Czechoslovak Mathematical Journal, 54 (129) (2004), 465–485

ON A CONNECTION OF NUMBER THEORY WITH GRAPH THEORY

Lawrence Somer, Washington, D.C.,
and Michal Křížek, Praha

(Received October 10, 2001)

Abstract. We assign to each positive integer n a digraph 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 $a^2 \equiv b \pmod n$. We establish necessary and sufficient conditions for the existence of isolated fixed points. We also examine when the digraph is semiregular. Moreover, we present simple conditions for the number of components and length of cycles. Two new necessary and sufficient conditions for the compositeness of Fermat numbers are also introduced.

Keywords: Fermat numbers, Chinese remainder theorem, primality, group theory, digraphs

MSC 2000: 11A07, 11A15, 11A51, 05C20, 20K01

1. Introduction

This paper extends results given in the works [1] by Bryant, [4] and [5] by Chassé, [12] by Szalay (motivated by [7] and [10]), and [11] by Rogers, which provide an interesting connection between number theory, graph theory and group theory. In the paper [12], Szalay investigated properties of the iteration digraph representing a dynamical system occurring in number theory. Each natural number has a specific iteration digraph corresponding to it. We will classify sets of positive integers whose iteration digraphs have particular structural characteristics.

We describe this iteration digraph below. For $n \geqslant 1$ let

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

This paper was supported by grant No. 201/02/1058 of the Grant Agency of the Czech Republic.

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 $x \in H$ (cf. Fig. 1).

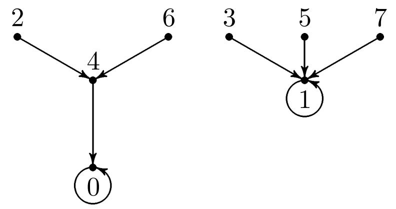

Figure 1. The iteration digraph corresponding to $n = 8$.

Note that f need not be a polynomial modulo n when n is not a prime. To see this, set $n = 4$, $f(0) = 0$, and $f(i) = 1$ for $i \neq 0$. Then $f(2) \not\equiv f(0) \pmod 2$ which implies that f is not a polynomial modulo 4.

For standard references concerning graphs and digraphs see [3] and [6].

Starting with an arbitrary element x_0 from H, we define the sequence of successive elements of H by

$$x_{j+1} = f(x_j), \quad j = 0, 1, \ldots.$$

This iteration scheme is called a *discrete iteration.* Since H is finite, the sequence $\{x_j\}$ has to be cyclic starting from some element x_k. If $x_k, x_{k+1}, \ldots, x_l$ are pairwise distinct and

$$\begin{aligned} x_{k+1} &= f(x_k), \\ &\vdots \\ x_l &= f(x_{l-1}), \\ x_k &= f(x_l), \end{aligned}$$

then the elements $x_k, x_{k+1}, \ldots, x_l$ constitute a *cycle* of length $l - k + 1$. Let us call a cycle of length 1 a *fixed point.* The cycles of length t are said to be t*-cycles.* Cycles are assumed to be oriented counterclockwise (see Fig. 2 for $n = 11$).

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

$$f(x) \in H \quad \text{and} \quad f(x) \equiv x^2 \pmod n. \tag{1.1}$$

This corresponds to the iteration scheme $x_{j+1} \equiv x_j^2 \pmod n$. From here on, whenever we refer to the iteration digraph of f, we assume that the mapping f is as given in (1.1) (for other choices of f see [7], [10], [12]).

We identify the vertex a of H with residues modulo n. For shorthand 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^2, we identify it with the remainder d such that $d \equiv a^2 \pmod n$ and $0 \leqslant d < n$.

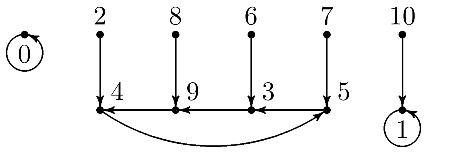

Figure 2. The iteration digraph corresponding to $n = 11$.

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

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

$$n = \prod_{i=1}^{s} p_i^{k_i}, \tag{1.2}$$

where $p_1 < p_2 < \ldots < p_s$ are primes and $k_i > 0$, i.e., $s = \omega(n)$. The next two theorems are proved in [12].

Theorem 1.1 (Szalay). *The number of fixed points of $G(n)$ is equal to $2^{\omega(n)}$.*

A *component* of the iteration digraph is a subdiagraph which is a maximal connected subgraph of the symmetrization of this digraph (i.e., the associated nondirected graph). When n is a prime, Rogers [11] describes completely the structure of each component of $G(n)$.

The digraph $G(n)$ is called *symmetric* if its set of components can be split into two sets in such a way that there exists a bijection between these two sets such that the corresponding digraphs are isomorphic (compare with Fig. 3).

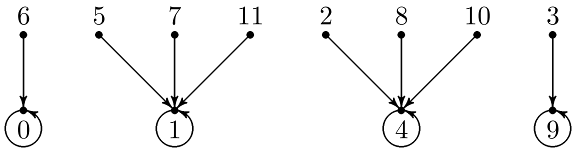

Figure 3. The iteration digraph corresponding to $n = 12$.

Theorem 1.2 (Szalay). *The iteration digraph $G(n)$ is symmetric if $n \equiv 2 \pmod 4$ or $n \equiv 4 \pmod 8$.*

Theorem 1.2 gives only a sufficient conditions for the symmetry of $G(n)$ which is not necessary (compare with $G(16)$ in Fig. 4 below).

2. Structure of iteration digraphs

The *indegree* of a vertex $a \in H$ of $G(n)$, 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. For simplicity, the subscript n will be omitted from now on. By the definition of f, the outdegree of each vertex of $G(n)$ is equal to 1. For an isolated fixed point, the indegree and outdegree are both equal to 1.

Theorem 2.1. *The number 0 is an isolated fixed point of $G(n)$ if and only if n is square-free.*

Proof. If $p^2 \mid n$ for some prime p, then

$$\left(\frac{n}{p}\right)^2 = n \cdot \frac{n}{p^2} \equiv 0 \pmod n,$$

and 0 is not an isolated fixed point, since n/p is mapped into 0.

Conversely, if n is square-free, then it is evident that $x \equiv 0 \pmod n$ is the only solution to the congruence $x^2 \equiv 0 \pmod n$, and hence 0 is an isolated fixed point of $G(n)$. □

The isolated and nonisolated fixed points 0 of $G(11)$ and $G(12)$ are illustrated in Figs. 2 and 3, respectively.

Let $N_n(a)$ denote the number of incongruent solutions of the congruence

$$x^2 \equiv a \pmod n.$$

Then obviously

$$N_n(a) = \operatorname{indeg}(a). \tag{2.1}$$

Theorem 2.2. *There are no isolated cycles of $G(n)$ of length greater than 1. The digraph $G(n)$ has an isolated fixed point $a \neq 0$ if and only if $2 \mid n$ and n is square-free. In this case, $a = n/2$.*

P r o o f. Assume that $a \neq 0$ is part of an isolated cycle of $G(n)$. We first show that n is an even square-free integer and next demonstrate that $a = n/2$ and that a is a fixed point.

Let $b^2 \equiv a \pmod{n}$. Since $(-b)^2 \equiv b^2 \pmod{n}$ and $\operatorname{indeg}(a) = N_n(a) = 1$, we get that $-b \equiv b \pmod{n}$. This implies that $2b \equiv 0 \pmod{n}$. Since $a \not\equiv 0 \pmod{n}$, we see that $2 \mid n$ and $b \equiv n/2 \pmod{n}$.

Now suppose that $p^2 \mid n$ for some prime p. If $p = 2$, then $a \equiv (n/2)^2 \equiv 0 \pmod{n}$, which is a contradiction. Next assume that p is odd and $2 \parallel n$. Note that if m is an odd integer, then

$$\frac{n}{2}m \equiv \frac{n}{2} \pmod{n}. \tag{2.2}$$

Since $n/2$ is odd, it now follows that

$$a \equiv \frac{n}{2}\frac{n}{2} \equiv \frac{n}{2} \equiv \frac{n}{2}\frac{n}{2p^2} \equiv \frac{n^2}{(2p)^2} \pmod{n},$$

which contradicts the assumption that $N_n(a) = 1$. Hence, n is square-free. We now observe by (2.2) that

$$a \equiv b^2 \equiv \frac{n}{2}\frac{n}{2} \equiv \frac{n}{2} \pmod{n}. \tag{2.3}$$

Consequently, $a \equiv n/2 \pmod{n}$ and a is a fixed point of $G(n)$.

We assume conversely that $2 \mid n$ and that n is square-free. Then $n/2$ is odd and $n/2 \not\equiv 0 \pmod{n}$. By (2.2) and (2.3), we find that

$$\frac{n}{2}\frac{n}{2} \equiv \frac{n}{2} \pmod{n}, \tag{2.4}$$

and $n/2$ is a fixed point of $G(n)$. Suppose that $b^2 \equiv n/2 \pmod{n}$. Since $n/2$ is odd and n is even, we obtain $b \equiv 1 \pmod{2}$. Since $n/2$ is square-free and $(n/2) \mid n$, it is easily seen that $b \equiv 0 \pmod{n/2}$. Noting that $\gcd(2, n/2) = 1$, we get from the Chinese remainder theorem (see, e.g., [8, p. 15]) that b is uniquely determined modulo n, and hence by (2.4), $b \equiv n/2 \pmod{n}$. Therefore, $n/2$ is an isolated fixed point of $G(n)$, and the result follows. $\square$

The following corollary follows immediately from Theorems 2.1 and 2.2.

Corollary 2.3. *Each digraph $G(n)$ has at most two isolated fixed points, and $G(n)$ has exactly two isolated fixed points if and only if $2 \mid n$ and n is square-free. Then the only isolated fixed points are 0 and $n/2$.*

Recall that a graph is regular if all its vertices have the same degree. The digraph $G(n)$ is said to be *semiregular* if there exists a positive integer d such that each vertex of $G(n)$ either has indegree d or 0 (see Fig. 4 for $d = 4$ and $n = 16$).

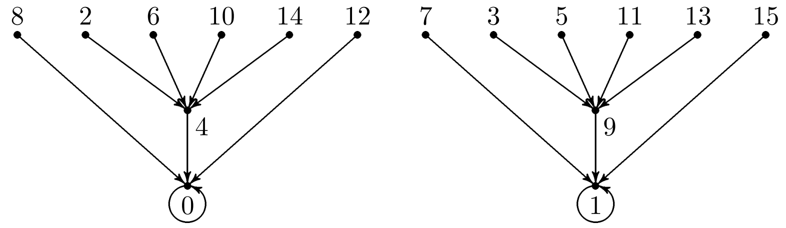

Figure 4. The iteration digraph corresponding to $n = 16$.

For a natural integer n we set

$$\varepsilon(n) = \begin{cases} -1 & \text{if } 2 \parallel n, \\ 0 & \text{if } 2 \nmid n \quad \text{or} \quad 4 \parallel n, \\ 1 & \text{if } 8 \mid n. \end{cases} \tag{2.5}$$

Further, we specify two particular subdigraphs of $G(n)$. Let $G_1(n)$ be the induced subdigraph of $G(n)$ on the set of vertices which are coprime to n and $G_2(n)$ be the induced subdigraph on the remaining, not coprime with n, vertices. We observe that $G_1(n)$ and $G_2(n)$ are disjoint and that $G(n) = G_1(n) \cup G_2(n)$, that is, no edge goes between $G_1(n)$ and $G_2(n)$. For example, the second component of Fig. 3 is $G_1(12)$ whereas the remaining three components make up $G_2(12)$. It is clear that 0 is always a vertex of $G_2(n)$. If $n > 1$ then 1 and $n - 1$ are always vertices of $G_1(n)$.

Theorem 2.4. *The digraph $G_1(n)$ is semiregular for all positive integers n. Moreover, if a is a vertex of $G_1(n)$ then*

$$\operatorname{indeg}(a) = 0 \quad \text{or} \quad \operatorname{indeg}(a) = 2^{\omega(n)+\varepsilon(n)}.$$

If $n \geqslant 2$, then $G_2(n)$ is semiregular if and only if $n = p^k$, where p is an odd prime for $k \in \{1, 2\}$, or $n = 2^k$ for $k \in \{1, 2, 3, 4, 6\}$.

The digraph $G(n)$ is semiregular if and only if $n = 2^k$ for $k = 0, 1, 2, 4$.

Before proving Theorem 2.4, we introduce the following lemma.

Lemma 2.5. *If* $\gcd(a,n)=1$ *and* $N_n(a)>0$, *then* $N_n(a)=2^{\omega(n)+\varepsilon(n)}$.

Proof. The result clearly holds when $n=1$, so assume that $n>1$. Since the residues coprime to n form a group under multiplication modulo n, it is easily seen that $N_n(a)=N_n(1)$ if $N_n(a)>0$ and $\gcd(a,n)=1$. Thus it suffices to determine only $N_n(1)$.

We first find $N_{p^k}(1)$, where p is a prime and $k\geqslant 1$. Notice that

$$a^2\equiv 1 \pmod{p^k} \tag{2.6}$$

if and only if

$$a^2-1=(a+1)(a-1)\equiv 0 \pmod{p^k}. \tag{2.7}$$

Suppose that p is an odd prime. Since $\gcd(a+1,a-1)\mid 2$, it follows that (2.6) holds if and only if $a\equiv\pm1 \pmod{p^k}$. Thus $N_{p^k}(1)=2$.

Now assume that $p=2$. Note that if (2.7) is satisfied, then 4 divides precisely one of the terms $a+1$ and $a-1$, and 2 exactly divides the other term. Hence, (2.6) holds if and only if $a\equiv 1 \pmod 2$ when $1\leqslant k\leqslant 3$ and $a\equiv\pm1 \pmod{2^{k-1}}$ when $k\geqslant 4$. Thus, $N_{2^k}(1)=2^{1+\varepsilon(2^k)}$. The result now follows from (2.5) and the Chinese remainder theorem. □

Proof of Theorem 2.4. It follows from Lemma 2.5 that if a is a vertex in $G_1(n)$ and $N_n(a)>0$, then

$$\operatorname{indeg}(a)=N_n(a)=2^{\omega(n)+\varepsilon(n)}. \tag{2.8}$$

Hence, $G_1(n)$ is semiregular for all n.

We now show the sufficiency of conditions for the semiregularity of $G_2(n)$. First let $n=p^k$, where p is an odd prime and $k\in\{1,2\}$. Then $\operatorname{indeg}(a)>0$ for the vertex a of $G_2(n)$ if and only if $a=0$. Therefore, $G_2(n)$ is semiregular in this case. In particular,

$$\operatorname{indeg}(0)=N_n(0)=p^{\lfloor k/2\rfloor}. \tag{2.9}$$

The sufficiency for the semiregularity of $G_2(n)$ for $n=2^k$, where $k\in\{1,2,3,4,6\}$ can be easily established by inspection. Moreover, if a is a vertex of $G_2(2^k)$ for $k\in\{1,2,3,4,6\}$ and $\operatorname{indeg}(a)>0$, then

$$\operatorname{indeg}(a)=2^{\lfloor k/2\rfloor}. \tag{2.10}$$

We now show the necessity for the semiregularity of $G_2(n)$. Assume that $n \geqslant 2$ and that $G_2(n)$ is semiregular. We first consider the case in which $\omega(n) \geqslant 2$ and $p^2 \mid n$ for some odd prime p. Suppose that $p^k \parallel n$, where $k \geqslant 2$. Let $q \neq p$ be a prime such that $q^l \parallel n$, where $l \geqslant 1$. Let $n = p^k n_1 = q^l n_2$. By the Chinese remainder theorem, we can find vertices a_1 and a_2 of $G_2(n)$ such that $a_1 \equiv 0 \pmod{p^k}$, $a_1 \equiv 1 \pmod{n_1}$, and $a_2 \equiv 0 \pmod{q^l}$, $a_2 \equiv 1 \pmod{n_2}$. According to (2.9), the Chinese remainder theorem again, and Lemma 2.5, we see that

$$\begin{aligned}\operatorname{indeg}(a_1) &= N_n(a_1) = N_{p^k}(a_1)N_{n_1}(a_1) = N_{p^k}(0)N_{n_1}(1)\\ &= \frac{p^k}{p^{\lceil k/2\rceil}}2^{\omega(n_1)+\varepsilon(n_1)} = p^{\lfloor k/2\rfloor}2^{\omega(n_1)+\varepsilon(n_1)}\end{aligned} \tag{2.11}$$

and

$$\begin{aligned}\operatorname{indeg}(a_2) &= N_n(a_2) = N_{q^l}(a_2)N_{n_2}(a_2) = N_{q^l}(0)N_{n_2}(1)\\ &= q^{\lfloor l/2\rfloor}2^{\omega(n_2)+\varepsilon(n_2)}.\end{aligned} \tag{2.12}$$

From (2.11) and (2.12), it follows that $p \mid \operatorname{indeg}(a_1)$, whereas $p \nmid \operatorname{indeg}(a_2)$. Hence, $G_2(n)$ is not semiregular in this case.

We next suppose that $\omega(n) \geqslant 2$ and $2^i \parallel n$, where $i \geqslant 1$ and $n/2^i$ is square-free. Let $n = 2^i n_3$. By the Chinese remainder theorem, there exist vertices a_3 and a_4 of $G_2(n)$ such that $a_3 \equiv 0 \pmod{2^i}$, $a_3 \equiv 0 \pmod{n_3}$, and $a_4 \equiv 0 \pmod{2^i}$, $a_4 \equiv 1 \pmod{n_3}$. Then by the proof of Theorem 2.1 and Lemma 2.5,

$$\operatorname{indeg}(a_3) = N_n(a_3) = N_{2^i}(a_3)N_{n_3}(a_3) = N_{2^i}(0)N_{n_3}(0) = 2^{\lfloor i/2\rfloor}\cdot 1 \tag{2.13}$$

and

$$\operatorname{indeg}(a_4) = N_n(a_4) = N_{2^i}(0)N_{n_3}(1) = 2^{\lfloor i/2\rfloor}2^{\omega(n_3)+\varepsilon(n_3)}. \tag{2.14}$$

Since $n_3 > 1$ and $2 \nmid n_3$, we see that $2^{\omega(n_3)+\varepsilon(n_3)} \geqslant 2$. It now follows from (2.13) and (2.14) that $G_2(n)$ is not semiregular.

Now suppose that $\omega(n) \geqslant 2$, n is odd, and n is square-free. Then $\operatorname{indeg}(0) = 1$. Let p be the smallest prime dividing n. Then $p^2 < n$ and $p^2 \equiv (n-p)^2 \pmod{n}$. Consequently, $\operatorname{indeg}(p^2) > 1$ and $G_2(n)$ is not semiregular.

From the above discussion it follows that if $G_2(n)$ is semiregular then $\omega(n) = 1$. Now we examine the case in which $n = p^k$, where p is an odd prime and $k \geqslant 3$. Then

$$\operatorname{indeg}(0) = N_{p^k}(0) = p^{\lfloor k/2\rfloor}. \tag{2.15}$$

Now consider the solutions of the congruence

$$x^2 \equiv p^2 \pmod{p^k}. \tag{2.16}$$

Clearly, p is a solution of (2.16). Since 0 is not a solution of (2.16), we see that whenever c is a solution of (2.16), then $n - c$ is also a solution of (2.16) and $n - c \not\equiv c \pmod{p^k}$. Hence, $N_{p^k}(p^2)$ is even. Consequently, it follows from (2.15) that $\operatorname{indeg}(0) \neq \operatorname{indeg}(p^2)$, and $G_2(p^k)$ is not semiregular.

The only remaining cases to consider are those for which $n = 2^k$, where $k = 5$ or $k \geqslant 7$. For these cases, we will show that $G_2(2^k)$ is not semiregular by finding a vertex 2^{2t} of $G_2(2^k)$ for which $2 \leqslant 2t < k$, $\operatorname{indeg}(2^{2t}) > 0$, and $\operatorname{indeg}(2^{2t}) \neq \operatorname{indeg}(0) = 2^{\lfloor k/2 \rfloor}$. Let $2 \leqslant 2t < k$. Then it is easily seen that $b^2 \equiv 2^{2t} \pmod{2^k}$ if and only if

$$b \equiv 2^t c \pmod{2^k} \tag{2.17}$$

for some integer c such that

$$c^2 \equiv 1 \pmod{2^{k-2t}}. \tag{2.18}$$

By the proof of Lemma 2.5, (2.18) holds if and only if

$$\begin{aligned} &c \equiv 1 \pmod{2} && \text{for } 1 \leqslant k - 2t \leqslant 3, \quad \text{or} \\ &c \equiv \pm 1 \pmod{2^{k-2t-1}} && \text{for } k - 2t \geqslant 4. \end{aligned}$$

Moreover, $2^t c_1 \equiv 2^t c_2 \pmod{2^k}$ if and only if

$$c_1 \equiv c_2 \pmod{2^{k-t}}. \tag{2.19}$$

From (2.17), (2.18), and (2.19), we see that if $2 \leqslant 2t < k$, then

$$N_{2^k}(2^{2t}) = \begin{cases} 2^{k-t-1} & \text{if } 1 \leqslant k - 2t \leqslant 3, \\ 2^{t+2} & \text{if } k - 2t \geqslant 4. \end{cases} \tag{2.20}$$

If $k \neq 7$, then it follows from (2.20) that $\operatorname{indeg}(0) = 2^{\lfloor k/2 \rfloor} \neq 8$, whereas $\operatorname{indeg}(2^2) = 8$, and hence $G_2(2^k)$ is not semiregular.

If $k = 7$, we see by (2.20) that $\operatorname{indeg}(0) = 2^{\lfloor 7/2 \rfloor} = 8$, whereas $\operatorname{indeg}(2^4) = 2^{7-2-1} = 16$, and $G_2(2^7)$ is also not semiregular.

We finally determine when $G(n)$ is semiregular. Let a be a vertex in $G_1(n)$ for which $\operatorname{indeg}(a) > 0$ and let b be a vertex in $G_2(n)$ for which $\operatorname{indeg}(b) > 0$. Let $n > 1$. Then $G(n)$ is semiregular if and only if $G_1(n)$ and $G_2(n)$ are both semiregular and $\operatorname{indeg}(a) = \operatorname{indeg}(b)$. By (2.8), (2.9), and (2.10), it now follows that $G(n)$ is semiregular if and only if $n = 2^k$ for $k \in \{0, 1, 2, 4\}$. $\square$

Theorem 2.6. *Let d be any positive integer. Then there exist positive integers n and a such that a is a vertex of $G_2(n)$ and* $\operatorname{indeg}(a) = d$.

Proof. If $d = 1$, we let $n = 2m$, where m is odd and square-free, and $a = n/2$. Now suppose that $d > 1$. Let k_1 be such that $d = 2^{k_1} d_1$, where d_1 is odd. We choose a positive integer d_2 such that $\omega(d_2) = k_1$ and $\gcd(2d_1, d_2) = 1$ (if $k_1 = 0$ then we set $d_2 = 1$). We now let

$$n = d_1^2 d_2 \quad \text{and} \quad a = d_1^2.$$

It now follows from Lemma 2.5 and the Chinese remainder theorem that

$$\operatorname{indeg}(a) = N_n(a) = N_{d_1^2}(d_1^2) N_{d_2}(d_1^2) = d_1 2^{k_1} = d.$$

□

A vertex a of $G(n)$ is said to be at *level* i, $i \geqslant 1$, if there exists a directed path of maximum length i which terminates at a and contains no directed edge belonging to a cycle. If such a path does not exist, the vertex is said to be at *level* 0. We say that a component of $G(n)$ has l *levels* if the highest level of a vertex in the component is $l - 1$. For instance, if $n = 16$ (see Fig. 4) then 2 and 8 are at level 0, the vertex 4 is at level 1, the vertex 0 is at level 2, and both the components have 3 levels.

Let C be a component of $G(n)$ which contains exactly l levels. It is clear that each vertex at level $l - 1$ is part of a cycle, since each vertex has outdegree 1. Moreover, if a and b are two distinct vertices at level i of C, where $0 \leqslant i < l$, then there does not exist a directed path from a to b. We thus have the following proposition.

Proposition 2.7. *Each component has exactly one cycle, i.e., the number of components of $G(n)$ is equal to the number of its cycles.*

Remark 2.8. We note that Proposition 2.7 is a general property of the iteration digraph of any mapping $f\colon H \to H$.

3. Application of the Carmichael lambda-function

Before proceeding further, we need to review some properties of the Carmichael lambda-function $\lambda(n)$, which was first defined in 1912 (see [2]) and which modifies the Euler totient function $\varphi(n)$.

Definition 3.1. Let n be a positive integer. Then the *Carmichael lambda-function* $\lambda(n)$ is defined as follows:

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

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

It immediately follows from Definition 3.1 that

$$\lambda(n) \mid \varphi(n)$$

for all n and that $\lambda(n) = \varphi(n)$ 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 [8, p. 20]) that $a^{\varphi(n)} \equiv 1 \pmod n$ if and only if $\gcd(a, n) = 1$. It shows that $\lambda(n)$ is a universal order modulo n.

Theorem 3.2 (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 the proof see [2] or [8, p. 21]. $\square$

Assume now that $\lambda(n)$ has the following prime power factorization:

$$\lambda(n) = \prod_{j=1}^{r} q_j^{l_j}, \tag{3.1}$$

where $q_1 < q_2 < \ldots < q_r$ are primes and $l_j > 0$. It is evident from the definition of λ that $q_1 = 2$ if $n > 2$.

Theorem 3.3. *There exists a cycle of length t in $G(n)$ if and only if $t = \operatorname{ord}_d 2$ for some odd positive divisor d of $\lambda(n)$.*

Proof. Suppose that a is a vertex of a t-cycle in $G(n)$. Then t is the least positive integer such that

$$a^{2^t} \equiv a \pmod{n}, \tag{3.2}$$

which implies that t is the least positive integer for which

$$a^{2^t} - a \equiv a\bigl(a^{2^t-1} - 1\bigr) \equiv 0 \pmod{n}. \tag{3.3}$$

Since $\gcd\bigl(a, a^{2^t-1}-1\bigr) = 1$, it follows from (3.3) that if $n_1 = \gcd(a, n)$ and $n_2 = n/n_1$, then t is the least positive integer such that

$$\begin{aligned} a &\equiv 0 \pmod{n_1}, \\ a^{2^t-1} &\equiv 1 \pmod{n_2}, \end{aligned} \tag{3.4}$$

and therefore $\gcd(n_1, n_2) = 1$. Hence, by the Chinese remainder theorem, there exists an integer b such that

$$\begin{aligned} b &\equiv 1 \pmod{n_1}, \\ b &\equiv a \pmod{n_2}. \end{aligned} \tag{3.5}$$

It follows from (3.4) and (3.5) that t is the least positive integer such that

$$b^{2^t-1} \equiv 1 \pmod{n}. \tag{3.6}$$

Let $d = \operatorname{ord}_n b$. Then $d \mid 2^t - 1$. Since, by (3.6), t is the least positive integer for which $d \mid 2^t - 1$, we see that $t = \operatorname{ord}_d 2$. Clearly, d is odd as $d \mid 2^t - 1$. Moreover, $d \mid \lambda(n)$ by Carmichael's Theorem 3.2.

Conversely, suppose that d is an odd positive divisor of $\lambda(n)$ and let $t = \operatorname{ord}_d 2$. By Carmichael's Theorem 3.2, there exists a residue g modulo n such that $\operatorname{ord}_n g = \lambda(n)$. Let $h = g^{\lambda(n)/d}$. Then $\operatorname{ord}_n h = d$. Since $d \mid 2^t - 1$ but $d \nmid 2^k - 1$ whenever $1 \leqslant k < t$, we see that t is the least positive integer for which

$$h^{2^t-1} \equiv 1 \pmod{n}. \tag{3.7}$$

Since, by (3.7),

$$h \cdot h^{2^t-1} = h^{2^t} \equiv h \pmod{n},$$

if follows that h is a vertex in a t-cycle of $G(n)$. $\square$

Let $A_t(G(n))$ denote the number of cycles of $G(n)$ of length t. In [12], Szalay gave a recursive formula for $A_t(G(n))$, which is in closed form when $t = 1$ or when $2^t - 1$ is a Mersenne prime, without using subdigraphs $G_1(n)$ or $G_2(n)$. In [11], Rogers completely determines $A_t(G(n))$ when $t \geqslant 1$ and n is a prime. He proves that the subgraphs attached to each of the vertices of all the cycles, except for the fixed point 0, are binary trees of the same structure. See also [4] for related results when n is prime.

When n is any positive integer, the number of square roots of any quadratic residue in $G_1(n)$ is equal to the number of square roots of 1 modulo n. It thus follows that for all $n \geqslant 2$, the subgraphs attached to each vertex of any cycle of $G_1(n)$ are all the same (see Figs. 2 and 5). The proof of this property is an immediate consequence of Theorem 2.4 and Theorem 4.4, which will be proved in the next section.

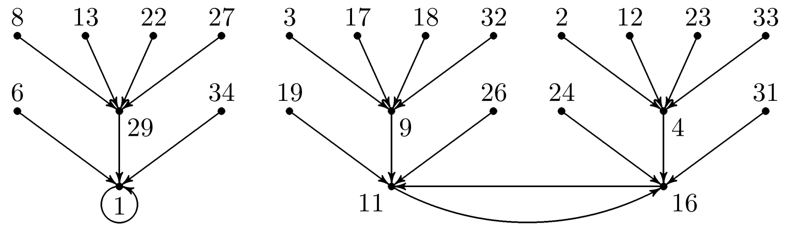

Figure 5. The subgraph $G_1(35)$.

We have the following theorem concerning $A_t(G_1(n))$ and $A_t(G_2(n))$.

Theorem 3.4. *If n is a positive integer, then $A_1(G_1(n)) = 1$ and $A_1(G_2(n)) = 2^{\omega(n)} - 1$. Moreover, if $t > 1$, then $A_t(G_1(n)) \geqslant 1$ whenever $A_t(G_2(n)) \geqslant 1$.*

Proof. First assume that $t = 1$. By Szalay's Theorem 1.1, $A_1(G(n)) = 2^{\omega(n)}$. Suppose that a is a fixed point in $G_1(n)$. Then

$$a^2 - a = a(a-1) \equiv 0 \pmod{n}. \tag{3.8}$$

Since $\gcd(a, n) = 1$, we see from (3.8) that $a \equiv 1 \pmod{n}$. Hence, $A_1(G(n)) = 1$ and $A_1(G_2(n)) = 2^{\omega(n)} - 1$.

Now suppose that $t > 1$ and that the vertex $a \in G_2(n)$ is part of a t-cycle. By (3.4), there exist integers n_1, n_2 such that $n_1 > 1$, $n_2 > 1$, $\gcd(n_1, n_2) = 1$, and $n_1 n_2 = n$ for which t is the least positive integer such that

$$\begin{aligned} a &\equiv 0 \pmod{n_1}, \\ a^{2^t-1} &\equiv 1 \pmod{n_2}. \end{aligned} \tag{3.9}$$

By the Chinese remainder theorem and the proof of Theorem 3.3, there exists a vertex $b \in G_1(n)$ such that b is part of a t-cycle and

$$b \equiv 1 \pmod{n_1}, \qquad b \equiv a \pmod{n_2}. \tag{3.10}$$

$\square$

Remark 3.5. We note that the number $A_t(G_1(n))$ can be substantially larger than $A_t(G_2(n))$ and vice versa. For example, if $n = 29 \cdot 43 = 1247$, then $A_3(G_1(n)) = 16$, whereas $A_3(G_2(n)) = 4$. On the other hand, if $n = 3 \cdot 5 \cdot 7 \cdot 29 = 3045$, then $A_3(G_2(n)) = 14$, while $A_3(G_1(n)) = 2$.

Remark 3.6. It can be further determined when $A_t(G_1(n)) > A_t(G_2(n)) = 0$. By the proof of Theorems 3.3 and 3.4, $A_t(G_1(n)) > 0$ if and only if there exists an odd divisor $d > 1$ of $\lambda(n)$ such that $t = \operatorname{ord}_d 2$. Let $A_t(G(n)) > 0$ for some $t > 1$. Then, by (3.4), Definition 3.1, and the proofs of Theorems 3.2 and 3.3, $A_t(G_2(n)) = 0$ if and only if there do not exist an integer $n_1 > 1$ and an odd integer $d_1 > 1$ such that $n_1 \mid n$, $n/n_1 > 1$, $\gcd(n_1, n/n_1) = 1$, $t = \operatorname{ord}_{d_1} 2$, and $d_1 \mid \lambda(n_1)$.

For example, let $n = 13 \cdot 29 = 377$ and let us examine the 6-cycles of $G(n)$. Notice that $\lambda(n) = 84$ and that the only odd divisor d of $\lambda(n)$ for which $\operatorname{ord}_d 2 = 6$ is $d = 21$. Observe that $21 \nmid \lambda(13) = 12$ and $21 \nmid \lambda(29) = 28$. Hence, $A_6(G_2(377)) = 0$. We find by inspection that $A_6(G_1(377)) = 2$.

Remark 3.7. By [9, p. 544], the number of quadratic nonresidues of $G_1(n)$ for $n \geqslant 3$ is greater than or equal to the number of quadratic residues. It thus follows that the number of vertices in $G_1(n)$ which have indegree 0 is greater than or equal to the number of vertices in $G_1(n)$ having a positive indegree. In particular, the number of vertices in $G_1(n)$ not lying on a cycle is greater than or equal to the number of vertices in $G_1(n)$ which lie on a cycle (cf. Figs. 1–5).

4. Application of the Euler totient function

Set

$$S = \{n \geqslant 1 \mid \varphi(n) \text{ is a power of } 2\},$$

where $\varphi(n)$ is the Euler totient function.

It is well known that a positive integer n belongs to S if and only if $n = 2^\alpha F_{m_1} \dots F_{m_j}$ for some $\alpha \geqslant 0$ and $j \geqslant 0$, where $F_{m_i} = 2^{2^{m_i}} + 1$ are distinct Fermat primes. 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 4.1. *There are no cycles in $G_1(n)$ of length greater than* 1 *if and only if $n \in S$. Moreover, there are no cycles in $G_2(n)$ of length greater than* 1 *if and only if $n \in S$ or n is a kth prime power for $k \geqslant 0$.*

Proof. According to the definition of the Carmichael lambda-function, $\lambda(n) = 2^i$ for some integer $i \geqslant 0$ if and only if $\varphi(n) = 2^j$ for some integer $j \geqslant i$. Let d is a positive odd integer. Then we also observe that $\operatorname{ord}_d 2 = 1$ if and only if $d = 1$. By Theorem 3.4, $A_t(G(n)) = 0$ for all $t \geqslant 2$ if and only if $A_t(G_1(n)) = 0$ for all $t \geqslant 2$.

First suppose that $n \in S$. Then 1 is the only positive odd divisor of $\lambda(n)$ and it follows from Theorem 3.3 that

$$A_t(G(n)) = A_t(G_1(n)) = A_t(G_2(n)) = 0$$

for all $t \geqslant 2$.

If $n \notin S$, then $\lambda(n)$ has an odd divisor $d > 1$. We see by Theorems 3.3 and 3.4 that $A_t(G_1(n)) \geqslant 1$ for $t = \operatorname{ord}_d 2 > 1$.

Observe that if n is a prime power, then the only cycle in $G_2(n)$ is the fixed point 0. Assume now that n is not a prime power and $n \notin S$. We show that $A_t(G_2(n)) > 0$ for some $t \geqslant 2$. Notice that there exists a prime power $p^k \notin S$ such that $p^k \parallel n$ for some $k \geqslant 1$. Furthermore, $\lambda(p^k)$ has an odd divisor $d > 1$. Moreover, $d \mid \lambda(n)$ since $\lambda(p^k) \mid \lambda(n)$. Let $t = \operatorname{ord}_d 2$. By (3.7), there exists a residue a such that t is the least positive integer for which

$$a^{2^t-1} \equiv 1 \pmod{p^k}. \tag{4.1}$$

Write $n = p^k n_1$, where $n_1 > 1$. Using the Chinese remainder theorem, we can now find a vertex $b \in G_2(n)$ such that

$$\begin{aligned} b &\equiv a \pmod{p^k}, \\ b &\equiv 0 \pmod{n_1}. \end{aligned} \tag{4.2}$$

Note that $\gcd(b, p^k) = \gcd(a, p^k) = 1$ by (4.1) and (4.2). It follows again from (4.1) and (4.2) that t is the least positive integer such that

$$b^{2^t} - b = b\big(b^{2^t-1} - 1\big) \equiv 0 \pmod{n}.$$

Hence, t is the least positive integer such that

$$b^{2^t} \equiv b \pmod{n},$$

and b is part of a t-cycle in $G_2(n)$. □

Corollary 4.2. *There are no cycles in $G(n)$ of length greater than* 1 *if and only if $n \in S$.*

Corollary 4.3. *The Fermat number F_m is composite if and only if there exists a cycle in $G(F_m)$ of length greater than* 1.

The next theorem generalizes a result of Rogers [11] from primes to natural numbers.

Theorem 4.4. *Each component of $G_1(n)$ has exactly $\nu_2(\lambda(n)) + 1$ levels, where $\nu_2(c)$ denotes the exponent in the highest power of* 2 *dividing c.*

Proof. The result clearly holds for $n \in \{1, 2\}$. So assume that $n > 2$. Let a be a vertex in a component C of $G_1(n)$ for which $d = \operatorname{ord}_n a$. Then $d \mid \lambda(n)$ by Theorem 3.2. By the proof of Theorem 3.3, a is part of a t-cycle in C, and thus at the highest level of C, if and only if d is odd.

Suppose that $b^2 \equiv a \pmod{n}$. Since

$$d = \operatorname{ord}_n a = \frac{\operatorname{ord}_n b}{\gcd(2, \operatorname{ord}_n b)}, \tag{4.3}$$

if follows that

$$\operatorname{ord}_n a \mid \operatorname{ord}_n b \mid 2 \operatorname{ord}_n a,$$

and $\operatorname{ord}_n b = 2 \operatorname{ord}_n a$ if $2 \mid \operatorname{ord}_n a$. We also see from (4.3) that all vertices in the same cycle of $G_1(n)$ have the same order modulo n, i.e., there exists an odd integer $d > 1$ such that

$$\operatorname{ord}_n a = d \tag{4.4}$$

for all vertices a in the t-cycle of $G_1(n)$.

Let $l = \nu_2(\lambda(n))$ and assume that $2^l \parallel \operatorname{ord}_n a$. Noting that $2 \mid \lambda(n)$ for $n > 2$, we see that if there exists a vertex $b \in G_1(n)$ such that $b^2 \equiv a \pmod{n}$, then $2^{l+1} \parallel \operatorname{ord}_n b$, which contradicts the fact that $\operatorname{ord}_n b \mid \lambda(n)$. Hence, a is at level 0 in this instance. Consequently, any component C of $G_1(n)$ has at most $l + 1$ levels.

Let a be a vertex of $G_1(n)$ for which $d = \operatorname{ord}_n a$ is odd. We will find a vertex b of $G_1(n)$ such that

$$b^{2^l} \equiv a \pmod{n}, \quad \operatorname{ord}_n b^{2^{l-1}} = 2 \operatorname{ord}_n a. \tag{4.5}$$

Then by the above discussion, $\operatorname{ord}_n b$ will be equal to $2^l d$ and b^{2^i} will be at level i for $i \in \{0, 1, \ldots, l\}$. Hence, C will have exactly $l + 1$ levels.

Let n have the prime factorization given in (1.2). By the definition of $\lambda(n)$, there exists a prime power factor $p_j^{k_j}$ of n such that $\nu_2(\lambda(p_j^{k_j})) = l$ for some $j \in \{1, 2, \ldots, s\}$.

Let d_i be the order of a modulo $p_i^{k_i}$ for $i = 1, 2, \ldots, s$. Then $d_i \mid d$, d_i is odd, and a is part of a cycle in $G_1(p_i^{k_i})$ of length $t_i = \mathrm{ord}_{d_i}(p_i^{k_i})$. First suppose that $\nu_2(\lambda(p_i^{k_i})) < l$. Choose the vertex $b_i \in G_1(p_i^{k_i})$ in the same t_i-cycle as the vertex a modulo $p_i^{k_i}$ which is l vertices from a in the clockwise direction (possibly going around the cycle more than once). Then $b_i^{2^l} \equiv a \pmod{p_i^{k_i}}$.

Now suppose that $2^l \parallel \lambda(p_i^{k_i})$ and either $p_i^{k_i} = 2$ or 4 or p_i is an odd prime. Then the vertices in $G_1(p_i^{k_i})$ form a cyclic group modulo $p_i^{k_i}$ with $\lambda(p_i^{k_i})$ elements. Consequently, there exists a primitive root $g_i \pmod{p_i^{k_i}}$ for which

$$g_i^{\lambda(p_i^{k_i})/d_i} \equiv a \pmod{p_i^{k_i}}.$$

Let $c_i = \lambda(p_i^{k_i})/(2^l d_i)$ and let $b_i \equiv g_i^{c_i} \pmod{p_i^{k_i}}$. Then $b_i^{2^l} \equiv a \pmod{p_i^{k_i}}$ and the order of $b_i^{2^{l-1}}$ modulo $p_i^{k_i}$ is equal to $2d_i$.

Finally, assume that $p_1 = 2$, $l \geqslant 3$, and $k_1 = l$, where $2^{k_1} \parallel \lambda(n)$. Then $a \equiv 1 \pmod{2^{k_1}}$, since the order of a modulo 2^{k_i} is odd. Moreover,

$$5^{2^l} \equiv 1 \equiv a \pmod{2^{k_1}}$$

and the order of 5^{2^l-1} modulo 2^{k_1} is equal to 2. Let $b_1 \equiv 5 \pmod{2^{k_1}}$.

Applying the Chinese remainder theorem, we obtain a vertex $b \in G_1(n)$ such that $b \equiv b_i \pmod{p_i^{k_i}}$ for $i = 1, \ldots, s$. We note that if c_i is the order of b_i modulo $p_i^{k_i}$, then

$$\mathrm{ord}_n\, b = \mathrm{lcm}[c_1, c_2, \ldots, c_s].$$

It now follows that b indeed satisfies the required properties given in (4.5). $\square$

Theorem 4.5. *Let a, b, c, d, e be any positive integers such that $b \geqslant a \geqslant 2$ and $d = 2^f$ for some $f \geqslant 2$. Then there exists a positive integer n such that*

(i) *each component of $G_1(n)$ has exactly a levels,*
(ii) *some component of $G_2(n)$ has at least b levels,*
(iii) *$G_1(n)$ has at least c components,*
(iv) *$G_2(n)$ has at least c components,*
(v) *each vertex of $G_1(n)$ not at level 0 has indegree equal to d, and*
(vi) *some vertex of $G_2(n)$ has indegree greater than or equal to e.*

Proof. By the Chinese remainder theorem and Dirichlet's theorem on the infinitude of primes in arithmetic progressions, we can find a prime p such that $p \equiv 1+2^{a-1} \pmod{2^a}$ and $p-1$ is divisible by ach of the c numbers $2_1-1, 2_2-1, \ldots, 2c-1$.

We choose the integer k such that $k \geqslant 2^{b-1}$ and $p^{\lfloor k/2 \rfloor} \geqslant e$. Next we choose n so that $p^k \parallel n$, $\omega(n) = f$, and each prime divisor $q \neq p$ of n is congruent to 3 modulo 4. Then

$$\nu_2(\lambda(n)) = \nu_2(\lambda(p^k)) = \nu_2(\lambda(p)) = a - 1,$$

and $G_1(n)$ has exactly a levels by Theorem 4.4. Hence, (i) holds.

Moreover, if i is a vertex of $G_1(n)$ and $\operatorname{indeg}(i) > 0$, then

$$\operatorname{indeg}(i) = 2^{\omega(n)+\varepsilon(n)} = 2^f = d,$$

and (v) is thus valid.

Noting that $p - 1 \mid \lambda(n)$ and the order of 2 modulo $2_t - 1$ equals t, it follows from Proposition 2.7, Theorem 3.3, (3.9), (3.10), and (4.4) that both $G_1(n)$ and $G_2(n)$ have at least c components. Therefore, (iii) and (iv) are satisfied.

It is evident that the number of levels in the component of $G_2(n)$ containing the vertex p is at least $\lfloor \log_2 k \rfloor + 1 \geqslant b$, i.e., (ii) is true.

Finally, we note that $0 \in G_2(n)$ and

$$\operatorname{indeg}(0) \geqslant \frac{p^k}{p^{\lceil k/2 \rceil}} = p^{\lfloor k/2 \rfloor} \geqslant e,$$

which implies (vi). □

Remark 4.6. We see from Theorems 2.4, 2.6, 4.1, 4.4, and 4.5 that $G_1(n)$ exhibits a more regular behavior than $G_2(n)$.

The next theorem enables us to separate the Fermat primes from the other odd primes. It generalizes an interesting result presented independently by Szalay and Rogers on Fermat primes (see [11], [12], and also [8]).

Theorem 4.7. *The digraph $G(n)$ has exactly 2 components if and only if n is a Fermat prime or n is a power of 2.*

Proof. The assertion follows immediately from Proposition 2.7, Theorem 1.1, and Corollary 4.2. □

In Fig. 1, we see the structure of $G(2^3)$. The following Fig. 6 shows the iteration digraph for the Fermat prime $F_2 = 17$. In [9], we show that only for a Fermat prime or twice a Fermat prime or 4, is the set of primitive roots equal to the set of quadratic nonresidues.

It was showen in [8, p. 94] that a Fermat number cannot be a perfect kth power for $k \geqslant 2$. As a consequence of this Theorems 1.1 and 4.7 we get:

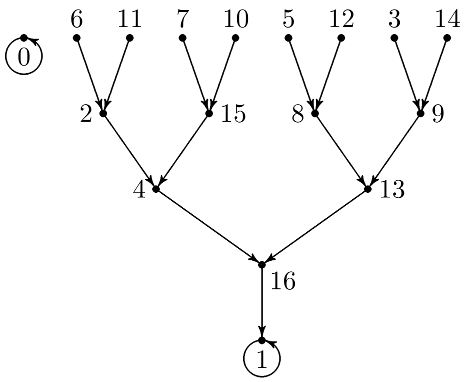

Figure 6. Iteration digraph corresponding to the Fermat prime $n = 17$.

Corollary 4.8. *The Fermat number F_m is composite if and only if there exists $x \in \{2, 3, \dots, F_m - 1\}$ such that $x^2 \equiv x \pmod{F_m}$.*

Remark 4.9. According to Theorem 2.1, the Fermat number F_m is square-free if and only if $x^2 \not\equiv 0 \pmod{F_m}$ for all $x \in \{1, \dots, F_m - 1\}$.

For Theorems 4.10 and 4.12 given below we assume that $\lambda(n)$ has the prime power factorization as given in (3.1). Theorem 4.10 generalizes a result by Rogers [11] from a prime n to a natural number n.

Theorem 4.10. *The digraph $G(n)$ has exactly 3 components if and only if $n = 9$ or $n = 25$ or n is a prime and $q = (n-1)/2^{l_1}$ is also a prime such that 2 is a primitive root modulo q.*

Proof. Suppose $G(n)$ has exactly 3 components. By Proposition 2.7 and Theorems 3.4, 4.1, and 4.7, this occurs if and only if $n = p^k$, where p is an odd prime and $k \geqslant 1$, and $G_1(n)$ has a unique cycle of length greater than 1. Let t be the length of this unique cycle in $G_1(n)$. By (4.4), there exists an odd integer $d > 1$ for which $\operatorname{ord}_n a = d$ if a is a vertex in the t-cycle of $G_1(n)$. Moreover, by Theorem 3.3, $t = \operatorname{ord}_d 2$ and $d \mid \lambda(n)$.

Since the vertices in $G_1(n)$ form a cyclic group under multiplication modulo n, the number of vertices a in $G_1(n)$ for which $\operatorname{ord}_n a = d$ is equal to $\varphi(d)$. Thus, there exists a unique t-cycle in $G_1(n)$ if and only if for d odd,

$$\sum_{\substack{d \mid \lambda(n) \\ \operatorname{ord}_d 2 = t}} \frac{\varphi(d)}{t} = \frac{\varphi(d)}{\operatorname{ord}_d 2} = 1.$$

Therefore, we require that $\lambda(n)$ has a unique odd divisor $d > 1$ and that 2 is a primitive root modulo d.

Now suppose that $k \geqslant 2$. Then $\lambda(n) = p^{k-1}(p-1)$. Hence, $\lambda(n)$ has a unique odd divisor $d > 1$ if and only if $k = 2$ and $p - 1$ is a power of 2. Then $d = p$ and d is a Fermat prime. However, 2 is a primitive root modulo the Fermat prime $F_m = 2^{2^m}+1$ if and only if $m \in \{0, 1\}$. Thus $n = 3^2 = 9$ or $n = 5^2 = 25$.

Further, assume that $k = 1$. Then $\lambda(n) = p-1$, and $p-1$ has a unique odd prime divisor $q > 1$ if and only if

$$n - 1 = \lambda(n) = 2^{l_1}q,$$

where q is an odd prime. The t-cycle in $G_1(n)$ is then unique if and only if 2 is a primitive root modulo q. The result now follows. □

Remark 4.11. For example, $G(n)$ has exactly three components if (compare with Fig. 2)

$$n = 7,\ 9,\ 11,\ 13,\ 23,\ 25,\ 41,\ 53.$$

The following theorem given without proof can be proved in a manner similar to Theorems 4.7 and 4.10.

Theorem 4.12. *The digraph $G(n)$ has exactly 4 components if and only if one of the following four conditions hold:*

(i) $n = 27$ *or* $n = 125$.

(ii) n *is a prime and* $p = (n-1)/2^{l_1}$ *is also a prime for which* $\operatorname{ord}_p 2 = (p-1)/2$.

(iii) n *is a prime such that* $(n-1)/2^{l_1}$ *is the square of a prime* q *for which* 2 *is a primitive root modulo* q^2.

(iv) n *is a product of two coprime integers* $q_1 > 1$ *and* $q_2 > 1$, *each of which is equal to a Fermat prime or to a power of* 2.

Remark 4.13. For example, the digraph $G(n)$ has exactly four components if (compare with Fig. 3)

$$n = 6,\ 10,\ 12,\ 15,\ 19,\ 20,\ 24,\ 27,\ 29,\ 34,\ 37,\ 40,\ 47,\ 48,\ 51.$$

Acknowledgement. The authors are indebted to Štefan Porubský and Andrzej Schinzel for fruitful discussions and to Pavel Křížek for his assistance in preparation of figures.

References

[1] *S. Bryant*: Groups, graphs, and Fermat's last theorem. Amer. Math. Monthly *74* (1967), 152–156.

[2] *R. D. Carmichael*: Note on a new number theory function. Bull. Amer. Math. Soc. *16* (1910), 232–238.

[3] *G. Chartrand and L. Lesniak*: Graphs and Digraphs (Third edition). Chapman & Hall, London, 1996.

[4] *G. Chassé*: Applications d'un corps fini dans lui-même. Dissertation, Univ. de Rennes I, 1984.

[5] *G. Chassé*: Combinatorial cycles of a polynomial map over a commutative field. Discrete Math. *61* (1986), 21–26.

[6] *F. Harary*: Graph Theory. Addison-Wesley Publ. Company, London, 1969.

[7] *P. Kiss*: Egy binom kongruenciáról. Az Egi Ho Si Mihn Tanárképzó Fóiskola füzetei (1978), 457–464.

[8] *M. Křížek, F. Luca and L. Somer*: 17 Lectures on the Fermat Numbers. From Number Theory to Geometry. Springer-Verlag, New York, 2001.

[9] *M. Křížek and L. Somer*: A necessary and sufficient condition for the primality of Fermat numbers. Math. Bohem. *126* (2001), 541–549.

[10] *F. Robert*: Discrete Iterations. Springer Series in Comput. Math. Vol. 6. Springer-Verlag, Berlin, 1986.

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

[12] *L. Szalay*: A discrete iteration in number theory. BDTF Tud. Közl. *8* (1992), 71–91. (In Hungarian.)

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, Mathematical Institute, Academy of Sciences of the Czech Republic, Žitná 25, CZ–115 67 Prague 1, Czech Republic, e-mail: `krizek@math.cas.cz`.