Czechoslovak Mathematical Journal

J. Skowronek-Kaziów

Properties of digraphs connected with some congruence relations

Czechoslovak Mathematical Journal, Vol. 59 (2009), No. 1, 39–49

Persistent URL: `http://dml.cz/dmlcz/140462`

Czechoslovak Mathematical Journal, 59 (134) (2009), 39–49

PROPERTIES OF DIGRAPHS CONNECTED WITH SOME CONGRUENCE RELATIONS

J. Skowronek-Kaziów, Zielona Góra

(Received April 12, 2006)

Abstract. The paper extends the results given by M. Křížek and L. Somer, *On a connection of number theory with graph theory*, Czech. Math. J. 54 (129) (2004), 465–485 (see [5]). For each positive integer n define a digraph $\Gamma(n)$ whose set of vertices is the set $H = \{0, 1, \ldots, n-1\}$ and for which there is a directed edge from $a \in H$ to $b \in H$ if $a^3 \equiv b \pmod{n}$. The properties of such digraphs are considered. The necessary and the sufficient condition for the symmetry of a digraph $\Gamma(n)$ is proved. The formula for the number of fixed points of $\Gamma(n)$ is established. Moreover, some connection of the length of cycles with the Carmichael λ-function is presented.

Keywords: digraphs, Chinese remainder theorem, Carmichael λ-function, group theory

MSC 2010: 20K01, 11A15, 05C-20

1. Introduction

In this paper we establish some properties of a digraph $\Gamma(n)$ connected with the congruence relation $a^3 \equiv b \pmod{n}$. We show an interesting connection between number theory, graph theory and group theory motivated by the results of S. Bryant [1], G. Chassé [3], M. Křížek and L. Somer [5], T. D. Rogers [7] and L. Szalay [9] who considered a digraph corresponding to the congruence relation $a^2 \equiv b \pmod{n}$.

For $n \geqslant 1$ let

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

We can consider a directed graph $\Gamma(n)$ whose vertices are the elements of H and such that there exists exactly one directed edge from a to b iff

$$(\star) \qquad a^3 \equiv b \pmod{n},$$

that is, iff b is the remainder of the division a^3 by n. As an example consider the digraph $\Gamma(13)$ presented below:

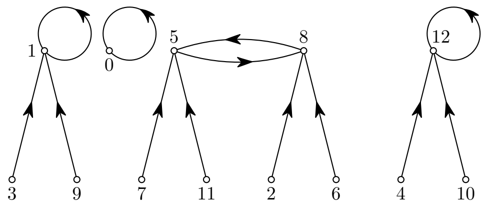

Figure 1. The digraph for $n = 13$

If $a_1, a_2, \ldots, a_t$ are pairwise distinct in H and

$$\begin{aligned} a_1^3 &\equiv a_2 \pmod n, \\ a_2^3 &\equiv a_3 \pmod n, \\ &\vdots \\ a_t^3 &\equiv a_1 \pmod n) \end{aligned}$$

then the elements $a_1, a_2, \ldots, a_t$ constitute a *cycle* of length t. Let us call a cycle of the length 1 a *fixed point*. The cycles of length t are called *t-cycles*. For instance, the digraph $\Gamma(11)$ contains two 4-cycles and three fixed points (see Fig. 2).

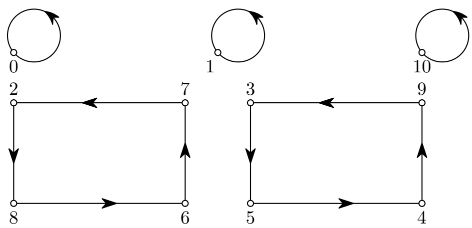

Figure 2. The digraph for $n = 11$

A *component* of a digraph is a subdigraph which is a maximal connected subgraph of the associated nondirected graph (for the definition details see [4]).

The digraph $\Gamma(n)$ 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 (cf. Fig. 3).

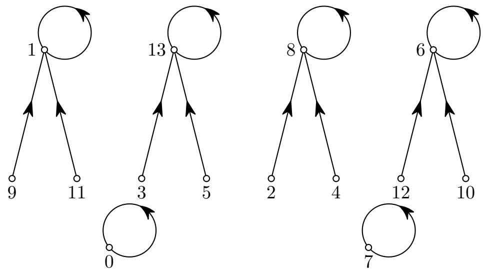

Figure 3. The digraph for $n = 14$

2. Structure and properties of the digraph $\Gamma(n)$

Denote by indeg(a) the number of directed edges coming to a and by outdeg(a) the number of directed edges leaving the vertex $a \in H = \{0, \ldots, n-1\}$. Of course indeg$(a) \geqslant 0$ and outdeg$(a) = 1$ by the definition of the function $f : H \to H$, where $f(x) = y$ iff $x^3 \equiv y \pmod{n}$ (we say that x is mapped into y). For an isolated fixed point, the indegree and the outdegree are both equal to 1.

We specify two subdigraphs of $\Gamma(n)$. Let $\Gamma_1(n)$ be the subdigraph induced on the set of vertices which are coprime to n and let $\Gamma_2(n)$ be the subdigraph induced on the set of vertices which are not coprime with n. We observe that $\Gamma_1(n)$ and $\Gamma_2(n)$ are disjoint and $\Gamma(n) = \Gamma_1(n) \cup \Gamma_2(n)$. For example, both the first and the second component of Fig. 3 are $\Gamma_1(14)$ and the last components belong to $\Gamma_2(14)$. It is clear that 0 is always a vertex of $\Gamma_2(n)$ and for $n > 1$ the numbers 1 and $n-1$ are in $\Gamma_1(n)$.

The outdegree of every vertex of a digraph $\Gamma(n)$ is equal to 1. Hence, the number of components of $\Gamma(n)$ is equal to the number of all cycles. The cycles can be isolated (see Fig. 5) or not isolated (see Fig. 1). Besides, for an arbitrary natural $t \geqslant 1$, by the definition of a cycle and by the properties of the congruence relation $(\star)$, the digraph $\Gamma(k^{3^t} - k)$ has a t-cycle containing the vertex k.

For example, $\Gamma(n)$ has a 3-cycle containing the vertex 2 iff

$$n \mid 2^{3^3} - 2 = 2 \cdot (2^{13} - 1) \cdot (2^{13} + 1).$$

Let $n = 2^{13} - 1 = 8191$. Then there is a 3-cycle containing the vertex 2 in the digraph $\Gamma(8191)$ (see Fig. 4).

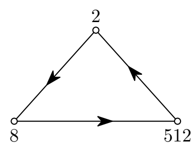

Figure 4. The 3-cycle of the digraph for $n = 2^{13} - 1 = 8191$

Lemma 1. *The numbers* $0, 1, n-1$ *are fixed points of* $\Gamma(n)$. *Moreover,* 0 *is an isolated fixed point of* $\Gamma(n)$ *if and only if* n *is square-free.*

Proof. It is clear that

$$0^3 \equiv 0 \pmod{n}, \;\; 1^3 \equiv 1 \pmod{n} \;\; \text{and} \;\; (n-1)^3 \equiv n-1 \pmod{n}.$$

Now, if n is not square-free then $p^2 \mid n$ for some prime p and

$$\left(\frac{n}{p}\right)^3 = n \cdot \frac{n}{p} \cdot \frac{n}{p^2} \equiv 0 \pmod{n}.$$

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

Conversely, if n is square-free then there exists no k, $1 \leqslant k \leqslant n-2$ such that $n \mid k^3$. So, there is no k, $1 \leqslant k \leqslant n-1$, such that $k^3 \equiv 0 \pmod{n}$ and 0 is an isolated fixed point of $\Gamma(n)$. □

Lemma 2. *Let* $1 \leqslant k, l \leqslant n-1$. *Then*

(i) *the number* k *is mapped into* 0 *(or into* $\frac{1}{2}n$ *for an even* n*) if and only if* $n-k$ *is mapped into* 0 *(or into* $\frac{1}{2}n$ *for an even* n*),*

(ii) *the number* k *is mapped into* l *if and only if* $n-k$ *is mapped into* $n-l$,

(iii) *the number* k *is an isolated fixed point if and only if* $n-k$ *is an isolated fixed point,*

(iv) *the number* k *is a part of a* t*-cycle if and only if* $n-k$ *is the element of some* t*-cycle. Moreover, the isolation of one of these* t*-cycles implies the isolation of the other.*

Proof. We can notice that

$$k^3 \equiv 0 \pmod{n} \Longleftrightarrow (n-k)^3 \equiv 0 \pmod{n}.$$

Also, for an even n, we have

$$k^3 \equiv \frac{n}{2} \pmod{n} \Longleftrightarrow (n-k)^3 \equiv n - \frac{n}{2} = \frac{n}{2} \pmod{n}.$$

So, the statement (i) is satisfied.

Besides, it is not hard to check that

$$l^3 \equiv k \pmod{n} \Longleftrightarrow n \mid l^3 - k \Longleftrightarrow (n-l)^3 \equiv n-k \pmod{n},$$
$$k^3 \equiv k \pmod{n} \Longleftrightarrow n \mid k^3 - k \Longleftrightarrow (n-k)^3 \equiv n-k \pmod{n}$$

and

$$k^{3^t} \equiv k \pmod{n} \Longleftrightarrow (n-k)^{3^t} \equiv n-k \pmod{n}.$$

The last three observations prove the satements (ii), (iii) and (iv) of the lemma, respectively. □

Let $\left\lfloor \frac{1}{2}n \right\rfloor = \begin{cases} \frac{1}{2}n, & \text{if } n \text{ is even,} \\ \frac{1}{2}(n-1), & \text{if } n \text{ is odd.} \end{cases}$

Every component of $\Gamma(n)$ is a cycle if and only if for every k, $2 \leqslant k \leqslant \left\lfloor \frac{1}{2}n \right\rfloor$, there exists $t \geqslant 1$ such that $k^{3^t} \equiv k \pmod{n}$.

For example, for $n = 2, 3, 5, 6, 10, 11, 17$ the digraph $\Gamma(n)$ contains only cycles. Thus, $\operatorname{indeg}(a) = 1$ for every $a \in H$ (cf. Fig. 5).

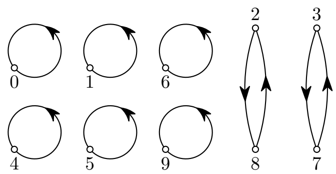

Figure 5. The digraph for $n = 10$.

We call a digraph regular if the indegree of each vertex is equal to 1. Every component of a regular digraph is a cycle. A digraph is semiregular if there exists a positive integer d such that each vertex has either indegree d or 0. The vertices of $\Gamma_1(n)$ form a group of order $\varphi(n)$ (where $\varphi(n)$ is the Euler totient function) with respect to the multiplication modulo n. Hence, the number of cubic roots (if they exist) of any cubic residue in $\Gamma_1(n)$ is equal to the number of cubic roots of 1 modulo n (see [8]). In the set of vertices of $\Gamma_1(n)$, the number of solutions of the congruence

$$x^3 \equiv 1 \pmod{n} \Leftrightarrow (x-1)(x^2+x+1) \equiv 0 \pmod{n}$$

is either 1 or some power of 3. In fact, let $n = p^\alpha$ for some prime p and $\alpha \geqslant 1$. If $3^2 \mid n$ or p is congruent to 1 modulo 3, then the number $\varrho(n)$ of solutions of the above congruence is 3. In the other cases $\varrho(n) = 1$.

Moreover, if n is an arbitrary natural number and f is a polynomial with integer coefficients, then the function

$$\varrho_f(n) = |\{0 \leqslant m \leqslant n-1 : f(m) \equiv 0 \pmod{n}\}|$$

is a multiplicative function.

Besides, the order of the element divides the order of the group. Thus, in the case $3 \nmid \varphi(n)$, every vertex in $\Gamma_1(n)$ has indegree equal to 1. Let $\omega_0(n)$ be the number of distinct primes dividing n which are congruent to 1 modulo 3. Let

$$\omega(n) = \begin{cases} \omega_0(n) + 1, & \text{if } 3^2 \mid n, \\ \omega_0(n), & \text{if } 3^2 \nmid n. \end{cases}$$

Then, for every natural n, the following corollary holds:

Corollary 1. *The digraph $\Gamma_1(n)$ is semiregular if and only if $3 \mid \varphi(n)$. In this case every vertex of $\Gamma_1(n)$ has either indegree $3^{\omega(n)}$ or 0. In the other case, i.e. $3 \nmid \varphi(n)$, the digraph $\Gamma_1(n)$ is regular (each component of $\Gamma_1(n)$ is a cycle). Moreover, if every component of a digraph $\Gamma(n)$ is a cycle then $3 \nmid \varphi(n)$ and n is square-free.*

For example, if $F_m = 2^{2^m} + 1$ is a Fermat prime number, $m \geqslant 1$, then every component of $\Gamma(F_m)$ is a cycle (see the digraph $\Gamma(17)$, Fig. 6).

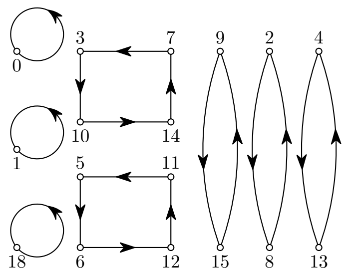

Figure 6. The digraph for $n = 17$.

Conjecture. *Let $n > 3$. Every component of the digraph $\Gamma(n)$ is a cycle if and only if $3 \nmid \varphi(n)$ and n is square-free.*

Lemma 3. *Let n be an even natural number. Then*
(i) $(\frac{1}{2}n)^3 \equiv 0 \pmod{n}$ *iff* $4 \mid n$,
(ii) $\frac{1}{2}n$ *is a fixed point iff* $4 \nmid n$.

Proof. (i) If n is even and $(\frac{1}{2}n)^3 \equiv 0 \pmod{n}$ then $n \mid (\frac{1}{2}n)^3$ and $\frac{1}{2}n$ must be even. Hence, $4 \mid n$.

If $4 \mid n$ then $4 \mid (\frac{1}{2}n)^3$ and $n \mid (\frac{1}{2}n)^3$.

(ii) If $4 \mid n$ then $(\frac{1}{2}n)^3$ is an even multiple of $\frac{1}{2}n$ and $(\frac{1}{2}n)^3 - \frac{1}{2}n$ is an odd multiple of $\frac{1}{2}n$. Hence $n \nmid (\frac{1}{2}n)^3 - \frac{1}{2}n$.

Conversely, if $4 \nmid n$ then $\frac{1}{2}n$ is odd and $(\frac{1}{2}n)^3$ is an odd multiple of $\frac{1}{2}n$. Hence, $(\frac{1}{2}n)^3 - \frac{1}{2}n$ is an even multiple of $\frac{1}{2}n$ and $n \mid (\frac{1}{2}n)^3 - \frac{1}{2}n$. □

Let $n = 2^m p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ be the prime power factorization of n, where $p_1 < p_2 < \dots < p_s$ are distinct odd primes and $\alpha_i \geqslant 1$, $m, s \geqslant 0$. The following theorem gives the formula for the number of fixed points of a digraph $\Gamma(n)$.

Theorem 1. *The number $L(n)$ of fixed points of $\Gamma(n)$ is equal to*

$$L(n) = \begin{cases} 3^s, & \text{if } m = 0, \\ 2 \cdot 3^s, & \text{if } m = 1, \\ 3 \cdot 3^s, & \text{if } m = 2, \\ 5 \cdot 3^s, & \text{if } m \geqslant 3. \end{cases}$$

P r o o f. The element a, where $2 \leqslant a \leqslant n-2$, is a fixed point of $\Gamma(n)$ if and only if $a^3 \equiv a \pmod{n} \Longleftrightarrow n \mid a^3 - a = (a-1)\cdot a \cdot (a+1)$.

Let $n = 2^m p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, where $p_1 < p_2 < \dots < p_s$ are distinct odd primes and $\alpha_i \geqslant 1$, $m, s \geqslant 0$. Then every factor $p_i^{\alpha_i}$ can divide $a-1$ or a or $a+1$, so we have three possibilities for $1 \leqslant i \leqslant s$.

If $m = 1$ then the factor 2 of n can appear either as a divisor of a or simultaneously as a divisor of $a-1$ and $a+1$ so, we have two possibilities.

If $m = 2$ then the factor 2^2 can be a divisor of a or $a-1$ (then $2 \mid a+1$) or it can be a divisor of $a+1$ (then $2 \mid a-1$), so we have 3 possibilities.

If $m \geqslant 3$ then the factor 2^m of n can divide a or

$$2^{m-1} \mid a-1 \quad \text{and} \quad 2 \mid a+1$$

or

$$2^{m-1} \mid a+1 \quad \text{and} \quad 2 \mid a-1$$

or

$$2^{m} \mid a-1 \quad \text{and} \quad 2 \mid a+1$$

or

$$2^{m} \mid a+1 \quad \text{and} \quad 2 \mid a-1,$$

so we get 5 possibilities.

Using elementary combinatorics and realizing that all $s+1$ factors of $n = 2^m p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ cannot divide the same factor of the product $(a-1)\cdot a\cdot(a+1)$, we obtain $2 \cdot 3^s - 3$ fixed points for $n = 2p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ and $3^{s+1} - 3$ fixed points for $n = 2^2 p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ and $5 \cdot 3^s - 3$ fixed points for $n = 2^m p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, $m \geqslant 3$.

The proof is completed since in every case 0, 1, $n-1$ are also fixed points in the digraph $\Gamma(n)$. □

Theorem 2. *The digraph $\Gamma(n)$ is symmetric if and only if $n \equiv 2 \pmod{4}$.*

P r o o f. If $4 \nmid n-2$ then (see Theorem 1) the digraph $\Gamma(n)$ has an odd number of fixed points. Hence, it cannot be symmetric.

Conversely, let $n \equiv 2 \pmod{4}$, then n is even and $\frac{1}{2}n$ is odd. Let $\mathrm{Com}(0)$, $\mathrm{Com}(\frac{1}{2}n)$ be two disjoint components of $\Gamma(n)$ containing the elements 0 and $\frac{1}{2}n$, respectively. Then $\Gamma(n) - \{\mathrm{Com}(0), \mathrm{Com}(\frac{1}{2}n)\}$ is symmetric by Lemma 2. It is enough to show that the subdigraph $\mathrm{Com}(0)$ is isomorphic to $\mathrm{Com}(\frac{1}{2}n)$.

If n is square-free then 0 is an isolated fixed point. We must show that $\frac{1}{2}n$ is also an isolated fixed point. Assume that $k^3 \equiv \frac{1}{2}n \pmod{n}$ for some odd k, where $3 \leqslant k \leqslant n-3$. Then

$$(n-k)^3 \equiv n - \frac{n}{2} = \frac{n}{2} \pmod{n}.$$

Hence,

$$n \mid k^3 - \frac{n}{2} \quad \text{and} \quad n \mid k^3 + \frac{n}{2}$$

and consequently $n \mid 2k^3$. The number n is square-free and $n = 2k$. Hence $\frac{1}{2}n$ is an isolated fixed point in $\mathrm{Com}(\frac{1}{2}n)$.

In the other case, if n is not square-free then 0 is not isolated. Let

$$k^3 \equiv 0 \pmod{n}.$$

Then k must be even, i.e. $k = 2^j \cdot c$, where $j \geqslant 1$ and c is an odd number. The number c^3 is an odd multiple of $\frac{1}{2}n$. Hence,

$$c^3 \equiv \frac{n}{2} \pmod{n}.$$

Now, assume that

$$k^3 \equiv 0 \pmod{n} \quad \text{and} \quad l^3 \equiv k \pmod{n} \quad \text{and} \quad l^9 \equiv 0 \pmod{n},$$

where $l = 2^r \cdot d$, $r \geqslant 1$ and d is an odd number. Of course $n \nmid l^3$ and that is why

$$\frac{n}{2} \nmid d^3 \quad \text{and} \quad n \nmid d^3 - \frac{n}{2}.$$

Besides, $n \mid l^9$, d^9 is an odd multiple of $\frac{1}{2}n$ and

$$d^9 \equiv \frac{n}{2} \pmod{n}.$$

From the above, there must exist f such that $3 \leqslant f \leqslant n-3$ and

$$d^3 \equiv f \pmod{n} \quad \text{and} \quad f^3 \equiv \frac{n}{2} \pmod{n}.$$

Conversely, let

$$c^3 \equiv \frac{n}{2} \pmod{n},$$

then c^3 is an odd multiple of $\frac{1}{2}n$ and $(2c)^3$ is an even multiple of $\frac{1}{2}n$. That is why

$$(2c)^3 \equiv 0 \pmod{n}.$$

Now, assume that

$$c^3 \equiv \frac{n}{2} \pmod{n} \quad \text{and} \quad d^3 \equiv c \pmod{n},$$

then d must be odd and

$$d^9 \equiv \frac{n}{2} \pmod{n}.$$

Of course $n \nmid d^3 - \frac{1}{2}n$. So,

$$\frac{n}{2} \nmid d^3 \quad \text{and} \quad n \nmid (2d)^3.$$

Besides, $n \mid d^9 - \frac{1}{2}n$, d^9 is an odd multiple of $\frac{1}{2}n$ and

$$(2d)^9 \equiv 0 \pmod{n}.$$

Therefore, there must exist an even number k such that $2 \leqslant k \leqslant n-2$,

$$k^3 \equiv 0 \pmod{n} \quad \text{and} \quad (2d)^3 \equiv k \pmod{n}.$$

That is why every directed edge in the subdigraph Com(0) yields an appropriate directed edge in Com($\frac{1}{2}n$) and conversely, too. Finally, the subdigraph Com(0) is isomorphic to Com($\frac{1}{2}n$). □

It can be noticed that the digraph $\Gamma(2k)$ for odd k always contains exactly two copies of the digraph $\Gamma(k)$. Hence, $\Gamma(2k)$ is symmetric, for every natural, odd number k.

3. Connection with the Carmichael λ-function

Recall the definition and some properties of the Carmichael λ-function $\lambda(n)$ which was first defined in [2] and which modifies the Euler function $\varphi(n)$.

Let n be a positive integer. The Carmichael λ-function $\lambda(n)$ is defined as follows:
$\lambda(1) = 1 = \varphi(1)$,
$\lambda(2) = 1 = \varphi(2)$,
$\lambda(4) = 2 = \varphi(4)$,
$\lambda(2^k) = 2^{k-2} = \frac{1}{2}\varphi(2^k)$ for $k \geqslant 3$,
$\lambda(p^k) = (p-1)p^{k-1} = \varphi(p^k)$ for any odd prime p and $k \geqslant 1$,
$\lambda(p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}) = \operatorname{lcm}(\lambda(p_1^{k_1}), \lambda(p_2^{k_2}), \dots, \lambda(p_s^{k_s}))$,
where $p_1, p_2, \dots, p_s$ are distinct primes for $k_i \geqslant 1$, $i \in \{1, \dots, s\}$ and $\operatorname{lcm}(a, b)$ denotes the least common multiple of numbers a and b.

By definition $\lambda(n) \mid \varphi(n)$. Let $t = \operatorname{ord}_n g$ denote the multiplicative order of g modulo n (that means t is the least natural number such that $g^t \equiv 1 \pmod{n}$).

The next theorem generalizes the well-known Euler's theorem which says that $a^{\varphi(n)} \equiv 1 \pmod{n}$ if and only if $\gcd(a, n) = 1$, where $\gcd(a, n)$ is the greatest common divisor of numbers a and n.

Lemma 4 (Carmichael's Theorem, see [2] and [6]). *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 $\operatorname{ord}_n g = \lambda(n)$.*

Theorem 3. *Let $n > 2$. Then there exists a cycle of length t in the digraph $\Gamma(n)$ if and only if $t = \operatorname{ord}_d 3$ for some even positive divisor d of $\lambda(n)$.*

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

$$a^{3^t} \equiv a \pmod{n},$$

which implies that t is the least positive integer for which

$$a^{3^t} - a \equiv a(a^{3^t-1} - 1) \equiv 0 \pmod{n}.$$

Then $\gcd(a, a^{3^t-1} - 1) = 1$. So if $n_1 = \gcd(a, n)$ and $n_2 = n/n_1$, then t is the least positive integer such that

$$a \equiv 0 \pmod{n_1}, \quad a^{3^t-1} \equiv 1 \pmod{n_2}$$

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

$$b \equiv 1 \pmod{n_1}, \quad b \equiv a \pmod{n_2}.$$

Therefore, t is the least positive integer such that

$$b^{3^t-1} \equiv 1 \pmod{n_1}, \quad b^{3^t-1} \equiv a^{3^t-1} \equiv 1 \pmod{n_2}$$

and consequently $b^{3^t-1} \equiv 1 \pmod{n}$. Let Let $c = \operatorname{ord}_n b$. Then (using the elementary group theory)

$$c \mid 3^t - 1 \quad \text{and} \quad 3^t \equiv 1 \pmod{c}.$$

If c is odd then from $3^t \equiv 1 \pmod{2}$ we get that t is the least positive integer such that $3^t \equiv 1 \pmod{2c}$.

Let

$$d = \begin{cases} 2c, & \text{if } c \text{ is odd,} \\ c, & \text{if } c \text{ is even.} \end{cases}$$

Then by Carmichael's Theorem (see Lemma 4) it follows that $t = \operatorname{ord}_d 3$ and $d \mid \lambda(n)$.

Conversely, suppose that d is an even positive divisor of $\lambda(n)$ and let $t = \operatorname{ord}_d 3$. By Carmichael's Theorem, there exists a residue g modulo n such that $\operatorname{ord}_n g = \lambda(n)$. Let $h = g^{\lambda(n)/d}$. Then $\operatorname{ord}_n h = d$. We have $d \mid 3^t - 1$ and $d \nmid 3^k - 1$ for $1 \leqslant k < t$. So, t is the least positive integer for which

$$h^{3^t-1} \equiv 1 \pmod{n} \quad \text{and} \quad h \cdot h^{3^t-1} = h^{3^t} \equiv h \pmod{n}.$$

Hence, h is a vertex of some t-cycle of $\Gamma(n)$. $\square$

Corollary 2. *Let $m \geqslant 1$. A Fermat number $F_m = 2^{2^m} + 1$ is a prime number if and only if the components of $\Gamma(F_m)$ are cycles of lengths which are powers of 2 (except three isolated fixed points at 0, 1 and $F_m - 1$).*

Proof. If a Fermat number is not a prime then it cannot be of the form p^α, where p is a prime and $\alpha > 1$. Therefore, by Theorem 1, the digraph $\Gamma(F_m)$ contains more than 3 fixed points.

Now, let F_m be a prime number. Then, by Theorem 3, there is a cycle of length t in $\Gamma(F_m)$ if and only if $t = \operatorname{ord}_d 3$ for some divisor d of $\varphi(F_m) = 2^{2^m}$. Of course, the order t of 3 in the multiplicative group of vertices of $\Gamma_1(F_m)$ must be a divisor of the group order equal to 2^{2^m}. Hence, t is a power of 2 and the only cycles of odd length are the fixed points equal to 0, 1, and $F_m - 1$. $\square$

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

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

[5] *M. Křížek and L. Somer*: On a connection of number theory with graph theory. Czech. Math. J. 54 (2004), 465–485.

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

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

[8] *W. Sierpiński*: Elementary Theory of Numbers. North-Holland, 1988.

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

Author's address: J. Skowronek-Kaziów, Faculty of Mathematics, University of Zielona Góra, ul. prof. Z. Szafrana 4a, 65-516 Zielona Góra, Poland, e-mail: `J.Skowronek-Kaziow@wmie.uz.zgora.pl`.