Journal of Mathematical Extension
Vol. 11, No. 1, (2017), 47-56
ISSN: 1735-8299
URL: http://www.ijmex.com

Some Digraphs Attached with the Congruence $x^5 \equiv y \,(\mathbf{mod}\, n)$

M. Rahmati
Payame Noor University

Abstract. In this paper, we associate to each natural number n a digraph $\Gamma(n)$ whose set of vertices is $H = \{0, 1, \cdots, n-1\}$ and for which there is a directed edge from $a \in H$ to $b \in H$ if $a^5 \equiv b \,(\mathrm{mod}\, n)$. We determine the number of the fixed points of $\Gamma(n)$. We also give the structure of $\Gamma(n)$ for $n = 2^k$ and $n = 5^k$, where k is a natural number. Making use of the Carmichael's Theorem, we present a simple condition for the existence of cycles in $\Gamma(n)$. Let $\Gamma_1(n)$ be the subdigraph induced by the vertices which are coprime to n. We discuss when $\Gamma_1(n)$ is regular or semiregular.

AMS Subject Classification: 11A07; 05C20
Keywords and Phrases: Digraph, carmichael λ-function, group

1. Introduction

Let n be a natural number and $H = \{0, 1, \ldots, n-1\}$. We consider the directed graph $\Gamma(n)$ whose vertices are the elements of H such that there exists exactly one directed edge from a to b if and only if $a^5 \equiv b \,(\mathrm{mod}\, n)$. If $a_1, a_2, \ldots, a_\ell$ are distinct elements of H and

$$a_1^5 \equiv a_2 \,(\mathrm{mod}\, n),\ a_2^5 \equiv a_3 \,(\mathrm{mod}\, n), \ldots,\ a_\ell^5 \equiv a_1 \,(\mathrm{mod}\, n),$$

then the elements $a_1, a_2, \ldots, a_\ell$ constitute a *cycle* of length ℓ. We call a cycle of length 1 a *fixed point*. A *component* of a digraph is a subdigraph

Received: March 2016; Accepted: September 2016

which is a maximal connected subgraph of the associated nondirected graph (see for example [4], page 13). For $a \in H$, denote the number of directed edges coming to a by $indeg(a)$ and denote the number of directed edges leaving the vertex a by $outdeg(a)$. The outdegree for every vertex of the digraph $\Gamma(n)$ is equal to 1. Therefore, the number of component of $\Gamma(n)$ is equal to the number of all cycles. The digraph $\Gamma(13)$ is presented in Figure 1.

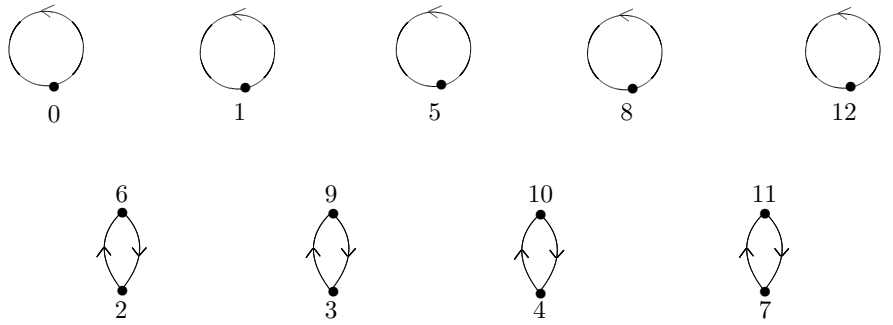

Figure 1. The digraph $\Gamma(13)$

We call a digraph *regular* if the indegree of each vertex is equal to 1. A digraph is *semiregular* if there exists a positive integer d such that each vertex either has indegree d or 0.

We consider two subdigraphs of $\Gamma(n)$. Let $\Gamma_1(n)$ be the subdigraph induced by the vertices which are coprime to n and $\Gamma_2(n)$ be the subdigraph induced by the vertices which are not coprime to n. It is easy to see that $\Gamma_1(n)$ and $\Gamma_2(n)$ are disjoint and $\Gamma(n) = \Gamma_1(n) \cup \Gamma_2(n)$. For this reason the main aim of this paper is to study the structure of these subdigraphs.

We give some connections between graph theory, group theory and number theory motivated by results of [1], [3], [6], [10], [8], and [12] as well as by the results of [9] which have considered a similar digraphs corre-

sponding to the congruence relations:

$$x^2 \equiv y \,(\mathrm{mod}\, n) \text{ and } x^3 \equiv y \,(\mathrm{mod}\, n).$$

The reader should be aware that some properties of the digraph corresponding to the general congruence relation $x^k \equiv y \,(\mathrm{mod}\, n)$ are given in the interesting article [11].
In this paper, the conditions for regularity and semiregularity of the subdigraph $\Gamma_1(n)$ are presented (see Theorem 2.1). We give a formula for the number of fixed points of the digraph $\Gamma(n)$ (see Theorem 2.2). Finally, we illustrate the structure of $\Gamma(2^k)$ and $\Gamma(5^k)$, where k is a natural number (see Theorems 2.6 and 2.7).

2. Main results

Let

$$\varepsilon(n) = \begin{cases} t+1 & \text{if } 25|n, \\ t & \text{if } 25 \nmid n, \end{cases}$$

where t be the number of distinct primes divided n which are congruent to 1 modulo 5. As an application of group theory and number theory, we have the following theorems:

Theorem 2.1. *The digraph $\Gamma_1(n)$ is semiregular if and only if $5|\varphi(n)$. Moreover, if a is a vertex of $\Gamma_1(n)$, then*

$$indeg(a) = 0 \qquad orindeg(a) = 5^{\varepsilon(n)}.$$

Proof. Since the residues coprime to n form a group under multiplication modulo n, it is easy to see that $indeg(a) = indeg(1)$ if $indeg(a) > 0$ and $gcd(a, n) = 1$, where $gcd(a, n)$ is the greatest common divisor of the numbers a and n. Therefore it suffices to determine only $indeg(1)$. Let $\rho(n)$ be the number of solutions of the congruence $x^5 \equiv 1 \,(\mathrm{mod}\, n)$. Now we find $\rho(n)$. Consider the following cases:
(1) Let $n = 5^\alpha$ and $\alpha \geqslant 2$. In this case, $\rho(n) = 5$. In fact, the set of solutions of $x^5 \equiv 1 \,(\mathrm{mod}\, n)$ is $\{1, 5^{\alpha-1}+1, 2.5^{\alpha-1}+1, 3.5^{\alpha-1}+1, 4.5^{\alpha-1}+1\}$.
(2) Let $n = p^\alpha$, where $\alpha \geqslant 1$ and p is congruent to 1 modulo 5. In this

case, $\rho(n) = 5$ by [7, Corollary 2.42].
In the other case, $\rho(n) = 1$ again by [7, Corollary 2.42]. Since $\rho(n)$ is a multiplicative function (see [5, Theorem 3.11]), $indeg(a) = 0$ or $indeg(a) = 5^{\varepsilon(n)}$.
Let $\Gamma_1(n)$ be a semiregular graph and let $a \in \Gamma_1(n)$ such that $indeg(a) = 5^{\varepsilon(n)}$. If

$$H = \{0 \leqslant m \leqslant n-1 | (m,n) = 1, m^5 \equiv 1 \,(\mathrm{mod}\, n)\},$$

then H is a subgroup of $\Gamma_1(n)$ and hence $|H| = 5^{\varepsilon(n)}$ divides $\varphi(n)$. Conversely, suppose that $5 \nmid \varphi(n)$. Then every vertex in $\Gamma_1(n)$ has indegree equal to 1. This completes the proof. □

Let n be an arbitrary natural number and f be a polynomial with integer coefficients. Then the function $\rho_f(n) = |\{0 \leqslant m \leqslant n-1 : f(m) \equiv 0 \,(\mathrm{mod}\, n)\}|$ is a multiplicative function (see [5, Theorem 3.11]).
The following theorem gives a formula for the number of fixed points of the digraph $\Gamma(n)$.

Theorem 2.2. *Let $n = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} q_1^{\beta_1} q_2^{\beta_2} \cdots q_t^{\beta_t}$, where p_i and q_i are distinct odd prime numbers and $p_i \equiv -1 \,(mod\, 4)$ and $q_i \equiv 1 \,(mod\, 4)$. Then the number $L(n)$ of fixed points of $\Gamma(n)$ is equal to*

$$L(n) = 3^s \times 5^t \times \begin{cases} \alpha + 1 & \text{if } \alpha \in \{0,1,2\} \\ 5 & \text{if } \alpha = 3 \\ 3^2 & \text{if } \alpha \geqslant 4 \end{cases}$$

Proof. Let $f(x) = x^5 - x$. It is easy to see that $\rho_f(2) = 2$, $\rho_f(2^2) = 3$ and $\rho_f(2^3) = 5$. For $n = 2^{\alpha}$, $\alpha \geqslant 4$, the zeros of f are in the set

$$\{0, 1, 2^{\alpha-1} \pm 1, 2^{\alpha-2} \pm 1, 3.2^{\alpha-2} \pm 1, n-1\}.$$

Hence $\rho(2^{\alpha}) = 3^2$.
For $n = p^{\alpha}$, where p is odd prime number such that $p \equiv -1 \,(\mathrm{mod}\, 4)$ and $\alpha \geqslant 1$, the zeros of f are in the set $\{0, 1, n-1\}$. Hence $\rho(p^{\alpha}) = 3$.
If $n = q^{\beta}$, where q is odd prime number such that $q \equiv 1 \,(\mathrm{mod}\, 4)$ and $\beta \geqslant 1$, then $\rho(q^{\beta}) = 5$, by [7, Corollary 2.42]. □

Let n be a positive integer. The Carmichael λ-function $\lambda(n)$ is defined as follows (see [2, page 232]):

$$\lambda(1) = \varphi(1),\ \lambda(2) = \varphi(2),\ \lambda(4) = \varphi(4),$$
$$\lambda(2^k) = \frac{1}{2}\varphi(2^k) \ \text{ for } k \geqslant 3,$$
$$\lambda(p^k) = \varphi(p^k) \text{ for any odd prime } p \ \text{ and } k \geqslant 1,$$

Let $t = ord_n g$ denote the multiplicative order of g modulo n. The following theorem generalizes the well-known Euler's Theorem:

Theorem 2.3. (Carmichael's Theorem) *Let $a, n \in \mathbb{N}$. Then*

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

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

$$ord_n g = \lambda(n).$$

Proof. See [2, page 233]. □

Theorem 2.4. *Let $n > 2$ be a natural number. Then there exists a cycle of length ℓ in the digraph $\Gamma(n)$ if and only if $\ell = ord_d 5$ for some positive divisor d of $\lambda(n)$.*

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

$$a^{5^\ell} \equiv a\,(\mathrm{mod}\, n),$$

which implies that ℓ is the least positive integer for which

$$a^{5^\ell} - a \equiv a(a^{5^\ell - 1} - 1) \equiv 0\,(\mathrm{mod}\, n).$$

Since $\gcd(a, a^{5^\ell - 1} - 1) = 1$, it follows that if $n_1 = \gcd(a, n)$ and $n_2 = n/n_1$, then ℓ is the least positive integer such that

$$a \equiv 0\,(\mathrm{mod}\, n_1),$$

$$a^{5^{\ell}-1} \equiv 1 \,(\mathrm{mod}\, n_2).$$

Therefore $\gcd(n_1, n_2) = 1$. Hence, by the Chinese reminder theorem there exits an integer b such that

$$b \equiv 1 \,(\mathrm{mod}\, n_1),$$

$$b \equiv a \,(\mathrm{mod}\, n_2).$$

Therefore ℓ is the least positive integer such that

$$b^{5^{\ell}-1} \equiv 1 \,(\mathrm{mod}\, n_1),$$

$$b^{5^{\ell}-1} \equiv a^{5^{\ell}-1} \equiv 1 \,(\mathrm{mod}\, n_2).$$

And consequently

$$b^{5^{\ell}-1} \equiv 1 \,(\mathrm{mod}\, n).$$

Let $d = ord_n b$. Then ℓ is the least positive integer such that $5^{\ell} \equiv 1 \,(\mathrm{mod}\, d)$. Therefore $\ell = ord_d 5$. Since $d = ord_n b$ and $gcd(b, n) = 1$, then by Carmichael's Theorem, we have $d \mid \lambda(n)$.
Conversely, suppose that d is a positive divisor of $\lambda(n)$ and let $\ell = ord_d 5$. by Carmichael's Theorem there exists a residue g modulo n such that $ord_n g = \lambda(n)$. Let $h = g^{\lambda(n)/d}$. Then $ord_n h = d$. Since $d|5^{\ell} - 1$ but $d \nmid 5^t - 1$ whenever $1 \leqslant t < \ell$, we see that ℓ is the least positive integer for which

$$h^{5^{\ell}-1} \equiv 1 \,(\mathrm{mod}\, n).$$

Therefore

$$h.h^{5^{\ell}-1} \equiv h^{5^{\ell}} \equiv h \,(\mathrm{mod}\, n).$$

It follows that h is a vertex in a ℓ-cycle of $\Gamma(n)$. $\square$

Theorem 2.5. *The number of components of* $\Gamma(n)$ *is 5 if* $n = 8$ *or* $n = q^k$*, where* k *is a natural number and* q *is a prime number such that* $q \equiv 1 \,(mod\, 4)$.

Proof. If $n = 8$, then we have clearly 5 components. If $n = q^k$, where k is a natural number and q is a prime number such that $q \equiv 1 \,(\mathrm{mod}\, 4)$, then we have exactly 5 fixed points. In the case that we have more

than 5 components, there exists a cycle of length $t > 1$ and $t = ord_d 5$ for some even positive divisor d of $\lambda(n)$. Then t is the least positive number such that $5^t \equiv 1 \pmod d$ and $d|5^t - 1$. Since also $d|\lambda(n)$, we have $d = 4|5^t - 1$, which is a contradiction by minimality of t. Thus $\Gamma(n)$ has 5 components. $\square$

For an arbitrary real number x, denote by $\lceil x \rceil$ the smallest natural number greater than or equal to x. In the rest of this paper, we show that the digraphs $\Gamma(2^k)$ and $\Gamma(5^k)$ have interesting structures (see Figures 2 and 3).

Theorem 2.6. *Let k be a natural number. The digraph $\Gamma_1(2^k)$ contains (except for 8 fixed points) only the cycles of lengths which are the powers of 2 and $\Gamma_2(2^k)$ is a tree with the root in 0. Moreover, $indeg(0) = 2^{k-\lceil k/5 \rceil}$.*

Proof. Let $n = 2^k$. Then every digraph $\Gamma_1(2^k)$ and $\Gamma_2(2^k)$ contains exactly $n = 2^{k-1}$ vertices. Of course $5 \nmid \varphi(n)$ and hence, $\Gamma_1(2^k)$ contains only cycles. It is easy to see that $1, 2^{k-1} \pm 1, 2^{k-2} \pm 1, 2^{k-2}.3 \pm 1, 2^k - 1$ are all fixed points of $\Gamma_1(2^k)$. We know that there is a cycle of length ℓ if and only if $\ell = ord_d 5$, for some divisor d of $\lambda(n) = 2^{k-2}$. On the other hand, the order ℓ of 5 in the multiplicative group of vertices of $\Gamma_1(2^k)$ must be a divisor of the group order equal to $\varphi(n) = 2^{k-1}$. Hence, ℓ is the power of 2.
It is not hard to check that we have exactly $2^{k-\lceil k/5 \rceil}$ elements in $\Gamma_2(2^k)$ namely $2^{\lceil k/5 \rceil}, 2.2^{\lceil k/5 \rceil}, 3.2^{\lceil k/5 \rceil}, \cdots, 2^{k-\lceil k/5 \rceil}.2^{\lceil k/5 \rceil} = 0$ which are mapped into 0. $\square$

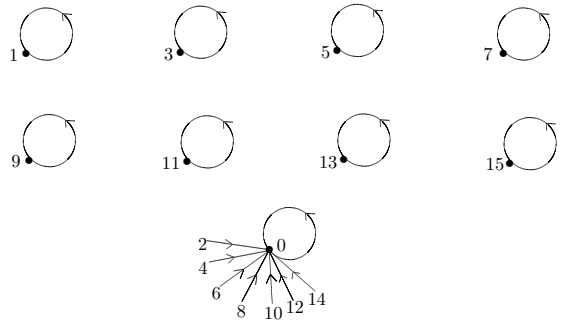

Figure 2. The digraph $\Gamma(2^4)$

We end this paper by the following theorem.

Theorem 2.7. *Let k be a natural number and $n = 5^k$. Then the digraph $\Gamma_1(n)$ consists of four isomorphic trees. Moreover, $\Gamma_2(n)$ is a tree with the root in 0 and $indeg(0) = 5^{k-\lceil k/5 \rceil}$.*

proof. Theorem 2.5 implies that the graph $\Gamma(n)$ has exactly five components with five fix points. It is easy to see that we have $5^{k-\lceil k/5 \rceil}$ elements in $\Gamma_2(n)$, namely $5^{\lceil k/5 \rceil}, 2.5^{\lceil k/5 \rceil}, 3.5^{\lceil k/5 \rceil}, \cdots, 5^{k-\lceil k/5 \rceil}.5^{\lceil k/5 \rceil} = 0$ which are mapped into 0. Since $5|\varphi(n) = 4.5^{k-1}$, we have $\Gamma_1(n)$ is a semiregular and every vertex either has degree 0 or 5. Therefore $\Gamma_1(n)$ consists of four trees. Now let $\{1, n-1, a, n-a\}$ be the set of all fix points of $\Gamma_1(n)$. Let T_1, T_{n-1}, T_a and T_{n-a} be the trees that contain the numbers $1, n-1, a$ and $n-a$, respectively. By definition of $\Gamma(n)$, we have $T_1 \cong T_{n-1}$ and $T_a \cong T_{n-a}$. Since $\gcd(a, n) = 1$, if we multiply each vertex of the tree T_1 by the number a, we reach the tree T_a. Hence $T_1 \cong T_a$ and so the proof is complete. □

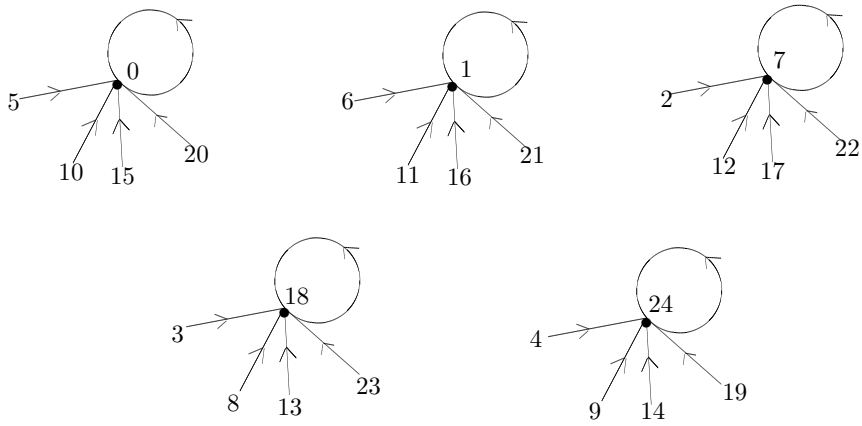

Figure 3. The digraph $\Gamma(5^2)$

Acknowledgment
I would like to thank Professor Ali Reza Naghipour for his helpful remarks which have contributed to improve the presentation of the paper.

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] G. A. Jones and J. Mary Jones, *Elementary Number Theory*, Springer-Verlag London, 1988.

[6] M. Křížek and L. Somer, Sophie Germain little suns, *Math. Slovaca*, 54 (5) (2004), 433-442.

[7] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An Introduction to the Theory of Numbers*, (John Wiley and Sons, Inc. 1991).

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

[9] J. Skowronek-Kazijów, Some digraphs arising from number theory and remarks on the zero-divisor graph of the Z_n, *Information Processing Letters*, 108 (2008), 165-169.

[10] L. Somer and M. Křížek, On a connection of number theory with graph theory, *Czechoslovak Math. J.*, 54 (129) (2004), 465-485.

[11] L. Somer and M. Křížek, The structure of digraph associated with the congruence $x^k \equiv y \pmod{n}$, *Czechoslovak Math. J.*, 61 (136) (2011), 337-358.

[12] L. Szalay, A discrete iteration in number theory, *Berzseneyi Dániel Tanárk. Föisk. Tud. Közl., Termtud.*, 8 (1992), 71-91. (In Hungarian.)

Marzieh Rahmati
Department of Mathematics
Instructor of Mathematics
Payame Noor University
Tehran, Iran
E-mail: m.rahmati@pnu.ac.ir