

It is clear that each component has exactly one cycle, since each vertex of the component has outdegree 1 and the component has only a finite number of vertices. It is also evident that cycle vertices have positive indegree. Cycles of length 1 are called *fixed points*.

Note that 0 and 1 are always fixed points of $G(n,k)$. Cycles of length t are called *t-cycles*. Let $A_t(G(n,k))$ denote the number of t-cycles in $G(n,k)$. Attached to each cycle vertex c of $G(n,k)$ is a tree $T(c)$ whose root is c and whose additional vertices are the noncycle vertices b for which $b^{k^i} \equiv c \pmod{n}$ for some $i \in \mathbb{N} = \{1, 2, \ldots\}$, but $b^{k^{i-1}}$ is not congruent to a cycle vertex modulo n. Let $J(n,k)$ be a component in $G(n,k)$ and let c be a cycle vertex in $J(n,k)$. It is evident that b is a vertex in $J(n,k)$ if and only if $b^{k^h} \equiv c \pmod{n}$ for some positive integer h. The *height* of a vertex b in $G(n,k)$ is the least nonnegative integer i such that b^{k^i} is congruent modulo n to a cycle vertex in $G(n,k)$. Note that cycle vertices have height equal to 0.

Further, we specify two particular subdigraphs of $G(n,k)$. Let $G_1(n,k)$ be the induced subdigraph of $G(n,k)$ on the set of vertices which are coprime to n and $G_2(n,k)$ the induced subdigraph on the remaining vertices not coprime with n. If $n > 1$ we observe that $G_1(n,k)$ and $G_2(n,k)$ are disjoint, nonempty, and that $G(n,k) = G_1(n,k) \cup G_2(n,k)$, that is, no edge goes between $G_1(n,k)$ and $G_2(n,k)$. Since $\gcd(a,n) = 1$ if and only if $\gcd(a^k, n) = 1$, it follows that both $G_1(n,k)$ and $G_2(n,k)$ are unions of components of $G(n,k)$. For example, the second component of Figure 2 is $G_1(12,2)$ whereas the remaining three components make up $G_2(12,2)$.

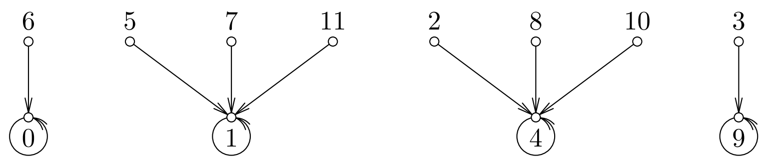

Figure 2. The iteration digraph $G(12,2)$.

It is clear that 0 is always a fixed point of $G_2(n,k)$. If $n > 1$, then 1 and $n-1$ are always vertices of $G_1(n,k)$. In Theorem 7.1, we show that if $G_2(n,k)$ contains a t-cycle, then $G_1(n,k)$ also contains a t-cycle. Theorem 7.6 determines the height of a vertex in $G_2(n,k)$.

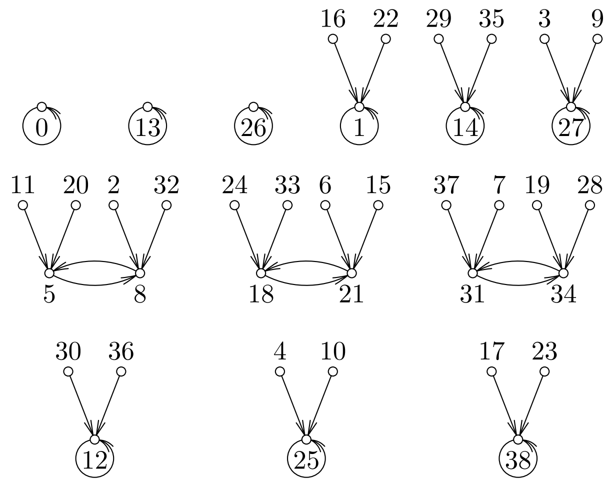

Figure 3. The iteration digraph $G(39,3)$.

Let $N(n,k,a)$ denote the number of incongruent solutions of the congruence

$$x^k \equiv a \pmod{n}.$$

Then obviously

$$N(n,k,a) = \operatorname{indeg}_n(a). \tag{1.3}$$

It follows from (1.3) and Theorem 2.20 in [9] that if n has the factorization given in (1.2), then

$$\operatorname{indeg}_n(a) = N(n,k,a) = \prod_{i=1}^{r} N(p_i^{\alpha_i},k,a) = \prod_{i=1}^{r} \operatorname{indeg}_{q_i}(a), \tag{1.4}$$

where $q_i = p_i^{\alpha_i}$.

2. Properties of the Carmichael lambda-function

Before proceeding further, we need to review some properties of the Carmichael lambda-function $\lambda(n)$. Its definition is a modification of the definition of the Euler totient function $\phi(n)$.

Definition 2.1. Let n be a positive integer. Then the *Carmichael lambda-function* $\lambda(n)$ is defined as follows (see [5, p. 21]):

$$\begin{aligned}
\lambda(1) &= 1 = \phi(1),\\
\lambda(2) &= 1 = \phi(2),\\
\lambda(4) &= 2 = \phi(4),\\
\lambda(2^k) &= 2^{k-2} = \tfrac{1}{2}\phi(2^k) \quad \text{for } k \geqslant 3,\\
\lambda(p^k) &= (p-1)p^{k-1} = \phi(p^k) \quad \text{for any odd prime } p \text{ and } k \geqslant 1,\\
\lambda(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}) &= \operatorname{lcm}[\lambda(p_1^{k_1}), \lambda(p_2^{k_2}), \dots, \lambda(p_r^{k_r})],
\end{aligned}$$

where $p_1, p_2, \dots, p_r$ are distinct primes and $k_i \geqslant 1$ for all $i \in \{1, \dots, r\}$.

It immediately follows from Definition 2.1 that

$$\lambda(n) \mid \phi(n)$$

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

The following theorem generalizes the well-known Euler's theorem which says (see [5, p. 20]) that $a^{\phi(n)} \equiv 1 \pmod n$ if and only if $\gcd(a, n) = 1$. It shows that $\lambda(n)$ is the smallest possible universal order modulo n.

Theorem 2.2 (Carmichael)**.** *Let* $a, n \in \mathbb{N}$. *Then*

$$a^{\lambda(n)} \equiv 1 \pmod n$$

if and only if $\gcd(a, n) = 1$. *Moreover, there exists an integer* g *such that*

$$\operatorname{ord}_n g = \lambda(n),$$

where $\operatorname{ord}_n g$ *denotes the multiplicative order of* g *modulo* n.

Proof. For a proof, see [5, p. 21]. □

3. Results on the indegree

We will need the following results concerning the indegrees of certain vertices in $G_1(n, k)$ and $G_2(n, k)$ in order to prove our main results.

Lemma 3.1. *Let n have the factorization given in* (1.2) *and let a be a vertex of positive indegree in $G_1(n,k)$. Then*

$$\operatorname{indeg}(a) = N(n,k,a) = \prod_{i=1}^{r} \varepsilon_i \gcd(\lambda(p_i^{\alpha_i}), k),$$

where $\varepsilon_i = 2$ if $2 \mid k$ and $8 \mid p_i^{\alpha_i}$, and $\varepsilon_i = 1$ otherwise.

P r o o f. This is proved in [16, pp. 231–232]. □

Lemma 3.2. *Let p be a prime and let $\alpha \geqslant 1$ and $k \geqslant 2$ be integers. Then*

$$N(p^\alpha, k, 0) = p^{\alpha - \lceil \alpha/k \rceil}.$$

P r o o f. This follows from the fact that $a^k \equiv 0 \pmod{p^\alpha}$ if and only if $p^{\lceil \alpha/k \rceil} | a$. □

4. Digraph product

Let $n = n_1 n_2$, where $\gcd(n_1, n_2) = 1$. We show that we can represent $G(n,k)$ as a product of the two digraphs $G(n_1,k)$ and $G(n_2,k)$. By the Chinese Remainder Theorem, we can uniquely represent each vertex $a \in G(n,k)$ as the ordered pair (a_1, a_2), where $0 \leqslant a_1 \leqslant n_1 - 1$, $0 \leqslant a_2 \leqslant n_2 - 1$, $a \equiv a_1 \pmod{n_1}$, and $a \equiv a_2 \pmod{n_2}$. For $a = (a_1, a_2)$ define

$$a^k = (a_1, a_2)^k = (a_1^k, a_2^k), \tag{4.1}$$

where we assume that a^k, a_1^k, and a_2^k are all reduced modulo n, n_1 and n_2, respectively.

Let $G(n_1,k) \times G(n_2,k)$ denote the digraph whose vertices are the ordered pairs (a_1, a_2), where $0 \leqslant a_1 \leqslant n_1 - 1$ and $0 \leqslant a_2 \leqslant n_2 - 1$. In addition, $\langle (a_1, b_1), (a_2, b_2) \rangle$ is a directed edge of $G(n_1,k) \times G(n_2,k)$ if and only if $a_2 \equiv a_1^k \pmod{n_1}$ and $b_2 \equiv b_1^k \pmod{n_2}$ (see [4]).

From (4.1) it follows that $G(n,k)$ is isomorphic to $G(n_1,k) \times G(n_2,k)$, i.e.,

$$G(n,k) \cong G(n_1,k) \times G(n_2,k)$$

and for simplicity we shall write further on

$$G(n,k) = G(n_1,k) \times G(n_2,k). \tag{4.2}$$

If n has the factorization given in (1.2), it follows from (4.2) that

$$G(n,k) = G(p_1^{\alpha_1},k) \times G(p_2^{\alpha_2},k) \times \ldots \times G(p_r^{\alpha_r},k).$$

5. Results on cycles and components

Consider a digraph $G(n,k)$ and let

$$\lambda(n) = lw, \tag{5.1}$$

where l is the largest divisor of $\lambda(n)$ relatively prime to k. We will need the following theorems and lemmas to prove some of our major results.

Lemma 5.1. *There exists a t-cycle in $G_1(n,k)$ if and only if*

$$t = \operatorname{ord}_d k$$

for some factor d of l. Moreover, $\operatorname{ord}_l k$ is the length of the longest cycle in $G_1(n,k)$.

Proof. Both statements are proved in [16, pp. 232–233]. □

Corollary 5.2. *Every cycle in $G_1(n,k)$ is a fixed point if and only if $k \equiv 1 \pmod{l}$, where l is defined as in (5.1).*

Lemma 5.3. *Let c_1 and c_2 be any two cycle vertices in $G_1(n,k)$ and let $T(c_1)$ and $T(c_2)$ be the trees attached to c_1 and c_2, respectively. Then $T(c_1) \cong T(c_2)$.*

Proof. This is proved in [16, p. 234]. □

Corollary 5.4. *Let $t \geqslant 1$ be a fixed integer. Then any two components in $G_1(n,k)$ containing t-cycles are isomorphic.*

Lemma 5.5. *The vertex c is a cycle vertex in $G_1(n,k)$ if and only if $\operatorname{ord}_n c \mid l$, where l is defined as in (5.1). Moreover, any two vertices in the same cycle of $G_1(n,k)$ have the same order modulo n.*

Proof. These assertions are proved in [16, pp. 232–233]. □

By virtue of Lemma 5.5, we define the order of a cycle in $G_1(n,k)$ to be the order of any vertex in the cycle.

Lemma 5.6. *Let n have the factorization given in* (1.2) *and let t be a positive integer. Then*

$$A_t(G_1(n,k)) = \frac{1}{t}\Bigl[\prod_{i=1}^{r}\delta_i \gcd(\lambda(p_i^{\alpha_i}), k^t-1) - \sum_{\substack{d\mid t\\ d\neq t}} dA_d(G_1(n,k))\Bigr] \tag{5.2}$$

and

$$A_t(G(n,k)) = \frac{1}{t}\Bigl[\prod_{i=1}^{r}(\delta_i \gcd(\lambda(p_i^{\alpha_i}), k^t-1)+1) - \sum_{\substack{d\mid t\\ d\neq t}} dA_d(G(n,k))\Bigr], \tag{5.3}$$

where $\delta_i = 2$ if $2 \mid k^t-1$ and $8 \mid p_i^{\alpha_i}$, and $\delta_i = 1$ otherwise.

P r o o f. Both (5.2) and (5.3) are proved in [13]. □

Lemma 5.7. *If b is a noncycle vertex in $G_1(n,k)$ and c is a cycle vertex in $G_1(n,k)$, then bc is a noncycle vertex in $G_1(n,k)$.*

P r o o f. This is proved in [16, p. 234]. □

Lemma 5.8. *Let $c=(c_1,c_2)$ be a vertex in $G(n,k)=G(n_1,k)\times G(n_2,k)$, where $n=n_1n_2$ and $\gcd(n_1,n_2)=1$. Then c is a cycle vertex in $G(n,k)$ if and only if c_i is a cycle vertex in $G(n_i,k)$ for $i=1,2$. Moreover, if $c=(c_1,c_2)$ is a vertex in a t-cycle of $G(n,k)$ and c_i is a vertex in a t_i-cycle of $G(n_i,k)$ for $i=1,2$, then $t=\operatorname{lcm}(t_1,t_2)$.*

P r o o f. These assertions are proved in [13]. □

Lemma 5.9. *Every vertex in $G_1(n,k)$ is a cycle vertex if and only if*

$$\gcd(\lambda(n),k)=1.$$

Moreover, every vertex in $G_1(n,k)$ is a fixed point if and only if $k\equiv 1 \pmod{\lambda(n)}$. Further, every vertex in $G(n,k)$ is a fixed point if and only if n is square-free and $k\equiv 1 \pmod{\lambda(n)}$.

P r o o f. The first assertion is proved in [16, p. 232]. The other assertions now follow from Corollary 5.2 and Lemma 5.6. □

Lemma 5.10. *Let $b\in G_1(n,k)$ and suppose that $\operatorname{ord}_n b = l'w'$, where $l' \mid l$ and $w' \mid w$ for l and w as defined in* (5.1)*. Then the height h of b is equal to the least nonnegative integer such that $w' \mid k^h$. Furthermore, the height of any tree attached to a cycle vertex in $G_1(n,k)$ is the least integer h_1 such that $w \mid k^{h_1}$.*

P r o o f. These statements are proved in [16, pp. 234–235]. □

Lemma 5.11. *Let $n = n_1 n_2$, where* $\gcd(n_1, n_2) = 1$. *Let $D(n_1, k)$ be a union of components of $G(n_1, k)$ and let $R(n_2, k)$ be a union of components of $G(n_2, k)$. Then $D(n_1, k) \times R(n_2, k)$ is a union of components of $G(n, k) = G(n_1, k) \times G(n_2, k)$. Moreover, if*

$$R(n_2, k) = \bigcup_{i=1}^{m} R_i(n_2, k),$$

where $R_i(n_2, k)$ are distinct components of $G(n_2, k)$ for $i = 1, 2, \ldots, m$, then

$$D(n_1, k) \times R(n_2, k) = \bigcup_{i=1}^{m} D(n_1, k) \times R_i(n_2, k), \tag{5.4}$$

where the union in (5.4) *is a disjoint union.*

P r o o f. These assertions are proved in [13]. □

As contrasted to the algebraic and elementary methods used in this paper to analyze the structure of $G(n, k)$, advanced analytic techniques have also been used in papers such as [2], [3], [6], [8], and [15] to obtain results related to the structure of $G(n, k)$.

In [2], the following result was proved concerning the average values of the number of cycle vertices and heights of vertices in $G_1(n, k)$, where p denotes a prime.

Theorem 5.12 (Chou and Shparlinski). *Let $T_0(p, k)$ denote the total number of cycle vertices in $G_1(p, k)$. Let $h_{p,k}(a)$ denote the height of the vertex a in $G_1(p, k)$. Let*

$$T(p, k) = \frac{1}{p-1} \sum_{a=1}^{p-1} h_{p,k}(a)$$

and let

$$S_0(k, N) = \frac{1}{\pi(N)} \sum_{p \leqslant N} T_0(p, k) \quad \text{and} \quad S(k, N) = \frac{1}{\pi(N)} \sum_{p \leqslant N} T(p, k),$$

where $\pi(N)$ denotes the number of primes not greater than N. Then for any integer $k \geqslant 2$, there are positive constants $C_1(k)$ and $C_2(k)$ such that the bounds

$$S_0 \sim C_1(k) N \quad \text{and} \quad S \sim C_2(k)$$

hold.

Theorem 5.12 generalizes Theorems 9 and 10 of [15] which treats only the case $k = 2$ and makes use of the Extended Riemann Hypothesis.

6. Subdigraphs for which all trees attached to cycle vertices are isomorphic

Let n have the factorization given by (1.2) and let $\mathcal{P}$ be the set of primes dividing n. Let $\mathcal{P}_1 \cup \mathcal{P}_2$ be a partition of the set $\mathcal{P}$ such that $\mathcal{P}_1 \cap \mathcal{P}_2 = \emptyset$. Let

$$m_1 = \prod_{p \in \mathcal{P}_1} p \quad \text{and} \quad m_2 = \prod_{p \in \mathcal{P}_2} p, \tag{6.1}$$

where $m_i = 1$ if $\mathcal{P}_i = \emptyset$. Let $G^*_{\mathcal{P}_i}(n,k)$, $i = 1, 2$, be the subdigraph of $G(n,k)$ induced by those vertices which are multiples of m_i and which are also relatively prime to m_j, where $j = 2/i$. Then $G^*_{\mathcal{P}_1}(n,k)$ and $G^*_{\mathcal{P}_2}(n,k)$ are called *fundamental constituents* of $G(n,k)$. The subdigraphs $G^*_{\mathcal{P}_1}(n,k)$ and $G^*_{\mathcal{P}_2}(n,k)$ were introduced by Wilson in [16].

Let $n = n_1 n_2$ have the factorization given in (1.2), where

$$n_1 = \prod_{p_i \in \mathcal{P}_1} p_i^{\alpha_i} \quad \text{and} \quad n_2 = \prod_{p_i \in \mathcal{P}_2} p_i^{\alpha_i}. \tag{6.2}$$

Let $L(n_2,k)$ denote the subdigraph of $G_2(n_2,k)$ induced by the vertices of $G_2(n_2,k)$ which are multiples of m_2. Note that the only cycle vertex in $L(n_2,k)$ is the fixed point 0. It is clear that $G^*_{\mathcal{P}_2}(n,k) \cong G_1(n_1,k) \times L(n_2,k)$ and thus, we shall write

$$G^*_{\mathcal{P}_2}(n,k) = G_1(n_1,k) \times L(n_2,k). \tag{6.3}$$

If $\mathcal{P}_1 = \emptyset$, then $n_2 = n$ and $G^*_{\mathcal{P}_2}(n,k) \cong L(n,k)$. If $\mathcal{P}_2 = \emptyset$, then $n_1 = n$ and $G^*_{\mathcal{P}_2}(n,k) \cong G_1(n,k)$. Let p be a prime. Since $p \mid a^k$ if and only if $p \mid a$, it follows that $L(n_2,k)$ is a single component of $G(n,k)$. It further follows from (6.3) and Lemma 5.11 that $G^*_{\mathcal{P}_1}(n,k)$ and $G^*_{\mathcal{P}_2}(n,k)$ are disjoint unions of components of $G(n,k)$. It is evident that $G_2(n,k)$ is a disjoint union of $G^*_{\mathcal{P}_2}(n,k)$ as $\mathcal{P}_2$ ranges over all nonempty subsets of $\mathcal{P}$.

Figure 4 shows the fundamental constituents of $G(56,2)$.

Let $J(n,k)$ be a component of $G(n,k)$ and let c be any cycle vertex in $G(n,k)$. Let $\mathcal{P}_2$ be the subset of primes in $\mathcal{P}$ which divide c. Since a is a vertex of $J(n,k)$ if and only if $a^{k^h} \equiv c \pmod{c}$ for some positive integer h it follows that $J(n,k)$ is a subdigraph of $G^*_{\mathcal{P}_2}(n,k)$.

The following theorem shows that all trees attached to cycle vertices in a fundamental constituent of $G(n,k)$ are isomorphic. Its proof generalizes the method of proof by Wilson of Theorem 4 in [16].

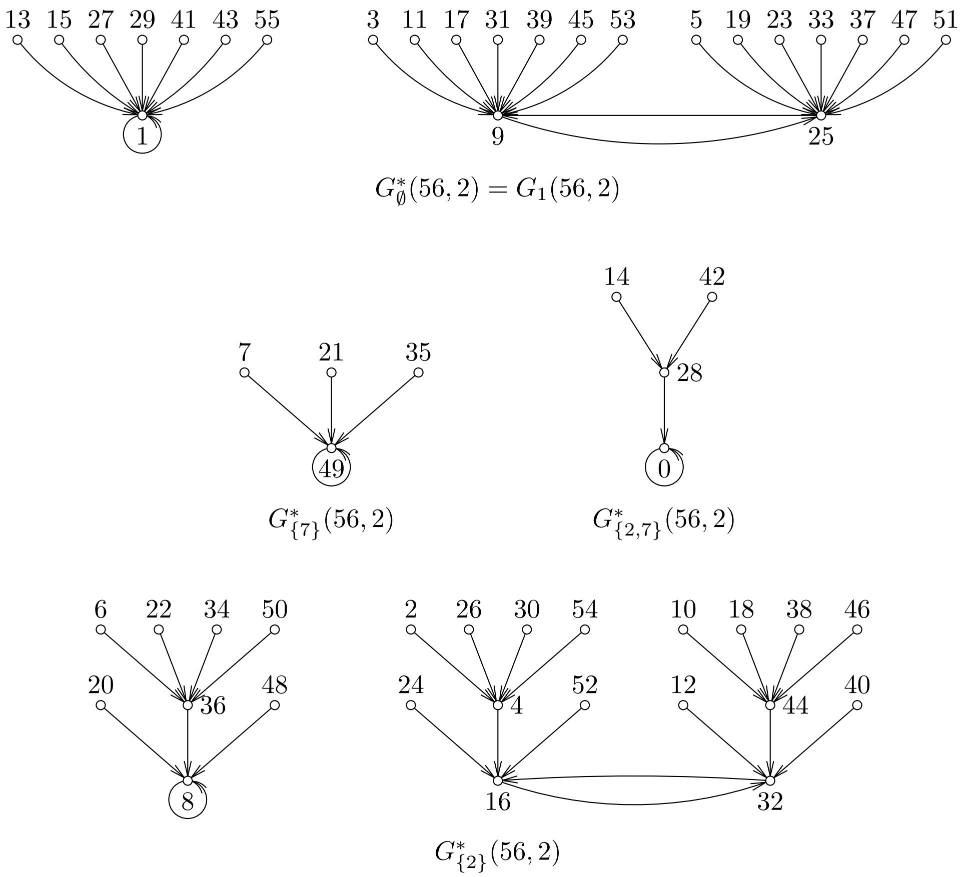

Figure 4. The four fundamental constituents of $G(56,2)$.

Theorem 6.1. *Let n have the factorization given in* (1.2) *and let $\mathcal{P}$ be the set of primes dividing n. Let a partition of $\mathcal{P}$ be given by $\mathcal{P}_1 \cup \mathcal{P}_2$ such that $\mathcal{P}_1 \cap \mathcal{P}_2 = \emptyset$. Let c_1 and c_2 be two cycle vertices in $G^*_{\mathcal{P}_2}(n,k)$ and let $T(c_1)$ and $T(c_2)$ be the trees attached to c_1 and c_2, respectively. Then $T(c_1) \cong T(c_2)$.*

Proof. If $\mathcal{P}_2 = \emptyset$, then $G^*_{\mathcal{P}_2}(n,k) = G_1(n,k)$, and the assertion follows from Lemma 5.3. Next suppose that $\mathcal{P}_2 = \mathcal{P}$. Then $n = n_2$, and $G^*_{\mathcal{P}_2}(n,k) = L(n,k)$. Since the only cycle vertex in $L(n,k)$ is the fixed point 0, there is only one tree in $G^*_{\mathcal{P}_2}(n,k)$, and the theorem holds trivially.

We now suppose that $\emptyset \neq \mathcal{P}_2 \neq \mathcal{P}$. Then

$$G^*_{\mathcal{P}_2}(n,k) = G_1(n_1,k) \times L(n_2,k),$$

where $n_1 > 1$ and $n_2 > 1$. By Lemma 5.8, we can write $c_1 = (d,0)$, where d is a cycle vertex in $G_1(n_1,k)$ and 0 is the unique cycle vertex in $L(n_2,k)$. In particular,

$(1,0)$ is a cycle vertex in $G_1(n_1,k)\times L(n_2,k)$ and is the unique cycle vertex in its component.

We complete the proof by showing that $T((1,0))\cong T((d,0))$. Let (u,v) be a vertex in $T((1,0))$. Suppose that (u,v) has height h in the tree $T((1,0))$. Let d_h be the unique vertex in $G_1(n_1,k)$ which is in the same cycle as d and such that $d_h^{k^h}\equiv d \pmod{n_1}$, that is, d_h is the cycle vertex which is h vertices before the cycle vertex d. Note that $d_0=d$. We define the mapping F from $T((1,0))$ into $G_1(n_1,k)\times L(n_2,k)$ by

$$F((u,v))=(ud_h,v).$$

We will show that F is a digraph isomorphism from $T((1,0))$ onto $T((d,0))$.

We first demonstrate that F is a mapping from $T((1,0))$ into $T((d,0))$ that sends vertices of height h into vertices of the same height h. If $(u,v)=(1,0)$, then $F((u,v))=(d,0)$, and both the vertices $(1,0)$ and $(d,0)$ have height 0. Now suppose that (u,v) is not a cycle vertex. Then

$$[F((u,v))]^{k^h}=(ud_h,v)^{k^h}=\left(u^{k^h}d_h^{k^h},v^{k^h}\right)=(1\cdot d,0)=(d,0).$$

Moreover, if $0\leqslant i<h$, then

$$(ud_h,v)^{k^i}=\left(u^{k^i}d_h^{k^i},v^{k^i}\right),$$

where either u^{k^i} or v^{k^i} is a noncycle vertex. If u^{k^i} is a noncycle vertex, then $u^{k^i}d_h^{k^i}$ is a noncycle vertex by Lemma 5.7, since $d_h^{k^i}$ is a cycle vertex. It now follows by Lemma 5.8 that $(ud_h,v)^{k^i}$ is a noncycle vertex. Therefore, $F((u,v))$ is a vertex in $T((d,0))$ that has height h.

We now show that F is a one-to-one mapping. Suppose that (u_1,v_1) and (u_2,v_2) have heights h_1 and h_2, respectively in $T((1,0))$ and

$$F((u_1,v_1))=(u_1d_{h_1},v_1)=(u_2d_{h_2},v_2)=F((u_2,v_2)). \tag{6.4}$$

By our argument above, it then follows that $F((u_1,v_1))$ has height h_1, while $F((u_2,v_2))$ has height h_2. If $h_1\neq h_2$, then $F((u_1,v_1))\neq F((u_2,v_2))$, which is a contradiction. Hence, $h_1=h_2$ and $d_{h_1}\equiv d_{h_2} \pmod{n_1}$. By (6.4), $v_1\equiv v_2 \pmod{n_2}$. Since d_{h_1} is a vertex in $G_1(n_1,k)$, d_{h_1} is invertible modulo n_1. It now follows from (6.4) that $u_1\equiv u_2 \pmod{n_1}$, which implies that F is one-to-one.

We next show that F is onto. Let (u',v') be a vertex of height h in $T((d,0))$. If $h=0$, then $(u',v')=(d,0)$ and $F((1,0))=(d,0)$. We now assume that $h\geqslant 1$. Consider the vertex $(u'd_h^{-1},v')$ in $G_1(n_1,k)\times L_2(n_2,k)$. We claim that $(u'd_h^{-1},v')$ is a vertex of height h in $T((1,0))$. Since d_h is a cycle vertex, $d_h^{k^j} \equiv d_h \pmod{n_1}$ for some positive integer j. Then

$$\left(d_h^{-1}\right)^{k^j} \equiv \left(d_h^{k^j}\right)^{-1} \equiv d_h^{-1} \pmod{n_1},$$

and d_h^{-1} is also a cycle vertex. Note that

$$\begin{aligned}(u'd_h^{-1}, v')^{k^h} &= \left((u')^{k^h}\left(d_h^{-1}\right)^{k^h}, (v')^{k^h}\right) = \left((u')^{k^h}\left(d_h^{k^h}\right)^{-1}, (v')^{k^h}\right)\\ &= (dd^{-1}, 0) = (1, 0).\end{aligned}$$

If $0 \leqslant i < h$, then

$$(u'd_h^{-1}, v')^{k^i} = \left((u')^{k^i}\left(d_h^{-1}\right)^{k^i}, (v')^{k^i}\right),$$

where either $(u')^{k^i}$ or $(v')^{k^i}$ is a noncycle vertex. If $(u')^{k^i}$ is a noncycle vertex, then by Lemma 5.7, $(u')^{k^i}(d_h^{-1})^{k^i}$ is a noncycle vertex, since $(d_h^{-1})^{k^i}$ is a cycle vertex. Thus, $(u'd_h^{-1}, v')^{k^i}$ is a noncycle vertex, and hence $(u'd_h^{-1}, v')$ is a vertex in $T((1,0))$ of height h. Now notice that

$$F((u'd_h^{-1}, v')) = (u'd_h^{-1}d_h, v') = (u', v'),$$

which implies that F is onto.

Finally, we show that F is edge-preserving. Suppose that $(u,v) \neq (1,0)$ is a vertex in $T((1,0))$ of height $h \geqslant 1$. Then $(u,v)^k$ is a vertex in $T((1,0))$ of height $h-1$ and

$$F((u,v)^k) = F((u^k, v^k)) = (u^k d_{h-1}, v^k) = (u^k d_h^k, v^k) = (ud_h, v)^k = [F((u,v))]^k.$$

The result now follows. □

Corollary 6.2. *Let $J(n,k)$ be a component in $G(n,k)$ and let c_1 and c_2 be any two cycle vertices in $J(n,k)$. Then $T(c_1) \cong T(c_2)$.*

P r o o f. This follows from Theorem 6.1 upon noting that $J(n,k)$ is a subdigraph of $G^*_{\mathcal{P}_2}(n,k)$ for some subset $\mathcal{P}_2$ of the set of primes dividing n. □

Corollary 6.3. *Let $n > 1$ be an integer and let $\mathcal{P}$ be the set of primes dividing n. Let $\mathcal{P}_2$ be a subset of $\mathcal{P}$. Let t be a fixed positive integer. Then all components in $G^*_{\mathcal{P}_2}(n,k)$ having a t-cycle are isomorphic.*

Example 6.4. In Figure 4, we observe that trees attached to cycle vertices in the same fundamental constituent of $G(56,2)$ are isomorphic, whereas trees attached to cycle vertices in different fundamental constituents are not isomorphic.

Example 6.5. From Figure 3 we can see that for the digraph $G(39,3)$, the fundamental constituents $G^*_{\emptyset}(39,3)$ and $G^*_{\{3\}}(39,3)$ have isomorphic nontrivial trees attached to their cycle vertices, while the fundamental constituents $G^*_{\{13\}}(39,3)$ (see the second and third components in Figure 3) and $G^*_{\{3,13\}}(39,3)$ (see the first component in Figure 3) have the trivial tree attached to their cycle vertices.

7. Possible cycle lengths and heights in $G_2(n,k)$

Theorem 7.1. *If C is a t-cycle in $G_2(n,k)$, then there exists a t-cycle in $G_1(n,k)$.*

Proof. Since $G_2(n,k)$ is the disjoint union of the fundamental constituents $G^*_{\mathcal{P}_2}(n,k)$ of $G(n,k)$ as $\mathcal{P}_2$ ranges over the nonempty subsets of $\mathcal{P}$, the set of primes dividing n, we see that C is a cycle in some fundamental constituent $G^*_{\mathcal{P}_2}(n,k)$. Then

$$G^*_{\mathcal{P}_2}(n,k) = G_1(n_1,k) \times L(n_2,k), \tag{7.1}$$

where n_1 and n_2 are defined as in (6.2). Let c be a vertex in the t-cycle C. Noting that the only cycle vertex in $L(n_2,k)$ is the fixed point 0, we see by Lemma 5.8 that we can write $c = (c_1, 0)$, where c_1 is a vertex in a t_1-cycle of $G_1(n_1,k)$. It further follows from Lemma 5.8 that $t = t_1 \cdot 1 = t_1$. Now consider the vertex $d = (c_1, 1)$ in $G_1(n,k) = G_1(n_1,k) \times G_1(n_2,k)$. Since c_1 is a cycle vertex in $G_1(n_1,k)$ and 1 is a fixed point in $G_1(n_2,k)$, we find that d is a cycle vertex in $G_1(n,k)$. By Lemma 5.8, we observe that d is part of a t-cycle also. □

Corollary 7.2. *Every cycle in $G(n,k)$ is a fixed point if and only if $k \equiv 1 \pmod{l}$, where l is as defined in* (5.1).

Proof. The proof follows from Corollary 5.2 and Theorem 7.1. □

Theorem 7.3. *Let n have the factorization given in* (1.2). *Suppose that $G_1(n,k)$ contains a t-cycle. Then the subdigraph $G_2(n,k)$ also contains a t-cycle if and only if there exist $i \in \{1,2,\ldots,r\}$ and an integer d relatively prime to $\lambda(n)$ such that $t = \operatorname{ord}_d k$ and $d \mid \lambda(n/p_i^{\alpha_i})$.*

Proof. As noted earlier, $G_2(n,k)$ is a disjoint union of $G^*_{\mathcal{P}_2}(n,k)$ as $\mathcal{P}_2$ ranges over all nonempty subsets of $\mathcal{P}$. Let C be a t-cycle in $G_2(n,k)$. Then C is a t-cycle in $G^*_{\mathcal{P}_2}(n,k)$ for some nonempty subset $\mathcal{P}_2$ of $\mathcal{P}$. By (7.1)

$$G^*_{\mathcal{P}_2}(n,k) \cong G_1(n_1,k) \times L(n_2,k),$$

where $n_1 \mid (n/p_i^{k_i})$ for some $i \in \{1, 2, \dots, r\}$. Recall that the only cycle vertex in $L(n_2, k)$ is the fixed point 0. It now follows from Lemmas 5.8, 5.1, and 5.5 that if d is any positive integer for which $d \mid \lambda(n_1)$ and $\gcd(d, k) = 1$, then there exists a t-cycle in $G^*_{\mathcal{P}_2}(n, k)$ such that $t = \mathrm{ord}_d k$. Since $\lambda(a) \mid \lambda(b)$ when $a \mid b$ by the property of the Carmichael-lambda function, the result now follows. $\square$

Example 7.4. Suppose that n has at least two distinct prime divisors. It was shown in Remark 3.6 of [11] that if $k = 2$, then $n = 203 = 7 \cdot 29$ is the least positive integer n for which there exists a positive integer t such that $G_1(n, k)$ has a t-cycle, but $G_2(n, k)$ does not have a t-cycle. In this case, $G_1(203, 2)$ has a 6-cycle, whereas $G_2(203, 2)$ does not have a 6-cycle. When $k = 3$ the least such integer n is $n = 115 = 5 \cdot 23$. In this instance, $G_1(115, 3)$ has a 10-cycle, while $G_2(115, 3)$ does not contain a 10-cycle. Note that $\lambda(115) = 44$. However, $44 \nmid \lambda(5) = 4$ and $44 \nmid \lambda(23) = 22$. Moreover, $\mathrm{ord}_{44} 3 = 10$, whereas $\mathrm{ord}_4 3 = 2$ and $\mathrm{ord}_{22} 3 = 5$.

The next corollary is a partial converse of Theorem 7.1.

Corollary 7.5. *Let $B(G(n, k))$ denote the set of integers t such that $G(n, k)$ has a t-cycle. Suppose that n is a prime or a prime power. Then $B(G_1(n, k)) = B(G_2(n, k))$ if and only if $k \equiv 1 \pmod{l}$, where l is defined as in (5.1).*

Proof. By Theorem 7.3, the only cycle in $G_2(n, k)$ is the fixed point 0. The result now follows from Corollary 5.2. $\square$

Theorem 7.6. *Let $n > 1$ be as defined in (1.2) and let $a \in \{1, 2, \dots, n\}$ be an integer such that $a \in G_2(n, k)$ and*

$$a = b \prod_{i=1}^{r} p_i^{l_i},$$

where $l_i \geqslant 0$ and $\gcd(b, n) = 1$. For $i = 1, 2, \dots, r$, define m_i by

$$m_i = \begin{cases} 0 & \text{if } l_i = 0, \\ \alpha_i & \text{if } 1 \leqslant l_i \leqslant \alpha_i, \\ l_i & \text{if } l_i > \alpha_i. \end{cases}$$

Let

$$n_1 = \prod_{i=1}^{r} p_i^{\alpha_i - \min(m_i, \alpha_i)}.$$

Then $\gcd(n_1, a) = 1$. Let l and w be as given in (5.1) and let $\mathrm{ord}_{n_1} a = l'w'$, where $l' \mid l$ and $w' \mid w$. Let $h(a)$ be the least nonnegative integer j such that $w' \mid k^j$. Then *the height of a is equal to*

$$\max\Big(\max_{1\leqslant i\leqslant r}\Big\lceil\log_k \frac{m_i}{l_i}\Big\rceil, h(a)\Big),$$

where we define $m_i/l_i = 1$ if $m_i = l_i = 0$.

Theorem 7.7. *Let $n > 1$ be as defined in* (1.2). *Let $e_i = n/p_i^{\alpha_i}$, $i = 1, 2, \ldots, r$, and let $\lambda(e_i) = l_i w_i$. Let h_i be the least nonnegative integer such that*

$$w_i \mid k^{h_i}.$$

Let $g = \max_{1\leqslant i\leqslant r} h_i$. Let h be the maximum height of any vertex in $G_2(n,k)$. Then

$$h = \max\big(\max_i\lceil\log_k \alpha_i\rceil, g\big).$$

Theorems 7.6 and 7.7 were proved for the case $k = 2$ in Theorems 3.10 and 3.14, respectively, of [11]. Moreover, the proofs of Theorems 7.6 and 7.7 are completely similar to the proofs of these theorems in [11] upon making use of Lemma 5.10 of our present paper.

8. Results on fixed points

As we mentioned earlier, fixed points are of interest, because any digraph $G(n,k)$ always has fixed points including 0 and 1. On the other hand, by Corollary 7.2, there exist digraphs $G(n,k)$ not having t-cycles for any $t > 1$.

We have the following two theorems on the number of fixed points and the number of isolated fixed points in $G(n,k)$. Note that an isolated fixed point is a fixed point with indegree 1.

Theorem 8.1. *Let $n > 1$.*

(i) *If k is even, then $A_1(G(n,k)) \geqslant 2^{\omega(n)}$ and $A_1(G_1(n,k)) \geqslant 1$. In particular, if $k = 2$, then $A_1(G(n,k)) = 2^{\omega(n)}$ and $A_1(G_1(n,k)) = 1$.*

(ii) *If $k \geqslant 3$ is odd and $2 \parallel n$, then $A_1(G(n,k)) \geqslant 2\cdot 3^{\omega(n)-1}$ and $A_1(G_1(n,k)) \geqslant 2^{\omega(n)-1}$. In particular, if $k = 3$, then we have $A_1(G(n,k)) = 2\cdot 3^{\omega(n)-1}$ and $A_1(G_1(n,k)) = 2^{\omega(n)-1}$.*

(iii) *If $k \geqslant 3$ is odd and either n is odd or $4 \parallel n$, then $A_1(G(n,k)) \geqslant 3^{\omega(n)}$ and $A_1(G_1(n,k)) \geqslant 2^{\omega(n)}$. In particular, if $k = 3$, then $A_1(G(n,k)) = 3^{\omega(n)}$ and $A_1(G_1(n,k)) = 2^{\omega(n)}$.*

(iv) *If* $k \geqslant 3$ *is odd and* $8 \parallel n$, *then* $A_1(G(n,k)) \geqslant 5 \cdot 3^{\omega(n)-1}$ *and* $A_1(G_1(n,k)) \geqslant 4 \cdot 2^{\omega(n)-1}$. *In particular, if* $k = 3$, *then* $A_1(G(n,k)) = 5 \cdot 3^{\omega(n)-1}$ *and* $A_1(G_1(n,k)) = 4 \cdot 2^{\omega(n)-1}$.

Proof. The proof follows from Lemma 5.6. □

It was proved in [10] that if $k = 2$ then $G(n,k)$ has a nonzero isolated fixed point if and only if $n = 2m$, where m is an odd square-free integer. In this case, a is a nonzero isolated fixed point if and only if $a = m$. In Theorem 8.2, we extend this result by counting isolated fixed points in $G(n,k)$ for any $n > 1$ and any $k \geqslant 2$.

Theorem 8.2. *Let* $n > 1$ *have the factorization given in* (1.2). *The number of isolated fixed points in* $G(n,k)$ *is given by*

$$\prod_{i=1}^{r}[\delta(\gcd(\lambda(p_i^{\alpha_i}),k)) \cdot \delta_i \gcd(\lambda(p_i^{\alpha_i}),k-1) + \delta(\alpha_i)],$$

where $\delta(m) = 1$ *if* $m = 1$ *and* $\delta(m) = 0$ *otherwise, and* δ_i *is defined as in Lemma 5.6.*

Proof. Let a be an isolated fixed point in $G(n,k)$. Then $\mathrm{indeg}_n(a) = 1$. By (1.4), $\mathrm{indeg}_n(a) = 1$ if and only if $\mathrm{indeg}_{q_i}(a) = 1$ for $i = 1,2,\ldots,r$, where $q_i = p_i^{\alpha_i}$. Clearly, a is a fixed point in $G(n,k)$ if and only if a is a fixed point in $G(q_i,k)$ for $1 \leqslant i \leqslant r$. Suppose that $a \in G_1(q_i,k)$ for some i such that $1 \leqslant i \leqslant r$. Then by Lemma 3.1, $\mathrm{indeg}_{q_i}(a) = 1$ if and only if $\varepsilon_i \gcd(\lambda(q_i),k) = 1$, where ε_i is defined as in Lemma 3.1. By Lemma 5.6, the number of fixed points in $G_1(q_i,k)$ is equal to $\delta_i \gcd(\lambda(q_i),k-1)$, where δ_i is defined as in Lemma 5.6.

Now suppose that a is a fixed point in $G_2(q_i,k)$. This occurs if and only if $a \equiv 0 \pmod{q_i}$. Note that $\mathrm{indeg}_{q_i}(0) = 1$ if and only if $\alpha_i = 1$. The result now follows. □

Remark 8.3. Note that by the proof of Theorem 8.2, the vertex 0 is an isolated fixed point of $G(n,k)$ if and only if n is square-free (see Figures 1–4).

9. Length of the longest cycle

In [7], the following theorem was proved giving an upper bound for the length of the longest cycle in $G(p,k)$ when $p > 5$ is a prime. We let $L(G(n,k))$ denote the length of the longest cycle in the digraph $G(n,k)$.

Theorem 9.1 (Lucheta et al.). *Let $p > 5$ be a prime. Then*

$$L(G(p,k)) \leqslant \frac{p-1}{2} - 1.$$

Moreover, if $(p-1)/2$ is also an odd prime, i.e., $(p-1)/2$ is a Sophie Germain prime, and k is a primitive root modulo $(p-1)/2$, then $L(G(p,k)) = (p-1)/2 - 1$. Furthermore, if $(p-1)/2$ is an odd prime and k is an odd primitive root modulo $(p-1)/2$, then $G(p,k)$ contains two cycles of length $(p-1)/2 - 1$.

Theorem 9.2 below extends Theorem 9.1 to digraphs $G(n,k)$ for any fixed positive integer n and an integer $k \geqslant 2$ which is allowed to vary. Improved bounds are also found for $L(G(n,k))$, and all values of k are determined for which $L(G(n,k)) \leqslant 2$ for all n.

Theorem 9.2. *Let $n \geqslant 1$ be a fixed integer. Then we have:*

(i) $\max_{k \geqslant 2} L(G(n,k)) = \lambda(\lambda(n))$.

(ii) *If k is a fixed integer and C is a t-cycle in $G(n,k)$, then $t \mid \lambda(\lambda(n))$.*

(iii) *The digraph $G(n,k)$ contains only cycles of length 1 (fixed points) for all $k \geqslant 2$ if and only if n is one of the 8 positive divisors of 24.*

(iv) $\max_{k \geqslant 2} L(G(n,k)) = 2$ *if and only if n is one of the 136 positive divisors of $2^5 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 = 131040$ which are not divisors of 24.*

(v) *If n is not a divisor of 24, then $\max_{k \geqslant 2} L(G(n,k))$ is an even integer.*

(vi) *Suppose that $n > 5$. If it is not the case that n is a prime of the form $n = 2p^i + 1$, where p is an odd prime and $i \geqslant 1$, then*

$$\max_{k \geqslant 2} L(G(n,k)) < \frac{n}{4}. \tag{9.1}$$

If n is a prime of the form $2p^i + 1$, then

$$\max_{k \geqslant 2} L(G(n,k)) = p^{i-1}(p-1) = \frac{n-1}{2} - \frac{n-1}{2p} > \frac{n}{4}. \tag{9.2}$$

In particular, when n is a prime such that $n = 2p^i + 1$, then

$$\frac{n-1}{3} \leqslant \max_{k \geqslant 2} L(G(n,k)) \leqslant \frac{n-1}{2} - 1. \tag{9.3}$$

The upper bound in (9.3) is attained if and only if n is a prime of the form $2p+1$, i.e., p is a Sophie Germain prime, and the lower bound in (9.3) is attained when n is a prime of the form $2 \cdot 3^i + 1$, where $i \geqslant 1$.

P r o o f. (i) By Lemma 5.1 and Theorem 7.1, the longest cycle in $G(n,k)$ is equal to $\operatorname{ord}_l k$, where l is the largest divisor of $\lambda(n)$ relatively prime to k. Clearly,

$$\operatorname{ord}_l k \mid \lambda(l) \mid \lambda(\lambda(n)).$$

By Theorem 2.2, there exists a positive integer k such that $\gcd(k, \lambda(n)) = 1$ and $\operatorname{ord}_{\lambda(n)} k = \lambda(\lambda(n))$. The assertion now follows.

(ii) By Lemma 5.1, there exists a divisor d of $\lambda(n)$ such that $\operatorname{ord}_d k = t$. By Theorem 2.2 on λ, $t \mid \lambda(d)$. It follows from the definition of λ that if $m \mid n$, then $\lambda(m) \mid \lambda(n)$. Hence,

$$t \mid \lambda(d) \mid \lambda(\lambda(n)).$$

(iii) We note that $\lambda(m) = 1$ if and only if $m = 1$ or 2. By the definition of $\lambda(n)$, we see that $\lambda(n) = 1$ or 2 if and only if n is a divisor of 24. The result now follows from part (i).

(iv) Observe that $\lambda(m) = 2$ if and only if $m = 3, 4, 6, 8, 12$, or 24. Using the definition of $\lambda(n)$, the result now easily follows.

(v) It follows from the properties of $\lambda(m)$ that $\lambda(m)$ is even if and only if $m \geqslant 3$. Our result now follows from the proof of part (iii).

(vi) First suppose that n is a prime of the form $2p^i + 1$. Then

$$\max_{k\geqslant 2} L(G(n,k)) = \lambda(\lambda(2p^i+1)) = \lambda(2p^i) = p^{i-1}(p-1) = \frac{n-1}{2} - \frac{n-1}{2p}. \tag{9.4}$$

The last inequality in (9.2) and the inequalities in (9.3) now follow immediately. It is easily seen that the upper bound in (9.3) is attained exactly when $n = 2p + 1$, whereas the lower bound in (9.3) is satisfied exactly when $n = 2 \cdot 3^i + 1$ for $i \geqslant 1$.

Now suppose that it is not the case that n is a prime of the form $2p^i + 1$. By part (i), it suffices to show that $\lambda(\lambda(n)) < n/4$. We make the following observations which derive from the definition of the Carmichael lambda-function. If $m \geqslant 2$ then $\lambda(m) < m$. If $2 \parallel m$ or $m = 4$, then $\lambda(m) \leqslant m/2$. Noting that $\lambda(m)$ is even for $m > 2$, we see that if $m > 4$ and $4 \mid m$, then $\lambda(m) \leqslant m/4$. Moreover, if m has $j \geqslant 2$ distinct prime divisors, then $\lambda(m) < m/2^{j-1}$.

We now suppose further that $4 \mid n$. Since $n > 5$ and $\lambda(n)$ is even, we see from our above comments that

$$\lambda(\lambda(n)) \leqslant \frac{\lambda(n)}{2} \leqslant \frac{n}{2 \cdot 4} = \frac{n}{8}.$$

Now assume that either $2 \parallel n$ or both n is odd and $\omega(n) \geqslant 2$. Since $n > 5$, we also have that $\omega(n) \geqslant 2$ if $2 \parallel n$. Then $\lambda(n) < n/2$ and $\lambda(n)$ is even. Hence,

$$\lambda(\lambda(n)) \leqslant \frac{\lambda(n)}{2} < \frac{n}{2 \cdot 2} = \frac{n}{4}.$$

We can now assume that n is odd and $\omega(n) = 1$. Suppose that $n = p^j$, where p is an odd prime and $j \geqslant 2$. Then

$$\lambda(\lambda(n)) = \lambda(\lambda(p^j)) = \lambda(p^{j-1}(p-1)). \tag{9.5}$$

If $p = 3$ and $j \geqslant 2$, then

$$\lambda(\lambda(n)) = 2 \cdot 3^{j-2} = \frac{2n}{9} < \frac{n}{4}.$$

Now suppose that $p \geqslant 5$ and $j \geqslant 2$. Then $\gcd(p, p-1) = 1$, $p-1$ is even, and $\lambda(p-1)$ is also even. From (9.5), we obtain

$$\begin{aligned} \lambda(\lambda(n)) &= \lambda(p^{j-1}(p-1)) \leqslant \operatorname{lcm}(p^{j-2}(p-1), \lambda(p-1)) \\ &\leqslant \frac{1}{2} p^{j-2}(p-1)\frac{p-1}{2} < \frac{p^j}{4} = \frac{n}{4}. \end{aligned} \tag{9.6}$$

We finally assume that n is a prime. If $4 \mid n-1$, then $\lambda(n-1) \leqslant (n-1)/4$, since $n-1 > 4$. Hence,

$$\lambda(\lambda(n)) = \lambda(n-1) \leqslant \frac{n-1}{4} < \frac{n}{4}.$$

For our last case, we assume that $4 \nmid n-1$. Then $2 \parallel n-1$ and $\omega(n-1) = l \geqslant 3$, since $n-1$ is even, $n-1 > 4$, and n is not of the form $2p^i + 1$, where p is an odd prime and $i \geqslant 1$. Then

$$\lambda(\lambda(n)) = \lambda(n-1) \leqslant \frac{n-1}{2^{l-1}} \leqslant \frac{n-1}{4} < \frac{n}{4}.$$

Our result now follows. □

Remark 9.3. It is noted in [3, p. 1592] that Theorem 9.2 (i) holds.

For the next theorem we let S be the set consisting of natural numbers of the form $2^\alpha F_{m_1} \dots F_{m_j}$ for some $\alpha \geqslant 0$ and $j \geqslant 0$, where $F_{m_i} = 2^{2^{m_i}} + 1$ are distinct Fermat primes. If $j = 0$ then we set $n = 2^\alpha$. It is well known that $n \in S$ if and only if $\phi(n) = 2^i$ for some $i \geqslant 0$, where ϕ is Euler's totient function (see [5, pp. 34–35]). By a celebrated theorem due to Gauss, $n \in S$ for $n \geqslant 3$ if and only if the regular polygon with n sides has a Euclidean construction with ruler and compass.

Theorem 9.4. *Let $n \geqslant 1$ be a fixed integer. Then*

$$\max_{k \text{ even}} L(G(n,k)) = 1$$

if and only if $n \in S$.

Proof. Suppose that $n \in S$. Since $\lambda(n) \mid \phi(n)$, it follows that $\lambda(n) = 2^i$ for some $i \geqslant 0$. Thus if k is even, then 1 is the only divisor of $\lambda(n)$ which is relatively prime to k. It follows from Lemma 5.1 and Theorem 7.1 that the only cycles in $G(n,k)$ are fixed points.

Now suppose that $n \notin S$. Then there exists an odd prime p such that $p \mid \lambda(n)$. Clearly, there exists an even integer k such that $\gcd(k,p) = 1$ and $k \not\equiv 1 \pmod{p}$. Then $\operatorname{ord}_p k \geqslant 2$ and the result follows from Lemma 5.1. □

It follows from Lemma 5.1 that if $a \in G_1(n,k)$, then the length of the cycle in the same component as a is less than or equal to $\operatorname{ord}_l k$, where l is defined as in (5.1) and depends on $\lambda(n)$. The following theorem, proved in [6] using analytic methods, gives lower bounds for $\operatorname{ord}_l k$, which are valid for a positive proportion of integers n.

Theorem 9.5 (Kurlberg and Pomerance)**.**
(i) *Suppose $\varepsilon(x)$ tends to zero arbitrarily slowly as $x \to \infty$. Then $\operatorname{ord}_l k \geqslant n^{1/2+\varepsilon(n)}$ for all but $o_\varepsilon(x)$ integers $n \leqslant x$.*
(ii) *There is a positive constant γ such that $\operatorname{ord}_l k \geqslant n^{1/2+\gamma}$ for a positive proportion of integers n.*
(iii) *Assuming the Generalized Riemann Hypothesis, for each fixed $\varepsilon > 0$ we have $\operatorname{ord}_l k > n^{1-\varepsilon}$ for all but $o_\varepsilon(x)$ integers $n \leqslant x$.*

The results in the paper [6] strengthen those given in [3].

As stated in Theorem 9.2 (i), $L(G(n,k)) \leqslant \lambda(\lambda(n))$. In [8], the following theorem is proved using analytic techniques regarding the order of $\lambda(\lambda(n))$.

Theorem 9.6 (Martin and Pomerance)**.** *We have*

$$\lambda(\lambda(n)) = n \exp\bigl(-1(1+o(1))(\log\log n)^2 \log\log\log n\bigr)$$

as $n \to \infty$ through a set of integers of asymptotic density 1.

References

[1] *W. Carlip, M. Mincheva*: Symmetry of iteration digraphs. Czech. Math. J. *58* (2008), 131–145.
[2] *W.-S. Chou, I. E. Shparlinski*: On the cycle structure of repeated exponentiation modulo a prime. J. Number Theory *107* (2004), 345–356.
[3] *J. B. Friendlander, C. Pomerance, I. E. Shparlinski*: Period of the power generator and small values of Carmichael's function. Math. Comput. *70* (2001), 1591–1605; Corrigendum ibid. *71* (2002), 1803–1806.
[4] *B. Hartnell, D. F. Rall*: Domination in Cartesian products: Vizing's conjecture. Domination in Graphs. Advanced Topics (T. Waynes, S. T. Hedetniemi, P. J. Slater, eds.). Dekker, New York, 1998, pp. 163–189.
[5] *M. Křížek, F. Luca, L. Somer*: 17 Lectures on Fermat Numbers: From Number Theory to Geometry. CMS Books in Mathematics, Vol. 9. Springer, New York, 2001.
[6] *P. Kurlberg, C. Pomerance*: On the periods of the linear congruential and power generators. Acta Arith. *119* (2005), 149–169.
[7] *C. Lucheta, E. Miller, C. Reiter*: Digraphs from powers modulo p. Fibonacci Q. *34* (1996), 226–239.
[8] *G. Martin, C. Pomerance*: The iterated Carmichael λ-function and the number of cycles of the power generator. Acta Arith. *118* (2005), 305–335.
[9] *I. Niven, H. S. Zuckerman, H. L. Montgomery*: An Introduction to the Theory of Numbers. 5th ed. John Wiley & Sons, New York, 1991.
[10] *L. Somer, M. Křížek*: On a connection of number theory with graph theory. Czech. Math. J. *54* (2004), 465–485.
[11] *L. Somer, M. Křížek*: Structure of digraphs associated with quadratic congruences with composite moduli. Discrete Math. *306* (2006), 2174–2185.
[12] *L. Somer, M. Křížek*: On semiregular digraphs of the congruence $x^k \equiv y \pmod{n}$. Commentat. Math. Univ. Carol. *48* (2007), 41–58.
[13] *L. Somer, M. Křížek*: On symmetric digraphs of the congruence $x^k \equiv y \pmod{n}$. Discrete Math. *309* (2009), 1999–2009.
[14] *L. Szalay*: A discrete iteration in number theory. Berzseneyi Dániel Tanárk. Föisk. Tud. Közl., Termtud. *8* (1992), 71–91. (In Hungarian.)
[15] *T. Vasiga, J. Shallit*: On the iteration of certain quadratic maps over GF(p). Discrete Math. *277* (2004), 219–240.
[16] *B. Wilson*: Power digraphs modulo n. Fibonacci Q. *36* (1998), 229–239.

Authors' addresses: L. Somer, Department of Mathematics, Catholic University of America, Washington, D.C. 20064, U.S.A., e-mail: somer@cua.edu; M. Křížek, Institute of Mathematics of the Academy of Sciences of the Czech Republic, Žitná 25, CZ-115 67 Prague 1, Czech Republic, e-mail: krizek@math.cas.cz.