

On semiregular digraphs of the congruence $x^k \equiv y \pmod{n}$

LAWRENCE SOMER, MICHAL KRŤÍŽEK

Abstract. We assign to each pair of positive integers n and $k \geq 2$ a digraph $G(n, k)$ whose set of vertices is $H = \{0, 1, \dots, n - 1\}$ and for which there is a directed edge from $a \in H$ to $b \in H$ if $a^k \equiv b \pmod{n}$. The digraph $G(n, k)$ is semiregular if there exists a positive integer d such that each vertex of the digraph has indegree d or 0 . Generalizing earlier results of the authors for the case in which $k = 2$, we characterize all semiregular digraphs $G(n, k)$ when $k \geq 2$ is arbitrary.

Keywords: Chinese remainder theorem, congruence, group theory, dynamical system, regular and semiregular digraphs

Classification: 11A07, 11A15, 05C20, 20K01

1. Introduction

This paper extends results given in the works [2] and [6] which provide an interesting connection between number theory, graph theory and group theory. In the papers [4] and [5] we investigated properties of the iteration digraph representing a dynamical system occurring in number theory.

For $n \geq 1$ let

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

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 $k \geq 2$ and for each $x \in H$ let $f(x)$ be the remainder of x^k modulo n , i.e.,

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

From here on, whenever we refer to the iteration digraph of f , we assume that the mapping f is as given in (1.1), see Figure 1. Each pair of natural numbers n and $k \geq 2$ has a specific iteration digraph corresponding to it.

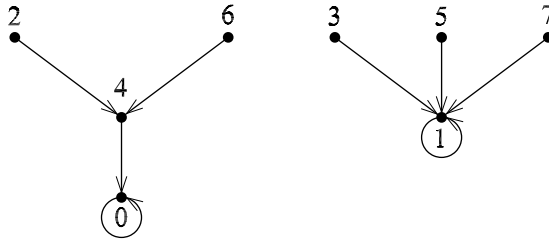


Figure 1. The iteration digraph corresponding to $n = 8$ and $k = 2$.

We identify the vertex a of H with its residue modulo 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). In this paper we will often identify the vertex n with the vertex 0 for convenience.

For particular values of n and k , we denote the iteration digraph of f by $G(n, k)$. It is obvious that $G(n, k)$ with n vertices also has exactly n directed edges.

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

$$(1.2) \quad n = \prod_{i=1}^r p_i^{\alpha_i},$$

where $p_1 < p_2 < \dots < p_r$ 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 subgraph of the associated nondirected graph.

The *indegree* of a vertex $a \in H$ of $G(n, k)$, denoted by $\text{indeg}_n(a)$, 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 frequently will simply write $\text{indeg}(a)$ 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 clear that each component has a unique cycle, since each vertex of the component has outdegree 1 and the component has only a finite number of vertices. Cycles of length 1 are called fixed points.

Remark 1.1. Recall that a graph is *regular* if all its vertices have the same degree. We say that the digraph $G(n, k)$ is *regular* if each of its vertices have the same indegree. The digraph $G(n, k)$ is said to be *semiregular* if there exists a positive integer d such that each vertex of $G(n, k)$ either has indegree d or 0. Note that the set of semiregular digraphs $G(n, k)$ includes the subset of regular digraphs.

Clearly, $G(n, k)$ is regular only if $G(n, k)$ has no vertices of indegree 0. Since each component of $G(n, k)$ has a unique cycle, we see that $G(n, k)$ is regular if and only if each component of $G(n, k)$ is a cycle and each vertex of $G(n, k)$ has indegree 1. Since any vertex of indegree 0 is a noncycle vertex and there is a path from any noncycle vertex to the cycle in its component, we see that $G(n, k)$ is regular if and only if each vertex of positive indegree has indegree equal to 1. Noting that each vertex of $G(n, k)$ has outdegree 1, we observe that $G(n, k)$ is regular as a digraph if and only if $G(n, k)$ is regular as an undirected graph. Figure 2 provides an example of a regular digraph, while Figure 3 gives an example of a semiregular digraph which is not regular.

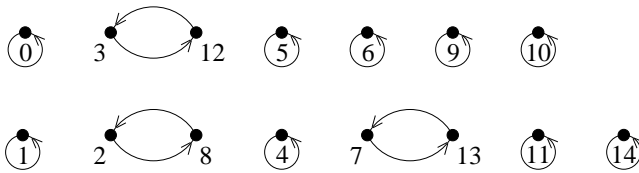


Figure 2. The iteration digraph corresponding to $n = 15$ and $k = 3$.

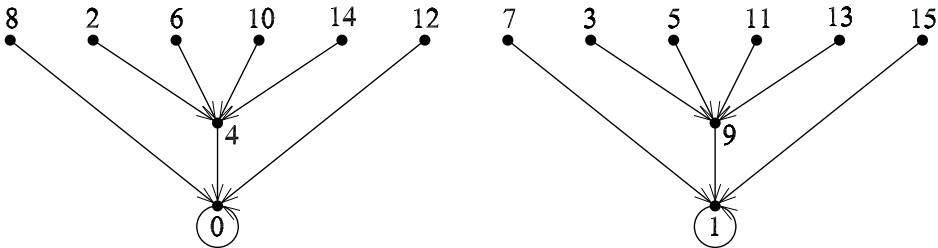


Figure 3. The iteration digraph corresponding to $n = 16$ and $k = 2$.

In [4] all semiregular digraphs $G(n, k)$ were characterized when $k = 2$. In this paper, given a fixed integer $k \geq 2$, we find all semiregular and regular digraphs $G(n, k)$. 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 $G_2(n, k)$ be the induced subdigraph on the remaining vertices not coprime with n . We observe that $G_1(n, k)$ and $G_2(n, k)$ are disjoint 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 $G_2(n, k)$. For example, the second component of Figure 4 is $G_1(12, 2)$ whereas the remaining three components make up $G_2(12, 2)$. 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 $G_1(n, k)$.

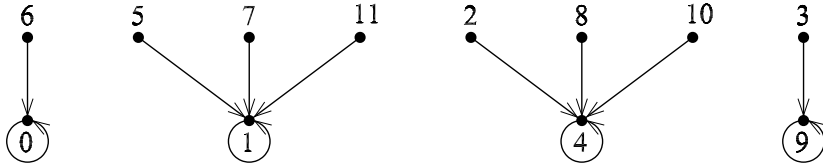


Figure 4. The iteration digraph corresponding to $n = 12$ and $k = 2$.

In Theorems 4.1 and 4.3, we will show that $G_1(n, k)$ is always semiregular. In Theorem 4.4 we will also determine when $G_2(n, k)$ is semiregular. Observe that in Figure 1, the subdigraph $G_2(8, 2)$ is semiregular but $G(8, 2)$ is not semiregular. Note further that in Figures 4 and 5, $G_2(n, k)$ is not semiregular, but each of its components is semiregular. We will characterize later those digraphs for which each of the components of $G_2(n, k)$ is semiregular.

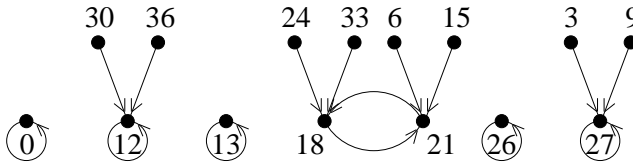


Figure 5. The iteration subdigraph $G_2(39, 3)$.

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

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

Then obviously

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

It follows from (1.3) and Theorem 2.20 in [3] that if n has the factorization given in (1.2), then

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

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 $\lambda(n)$, which modifies 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:

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

where p_1, p_2, \dots, p_r are distinct primes and $k_i \geq 1$ 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 $k \geq 1$.

The following theorem generalizes the well-known Euler's theorem which says (see [1, 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 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

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

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

For the proof see [1, p. 21].

3. Results on the indegree

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

Theorem 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*

$$\text{indeg}(a) = \varepsilon \prod_{i=1}^r \gcd(\lambda(p_i^{\alpha_i}), k),$$

where $\varepsilon = 2$ if $2 \mid k$ and $8 \mid n$, and $\varepsilon = 1$ otherwise.

This is proved in [6, pp. 231–232].

Theorem 3.2. *Let n have the factorization given in (1.2), let a be a vertex of positive indegree in $G_2(n, k)$, and let*

$$a = Q \prod_{i=1}^r p_i^{\beta_i},$$

where $\gcd(Q, n) = 1$, $\beta_i \geq 0$ for $1 \leq i \leq r$, and $\beta_i \geq 1$ for at least one value of i . Then for $i = 1, 2, \dots, r$ either $\beta_i \geq \alpha_i$, or both $\beta_i < \alpha_i$ and $\beta_i = kt_i$ for some nonnegative integer t_i . Moreover,

$$\text{indeg}(a) = \prod_{i=1}^r A_i B_i,$$

where

$$A_i = \begin{cases} p_i^{\alpha_i - \lceil \alpha_i/k \rceil} & \text{if } \beta_i \geq \alpha_i, \\ p_i^{(k-1)t_i} & \text{if } 0 \leq \beta_i < \alpha_i, \end{cases}$$

and

$$B_i = \varepsilon_i \gcd(\lambda(p_i^{\alpha_i - \min(\alpha_i, \beta_i)}), k),$$

where $\varepsilon_i = 2$ if $p_i = 2$, $2 \mid k$ and $\alpha_i - \beta_i \geq 3$, and $\varepsilon_i = 1$ otherwise.

PROOF: By the Chinese remainder theorem, $\text{indeg}(a) > 0$ if and only if for $i = 1, 2, \dots, r$ there exists an integer b_i , a nonnegative integer t_i and an integer c_i coprime to p_i such that

$$(3.1) \quad b_i^k \equiv (p_i^{t_i} c_i)^k \equiv p_i^{kt_i} c_i^k \equiv a \equiv p_i^{\beta_i} (a/p_i^{\beta_i}) \pmod{p_i^{\alpha_i}}.$$

If $\beta_i \geq \alpha_i$, then $b_i \equiv 0 \pmod{p_i^{\alpha_i}}$ satisfies congruence (3.1). Now suppose that $\beta_i < \alpha_i$. Then congruence (3.1) is satisfied only if $kt_i = \beta_i$.

By (1.4), the remainder of our assertion will follow if we can show that

$$N(p_i^{\alpha_i}, k, a) = A_i B_i$$

for $i = 1, 2, \dots, r$. First suppose that $\beta_i \geq \alpha_i$. Then

$$N(p_i^{\alpha_i}, k, a) = N(p_i^{\alpha_i}, k, 0) = p_i^{\alpha_i - \lceil \alpha_i/k \rceil} = A_i = A_i B_i.$$

Now suppose that $\beta_i < \alpha_i$. Let b_i be a residue such that $b_i^k \equiv a \pmod{p_i^{\alpha_i}}$. By (3.1),

$$b_i \equiv p_i^{t_i} c_i \pmod{p_i^{\alpha_i}},$$

where t_i is a nonnegative integer and c_i is an integer such that $\gcd(c_i, p_i) = 1$ and

$$c_i^k \equiv a/p_i^{\beta_i} \pmod{p_i^{\alpha_i - \beta_i}}.$$

Moreover, since $(\mathbb{Z}/p_i^{\alpha_i})^*$ is a group under multiplication, there exists an integer d_i such that

$$(3.2) \quad d_i^k \equiv b_i^k \equiv a \equiv p_i^{kt_i} c_i^k \pmod{p_i^{\alpha_i}}$$

if and only if

$$(3.3) \quad d_i \equiv p_i^{t_i} c_i e_i \pmod{p_i^{\alpha_i}}$$

for some integer e_i such that

$$(3.4) \quad e_i^k \equiv 1 \pmod{p_i^{\alpha_i - kt_i}}.$$

Furthermore,

$$(3.5) \quad p_i^{t_i} c_i e_i \equiv p_i^{t_i} c_i e'_i \pmod{p_i^{\alpha_i}}$$

if and only if

$$(3.6) \quad e_i \equiv e'_i \pmod{p_i^{\alpha_i - t_i}}.$$

We note that if $e_i^k \equiv 1 \pmod{p_i^{\alpha_i - kt_i}}$ and $e_i \equiv e'_i \pmod{p_i^{\alpha_i - t_i}}$, then $(e'_i)^k \equiv 1 \pmod{p_i^{\alpha_i - kt_i}}$. It now follows from (3.2)–(3.6) that

$$N(p_i^{\alpha_i}, k, a) = p_i^{(\alpha_i - t_i) - (\alpha_i - kt_i)} C_i = p_i^{(k-1)t_i} C_i = A_i C_i,$$

where C_i denotes the number of solutions to the congruence

$$x^k \equiv 1 \pmod{p_i^{\alpha_i - kt_i}}.$$

By Theorem 3.1, $C_i = B_i$, and we obtain the required result. \square

An even more complicated version of Theorem 3.2 is proved in [6, pp. 236–237].

4. On regularity and semiregularity of digraphs

We now present our main theorems.

Theorem 4.1. *Let $n \geq 1$ and $k \geq 2$ be integers. Then*

- (i) $G_1(n, k)$ is regular if and only if $\gcd(\lambda(n), k) = 1$;
- (ii) $G_2(n, k)$ is regular if and only if either n is square-free and $\gcd(\lambda(n), k) = 1$, or $n = p$, where p is a prime;
- (iii) $G(n, k)$ is regular if and only if n is square-free and $\gcd(\lambda(n), k) = 1$.

PROOF: We suppose that n has the factorization given in (1.2).

(i) By Remark 1.1 and Theorem 3.1, it suffices to show that

$$(4.1) \quad \prod_{i=1}^r \gcd(\lambda(p_i^{\alpha_i}), k) = 1.$$

However, (4.1) is satisfied if and only if $\gcd(\lambda(n), k) = 1$.

(ii) First suppose that n is not square-free and $q^2 \mid n$ for some prime q . Then by Theorem 3.2, $q \mid \text{indeg}(0)$, and consequently $\text{indeg}(0) > 1$. Thus $G_2(n, k)$ is not regular in this case.

Now suppose that n is square-free and $n = p$. Then $G_2(n, k)$ consists solely of the fixed point p and $G_2(n, k)$ is regular.

We next suppose that $n = p_1 p_2 \cdots p_r$, where $r \geq 2$. By Theorem 3.2 and Remark 1.1 the subdigraph $G_2(n, k)$ is regular if and only if for each vertex $a \in G_2(n, k)$,

$$(4.2) \quad \prod_{i=1}^r A_i B_i = 1,$$

where A_i and B_i are defined as in Theorem 3.2. Equation (4.2) holds if and only if $A_i = B_i = 1$ for $i = 1, 2, \dots, r$. If $a \equiv 0 \pmod{p_i}$, then $A_i = B_i = 1$. We further note that if p_i is any prime such that $1 \leq i \leq r$, then there exists a vertex $a \in G_2(n, k)$ such that $a \not\equiv 0 \pmod{p_i}$. In this case, $\alpha_i = 1$, $\beta_i = 0$, $t_i = 0$, $A_i = 1$, and

$$B_i = \gcd(\lambda(p_i), k).$$

Hence, $G_2(n, k)$ is regular if and only if

$$(4.3) \quad \gcd(\lambda(p_i), k) = 1$$

for $i = 1, 2, \dots, r$. However, (4.3) holds if and only if

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

The result now follows.

(iii) This is a consequence of (i) and (ii). □

Remark 4.2. Part (i) of Theorem 4.1 was also proved in [6, p. 232].

Theorem 4.3. *Let $k \geq 2$ be an integer and let $n \geq 2$ have the canonical factorization given in (1.2). If $\gcd(\lambda(n), k) > 1$, then $G_1(n, k)$ is semiregular but not regular. If $a \in G_1(n, k)$ and $\text{indeg}(a) > 0$, then*

$$(4.4) \quad \text{indeg}(a) = \varepsilon \prod_{i=1}^r \gcd(\lambda(p_i^{\alpha_i}), k),$$

where $\varepsilon = 2$ if $2 \mid k$ and $8 \mid n$, and $\varepsilon = 1$ otherwise.

PROOF: By Theorem 4.1, $G_1(n, k)$ is not regular if $\gcd(\lambda(n), k) > 1$. By Theorem 3.1, $G_1(n, k)$ is semiregular and (4.4) holds. \square

Theorems 4.1 and 4.3 completely specify when the digraph $G_1(n, k)$ is either regular or semiregular. Theorem 4.4 will determine exactly when the digraphs $G_2(n, k)$ and $G(n, k)$ are semiregular. We can then use Theorem 4.1 to separate out the cases in which $G_2(n, k)$ and $G(n, k)$ are also regular. We use the notation $\prod_{i=1}^0 a_i$ to denote that the corresponding product is empty and set equal to 1 by convention.

Theorem 4.4. *Let $k \geq 2$ be a fixed integer with the factorization*

$$(4.5) \quad k = Q \prod_{i=1}^{\ell} p_i^{\alpha_i},$$

where each p_i is a prime such that $\gcd(p_i - 1, k) = 1$ and in addition, $\ell \geq 1$, $\alpha_i \geq 1$, $\gcd(Q, p_1 p_2 \cdots p_{\ell}) = 1$, and $\gcd(q - 1, k) > 1$ for each prime q dividing Q . Let $n \geq 2$ have the prime power factorization

$$n = \prod_{i=1}^{\ell} p_i^{\beta_i} \prod_{i=1}^m q_i^{\gamma_i} \prod_{i=1}^s h_i^{\delta_i},$$

where $\beta_i \geq 0$, $m \geq 0$, $s \geq 0$, $\gamma_i \geq 1$, $\delta_i \geq 1$, $\gcd(q_i(q_i - 1), k) = 1$ for $i = 1, 2, \dots, r$, and $\gcd(h_i - 1, k) > 1$ for $i = 1, 2, \dots, s$.

(i) $G_2(n, k)$ is semiregular if and only if one of the following conditions holds:

- (a) $n = \prod_{i=1}^{\ell} p_i^{\beta_i} \prod_{i=1}^m q_i$ for $0 \leq \beta_i \leq \alpha_i + 1$ and $\omega(n) \geq 2$,
- (b) $n = p_i^{\beta_i}$ for some $i \in \{1, 2, \dots, \ell\}$, where $1 \leq \beta_i \leq k + \alpha_i + 1$ and p_i is odd,
- (c) $n = q_1^{\gamma_1}$ for $1 \leq \gamma_1 \leq k + 1$,
- (d) $n = h_i^{\delta_i}$ for $1 \leq \delta_i \leq k$,
- (e) $n = 2^{\beta_1}$ for $\beta_1 \in \{1, 2, 3, 4, 6\}$ when $k = 2$,
- (f) $n = 2^{\beta_1}$ for $1 \leq \beta_1 \leq 9$ when $k = 2^2$,
- (g) $n = 2^{\beta_1}$ for $1 \leq \beta_1 \leq k + \alpha_1 + 2$ when $p_1 = 2$ and $k \geq 6$,

(ii) $G(n, k)$ is semiregular if and only if one of the following conditions holds:

- (a) $n = \prod_{i=1}^{\ell} p_i^{\beta_i} \prod_{i=1}^m q_i$ for $0 \leq \beta_i \leq \alpha_i + 1$ and $m \geq 0$ when p_i is odd for each $i \in \{1, 2, \dots, \ell\}$,
- (b) $n = 2^{\beta_1}$ for $\beta_1 \in \{1, 2, 4\}$ when $k = 2$,
- (c) $n = 2^{\beta_1}$ for $1 \leq \beta_1 \leq 5$ when $k = 2^2$,
- (d) $n = 2^{\beta_1}$ for $1 \leq \beta_1 \leq \alpha_1 + 2$ when $p_1 = 2$ and $k \geq 6$.

Remark 4.5. Note that in the hypotheses of Theorem 4.4, there exists at least one prime p_1 dividing k such that $\gcd(p_1 - 1, k) = 1$. Simply choose p_1 to be the least prime dividing k . We further observe that if $2 \mid k$, there does not exist a prime q_i such that $\gcd(q_i(q_i - 1), k) = 1$. We finally notice that in Theorem 4.4, we allow both the possibility that h_i does divide k and also the possibility that h_i does not divide k , where $1 \leq i \leq s$.

PROOF OF THEOREM 4.4: (i) The necessity and sufficiency of condition (e) for the case in which $k = 2$ were shown in [4]. For the remainder of the proof of (i), we assume that $k \neq 2$ and treat only conditions (a)–(d) and (f)–(g).

Let q be a prime. If $1 \leq \beta \leq k$, then clearly $G_2(q^\beta, k)$ is semiregular, since the only vertex in $G_2(q^\beta, k)$ having positive indegree is the vertex 0. From here on, when we consider digraphs $G_2(n, k)$ we assume that either $\omega(n) \geq 2$ or n is of the form q^β for $\beta \geq k + 1$.

We note for future reference that if $n = q^\beta$, where q is a fixed prime and the positive integer β varies, then the function

$$\text{indeg}(q^\beta) = N(q^\beta, k, q^\beta) = q^{\beta - \lceil \beta/k \rceil}$$

is nondecreasing as β increases. We will also frequently make use of the facts that both $N(n, k, 0) > 0$ and $N(n, k, 1) > 0$ for all n and k , and in addition $N(p^\alpha, k, p^{jk}) > 0$ when p is a prime and $\alpha > jk$.

First assume that $\omega(n) \geq 2$. We show that $G_2(n, k)$ is semiregular if and only if $G(q^{\nu_q(n)}, k)$ is semiregular for every prime q dividing n , where $\nu_q(n)$ is the exponent β such that $q^\beta \mid n$ but $q^{\beta+1} \nmid n$, that is $q^{\nu_q(n)} \parallel n$. For each prime q dividing n , let $q(n) = q^{\nu_q(n)}$. Since, by (1.4),

$$\text{indeg}_n(a) = \prod_{q \mid n} \text{indeg}_{q(n)}(a)$$

for each vertex $a \in G_2(n, k)$, we see that $G_2(n, k)$ is semiregular if $G(q^{\nu_q(n)}, k)$ is semiregular for each prime q dividing n .

Now suppose that $q \mid n$ and $G(q^{\nu_q(n)}, k)$ is not semiregular. Then there exist nonnegative integers a and b , each having positive indegree in $G(q^{\nu_q(n)}, k)$, such that $\text{indeg}_{q(n)}(a) \neq \text{indeg}_{q(n)}(b)$. Let $n = q^{\nu_q(n)}M$, where $M > 1$ and $q \nmid M$. By

the Chinese remainder theorem, we can find vertices a_1 and a_2 in $G_2(n, k)$ such that $a_1 \equiv a \pmod{q^{\nu_q(n)}}$, $a_1 \equiv 0 \pmod{M}$, and $a_2 \equiv b \pmod{q^{\nu_q(n)}}$, $a_2 \equiv 0 \pmod{M}$. Then

$$\text{indeg}_n(a_1) = \text{indeg}_{q(n)}(a) \text{indeg}_M(0) \neq \text{indeg}_n(a_2) = \text{indeg}_{q(n)}(b) \text{indeg}_M(0),$$

and $G_2(n, k)$ is not semiregular.

Note that the above arguments also show that when $\omega(n) \geq 2$, $G_2(n, k)$ is semiregular if and only if $G(n, k)$ is semiregular.

We now prove that no prime h_1 divides n when $\omega(n) \geq 2$ and $G_2(n, k)$ is semiregular. Suppose that $h_1^{\delta_1} \parallel n$, where $\delta_1 \geq 1$. Note that by definition, $h_1 \neq 2$. Then by Theorems 3.1 and 3.2,

$$N(h_1^{\delta_1}, k, 0) = h_1^{\delta_1 - \lceil \delta_1/k \rceil}$$

and

$$N(h_1^{\delta_1}, k, 1) = \gcd(\lambda(h_1^{\delta_1}), k) = \gcd(h_1^{\delta_1 - 1}(h_1 - 1), k).$$

Since $\gcd(h_1 - 1, k) > 1$, there exists a prime p such that $p \mid \gcd(h_1 - 1, k)$. Hence, $p \mid N(h_1^{\delta_1}, k, 1)$, but $p \nmid N(h_1^{\delta_1}, k, 0)$. Thus, $G(h_1^{\delta_1}, k)$ is not semiregular, which implies that $G_2(n, k)$ is not semiregular. Consequently, if $G_2(n, k)$ is semiregular and $\omega(n) \geq 2$, then $\gcd(q - 1, k) = 1$ for each prime q dividing n . Thus, $p_i \neq 2$ for $1 \leq i \leq \ell$ if $G_2(n, k)$ is semiregular and $\omega(n) \geq 2$.

Next suppose that $G_2(n, k)$ is semiregular and $q_i^2 \mid n$ for some $i \in \{1, 2, \dots, m\}$. Then

$$N(q_i^{\gamma_i}, k, 1) = \gcd(\lambda(q_i^{\gamma_i}), k) = \gcd(q_i^{\gamma_i - 1}(q_i - 1), k) = 1,$$

whereas

$$q_i \mid N(q_i^{\gamma_i}, k, q_i^{\gamma_i}) = q_i^{\gamma_i - \lceil \gamma_i/k \rceil}.$$

Hence, $G(q_i^{\gamma_i}, k)$ is not semiregular, which again implies that $G_2(n, k)$ is not semiregular.

We observe by Theorem 4.1 that $G(q_i, k)$ is regular and thus semiregular for $1 \leq i \leq m$. We now show that $G(p_i^{\beta_i}, k)$ is semiregular for $1 \leq i \leq \ell$ when p_i is odd and $1 \leq \beta_i \leq \alpha_i + 1$. This will establish the sufficiency of condition (a) when $\omega(n) \geq 2$. Clearly, if $\beta_i \leq \alpha_i + 1$, then $\beta_i < p_i^{\alpha_i} \leq k$ for p_i an odd prime. Then $\text{indeg}(a) > 0$ for $a \in G_2(p_i^{\beta_i}, k)$ if and only if $a = 0$. If $c \in G_1(p_i^{\beta_i}, k)$ and $\text{indeg}(c) > 0$, then by Theorems 3.1 and 3.2,

$$\text{indeg}(c) = \gcd(\lambda(p_i^{\beta_i}), k) = \gcd(p_i^{\beta_i - 1}(p_i - 1), k) = p_i^{\beta_i - 1} = \text{indeg}(0),$$

and $G(p_i^{\beta_i}, k)$ is semiregular.

At this point, we assume that $p_i^{\alpha_i+2} | n$. By our earlier observation, $p_i \neq 2$. Noting that $\gcd(p_i - 1, k) = 1$ and $\beta_i \geq \alpha_i + 2$, we see by (4.5) that

$$(4.6) \quad \begin{aligned} N(p_i^{\beta_i}, k, 1) &= \gcd(\lambda(p_i^{\beta_i}), k) = \gcd(p_i^{\beta_i-1}(p_i - 1), k) \\ &= p_i^{\alpha_i} < N(p_i^{\alpha_i+2}, k, p_i^{\alpha_i+2}) = p_i^{\alpha_i+2-\lceil(\alpha_i+2)/k\rceil} \\ &= p_i^{\alpha_i+1} \leq N(p_i^{\beta_i}, k, p_i^{\beta_i}). \end{aligned}$$

In the last equality in (4.6), we made use of the fact that if $p_i^{\alpha_i} \| k$, where $\alpha_i \geq 1$, then $\alpha_i + 2 \leq p_i^{\alpha_i} \leq k$ when p_i is an odd prime. Thus, $G(p_i^{\beta_i}, k)$ is not semiregular in this case. We have now established the necessity of condition (a) when $\omega(n) \geq 2$.

We assume from here on that $\omega(n) = 1$. First suppose that $n = h_1^{\delta_1}$, where $\delta_1 \geq k + 1$. Let p be a prime such that $p \mid \gcd(h_1 - 1, k)$. Then by Theorem 3.2,

$$p \nmid N(h_1^{\delta_1}, k, h_1^{\delta_1}) = h_1^{\delta_1 - \lceil \delta_1/k \rceil},$$

whereas

$$p \mid N(h_1^{\delta_1}, k, h_1^k) = h_1^{k-1} \gcd(\lambda(h_1^{\delta_1-k}), k) = h_1^{k-1} \gcd(h_1^{\delta_1-k-1}(h_1 - 1), k).$$

Thus, $G_2(h_1^{\delta_1}, k)$ is not semiregular in this case. We have now established condition (d).

Now assume that $n = q_1^{\gamma_1}$, where $\gamma_1 \geq k + 2$. Then by Theorems 3.1 and 3.2,

$$(4.7) \quad \begin{aligned} N(q_1^{\gamma_1}, k, q_1^k) &= q_1^{k-1} \gcd(\lambda(q_1^{\gamma_1-k}), k) = q_1^{k-1} \gcd(q_1^{\gamma_1-k-e_1}(q_1 - 1), k) \\ &= q_1^{k-1} < N(q_1^{k+2}, k, q_1^{k+2}) = q_1^{k+2-\lceil(k+2)/k\rceil} \\ &= q_1^k \leq N(q_1^{\gamma_1}, k, q_1^{\gamma_1}), \end{aligned}$$

where $e_1 = 2$ if $q_1 = 2$ and $\gamma_1 - k \geq 3$ and $e_1 = 1$ otherwise. The last equality in (4.7) follows from the fact that $k + 2 \leq 2k$, since $k \geq 2$. Thus $G_2(q_1^{\gamma_1}, k)$ is not semiregular in this case.

We note that $G_2(q_1^{\gamma_1}, k)$ is semiregular when $\gamma_1 = k + 1$. Observe that $\text{indeg}(a) > 0$ for $a \in G_2(q_1^{k+1}, k)$ only if $q_1^k \| a$ or $a \equiv 0 \pmod{q_1^{k+1}}$. Then

$$\begin{aligned} N(q_1^{k+1}, k, q^k) &= q_1^{k-1} \gcd(\lambda(q_1^{k+1-k}), k) = q_1^{k-1} \gcd(q_1 - 1, k) = q_1^{k-1} \\ &= N(q_1^{k+1}, k, q_1^{k+1}) = q_1^{k+1-\lceil(k+1)/k\rceil} = q_1^{k-1}. \end{aligned}$$

Hence, $G_2(q_1^{k+1}, k)$ is semiregular by Theorem 3.2. We have now established condition (c).

Further, assume that $n = p_i^{\beta_i}$, where $i \in \{1, 2, \dots, \ell\}$ and either p_i is odd or $p_i = 2$ and $k \geq 6$. First suppose that $\beta_i \geq k + \alpha_i + 2 + \mu(p_i)$, where $\mu(p_i) = 0$ if p_i is odd and $\mu(p_i) = 1$ if $p_i = 2$. Note that $\alpha_i + 2 + \mu(p_i) \leq p_i^{\alpha_i} \leq k$ if p_i is odd and $\alpha_i + 2 + \mu(p_i) < k$ if $p_i = 2$. Then by Theorem 3.2,

$$\begin{aligned}
 N(p_i^{\beta_i}, k, p^k) &= p_i^{k-1} \varepsilon_i \gcd(\lambda(p_i^{\beta_i-k}), k) = p_i^{k-1} \varepsilon_i \gcd(p_i^{\beta_i-k-\varepsilon_i} (p_i - 1), k) \\
 &= p_i^{k+\alpha_i-1} < N(p_i^{k+\alpha_i+2+\mu(p_i)}, k, p_i^{k+\alpha_i+2+\mu(p_i)}) \\
 (4.8) \quad &= p_i^{k+\alpha_i+2+\mu(p_i) - \lceil (k+\alpha_i+2+\mu(p_i))/k \rceil} \\
 &= p_i^{k+\alpha_i+\mu(p_i)} \leq N(p_i^{\beta_i}, k, p_i^{\beta_i}),
 \end{aligned}$$

where $\varepsilon_i = 2$ if $p = 2$ and $\beta_i - k \geq 3$, and $\varepsilon_i = 1$ otherwise. Therefore, $G_2(p_i^{\beta_i}, k)$ is not semiregular in this case.

Now suppose that $k + 1 \leq \beta_i \leq k + \alpha_i + 1 + \mu(p_i)$. Since $k < \beta_i \leq k + \alpha_i + 1 + \mu(p_i) < 2k$ for $i \in \{1, 2, \dots, \ell\}$, we see that $\text{indeg}(a) > 0$ for $a \in G_2(p_i^{\beta_i}, k)$ only if $p_i^k \parallel a$ or $a \equiv 0 \pmod{p_i^{\beta_i}}$. Similarly to (4.8) we get

$$\begin{aligned}
 N(p_i^{\beta_i}, k, p^k) &= p_i^{k-1} \varepsilon_i \gcd(p_i^{\beta_i-k-\varepsilon_i} (p_i - 1), k) \\
 &= p_i^{k-1} \varepsilon_i p_i^{\beta_i-k-\varepsilon_i} = p_i^{\beta_i-2} = N(p_i^{\beta_i}, k, p_i^{\beta_i}) \\
 &= p_i^{\beta_i - \lceil \beta_i/k \rceil} = p_i^{\beta_i-2},
 \end{aligned}$$

where ε_i is defined as before. Thus $G_2(p_i^{\beta_i}, k)$ is semiregular in this instance. Conditions (b) and (g) are now established.

It only remains to show that when $k = 4$, then $G_2(n, 4)$ is semiregular if and only if condition (f) holds. First suppose that $k = 4$ and $n = 2_1^{\beta_1}$, where $\beta_1 \geq 10$. Then, by Theorem 3.2,

$$\begin{aligned}
 N(2^{\beta_1}, 4, 2^4) &= 2^3 \cdot 2 \cdot \gcd(\lambda(2^{\beta_1-4}), 2^2) = 2^3 \cdot 2 \cdot 2^2 = 2^6 < N(2^{10}, 4, 2^{10}) \\
 &= 2^{10 - \lceil 10/4 \rceil} = 2^7 \leq N(2^{\beta_1}, 4, 2^{\beta_1})
 \end{aligned}$$

and $G_2(2^{\beta_1}, 4)$ is not semiregular.

Finally, we show that $G_2(2^{\beta_1}, 4)$ is semiregular when $5 \leq \beta_1 \leq 9$. First assume that $5 \leq \beta_1 \leq 8$. Then $\text{indeg}(a) > 0$ for $a \in G_2(2^{\beta_1}, 4)$ only if $2^4 \parallel a$ or $a \equiv 0 \pmod{2^{\beta_1}}$. Observe that

$$\begin{aligned}
 N(2^{\beta_1}, 4, 2^4) &= 2^3 \cdot \varepsilon_1 \cdot \gcd(\lambda(2^{\beta_1-4}), 2^2) = 2^3 \cdot \varepsilon_1 \cdot 2^{\beta_1-4-\varepsilon_1} = 2^{\beta_1-2} \\
 &= 2^{\beta_1 - \lceil \beta_1/4 \rceil} = N(2^{\beta_1}, 4, 2^{\beta_1})
 \end{aligned}$$

where $\varepsilon_1 = 2$ if $\beta_1 - 4 \geq 3$ and $\varepsilon_1 = 1$ otherwise. Therefore, $G_2(2^{\beta_1}, 4)$ is semiregular in this case.

Now assume that $\beta_1 = 9$. Then $\text{indeg}(a) > 0$ for $a \in G_2(2^9, 4)$ only if $2^4 \parallel a$, or $2^8 \parallel a$, or $a \equiv 0 \pmod{2^9}$. Then by Theorem 3.2,

$$\begin{aligned} N(2^9, 4, 2^4) &= 2^3 \cdot 2 \cdot \gcd(\lambda(2^{9-4}), 2^2) = 2^3 \cdot 2 \cdot 2^2 = 2^6 \\ &= N(2^9, 4, 2^8) = 2^{3 \cdot 2} \gcd(\lambda(2^{9-8}), 2^2) = 2^6 \gcd(1, 4) = 2^6 = 2^{9 - \lceil 9/4 \rceil} \\ &= N(2^9, 4, 2^9), \end{aligned}$$

and $G_2(2^9, 4)$ is also semiregular. Condition (f) is now established and part (i) is proved.

(ii) Note that $G(n, k)$ is semiregular if and only if $G_1(n, k)$ and $G_2(n, k)$ are both semiregular, and for any two vertices $a \in G_1(n, k)$ and $b \in G_2(n, k)$ having positive indegree, $\text{indeg}(a) = \text{indeg}(b)$. Part (ii) now follows from the proof of part (i) of this theorem and from Theorems 4.1 and 4.3. \square

5. Digraphs for which some components are semiregular

We saw in Theorems 4.1 and 4.3 that $G_1(n, k)$ is always semiregular for any n and k . By Theorem 4.4, $G_2(n, k)$ is, in general, not semiregular. Theorems 5.1 and 5.4 below present cases in which some but not necessarily all of the components of $G_2(n, k)$ are semiregular or regular. We also determine when all of the components of $G_2(n, k)$ are semiregular even if $G_2(n, k)$ is not itself necessarily semiregular. By our comments above, if each component of $G_2(n, k)$ is semiregular, so is each component of $G(n, k)$. Clearly, $G(n, k)$ is regular if and only if each component of $G(n, k)$ is regular.

Before presenting Theorems 5.1 and 5.4, we need to define some subdigraphs of $G_2(n, k)$ as given in [6]. Let $\mathcal{P} = \{p_1, p_2, \dots, p_r\}$ be the set of prime divisors of $n \geq 2$ and consider a partition of this set given by $\mathcal{P} = \mathcal{P}_1 \cup \mathcal{P}_2$, where \mathcal{P}_1 and \mathcal{P}_2 are disjoint and \mathcal{P}_1 is nonempty. Let $G_{\mathcal{P}_1}^*(n, k)$ be the subdigraph of $G(n, k)$ induced by the vertices which are multiples of $\prod_{p \in \mathcal{P}_1} p$ and which are also relatively prime to all primes $q \in \mathcal{P}_2$. Let ℓ be a prime and m a positive integer. Noting that $\gcd(a, \ell^m) > 1$ if and only if $\gcd(a^k, \ell^m) > 1$, we see by the Chinese remainder theorem that $G_{\mathcal{P}_1}^*(n, k)$ is a union of components of $G_2(n, k)$ for all nonempty subsets \mathcal{P}_1 of \mathcal{P} . It is also evident that $G_2(n, k)$ is the disjoint union of $G_{\mathcal{P}_1}^*(n, k)$ as \mathcal{P}_1 ranges over all nonempty subsets of \mathcal{P} . One further sees that if $a \in G_{\mathcal{P}_1}^*(n, k)$, then $a \in G_2(p^{\nu_p(n)}, k)$ for each prime $p \in \mathcal{P}_1$ and $a \in G_1(q^{\nu_q(n)}, k)$ for each prime $q \in \mathcal{P}_2$. Moreover, if a is a cycle vertex of $G_{\mathcal{P}_1}^*(n, k)$ and $p \in \mathcal{P}_1$, then $a \equiv 0 \pmod{p^{\nu_p(n)}}$. This follows since if a is part of a t -cycle in $G_{\mathcal{P}_1}^*(n, k)$ and $p \in \mathcal{P}_1$, then $a^{k^t} \equiv a \pmod{p^{\nu_p(n)}}$, which implies that

$$a^{k^t} - a = a(a^{k^t-1} - 1) \equiv 0 \pmod{p^{\nu_p(n)}}.$$

Since $\gcd(a, a^{k^t-1} - 1) = 1$ and $p \mid a$, we see that $p^{\nu_p(n)} \mid a$.

Theorem 5.1. *The digraph $G_{\mathcal{P}_1}^*(n, k)$ is semiregular if and only if $G_2(p^{\nu_p(n)}, k)$ is semiregular for each prime $p \in \mathcal{P}_1$.*

PROOF: First suppose that $G_2(p^{\nu_p(n)}, k)$ is semiregular for each $p \in \mathcal{P}_1$. Let a and b be vertices in $G_{\mathcal{P}_1}^*(n, k)$ such that $\text{indeg}(a) > 0$ and $\text{indeg}(b) > 0$. Then both a and b are vertices in $G_2(p^{\nu_p(n)}, k)$ for $p \in \mathcal{P}_1$, and a and b are both vertices in $G_1(q^{\nu_q(n)}, k)$ for $q \in \mathcal{P}_2$. Since $G_1(q^{\nu_q(n)}, k)$ is semiregular for all $q \in \mathcal{P}_2$ by Theorems 4.1 and 4.3, we see by (1.4) that $\text{indeg}_n(a) = \text{indeg}_n(b)$. Thus, $G_{\mathcal{P}_1}^*(n, k)$ is semiregular.

We now prove that if any component of $G_{\mathcal{P}_1}^*(n, k)$ is semiregular, then the digraph $G_2(p^{\nu_p(n)}, k)$ is semiregular for each prime $p \in \mathcal{P}_1$. This is a somewhat stronger result than the converse implication. Let C be a semiregular component in $G_{\mathcal{P}_1}^*(n, k)$. Let

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

and $Q_i = p_i^{\alpha_i}$. By way of contradiction, we can assume without loss of generality that $p_1 \in \mathcal{P}_1$ and $G_2(p_1^{\alpha_1}, k)$ is not semiregular. By relabeling the primes dividing n if necessary, we can also assume that $p_1, p_2, \dots, p_s \in \mathcal{P}_1$ and $p_{s+1}, p_{s+2}, \dots, p_r \in \mathcal{P}_2$.

Suppose that a_1 and b_1 are vertices in $G_2(p_1^{\alpha_1}, k)$ having positive indegree such that $\text{indeg}_{Q_1}(a_1) \neq \text{indeg}_{Q_1}(b_1)$. Since p_1 divides both a_1 and b_1 , there exists a least nonnegative integer h such that

$$a_1^{k^h} \equiv b_1^{k^h} \equiv 0 \pmod{p_1^{\alpha_1}}.$$

Let c be a cycle vertex in C . Let c_h be the cycle vertex in C which is h vertices before c , that is, $c^{k^h} \equiv c \pmod{n}$. Note that $c \equiv 0 \pmod{Q_i}$ for $i = 1, 2, \dots, s$ and $\gcd(c_h, Q_i) = \gcd(c, Q_i) = 1$ for $i = s+1, s+2, \dots, r$. By the Chinese remainder theorem, we can find vertices a_2 and b_2 in $G_{\mathcal{P}_1}^*(n, k)$ such that $a_2 \equiv a_1 \pmod{Q_1}$, $b_2 \equiv b_1 \pmod{Q_1}$, $a_2 \equiv b_2 \equiv 0 \pmod{Q_i}$ for $2 \leq i \leq s$, and $a_2 \equiv b_2 \equiv c_h \pmod{Q_i}$ for $s+1 \leq i \leq r$. Then

$$a_2^{k^h} \equiv b_2^{k^h} \equiv 0 \pmod{Q_i}$$

for $1 \leq i \leq s$, and

$$a_2^{k^h} \equiv b_2^{k^h} \equiv c_h^{k^h} \equiv c \pmod{Q_i}$$

for $s+1 \leq i \leq r$. Applying the Chinese remainder theorem again, one sees that $a_2^{k^h} \equiv b_2^{k^h} \equiv c \pmod{n}$, and both a_2 and b_2 are vertices in the component C .

By (1.4),

$$\text{indeg}_n(a_2) = \text{indeg}_{G_1}(a_1) \prod_{i=2}^s \text{indeg}_{Q_i}(0) \prod_{i=s+1}^r \text{indeg}_{Q_i}(c_h)$$

and

$$\text{indeg}_n(b_2) = \text{indeg}_{G_1}(b_1) \prod_{i=2}^s \text{indeg}_{Q_i}(0) \prod_{i=s+1}^r \text{indeg}_{Q_i}(c_h).$$

Since 0 is a cycle vertex in $G_2(Q_i, k)$ for $2 \leq i \leq s$ and c_h is a cycle vertex in $G_1(Q_i, k)$ for $s+1 \leq i \leq r$, we see that both the vertices a_2 and b_2 have positive indegree in the component C and $\text{indeg}_n(a_2) \neq \text{indeg}_n(b_1)$. Thus, the component C is not semiregular, which is a contradiction. The result now follows. \square

By the proof and the discussion preceding Theorem 5.1, we have the following two immediate corollaries.

Corollary 5.2. *The digraph $G_{\mathcal{P}_1}^*(n, k)$ is semiregular if and only if at least one of its components is semiregular.*

Corollary 5.3. *Each component of $G(n, k)$ is semiregular if and only if the digraph $G_2(p^{\nu_p(n)}, k)$ is semiregular for each prime p dividing n .*

Theorem 5.4. *Let $n = n_1 n_2$, where*

$$n_1 = \prod_{p \in \mathcal{P}_1} p^{\nu_p(n)} \quad \text{and} \quad n_2 = \prod_{p \in \mathcal{P}_2} p^{\nu_p(n)}.$$

Then $G_{\mathcal{P}_1}^(n, k)$ is regular if and only if n_1 is square-free and $\gcd(\lambda(n_2), k) = 1$.*

PROOF: First suppose that n_1 is square-free and $\gcd(\lambda(n_2), k) = 1$. Then $\nu_p(n) = 1$ for each prime $p \in \mathcal{P}_1$ and thus by Theorem 4.1(ii), $G_2(p^{\nu_p(n)}, k)$ is regular for each $p \in \mathcal{P}_1$. Moreover, by the definition of the Carmichael lambda-function, $\lambda(p^{\nu_p(n)}) \mid \lambda(n_2)$ and hence, $\gcd(\lambda(p^{\nu_p(n)}), k) = 1$ for each prime $p \in \mathcal{P}_2$. Therefore, by Theorem 4.1, $G_1(p^{\nu_p(n)}, k)$ is regular for each $p \in \mathcal{P}_2$. Let a be a vertex in $G_{\mathcal{P}_1}^*(n, k)$. Then $a \in G_2(p^{\nu_p(n)}, k)$ for $p \in \mathcal{P}_1$ and $a \in G_1(p^{\nu_p(n)}, k)$ for $p \in \mathcal{P}_2$. By (1.4),

$$\text{indeg}_n(a) = \prod_{p \in \mathcal{P}_1} N(p^{\nu_p(n)}, k, a) \cdot \prod_{p \in \mathcal{P}_2} N(p^{\nu_p(n)}, k, a) = \prod_{p \in \mathcal{P}_1} 1 \cdot \prod_{p \in \mathcal{P}_2} 1 = 1.$$

Consequently, we see by Remark 1.1 that $G_{\mathcal{P}_1}^*(n, k)$ is regular.

We now suppose that C is a regular component in $G_{\mathcal{P}_1}^*(n, k)$. We will show that n_1 is square-free and $\gcd(\lambda(n_2), k) = 1$. We can assume without loss of

generality that $p_1, p_2, \dots, p_s \in \mathcal{P}_1$ and $p_{s+1}, p_{s+2}, \dots, p_r \in \mathcal{P}_2$. Let c be a cycle vertex of C . Then $c \equiv 0 \pmod{p^{\nu_p(n)}}$ for each $p \in \mathcal{P}_1$. Let the factorization of n be as given in (1.2). Then

$$\text{indeg}_n(c) = 1 = \prod_{i=1}^s N(p_i^{\alpha_i}, k, 0) \cdot \prod_{i=s+1}^r N(p_i^{\alpha_i}, k, c).$$

Hence, $N(p_i^{\alpha_i}, k, 0) = 1$ for $1 \leq i \leq s$ and $N(p_i^{\alpha_i}, k, c) = 1$ for $s+1 \leq i \leq r$. If $\alpha_i \geq 2$ for some $i \in \{1, 2, \dots, s\}$, then by Theorem 3.2,

$$N(p_i^{\alpha_i}, k, 0) = p_i^{\alpha_i - \lceil \alpha_i/k \rceil} \geq p > 1,$$

which is a contradiction. Thus, $\alpha_i = 1$ for $1 \leq i \leq s$, and consequently, n_1 is square-free. Since $N(p_i^{\alpha_i}, k, c) = 1$ for $s+1 \leq i \leq r$, it follows from Theorem 3.1 that $\gcd(\lambda(p_i^{\alpha_i}), k) = 1$ for $s+1 \leq i \leq r$. Since

$$n_2 = \prod_{i=s+1}^r p_i^{\alpha_i},$$

it follows from the definition of λ that

$$\lambda(n_2) \mid \prod_{i=s+1}^r \lambda(p_i^{\alpha_i}).$$

Hence, $\gcd(\lambda(n_2), k) = 1$. □

By the proof of Theorem 5.4 we have the following corollary.

Corollary 5.5. *The digraph $G_{\mathcal{P}_1}^*(n, k)$ is regular if and only if at least one component of $G_{\mathcal{P}_1}^*(n, k)$ is regular.*

Acknowledgment. This paper was supported by Institutional Research Plan nr. AV0Z 10190503 and Grant nr. 1P05ME749 of the Ministry of Education of the Czech Republic.

REFERENCES

- [1] Křížek M., Luca F., Somer L., *17 Lectures on Fermat Numbers: From Number Theory to Geometry*, CMS Books in Mathematics, vol. 9, Springer, New York, 2001.
- [2] Lucheta C., Miller E., Reiter C., *Digraphs from powers modulo p* , *Fibonacci Quart.* **34** (1996), 226–239.
- [3] Niven I., Zuckerman H.S., Montgomery H.L., *An Introduction to the Theory of Numbers*, fifth edition, John Wiley & Sons, New York, 1991.

- [4] Somer L., Krížek M., *On a connection of number theory with graph theory*, Czechoslovak Math. J. **54** (2004), 465–485.
- [5] Somer L., Krížek M., *Structure of digraphs associated with quadratic congruences with composite moduli*, Discrete Math. **306** (2006), 2174–2185.
- [6] Wilson B., *Power digraphs modulo n* , Fibonacci Quart. **36** (1998), 229–239.

DEPARTMENT OF MATHEMATICS, CATHOLIC UNIVERSITY OF AMERICA, WASHINGTON, D.C.
20064, U.S.A.

E-mail: somer@cua.edu

INSTITUTE OF MATHEMATICS, ACADEMY OF SCIENCES, ŽITNÁ 25, CZ–115 67 PRAGUE 1,
CZECH REPUBLIC

E-mail: krizek@math.cas.cz

(Received April 3, 2006)