Discrete Mathematics 309 (2009) 1999–2009

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

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

Lawrence Somer [a], Michal Křížek [b]

[a] Department of Mathematics, Catholic University of America, Washington, DC 20064, USA

[b] Institute of Mathematics, Academy of Sciences, Žitná 25, CZ – 115 67 Prague 1, Czech Republic

ARTICLE INFO

*Article history:*
Received 30 November 2007
Received in revised form 20 March 2008
Accepted 3 April 2008
Available online 16 May 2008

*Keywords:*
Chinese Remainder Theorem
Congruence
Symmetric digraphs

ABSTRACT

We assign to each pair of positive integers $n$ and $k \geq 2$ a digraph $G(n, k)$ whose set of vertices is $H = \{0, 1, \ldots, n-1\}$ and for which there is a directed edge from $a \in H$ to $b \in H$ if $a^k \equiv b \pmod{n}$. The digraph $G(n, k)$ is symmetric of order $M$ if its set of components can be partitioned into subsets of size $M$ with each subset containing $M$ isomorphic components. We generalize earlier theorems by Szalay, Carlip, and Mincheva on symmetric digraphs $G(n, 2)$ of order 2 to symmetric digraphs $G(n, k)$ of order $M$ when $k \geq 2$ is arbitrary.



## 1. Introduction

This paper extends the results given in the works [4,6,9], which provide an interesting connection between number theory, graph theory and group theory. In the papers [6,7], we investigated properties of the iteration digraph representing a dynamical system occurring in number theory.

For $n \geq 1$ 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 $k \geq 2$ 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 $k \geq 2$ has a specific iteration digraph corresponding to it.

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). For particular values of $n$ and $k$, we denote the iteration digraph of $f$ by $G(n, k)$, see Fig. 1.

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

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

where $p_1 < p_2 < \cdots < p_r$ 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 maximal connected subgraph of the associated nondirected graph.

*E-mail addresses:* somer@cua.edu (L. Somer), krizek@math.cas.cz (M. Křížek).

0012-365X/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2008.04.009

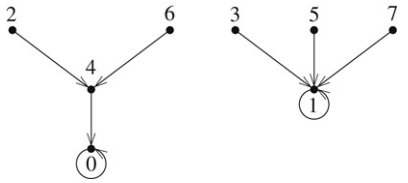


**Fig. 1.** The iteration digraph $G(8, 2)$.

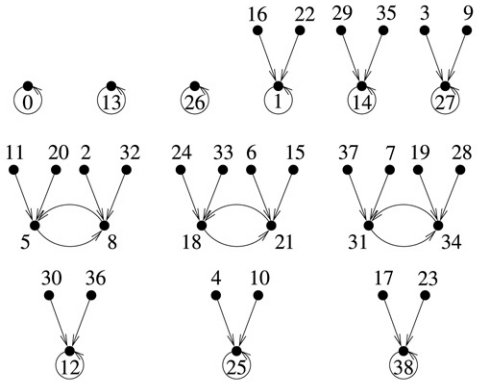


**Fig. 2.** The symmetric iteration digraph $G(39, 3)$ of order 3.

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 obvious that $G(n, k)$ with $n$ vertices also has exactly $n$ directed edges. Thus, if $b_i$, $i = 1, 2, \ldots, q$, denote all the vertices of $G(n, k)$ having positive indegree, then

$$\sum_{i=1}^{q} b_i = n. \tag{1.3}$$

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. 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 $i \in \mathbb{N}$, 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.

**Definition 1.1.** Let $M \geq 2$ be an integer. The digraph $G(n, k)$ is said to be *symmetric of order M* if its set of components can be partitioned into subsets of size $M$, each containing $M$ isomorphic components.

Fig. 2 shows a symmetric digraph $G(39, 3)$ of order 3, while Fig. 3 exhibits a symmetric digraph of order 5. In Szalay [8], it was shown that $G(n, 2)$ is symmetric of order 2 if $2 \parallel n$ or $2^2 \parallel n$, where $2^i \parallel n$ if $2^i \mid n$, but $2^{i+1} \nmid n$. In [1], it was also proved that $G(n, 2)$ is symmetric of order 2 if $n = 16q$, where $q$ is a Fermat prime, that is, a prime $q = 2^{2^m} + 1$ for some nonnegative integer $m$ (see [3] for properties of Fermat primes). In this paper, we will generalize these results by determining symmetric digraphs $G(n, k)$ of order $M \geq 2$ for all integers $k \geq 2$.

The digraph in Fig. 1 is not symmetric of order $M$ for any $M \geq 2$ while the digraphs in Figs. 4–6 are each symmetric of order 2.

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 $G_2(n, k)$. 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 Fig. 6 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 $G_1(n, k)$.