Czechoslovak Mathematical Journal

Guixin Deng; Pingzhi Yuan

Isomorphic digraphs from powers modulo p

Czechoslovak Mathematical Journal, Vol. 61 (2011), No. 3, 771–779

Persistent URL: http://dml.cz/dmlcz/141637

Czechoslovak Mathematical Journal, 61 (136) (2011), 771–779

ISOMORPHIC DIGRAPHS FROM POWERS MODULO p

Guixin Deng, Pingzhi Yuan, Guangzhou

(Received May 12, 2010)

Abstract. Let p be a prime. We assign to each positive number k a digraph G_p^k whose set of vertices is $\{1, 2, \ldots, p-1\}$ and there exists a directed edge from a vertex a to a vertex b if $a^k \equiv b \pmod p$. In this paper we obtain a necessary and sufficient condition for $G_p^{k_1} \simeq G_p^{k_2}$.

Keywords: congruence, digraph, component, height

MSC 2010: 05C20, 05C38, 11A15

1. Introduction

This paper solves a problem asked in [1]. Let p be a prime and k a positive integer. In [1] the authors constructed a digraph whose set of vertices is $\{1, 2, \ldots, p-1\}$ and there exists a directed edge from a vertex a to a vertex b if $a^k \equiv b \pmod p$. It is easy to see that $G_p^{k_1} = G_p^{k_2}$ if and only if $k_1 \equiv k_2 \pmod{(p-1)}$. And in [1] the authors noted that $G_p^{k_1}$ and $G_p^{k_2}$ can be isomorphic without the above condition. For example, $G_{11}^2 \simeq G_{11}^8$. In this paper we obtain a necessary and sufficient condition for $G_p^{k_1} \simeq G_p^{k_2}$.

First, we introduce some concepts and notation. The *indegree* of a vertex $a \in G_p^k$, denoted by $\operatorname{indeg}_p^k(a)$, is the number of directed edges coming to a, and the *outdegree* of a is the number of edges leaving a. It is easy to see that the indegree of a vertex in G_p^k is $\gcd(p-1, k)$ or 0. Cycles of length t are called t-cycles. It is clear that each component of G_p^k contains a unique cycle. Let $\mathscr{A}(G_p^k)$ denote the set of integers such that $m \in \mathscr{A}(G_p^k)$ if and only if G_p^k contains an m-cycle. And for any positive integer t, let $A_t(G_p^k)$ denote the number of t-cycles in G_p^k.

Supported by the NSF of China (No. 10571180) and Guangdong Provincial Natural Science Foundation (No. 8151027501000114).

2. Results on cycles and heights

Consider a digraph G_p^k, where p is a prime, and express the factor $p-1$ as

$$p-1=uv, \tag{2.1}$$

where u is the largest divisor of $p-1$ relatively prime to k. Then we need the following definitions and results.

Definition 2.1. First we define the height function on the vertices and components of G_p^k. Let c be a vertex of G_p^k, we define $h(c)$ to be the minimal nonnegative integer i such that c^{k^i} is congruent modulo p to a cycle vertex in G_p^k. And if C is a component of G_p^k, we set $h(C)=\sup\limits_{c\in C} h(c)$. Finally, we define $h(G_p^k)=\sup\limits_{c\in G_p^k} h(c)$.

Definition 2.2. For any nonnegative integer $i \geqslant 0$, if C is a component of G_p^k, we define

$$\mathscr{F}^i(C)=\{c\in C \mid h(c)=i\},$$

and

$$\mathscr{F}^i(G_p^k)=\{c\in G_p^k \mid h(c)=i\}.$$

Theorem 2.1. *There exists a t-cycle in G_p^k if and only if*

$$t=\operatorname{ord}_d k \tag{2.2}$$

for some divisor d of u, where $\operatorname{ord}_d k$ denotes the multiplicative order of k modulo d.

Corollary 2.1. *Let $p-1=uv$, where u is the largest divisor of $p-1$ relatively prime to k. Then*

$$\mathscr{A}(G_p^k)=\{\operatorname{ord}_d k \mid d \ \text{ is a divisor of } u\}. \tag{2.3}$$

Theorem 2.2. *Let c be a cycle vertex and let $T(c)$ denote the tree whose root is c and whose additional vertices are the noncycle vertices b for which $b^{k^i}\equiv c \pmod p$ for some $i\in\mathbb{N}$, but $b^{k^{i-1}}$ is not congruent to a cycle vertex modulo p. Then for any two cycle vertices c_1, c_2 we have $T(c_1)\simeq T(c_2)$.*

Corollary 2.2. *For any component C of G_p^k, $h(C)=h(G_p^k)$.*

Theorem 2.3. *Let c be a vertex of G_p^k. If i is the minimal nonnegative integer such that $\operatorname{ord}_p c \mid k^i u$, then $h(c) = i$.*

Theorem 2.4. *Let $p-1 = uv$, where u, v are as above. Then the number of all cycle points contained in G_p^k is equal to u.*

Corollary 2.3. *Let $t \geqslant 1$ be a fixed integer. Then any two components in G_p^k containing t-cycles are isomorphic. And if C is the component of G_p^k containing 1, then for any $i \geqslant 0$ we have*

$$|\mathscr{F}^i(C)| = \frac{|\mathscr{F}^i(G_p^k)|}{u}. \tag{2.4}$$

Theorems 2.1, 2.2, 2.3 and 2.4 were proved in [1].

Theorem 2.5. *Let $t \in \mathscr{A}(G_p^k)$. Then*

$$A_t(G_p^k) = \frac{1}{t}\left[\gcd(p-1, k^t-1) - \sum_{d \mid t, d \neq t} dA_d(G_p^k)\right]. \tag{2.5}$$

This was proved in [2].

3. The main results

Our main theorem, Theorem 3.2, gives a characterization for $G_p^{k_1}$ to be isomorphic to $G_p^{k_2}$ for any two positive integers k_1, k_2 and a prime p.

The following theorem is easy to prove.

Theorem 3.1. *Let p be a fixed prime and k_1, k_2 two positive integers. Let C_i be the component of $G_p^{k_i}$ containing the vertex 1. Then $G_p^{k_1} \simeq G_p^{k_2}$ if and only if*

(i)

$$\mathscr{A}(G_p^{k_1}) = \mathscr{A}(G_p^{k_2}); \tag{3.1}$$

(ii) *for any positive integer t,*

$$A_t(G_p^{k_1}) = A_t(G_p^{k_2}); \tag{3.2}$$

(iii)

$$C_1 \simeq C_2. \tag{3.3}$$

Theorem 3.2 (Main Theorem)**.** *Let p be a fixed prime and k_1, k_2 two positive integers. Then $G_p^{k_1} \simeq G_p^{k_2}$ if and only if the following two conditions are satisfied.*

(i)

$$\gcd(p-1, k_1) = \gcd(p-1, k_2); \tag{3.4}$$

(ii) *there exists a factorization of $p-1 = uv$, where u is the largest divisor of $p-1$ relatively prime to k_1 as well as the largest divisor of $p-1$ relatively prime to k_2. Moreover, for any d such that $d \mid u$ we have*

$$\operatorname{ord}_d k_1 = \operatorname{ord}_d k_2. \tag{3.5}$$

Proof. We only prove the necessity of the theorem here and leave the rest of proof to Section 4. Now assume that $\varphi\colon\ G_p^{k_1} \longrightarrow G_p^{k_2}$ is an isomorphism of digraphs. Then φ must preserve indgeree of vertices. Hence, $\gcd(p-1, k_1) = \gcd(p-1, k_2)$. (i) holds. The first part of (ii) follows from (i). For the other part by Theorem 3.1 we have $\mathscr{A} = \mathscr{A}(G_p^{k_1}) = \mathscr{A}(G_p^{k_2})$, and $A_t(G_p^{k_1}) = A_t(G_p^{k_2})$ for any positive integer t. By Corollary 2.1 and Theorem 2.5 we have

$$\{\operatorname{ord}_d k_1 \mid d \text{ is a divisor of } u\} = \{\operatorname{ord}_d k_2 \mid d \text{ is a divisor of } u\}, \tag{3.6}$$

and for any $t \in \mathscr{A}$

$$\begin{aligned}\frac{1}{t}\Big[\gcd(p-1, k_1^t - 1) - \sum_{d\mid t, d\neq t} dA_d(G_p^{k_1})\Big] \\ = \frac{1}{t}\Big[\gcd(p-1, k_2^t - 1) - \sum_{d\mid t, d\neq t} dA_d(G_p^{k_2})\Big].\end{aligned} \tag{3.7}$$

Hence, $\gcd(p-1, k_1-1) = \gcd(p-1, k_2-1)$; since $1 \in \mathscr{A}$, by induction on the length of cycles we see that $\gcd(p-1, k_1^t - 1) = \gcd(p-1, k_2^t - 1)$ for any $t \in \mathscr{A}$. Now if $d \mid u$, $t_1 = \operatorname{ord}_d k_1, t_2 = \operatorname{ord}_d k_2$, then $t_1 \in \mathscr{A}, t_2 \in \mathscr{A}$. We have

$$\gcd(uv, k_1^{t_1} - 1) = \gcd(uv, k_2^{t_1} - 1),$$

but $d \mid u$, $d \mid k_1^{t_1} - 1$, hence $d \mid k_2^{t_1} - 1$, i.e. $t_2 \mid t_1$. Similarly we get $t_1 \mid t_2$. Hence, $t_1 = t_2$. $\square$

4. Proof of some lemmas and of the main theorem

Our main theorem follows directly from Lemma 4.1 and Lemma 4.6.

Lemma 4.1. *For any fixed prime p and two positive integers k_1, k_2, the conditions* (3.4), (3.5) *in Theorem* 3.2 *imply* (3.1) *and* (3.2).

Proof. From Corollary 2.1 we get $\mathscr{A}(G_p^{k_1}) = \mathscr{A}(G_p^{k_2})$, and by the proof of Theorem 3.2 it is sufficient to show that $\gcd(uv, k_1^t - 1) = \gcd(uv, k_2^t - 1)$ for any $t \in \mathscr{A}(G_p^{k_1})$. But $\gcd(v, k_1^t - 1) = \gcd(v, k_2^t - 1) = 1$, hence if $c \mid \gcd(uv, k_1^t - 1)$ then $c \mid u$. Let $t_1 = \operatorname{ord}_c k_1 = \operatorname{ord}_c k_2$, then $t_1 \mid t$, hence $c \mid k_2^t - 1$. We have $c \mid \gcd(uv, k_2^t - 1)$. Similarly if $d \mid \gcd(uv, k_2^t - 1)$, then $d \mid \gcd(uv, k_1^t - 1)$. We get $\gcd(uv, k_1^t - 1) = \gcd(uv, k_2^t - 1)$. □

Lemma 4.2. *For any fixed prime p and two positive integers k_1, k_2, let C_i be the component of $G_p^{k_i}$ containing the vertex 1. If (3.4) holds, then $|\mathscr{F}^j(C_1)| = |\mathscr{F}^j(C_2)|$ for any integer $j \geqslant 0$.*

Proof. By hypothesis there exists a factorization of $p - 1 = uv$, where u is the largest divisor of $p - 1$ relatively prime to k_1 as well as the largest divisor of $p - 1$ relatively prime to k_2. Hence, if q is a prime divisor of v, then q is also a prime divisor of k_i $(i = 1, 2)$. Then we have the following factorization of v, k_1 and k_2:

$$v = \prod_{i=1}^{r} p_i^{e_i}, \quad k_1 = m \prod_{i=1}^{r} p_i^{x_i}, \quad k_2 = n \prod_{i=1}^{r} p_i^{y_i},$$

where p_i are primes and $e_i \geqslant 1$, $x_i \geqslant 1$, $y_i \geqslant 1$, and $\gcd(m, uv) = \gcd(n, uv) = 1$. If $e_i > \min\{x_i, y_i\}$, then $x_i = y_i$ since

$$\gcd(uv, k_1) = \gcd(uv, k_2) = \prod_{i=1}^{r} p_i^{\min\{e_i, x_i\}} = \prod_{i=1}^{r} p_i^{\min\{e_i, y_i\}}.$$

Then after a permutation of indices there is an s such that $x_i = y_i$ and $x_i < e_i$ if $1 \leqslant i \leqslant s$, and $x_i \geqslant e_i$, $y_i \geqslant e_i$ if $s + 1 \leqslant i \leqslant r$.

Now let c be a nonzero vertex. If $c \in \mathscr{F}^j(G_p^{k_1})$ we have

$$\operatorname{ord}_p c \nmid k_1^{j-1} u \quad \text{and} \quad \operatorname{ord}_p c \mid k_1^j u.$$

But by the above discussion we also have

$$\operatorname{ord}_p c \nmid k_2^{j-1} u \quad \text{and} \quad \operatorname{ord}_p c \mid k_2^j u.$$

Hence, $c \in \mathscr{F}^j(G_p^{k_2})$. Consequently, $\mathscr{F}^j(G_p^{k_1}) \subseteq \mathscr{F}^j(G_p^{k_2})$, similarly $\mathscr{F}^j(G_p^{k_2}) \subseteq \mathscr{F}^j(G_p^{k_1})$, i.e. $\mathscr{F}^j(G_p^{k_1}) = \mathscr{F}^j(G_p^{k_2})$. Then by Corollary 2.3

$$|\mathscr{F}^j(C_1)| = \frac{|\mathscr{F}^j(G_p^{k_1})|}{u} = \frac{|\mathscr{F}^j(G_p^{k_2})|}{u} = |\mathscr{F}^j(C_2)|.$$

□

Now we consider the structure of the tree attached to the cycle point in G_p^k. Let G be any digraph and S a nonempty subset of vertices of G. We recall that the subdigraph K of G induced by S is a digraph whose vertices are those of S, and for any two vertices $a \in S$ and $b \in S$, the number of directed edges from a to b in K is equal to the number of directed edges from a to b in G.

The following notation is useful in the proof of our key lemma.

Definition 4.1. Given a prime p and a positive integer k, let a be a vertex in G_p^k. Then for any nonnegative integers i, j, we define

$$\begin{aligned} &\mathscr{F}^0(a) = \{a\},\\ &\mathscr{F}^i(a) = \{b \in G_p^k \mid b^{k^i} \equiv a \pmod p,\ b^{k^{i-1}} \text{ is not congruent modulo } p\\ &\qquad\qquad \text{to a cycle vertex, and } b \text{ is not a cycle point.}\} \text{ if } \ i > 0. \end{aligned}$$

Now define $a(j)$ to be the subdigraph of G_p^k induced by the vertices set $\bigcup\limits_{i=0}^{j} \mathscr{F}^i(a)$, and define the *height* of $a(j)$ as

$$h(a(j)) = \max\{i \mid i \leqslant j \text{ and } \mathscr{F}^i(a) \neq \emptyset\}.$$

Remark 4.1. Note that if $h(a) > 0$, then $\mathscr{F}^i(a) = \mathscr{F}^j(a)$ if and only if $i = j$ or they are both empty, and in this case $\mathscr{F}^1(a)$ is just the set of vertices coming into a.

Lemma 4.3. *Let C be the component of G_p^k containing* 1. *Then for any i, $1 \leqslant i \leqslant h(C)$ and any $a \in G_p^k$ with $h(a) > 0$, we have*

$$|\mathscr{F}^i(a)| = \sum_{j=0}^{i} |\mathscr{F}^j(C)| \text{ or } 0. \tag{4.1}$$

P r o o f. Note that $\sum\limits_{j=0}^{i} |\mathscr{F}^j(C)| = \operatorname{indeg}_p^{k^i}(1) > 0$ for any i, $1 \leqslant i \leqslant h(C)$. And $|\mathscr{F}^i(a)| = \operatorname{indeg}_p^{k^i}(a)$ since $h(a) > 0$. □

Lemma 4.4. *Let a be a vertex with positive height in G_p^k and let $\mathscr{F}^1(a) \neq \emptyset$. Then*

$$\mathscr{F}^{i+1}(a) = \biguplus_{b \in \mathscr{F}^1(a)} \mathscr{F}^i(b), \tag{4.2}$$

where $\biguplus$ means disjoint union.

Proof. It is immediate from Definition 4.1. $\square$

Lemma 4.5. *Let p be a prime and k_1, k_2 two positive integers, and let C_i be the component of $G_p^{k_i}$ which contains the vertex 1 ($i = 1, 2$). Let $a \in C_1$, $b \in C_2$ be two vertices of positive heights. If $a(i) \simeq b(j)$ for some i, j, then $h(a(i)) = h(b(j))$, and for any nonnegative integer $t \leqslant h(a(i))$, we have*

$$|\mathscr{F}^t(a)| = |\mathscr{F}^t(b)|. \tag{4.3}$$

Proof. Let $h_1 = h(a(i))$ and $h_2 = h(b(j))$. By symmetry we only need to prove $|\mathscr{F}^t(a)| \leqslant |\mathscr{F}^t(b)|$ and $h_1 \leqslant h_2$. Let $\varphi\colon\ a(i) \to b(j)$ be an isomorphism of digraphs. Then it is sufficient to show that φ maps $\mathscr{F}^t(a)$ into $\mathscr{F}^t(b)$.

We prove it by induction on t. If $t = 0$, then $\mathscr{F}^0(a) = \{a\}$ and $\mathscr{F}^0(b) = \{b\}$. It is clear that a is the only point with outdegree 0 in $a(i)$ and b is the only point with outdegree 0 in $b(j)$. And φ must preserve outdegree, thus $\varphi(a) = b$.

Now assume that for any $l < t$, φ maps $\mathscr{F}^l(a)$ into $\mathscr{F}^l(b)$. If $\mathscr{F}^t(a) = \emptyset$, the proof is completed. If there exists a vertex $c \in \mathscr{F}^t(a)$, then there exists a vertex $d \in \mathscr{F}^{t-1}(a)$ and $c^{k_1} \equiv d \pmod p$, i.e. there is a directed edge from c to d. Thus, there is also a directed edge from $\varphi(c)$ to $\varphi(d)$. But by induction $\varphi(d) \in \mathscr{F}^{t-1}(b)$, so we get $\varphi(c) \in \mathscr{F}^t(b)$. $\square$

The following lemma is the key to our main result.

Lemma 4.6. *Let p be a prime and k_1, k_2 two positive integers, and let C_i be the component of $G_p^{k_i}$ which contains the vertex 1 ($i = 1, 2$). If (3.4) holds, then $C_1 \simeq C_2$.*

Proof. We first show that for any two vertices $a \in C_1$ and $b \in C_2$ both with positive heights and any integer $i \geqslant 0$, if $h(a(i)) = h(b(i))$, then $a(i) \simeq b(i)$. We prove it by induction on $m = h(a(i)) = h(b(i))$. The assertion is obvious when $m = 0, 1$. Now assume that $m = h(a(i)) = h(b(i))$. Then $a(i) = a(m)$, $b(i) = b(m)$. Let $l = \gcd(p-1, k_1) = \gcd(p-1, k_2)$ and assume that we have $\mathscr{F}^1(a) = \{a_1, a_2, \ldots, a_l\}$, $\mathscr{F}^1(b) = \{b_1, b_2, \ldots, b_l\}$.

For $1 \leqslant i \leqslant m-1$, let $A_i = \{a_j \mid j \in \{1,2,\ldots,l\}$ and $h(a_j(m-1)) = i\}$, $B_i = \{b_j \mid j \in \{1,2,\ldots,l\}$ and $h(b_j(m-1)) = i\}$. We have

$$\mathscr{F}^1(a) = \biguplus_{i=1}^{m-1} A_i, \qquad \mathscr{F}^1(b) = \biguplus_{i=1}^{m-1} B_i. \tag{4.4}$$

Now we claim that $|A_i| = |B_i|$ for $i = 1,2,\ldots,m-1$. Otherwise there exists an integer t, $|A_t| \neq |B_t|$ and for any j such that $t < j \leqslant m-1$, $|A_j| = |B_j|$. By (4.2) and (4.4)

$$\begin{aligned}|\mathscr{F}^{t+1}(a)| &= \Sigma_{a_j\in A_1}|\mathscr{F}^t(a_j)| + \Sigma_{a_j\in A_2}|\mathscr{F}^t(a_j)| + \ldots + \Sigma_{a_j\in A_{m-1}}|\mathscr{F}^t(a_j)| \\ &= \Sigma_{a_j\in A_t}|\mathscr{F}^t(a_j)| + \Sigma_{a_j\in A_{t+1}}|\mathscr{F}^t(a_j)| + \ldots + \Sigma_{a_j\in A_{m-1}}|\mathscr{F}^t(a_j)|\end{aligned}$$

since $\mathscr{F}^t(a_j) = \emptyset$ for any $a_j \in A_s (s < t)$. Similarly we have

$$\begin{aligned}|\mathscr{F}^{t+1}(b)| &= \Sigma_{b_j\in B_1}|\mathscr{F}^t(b_j)| + \Sigma_{b_j\in B_2}|\mathscr{F}^t(b_j)| + \ldots + \Sigma_{b_j\in B_{m-1}}|\mathscr{F}^t(b_j)| \\ &= \Sigma_{b_j\in B_t}|\mathscr{F}^t(b_j)| + \Sigma_{b_j\in B_{t+1}}|\mathscr{F}^t(b_j)| + \ldots + \Sigma_{b_j\in B_{m-1}}|\mathscr{F}^t(b_j)|.\end{aligned}$$

By induction $a_i(m-1) \simeq b_j(m-1)$ if $a_i \in A_s$, $b_j \in B_s$. By Lemma 4.5

$$|\mathscr{F}^t(a_i)| = |\mathscr{F}^t(b_j)|. \tag{4.5}$$

Choose an $a_{i_s} \in A_s$ and a $b_{i_s} \in B_s$ for any $t \leqslant s \leqslant m-1$ if $A_s \neq \emptyset$. Then

$$|\mathscr{F}^{t+1}(a)| = \sum_{s=t}^{m-1} |A_s| \cdot |\mathscr{F}^t(a_{i_s})|, \tag{4.6}$$

$$|\mathscr{F}^{t+1}(b)| = \sum_{s=t}^{m-1} |B_s| \cdot |\mathscr{F}^t(b_{i_s})|. \tag{4.7}$$

By Lemma 4.3 and Lemma 4.2,

$$|\mathscr{F}^{t+1}(a)| = \sum_{i=0}^{t+1} |\mathscr{F}^i(C_1)| = \sum_{i=0}^{t+1} |\mathscr{F}^i(C_2)| = |\mathscr{F}^{t+1}(b)|. \tag{4.8}$$

Combine (4.5), (4.6), (4.7), (4.8) with $|A_j| = |B_j|$ $(t < j \leqslant m-1)$. We get

$$|A_t| = |B_t|,$$

which is a contradiction. Thus our claim is true.

Then after a permutation of indices we can assume that $h(a_i(m-1)) = h(b_i(m-1))$ for any i $(1 \leqslant i \leqslant l)$, by induction $a_i(m-1) \simeq b_i(m-1)$, hence $a(m) \simeq b(m)$.

Now we come to proving $C_1 \simeq C_2$. Let $\mathscr{F}^1(C_1) = \{c_1, c_2, \ldots, c_{l-1}\}$, $\mathscr{F}^1(C_2) = \{d_1, d_2, \ldots, d_{l-1}\}$. Using the same arguments we can show that after a permutation of indices we have $h(c_i(h-1)) = h(d_i(h-1))$ for any i $(1 \leqslant i \leqslant l-1)$, where $h = h(C_1) = h(C_2)$. Hence, we have $c_i(h-1) \simeq d_i(h-1)$, $C_1 \simeq C_2$. □

P r o o f of Theorem 3.2. It follows from Lemma 4.1 and Lemma 4.6. □

References

[1] *C. Lucheta, E. Miller, C. Reiter*: Digraphs from powers modulo p. Fibonacci Quart. *34* (1996), 226–239.

[2] *L. Somer, M. Křížek*: On symmetric digraphs of the congruence $x^k \equiv y \pmod{n}$. Discrete Math. *309* (2009), 1999–2009.

Authors' addresses: G u i x i n D e n g, School of Mathematics, Sun Yat-Sen University, Guangzhou, 510275, P.R. China, e-mail: `oldlao@163.com`; P i n g z h i Y u a n, School of Mathematics, South China Normal University, Guangzhou 510631, P.R. China, e-mail: `mcsypz@mail.sysu.edu.cn`.