三重大学教育学部研究紀要　第59巻　自然科学　(2008)　1－23頁

初等力学グラフの構造

蟹江幸博*

Structures of Elementary Dynamical Graphs

Yukihiro KANIE

Contents

Introduction

I proposed the concept of dynamical graphs for Clinical Mathematics Education in [2], and discussed their mathematical theory in the case of reduced divisor sums in [3], and in the case of reversed differences in [5]. And in [8], I determined the number of the isomorphism classes of dynamical graphs with vertex number $k \leqq 10$. There we know the structures of dynamical graphs are rather complicated even in such a small size case.

In this note, we will describe some structures of basic elementary dynamical graphs, especially of addition graphs and multiplication graphs. We use somtimes the abbreviation DG for dynamical graphs.

* .Math. Dept. of Fac. of Ed., Mie University

§1. Brief Reviews of Finite Dynamical Graphs

Let V be a finite set. A dynamical graph $G = (V, E)$ is an oriented graph on V whose every vertex $v \in V$ has only one outgoing edge from v, that is, there is only one vetex w with $(v, w) \in E$. An oriented edge $(v, w) \in E$ is sometimes drawn as $v \to w$ and is called an *arrow*.

Denote by $\mathcal{D}(V)$ the set of all dynamical graphs on V, which is bijective to the set $Map(V, V)$ of the maps of V to itself. The correspondence is given as follows.

Given $f \in Map(V, V)$, take the graph $E(f) = \{(v, f(v)) \mid v \in V\}$ of the map f as the set of edges of G, then $G(f) = (V, E(f))$ is a dynamical graph.

Conversely, given a dynamical graph $G = (V, E)$ on V, for any $v \in V$ we have only one vertex $w \in V$ with $(v, w) \in E$. So let $f(v) = w$. Denoting f by $f(G)$, we get that $G = G(f(G))$ and $f = f(G(f))$.

Two maps $f \in Map(V, V)$ and $g \in Map(W, W)$ are called *isomorphic*, if there exists a bijection $\varphi : V \to W$ (called an *isomorphism*) satisfying the equality

$$\varphi \circ f = g \circ \varphi \Leftrightarrow f = \varphi^{-1} \circ g \circ \varphi.$$

Then we write as $f \cong g$, and call the dynamical graphs $G(f)$ and $G(g)$ are *isomorphic* with each other and denoted by $G(f) \cong G(g)$.

In describing structures explicitely, there are some cases where it is important to specify labels of verteces, and to distinguish isomorphic DG's. So we denote $\varphi * f = \varphi \circ f \circ \varphi^{-1}$ and $\varphi * G(f) = G(\varphi * f)$, and call $\varphi * G(f)$ the *φ-transfer* of the DG $G(f)$. Then we say that the DG $G(f)$ on V is φ-transfered to the DG $\varphi * G(f)$ on W. Moreover, if G' is a DSG of G, then $\varphi * G'$ is also a DSG of $\varphi * G(f)$.

If f is bijective, the dynamical graph $G(f^{-1})$ defined by the inverse mapping f^{-1} is called the *inverse graph* of $G = G(f)$, and G is called *invertible*. Write $G^{-1} = G(f^{-1})$ for the inverse of G, then it can be obtained by reversing all directions of arrows of G

Denote by $\mathcal{D}(V)$ the set of all dynamical graphs on V, and by $\mathcal{D}'(V)$ the set of all invertible dynamical graphs on V. The cardinality of V is called of *size* of $G = (V, E)$, denoted by $s = s(G)$, which coincides with the number $\#E$ of edges of G.

Denote by $\mathfrak{D}(V)$ and $\mathfrak{D}'(V)$ the set of isomorphism classes of $\mathcal{D}(V)$ and $\mathcal{D}'(V)$ respectively.

Now we prepare some basic notions about DG.

Let $G = (V, E) = G(f)$ be a DG. A dynamical graph $G' = (V', E')$ is called *dynamical subgraph*(DSG) of G, if $V' \subset V$, $E' \subset E$ and every edge in E' consists of verteces in V'.

For a vertex $v \in V$, the set of all 'descendants' of v:

$$V^+(v) = \{w \in V \mid w = f^a(v) \text{ for some } a \geq 0\}$$

is a DSG by v and is called the *future* of v. This subgraph is the minimal subgraph containing the vertex v, so it is also called the subgraph generated by v and is denoted by $\langle v \rangle$. For any subset $U \subset V$, denote by $\langle U \rangle$ the DG generated by U.

For a vertex $v \in V$, the set of all 'ancesterts' of v:

$$V^-(v) = \{w \in V \mid v = f^a(w) \text{ for some } a \geq 0\}$$

is called the *past* of v, but it is not a DSG in general.

For an integer $n \geqq 0$, denote by $G^{(n)}$ the subgraph $G(f|_{f^n(V)}) = \langle f^n(V) \rangle$ on the f-invariant subset $f^n(V)$, and call it the *n-th future graph*. Also denote $G^{(1)} = G'$, and call it the *derived graph* of G. Then we get

$$V = f^0(V) \supsetneqq f^1(V) \supsetneqq \cdots \supsetneqq f^h(V) = f^{h+1}(V) = \cdots$$

for some $h > 0$. Introduce the set

$$\mathcal{L}_n(G) = f^{n-1}(V) \setminus f^n(V) \qquad (1 \leqq n < \infty), \quad \mathcal{L}_\infty(G) = f^h(V).$$

A vertex $v \in \mathcal{L}_n(G)$ is called of *life* n ($\mathrm{lf}(v) = n$), and v of life 1 is called a *leaf*.

A DG G is called *connected*, if $\langle v \rangle \cap \langle w \rangle \neq \emptyset$ for any $v, w \in V$,

For a vertex v or a connected subgraph G', the maximal connected DSG $\mathcal{F}$ containing v or G' is called the *connected component* of v or G', denoted by $\mathcal{F}(v) = \mathcal{F}(v; G)$ or $\mathcal{F}(G') = \mathcal{F}(G'; G)$ respectively. The number $c = c(G)$ of connected components in G is called *connectivity* of G. $c = 1$ means that G is connected.

§1..1 Cycles and invertible DG

If a subset $C = \{v_1, \cdots, v_p\}$ of (mutually different) verteces satisfies

$$f(v_i) = \begin{cases} v_{i+1} & (i < p) \\ v_1 & (i = p), \end{cases}$$

then the subgraph $\langle C \rangle$ is called a *cycle*. Sometimes the set C itself is also called cycle. The number $p = p(C)$ is called the *period* of the cycle C, and is nothing but the size of C. For any vertex v of C, $C = \langle v \rangle = V^-(v)$. Denote by C_p the isomorphism class of a cycle of period p.

Let G be a dynamical graph, then every connected component contains only one cycle. A cycle C of G is called a *limit cycle* of G, if $\mathcal{F}(C) \supsetneqq C$. For any vertex v of a limit cycle C the set $V^-(v) = V^-(C) = \mathcal{F}(v) = \mathcal{F}(C)$ is a DSG. A DG G is called *of cycle type*, if its every conneted component is a cycle. The subgraph $\mathcal{L}_\infty(G)$ consists of all limit cycles, and is of cycle type.

A cycle of period 1 consists of a single vertex, and is also called a *fixed point* (so denoted as C_1). A connected DG T is called *pseudo-tree*, if the limit cycle of T is a fixed point. In a pseudo-tree T, the cycle consists of a single vertex v, this unique gate v is called a *root* of T.

The subgraph $\langle v \rangle$ generated by a vertex $v \in V$ has no branch points outside its limit cycle. A pseudo-tree T is called *linear*, if the fixed point is the only one branch point.

Let v be a vertex of a limit cycle C, then a vertex $w \notin C$ is called a *gate* of C to v, if $w \to v$. For a vertex v of C, let $W = W(v)$ be the set of gates to v, that is,and its past $V^-(W)$ is called the *outer past* of v, and is denoted by $O^-(v) \supset W$. And consider two number, the *width* $w(v) = \#W(v) = \deg v - 1$ and the *weight* $\mathrm{wt}(v) = \#O^-(v)$ of the vertex $v \in C$.

A vertex $u \in C$ is called the *n-th cyclic past* of v, if $f^n(u) = v$. Then u is uniquely determined by u and n, and is denoted by $u = f^{*n}(v)$.

Remark. Here we changed the definition of the gate in [8], but other definitions are not unchanged around the concept of gates.

Let C be a cycle of G. For a vertex $v \in \mathcal{F}(C)$, put

$$\mathrm{ht}(v) = \mathrm{ht}_C(v) = \min\{n \geqq 0 \mid f^n(v) \in C\},$$

and call it the *height* of v w.r.t. the cycle C. Write the set of verteces of height h as $\mathcal{F}_h(C) = \{v \in \mathcal{F}(C) \mid \mathrm{ht}_C(v) = h\}$, then

$$\mathcal{F}(C) = \bigcup_{h \geqq 0} \mathcal{F}_h(C) = \bigcup_{h=0}^{h(C)} \mathcal{F}_h(C), \quad \mathcal{F}_0(C) = C.$$

where $h(C)$ is the maximal height $h(C) = \max\{h_C(v) \mid v \in \mathcal{F}(C)\}$ in $\mathcal{F}(C)$, and $f^{h(C)}(\mathcal{F}(C)) = C$.

§1..2 Degrees and Size and Period Characterisitc

For a vertex $v \in V$, the number of arrows whose target is v is called the *degree* of v, and is denoted by $\deg(v)$. That is, $\deg(v)$ is the number of the preimage of v by $f = f(G)$:

$$\deg(v) = \sharp f^{-1}(v) = \#\{w \in V \mid w \to v\}.$$

Let $\mathcal{D}_i(G) = \{v \in V \mid \deg(v) = i\}$, then $\mathcal{D}_0 = \mathcal{L}_1$ is the set of all leaves.

Put $D_i(G) = \sharp\mathcal{D}_i(G)$ and $\mathbb{D}(G) = (D_0, D_1, \ldots) = \sum_{i \geqq 0} D_i \Bbbk_i$, then there holds the degree equation:

$$s(G) = \#E = \sum_{v \in V} \deg v = \sum_{i \geqq 0} D_i = \sum_{i \geqq 1} iD_i.$$

We say that a vertex v is a *branch point* if $\deg(v) > 1$, then cycles have no leaves and no branch points.

Proposition 1 *The followings are equivalent with each other.*

(1) *f is bijective, that is, G is invertible.*

(2) *$\deg v = 1$ for every vertex v, that is, $\mathbb{D}(G) = s(G)\Bbbk_1 = 1^{s(G)}$.*

(3) *G is of cycle type.*

(4) $\mathbb{P}(G) = \mathbb{S}(G)$.

Remark. In an ordinary graph theory, this notion of degree is called the *indegree*. The reason why we choose this definition, the outdegree of every vertex is 1(constant) in our theory.

In DG theory, (2) in Proposition 2 means the the homogeneity in degrees, that is $\deg v$ are the same for any verteces v, A DG G is called *quasi-homogeneous*, if the degree characteristic $\mathbb{D}(G)$ has two nonzero components. Then $\mathbb{D}(G)$ has the form $(s(G) - c)\Bbbk_0 + c\Bbbk_d$, where $cd = s(G)$.

Let $G = G(f)$ be a finite DG, and $c = c(G)$ be the connectivity $c = c(G)$. Let $\{G^1, \cdots, G^c\}$ be the set of connected components of G, C^i be the unique cycle of G^i $(1 \leqq i \leqq c)$. In this situation, G is written as a disjoint sum $G = \cup_{i=1}^c G^i$ of all connected components, and $\mathcal{L}_\infty(G) = \cup_{i=1}^c C^i$ is the sum of all limit cycles.

Now introduce the *size characteristic* $\mathbb{S}(G) = \{s^1, \cdots, s^c\}$ and the *period characteristic* $\mathbb{P}(G) = (p^1, \cdots, p^c)$ of the dynamical graph G, where $s^i = s(G^i)$ and $p^i = p(C^i)$. Then $s(G) = s^1 + \cdots + s^c$.

For covenience sake, we use the following notation for sets $\mathbb{S} = \{s_1, \cdots, s_c\}$ of c natural numbers. Let $n_j = \#\{s_i \mid s_i = j\}$, then write $\mathbb{S} = \sum_{j \geqq 0} n_j \Bbbk_j = \prod_{j \geqq 0} j^{n_j}$. Then we get

$$\sum_{j=1}^{c} s_j = \sum_{j \geqq 1} n_j j, \qquad c = \sum_{j \geqq 1} n_j.$$

If every G^i $(1 \leqq i \leqq c)$ is isomorphic to a graph $\overline{G}$, then we use the abbreviation $c\overline{G}$ for $\cup_{i=1}^c G^i$. Then $\mathbb{S}(c\overline{G}) = c\mathbb{S}(\overline{G})$, $\mathbb{P}(c\overline{G}) = c\mathbb{P}(\overline{G})$, $\mathbb{D}(c\overline{G}) = c\mathbb{D}(\overline{G})$. Moreover, $\mathbb{S}(C_p) = \Bbbk_p, \mathbb{P}(C_p) = \Bbbk_p$, $\mathbb{D}(C_p) = p\Bbbk_1$.

§1..3 Attaching

Given a graph $G = G(f) \in \mathcal{D}(V)$, a vertex $v \in V$, a pseudo-tree $T = G(t) = (U, F) \in \mathcal{T}$ with the root $u \in U$, then define the dynamical graph $G(h) \in \mathcal{D}(V')$ one the set $V' = V \cup (U \setminus \{u\})$ by

$$h(w) = \begin{cases} f(w) & (w \in V) \\ t(w) & (w \in U \text{ and } t(w) \neq u) \\ v & (w \in U \text{ and } t(w) = u). \end{cases}$$

We say that $G(h)$ is obtained from G *attached by* T *at* v, and denote $G(h) = G \vee_v T$. Then

$$s(G \vee_v T) = s(G) + s(T) - 1 = s(G) + \mathrm{wt}(T),$$
$$c(G \vee_v T) = c(G),\ \mathbb{P}(G \vee_v T) = \mathbb{P}(G).$$

Any connected dynamical graphs can be expressed as a cycle C with pseudo-trees T_i attached at gates v_i $(i = 1, \cdots, g)$: $G = C \vee_{v_1} T_1 \cdots \vee_{v_g} T_g$. Then the size of G is given as

$$s(G) = p(G) + \sum_{i=1}^{g} \mathrm{wt}(T_i).$$

Linear pseudo-trees of weight w are isomorphic with each others, so denote their isomorphism class by L_w.

Any pseudo-tree T can be expressed as a linear pseudo-tree L_{w_0} with linear pseudo-trees L_{w_i} attached at branch points v_i $(i = 1, \cdots, b(T))$: $T = ((\cdots(L_{w_0} \vee_{v_1} L_{w_1}) \cdots) \vee_{v_b} L_{w_b}$. Then $s(T) = 1 + \sum_{i=0}^{b} w_i$.

In particular, $L_0 = K_1^0 = C_1$, and attaching L_0 does not change any graph: $G \vee_v L_0 = G$ for any $v \in V$.

If v is a leaf of a linear pseudo-tree T_w, then $L_w \vee_v L_{w'} = L_{w+w'}$, in particular $L_w \vee_v L_0 = L_w$.

§1..4 p-nary Pseudo-tree

Fix (p, ℓ) $(p > 1, \ell > 0)$, we define *p-nary pseudo-trees* B_p^ℓ inductively on ℓ as follows: At first let $B_p^0 = L_0$, and put

$$B_p^{\ell+1} = L_0 \vee_0 p(L_1 \vee_1 B_p^\ell).$$

Then B_p^ℓ is a pseudo-tree of height ℓ, $\#\mathcal{L}_1(B_p^\ell) = p^\ell$(the number of leaves), and

$$s(B_p^\ell) = \sum_{i=1}^{\ell} p^i = \frac{p^{\ell+1} - 1}{p - 1}, \quad \mathrm{wt}(B_p^\ell) = p\frac{p^\ell - 1}{p - 1}, \quad \mathbb{D}_0(B_p^\ell) = p^\ell \Bbbk_0 + \frac{p^\ell - 1}{p - 1} \Bbbk_p.$$

In fact, we can verify inductively

$$\mathrm{wt}(B_p^{\ell+1}) = p\left(1 + p\frac{p^\ell - 1}{p - 1}\right) = p\frac{p^{\ell+1} - 1}{p - 1}.$$

B_1^ℓ is a linear pseudo-tree L_ℓ of weight ℓ, and B_2^k is called a binary pseudo-tree of height ℓ.

The multiplication graph $M_{2^\ell}^2$ is expressed as $L_1 \vee_1 B_2^{\ell-1}$, and in general the multiplication graph $M_{p^\ell}^p$ is expressed as $L_0 \vee_0 (p-1)(L_1 \vee_1 B_p^{\ell-1})$. Its size can be computed as

$$s(M_{p^\ell}^p) = 1 + \mathrm{wt}(M_{p^\ell}^p) = 1 + (p-1)(1 + \frac{p^\ell - 1}{p - 1} - 1) = p^k.$$

§2. Realization of Dynamical Graphs

For explicit realizations of dynamical graphs, fix the size k, and take the k-skelton of $\mathbb{N}$:

$$I_k = \begin{cases} \{i \in \mathbb{N} \mid 0 \leqq i < k\} = \{0, 1, 2 \ldots, k-1\} & (k : finite) \\ \mathbb{N} & (k = \infty) \end{cases}$$

as a set of verteces. Then I_k is a representative system of the quotient ring $\mathbb{Z}_k (= \mathbb{Z}/k\mathbb{Z})$. In this note, we identify I_k with $\mathbb{Z}_k$ and use the notation $\overline{m}$ for the residue class of $m \in \mathbb{Z}$.

Denote $\mathcal{D}(I_k)$ and $\mathcal{D}'(I_k)$ by $\mathcal{D}_k$ and $\mathcal{D}'_k$ respectively. And $\mathfrak{D}_k$ and $\mathfrak{D}'_k$ by $\mathfrak{D}(I_k)$ and $\mathfrak{D}'(I_k)$ respectively. We know easily that $\#\mathcal{D}_k = k^k$, $\#\mathcal{D}'_k = k!$ and $\#\mathfrak{D}'_k = p(k)$, where $p(k)$ is the partition number of k. By [8], we know the number $\delta_k = \#\mathfrak{D}_k$ as follows.

k	1	2	3	4	5	6	7	8	9	10
δ_k	1	3	7	18	46	130	343	951	2615	7207

Thus there are so many different nonisomorphic DG's, even if the number of verteces is small as 10. For an educational purpose, we want to clearify the structures of DG's at least with the size $\leqq 100$, then we must restrct ourselves to small groups of DG's such as elementary dynamical graphas(EDG).

§2..1 Shifts anf Extension

Let $V = I_k$ for some $k > 0$ and $G = G(f)$ be a DG on V.

For any $b \in \mathbb{Z}$, define the bijection $\varphi : V \to V$ defined by $\varphi(i) = \overline{i+b}$. If $\varphi f = f\varphi$, then the φ-transfer operation gives an automorphism of the DG $G = G(f)$, which we call the *b-shift* and denote by T_b. Note T_0 is the identity mapping. Then if G' is a DSG of G, then T_bG' is a DSG of G. And if G' is a connected component or a cycle of G, then T_bG' is also a connected component or a cycle respectively.

For an integer $b > 0$, define the injection $\varphi : I_k \to I_{bk}$ defined by $\varphi(i) = \overline{bi}$, then we denote the φ-transfer $\varphi * G$ on the subset $\{bi \mid i \in I_k\}$ of I_{bk} by E_cG, which we call the *times b-extension* or simply *b-extension* of G.

§2..2 Elementary DG

Let $P \in \mathbb{Z}[x]$ be a polynomial with integral coefficients, then define a mapping $P_k : I_k \to I_k$ as

$$P_k(i) = \overline{P(i)},$$

and the corresponding dynamical graph $G(P_k)$ is also denoted by $G_k(P)$. Such dynamical graphs are called *elementary.*

Note that $P_k = Q_k$ may happen even if $P \neq Q \in \mathbb{Z}[x]$. In general, there are numbers $h > h'(> 0)$ such that $(x^h)_k = (x^{h'})_k$. For example, $(x^2)_2 = (x)_2$, $(x^3)_3 = (x)_3$, $(x^4)_4 = (x^2)_4$, $(x^5)_5 = (x)_5$, $(x^3)_6 = (x)_6$, $(x^7)_7 = (x)_7$, $(x^5)_8 = (x^3)_8$, $(x^8)_9 = (x^2)_9$, $(x^5)_{10} = (x)_{10}$.

In this note, we will treat the following three groups of elementary DG's on I_k. Let a be an integer.

The *Constant Graph* K_k^a stands for $G_k(P)$, where $P(x) = a$. K_k^a is a pseudo-tree of height 1, a is the root of degree k, and $\mathbb{S}(K_1^a) = \mathbb{k}_k$, $\mathbb{P}(K_1^a) = \mathbb{k}_1$, $\mathbb{D}(K_k^a) = (k-1)\mathbb{k}_0 + \mathbb{k}_k$.

The *Addition Graph* A_k^a stands for $G_k(P)$, where $P(x) = x + a$. Obviously, $A_k^{a+k} = A_k^a$ and the mapping P_k is bijective, so A_k^a is of cycle type. In particular, $\mathbb{S}(A_k^1) = \mathbb{P}(A_k^1) = \mathbb{k}_k$, $\mathbb{D}(A_k^1) = k\mathbb{k}_1$. In particular, $\mathbb{S}(K_1^0) = \mathbb{P}(K_1^0) = \mathbb{D}(K_1^0) = 1^1 = \mathbb{k}_1$.

The *Multiplication Graph* M_k^a stands for $G_k(P)$, where $P(x) = ax$. Obviously, $M_k^{a+k} = M_k^a$ and the mapping P_k is not bijective in general. M_k^a is of cycle type, if and only if a and k are coprime, that is, $(a, k) = 1$.

$A_k^0 = M_k^1 = kK_1^0$ is the identity graph w.r.t. the pointwise product in $\mathcal{D}_k$.

§3. Facts from Elementary Number Theory

In this section, we summarize the facts from elementary number theory which will be used below. For references, see [1] or [10] for example.

§3..1 The Group of Reduced Residue Classes

For an integer $k > 0$, denote the ring of residue classes modulo k by $\mathbb{Z}/k\mathbb{Z}$. For an element $x \in \mathbb{Z}/k\mathbb{Z}$, define the *order* $o_k(x)$ of x as the minimal positive integer n such that $nx \equiv 0 \pmod{k}$, that is, $\overline{nx} = 0$.

(Here, the same statement holds, even if x is an integer. So we sometimes use the notation x for $\overline{x}$ in the set $\mathbb{Z}/k\mathbb{Z}$ of congruence classes modulo k.) It is wellknown that $o_k(x) = k/d$, where d is the greatest common divisor $d = (x,k)$ of x and k, and $\{ix \mid 0 \leqq i < k\} = \{ix \mid 0 \leqq i < k/d\}$. In particular, if $(x,k) = 1$, then $\{ix \mid 0 \leqq i < k\} = \mathbb{Z}_k$. The additive subgroup $\langle x \rangle$ generated by x concides with the set $\{i\bar{x} \mid 0 \leqq < k/d\}$.

In this note, we will use the notation K_k for the set $\{\overline{x} \mid (x,k) = 1, 0 < x < k\}$. K_k is a multiplicative group, usually denoted by $(\mathbb{Z}/k\mathbb{Z})^\times$ and called the group of reduced residue classes modulo k. The set K_k is also obtained as the set of units(invertible elements) of the ring $\mathbb{Z}/k\mathbb{Z}$. For an element $a \in K_k$, define the *multiplicative order* $o_k(a)$ of a as the minimal positive integer n such that $a^n \equiv 1 \pmod{k}$. In other words, $o_k(a) = \#\langle a \rangle$ as multiplicative subgroups. If $K_k = \langle a \rangle$, then a is a *generator* and is called a *primitive root modulo* k.

Define the *Euler's function* $\varphi(k)$ by $\varphi(k) = \#K_k$. By Lagrange's theorem, $o_k(a)$ is a divisor of $\varphi(k)$. Then

Theorem 1 (1) *Let p be a prime number, then $\varphi(p) = p-1$ and $\varphi(p^n) = p^{n-1}(p-1)$. In particular, $\varphi(2^n) = 2^{n-1}$.*

(2) *Let p be an odd prime, then $(\mathbb{Z}/p^e\mathbb{Z})^\times \cong \mathbb{Z}_{p^{e-1}(p-1)} \cong \mathbb{Z}_{p^{e-1}} \oplus \mathbb{Z}_{p-1}$. Here consider a multiplication group on the left hand side, and an additive group on the right hand side.*

(3) $(\mathbb{Z}/2^{e}Z)^\times \cong \begin{cases} \mathbb{Z}_{2^{e-1}} & (e = 1,2) \\ \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{e-2}} & (e \geqq 3) \end{cases}$

(4) *If $(k,n) = 1$, then $\varphi(k)\varphi(n) = \varphi(kn)$.*

(5) (Euler's Theorem) *If $(a,n) = 1$ (that is, $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$) , then $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

(6) (Chinese Remainder Theorem) *Assume $(m,n) = 1$. Then*

(i) $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z}$, $a \oplus b \mapsto ab$.

(ii) $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/mn\mathbb{Z})^\times$.

(7) *Let $k = p_1^{e_1} \cdot p_2^{e_2} \cdots p_m^{e_m}$ be the prime factorization of k, then*

$$(\mathbb{Z}/k\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{e_2}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_m^{e_m}\mathbb{Z})^\times,$$

and so

$$\varphi(k) = \prod_{j=1}^{m} \varphi(p_j^{e_j}) = \prod_{j=1}^{m} p_j^{e_j-1}(p_j - 1) = \prod_{j=1}^{m} p_j^{e_j}\left(1 - \frac{1}{p_j}\right) = k\prod_{j=1}^{m}\left(1 - \frac{1}{p_j}\right).$$

Remark. $\mathbb{Z}/p-1\mathbb{Z}$ is decomposed according to the prime factorization of $p-1$, where other prime factors q's or factors of $q-1$ may occur. In particular, if there are two odd primes, then the factor 2 actually occurs in different $q-1$'s.

Hence by Theorem 1 (6-i), $(\mathbb{Z}/k\mathbb{Z})^\times$ can be written as $(\mathbb{Z}/p^{e_1}\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/p^{e_x}\mathbb{Z}) \oplus (\mathbb{Z}/q^{f_1}\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/q^{f_y}\mathbb{Z}) \oplus \cdots$. Then, the number $p^e q^f \cdots$, where $e = \max\{e_1, \ldots, e_x\}$, $f = \max\{f_1, \ldots, f_y\}$, $\cdots$ is the maximal order $o_k(a)$ of elements $a \in (\mathbb{Z}/k\mathbb{Z})^\times$, and there are elements with the maximal order, which will be denote by mo_k in this note. Moreover, there exist elements with orders which are factors of mo_k.

In particular, assume that $k = p$ is odd prime. Then, threre are $\varphi(p-1)$ generators b of the multiplication group $(\mathbb{Z}/p\mathbb{Z})^\times$, and any element $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ can be uniquely expressed as $a = b^t$ $(0 \leq t < p-1)$.

For $t = 0$, $a = b^0 = 1$ and $o(a) = 1$, and so $M_p^1 \cong pC_1$. Let $t > 0$. If $d = (t, p-1)$, then $o_p(a) = (p-1)/d$ and $M_p^a \cong C_1 \cup dC_{(p-1)/d}$. In particular, if t and $p-1 = \varphi(p)$ is coprime, then a is also a generator, $o(a) = p-1$ and $\langle a \rangle = (\mathbb{Z}/p\mathbb{Z})^\times$.

§3..2 Quadratic Residues

Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$. We call a *a quadratic residue modulo* n, if the equation $x^2 \equiv a \pmod{n}$ has a solution. And call a is *a quadratic non-residue modulo* n, if the equation $x^2 \equiv a \pmod{n}$ has no solutions.

Theorem 2 *a is a quadratic residue modulo n, if and only if the following two conditions are satisfied.*

(1) *a is a quadratic residue modulo p for any odd prime factors p of n.*

(2) *$a \equiv 1 \pmod{4}$ in the case where $n \equiv 0 \pmod{4}$, and $a \equiv 1 \pmod{8}$ in the case where $n \equiv 0 \pmod{8}$.*

Introduce the *Legendre symbol* for an odd prime p and an integer a with $p \nmid a$, defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ is a quadratic residue modulo } p \\ -1 & a \text{ is a quadratic nonresidue modulo } p \end{cases}$$

then the following theorem holds.

Theorem 3 (1) *If $a \equiv b \pmod{p}$, then* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(2) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

(3) (Euler' criterion) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

(4) (law of quadratic reciprocity) $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/2}$ *for odd primes $p, q (p \neq q)$.*

(5) (first and second complementary laws)

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}, \qquad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$$

for an odd prime p.

§4. Addition Graph A_k^a

In this section, we consider addition graphs A_k^a. They are of cycle type, and the inverse graph $(A_k^a)^{-1}$ of A_k^a is nothing but A_k^{k-a}. As for isomorphism classes, it is necessary to consider A_k^a with a $(1 \leqq a \leqq \left[\frac{k}{2}\right])$, since $A_k^{a+k} = A_k^a$ and $A_k^0 = kK_1^0$. More precisely,

Theorem 4 *Let $k > 0$. For any a $(0 \leqq a < k)$, A_k^a is of cycle type, and $\mathbb{S}(A_k^a) = \mathbb{P}(A_k^a)$ and $\mathbb{D}(A_k^a) = 1^k = k\mathbb{k}_1$. In particular, there are no leaves: $\mathcal{L}_1(A_k^a) = \emptyset$.*

(1) *If $(a, k) = 1$, then A_k^a is a cycle of period k. $A_k^a \cong C_k$, $\mathbb{P}(A_k^a) = \mathbb{k}_k$.*

(2) *If $(a, k) = d > 1$, then $A_k^a = \bigcup_{i=0}^{d-1} T_i(E_d(A_{k'}^a)) \cong dE_d(A_{k'}^a) \cong dC_{d'}$, where $k' = k/d$. $\mathbb{P}(A_k^a) = d\mathbb{k}_{k'}$.*

There are distinct δ non-isomorphic DG's among addition DG's A_k^a, where $\delta = \delta(k)$ is the number of divisors of k.

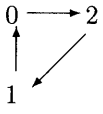
(3) *Dynamical graphs G with homogeneous periodic chartacteristic, that is $\mathbb{P}(G) = c\mathbb{k}_p$ for some $c, p > 0$, can be realized as an addition DG, for example, $\mathbb{P}(A_{cp}^c) = c\mathbb{k}_p$.*

Proof. (1) By elementary number theory, $\#\{\overline{ia} \mid 0 \leqq i < k\} = k$.

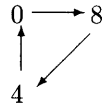
(2) Since $(a, k') = 1$, $A_{k'}^a$ is a cycle of period k', by (1). Its d-extension $G' = E_d(A_{k'}^a)$ is a DSG of A_k^a. For any $b \in \mathbb{Z}$, the b-shift $T_b(G')$ is also a cycle and DSG of A_k^a. Then we can check easily that

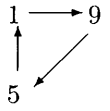
$T_b(G') = T_{b'}(G')$ if and only if $b \equiv b' \pmod{d}$. Hence $T_b(G')$ $(0 \leqq b < d)$ are mutually disjoint. Thus we get $A_k^a = \bigcup_{i=0}^{d-1} T_i(E_d(A_{k'}^a)) \cong dC_{k'}$. *qed.*

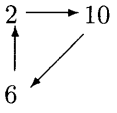
Example. $k = 12$, $a = 8$, $d = (a,k) = 4$, $d' = k/d = 3$.

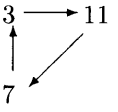
$A_{d'}^a = A_3^8 (= A_3^2)$: 

, $A_{12}^8 = \bigcup_{i=0}^{3} T_i(E_4(A_3^8))$:

$E_4(A_3^8)$: 

$T_1(E_4(A_3^8))$: 

$T_2(E_4(A_3^8))$: 

$T_3(E_4(A_3^8))$: 

§5. Multiplication Graph M_k^a

Fix an integer $k > 0$. In this section, we consider multipication graphs M_k^a. They are not of cycle type in general, but they have rather simple structures. For example, $\langle 0 \rangle$ is a cycle of period 1, and the connected component $\mathcal{F}(0)$ is either a cycle or a pseudo-tree. Remember that the set $\mathcal{L}_\infty(G)$ is the subgraph consisting of all limit cycles for any DG G. Denote by $\tilde{C}(G) = \mathcal{L}_\infty(G)$ this DG of cycle type. Main result is that it is sufficient to study the structures of the pseudo-tree T and $\tilde{C}(M_k^a)$. In fact,

Theorem 5 *Let $k > 0$ be an integer.*

(1) $M_k^a = M_k^{a+k}$, *for any integer a.*

(2) *If $(a,k) = 1$, then M_k^a is of cycle type.* $\mathbb{S}(M_k^a) = \mathbb{P}(M_k^a)$, $\mathbb{D}(M_k^a) = k\Bbbk_1$.

In the following, assume that $(a,k) = d > 1$. Put $k' = k/d$.

(3) *M_k^a is not of cycle type, and the the connected component $\mathcal{F}(0)$ is a pseudo-tree T of a positive height h. M_k^a is isomorphic to $\tilde{C} = \tilde{C}(M_k^a)$ attached at all verteces by T:*

$$M_k^a \cong \tilde{C}(M_k^a) \vee_{v \in \tilde{C}} T.$$

In particular, the width and weight of all verteces v of $\tilde{C}$ are given as

$$w(v) = w(0) = d - 1, \qquad \mathrm{wt}(v) = \mathrm{wt}(0).$$

(4) *For every vertex $c \in \tilde{C}$, the outer past $O^-(v)$ is obtained from T as*

$$O^-(v) = \{w + f^{*n}(v) \mid w \in T,\ n = \mathrm{ht}(w)\},$$

where $f^{*n}(v)$ is the n-th cyclic past of v.

(5) *The degrees of all verteces $v \notin \mathcal{L}_1(M_k^a)$ are the same:* $\deg(0) = d$. *Moreover, $D_d = k'$.*

(6) *The set $\mathcal{L}_1(M_k^a)$ of all leaves is $\{w \in I_k \mid a \not| w\}$, and so its cardinality is $k - k'$. Hence* $\mathbb{D}(M_k^a) = (k - k')\Bbbk_0 + k'\Bbbk_d$.

Proof. (1) and (2) is obvious. (4) implies imediately (3). (3) Since $n = \mathrm{ht}(w)$, $f^n(w) = a^n w \equiv 0 \pmod{k}$ and $v = f^n(f^{*n}(v)) = a^n f^{*n}(v)$, thererfor $f^n(w + f^{*n}(v)) = a^n(w + f^{*n}(v)) \equiv 0 + v = v \pmod{k}$. Since $f(w) \in T$ and $\mathrm{ht}(f(w)) = n - 1$, $w + f^{*n}(v) \to f(w) + f^{*(n-1)}(v) \in O^-(v)$.

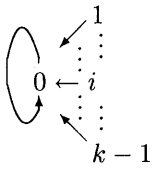
(5) implies (6). (5) $v \to 0 \Leftrightarrow av \equiv 0 \pmod{k} \Leftrightarrow dv \equiv 0 \pmod{k}$, since $a = a'd$, $(a', k) = 1$. Put $k' = k/d$. For every i $(0 \leqq i < d-1)$, $0 \leqq ik' < k$ and $ik' \to \overline{aik'} = \overline{a'dik'} = \overline{a'ik} = 0$. Hence $\deg(0) \geqq d$.

Take a vertex v with $\deg(v) > 0$. Then there exists a vertex w such that $w \to v$. So $w + w' \to v$ for any $w' \to 0$, hence $\deg v \geqq d$.

On the other hand, $\{v \in I_k \mid \deg(v) > 1\} \supset \{\overline{ai} \mid 0 \leqq i < k'\} = \{\overline{di} \mid 0 \leqq i < k'\}$. Since $dk' = k$, $\#\{v \in I_k \mid \deg(v) > 1\} = k'$ and $\deg(0) = d$. *qed.*

Now we will show the special cases of MDG.

Proposition 2 (1) $M_k^k = M_k^0 = K_k^0$: *Constant Graph.*



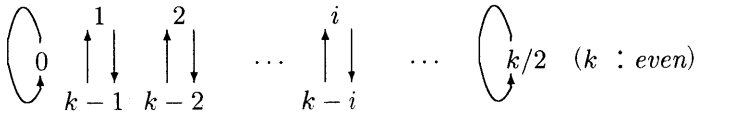
pseuo-tree of height 1. $\mathbb{P} = \Bbbk_1$, $\mathbb{D} = (k-1)\Bbbk_0 + \Bbbk_k$

(2) *Two special cases of cyclic type:*

(2-1) $M_k^1 = kK_1^0 \cong kC_1$:

$\mathbb{P} = 1^k$

(2-2) M_k^{k-1} :



$(k$: *even*$)$

$$M_k^{k-1} \cong \begin{cases} C_1 \cup \dfrac{k-1}{2} C_2 \\ 2C_1 \cup \left(\dfrac{k}{2} - 1\right) C_2 \end{cases}, \quad \mathbb{P}(M_k^{k-1}) = \begin{cases} \Bbbk_1 + \dfrac{k-1}{2}\Bbbk_2 & (k : odd) \\ 2\Bbbk_1 + \left(\dfrac{k}{2} - 1\right)\Bbbk_2 & (k : even) \end{cases}.$$

(3) *Let* $k = c^n$.

(3-1) *If* $c = a$, *then* $d = a$, $k' = a^{n-1}$, $M_{a^n}^a$ *is a pseudo-tree of height* n, *and* $M_{a^n}^a \cong L_0 \vee_0 (a-1)(L_1 \vee_1 B_a^{n-1})$. $\mathbb{D}(M_{a^n}^a) = a^{n-1}(a-1)\Bbbk_0 + a^{n-1}\Bbbk_a$.

$$\mathcal{L}_j(M_{a^n}^a) = \begin{cases} \{i \in I_{a^n} \mid a^{j-1} | i,\ a^j \nmid i\} & (1 \leqq j \leqq n) \\ \{0\} & (j = \infty) \end{cases}.$$

(3-2) *If* $c | a$, *that is* $a = bc$ *for some* $b > 0$, *then* $M_{c^n}^a$ *is a pseuodo-tree whose height is at most* n. *Moreover, if* $(b, c) = 1$, *then* $M_{c^n}^a \cong M_{c^n}^c$.

(4) *For any* $a \in \mathbb{Z}_k^\times$, M_k^a *is of cycle type. The connected component* $\mathcal{F}(1; M_k^a)$ *is nothing but the subgroup* $\langle a \rangle$. *Its period is the order of* a *and is a divisor of* $\varphi(k)$.

Moreover If k *is prime, then* $\mathbb{Z}_p^\times = \mathbb{Z} \setminus \{0\}$ *and* $\varphi(p) = p - 1$. *The coset decomposition by* $\langle a \rangle$ *gives a connected component decomposition of the MDG* M_p^a .

(5) *If* $a \in \mathbb{Z}_k^\times$, *then there exists* $b \in \mathbb{Z}_k^\times$ *such that* $ab \equiv 1 \pmod{k}$, *and* $(M_k^a)^{-1} = M_k^b$.

(6) *If* $\mathcal{F}(1; M_k^a) = V^+(1)$, *then it is a cycle and* $a \in \mathbb{Z}_k^\times$. *And* $\mathcal{F}(1; M_k^a) = \langle a \rangle$ *is a subgroup of* $\mathbb{Z}_k^\times$. *The period of this cycle is the order of* a, *and a divisor of* $\varphi(k) = |\mathbb{Z}_k^\times|$.

Proof. (3-2) $a^n v \equiv 0 \pmod{c^\ell}$ for any $v \in I_k$.

Assume $(b, c) = 1$. Consider the reduction scheme:

$$M_{c^n}^a \Longrightarrow M_{c^{n-1}}^a \Longrightarrow \cdots \Longrightarrow M_{c^2}^a \Longrightarrow M_c^a = M_c^0 = K_c^0$$

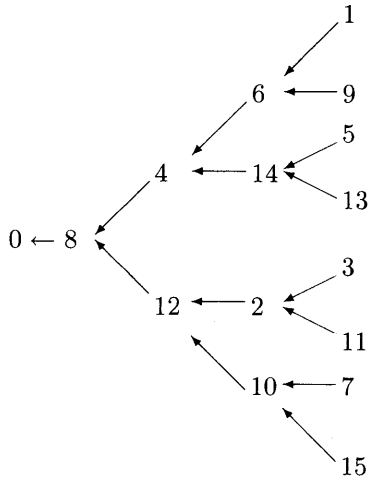
$M^a_{c^2}$ is obtained from $E_c(M^0_c)$ by attaching K^0_c at each leaves of $E_c(M^0_c)$. In fact, $(b,c)=1$, hence $b \in \mathbb{Z}_c^\times$ and there exist integers x, y such that $xb + yc = 1$. Then introduce the number w $(0 < w < c)$ by $w \equiv xv \pmod{c}$. For every leaf cv $(1 \leqq v < c)$ of $E_c(M^0_c)$, take verteces $\{w + ci \mid 0 \leqq i < c\}$, then

$$\begin{aligned} w + ci \quad &\to \quad a(w+ci) \equiv bc(xv + ci) = cvbx + (cb)ci = cv(1 - yc) + c^2bi \\ &= \quad cv + c^2(bi - yv) \equiv cv \pmod{c^2}, \end{aligned}$$

and the number of these new verteces is $(c-1)c = c^2 - c$, so no other verteces remain in $M^a_{c^2}$.

By induction on n, we will show $M^c_{c^n} \cong L_0 \vee_0 (c-1)(L_1 \vee_1 B^{n-1}_c)$. Assume $M^a_{c^{n-1}} \cong L_0 \vee_0 (c-1)(L_1 \vee_1 B^{n-2}_c)$. As for the case $n = 2$, $\mathcal{L}_1(E_c(M^a_{c^{n-1}})) = \{cv \mid 1 \leq v < c\}$. Consider the set $\{w + ci \mid 0 \leqq i < c\}$, where w $(0 < w < c)$ is defined by $w \equiv xv \pmod{c}$, then $c(w + ci) \equiv cv \pmod{c^2}$. However, $c \leq cv < c^2$, hence cv deterimined also as modulo c^n. *qed.*

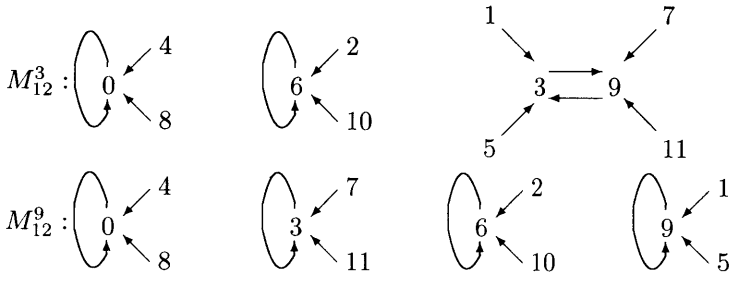
Examples for (3-2). (1) M^6_{16}, $c = 2, n = 4, a = 6, (c^n, a) = c$. $\mathbb{D}(M^6_{16}) = 8\Bbbk_0 + 8\Bbbk_2$, $\mathcal{L}_1 = \mathcal{D}_0 = \{v \mid (v,2) = 1\}$, $\mathcal{L}_2 = \{v \mid 2|v,\ 4 \nmid v\}$, $\mathcal{L}_3 = \{v \mid 4|v,\ 8 \nmid v\}$, $\mathcal{L}_4 = \{v \mid 8|v,\ 16 \nmid v\} = \{8\}$, $\mathcal{L}_\infty = \{0\}$.



(2) M^{12}_{36}, $c = 6, n = 2, a = 12, (c^n, a) = a = 2c$. $\mathbb{D}(M^{12}_{36}) = 33\Bbbk_0 + 3\Bbbk_{12}$, $\mathcal{L}_1 = \mathcal{D}_0 = I_{36} \setminus \mathcal{L}_\infty$, $\mathcal{L}_\infty = \{0\}$, $\mathcal{D}_{12} = \{0, 12, 24\}$.

$W(0) = \{3v \mid 1 \leqq v < 12\} \subset E_3(M^0_{12})$, $O^-(12) = \{3v + 1 \mid 0 \leqq v < 12\} = 1 + E_3(M^0_{12})$, $O^-(24) = \{3v + 2 \mid 0 \leqq v < 12\} = 2 + E_3(M^0_{12})$.

Remark 1. By Theorem 5 (6), if $(k,a) = (k,b)$, then the degree characterisic coincide: $\mathbb{D}(M^a_k) = \mathbb{D}(M^b_k)$, but they are not necessarily isomorphic with each other. For example, $M^9_{12} \ncong M^3_{12}$, since $\mathbb{P}(M^3_{12}) = 2\Bbbk_1 + \Bbbk_2$, $\mathbb{P}(M^9_{12}) = 4\Bbbk_1$.



Remark 2. It is very difficult problem that to determine the order $o_k(a)$ explicitely. For example, it is not yet known whether for infinite number of primes p, the number 2 is a generator of $(\mathbb{Z}/p^e\mathbb{Z})^\times$ for some

$e > 0$. This is a partial form of Artin's conjecture on primitive roots.

Remark 3. If a is a generator of the group $(\mathbb{Z}/k\mathbb{Z})^\times$ of reduced residue classes modulo k, this group is a cycle of period $\varphi(k)$.

Remark 4. Let $k = p$ be prime. Then $\mathbb{P}(M_p^a) = \Bbbk_0 + \Bbbk_{p-1}$ is equivalent with that a is a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$.

Remark 5. Let $k = p^e$ $(e > 0)$ be a power of a prime p. Then the group $(\mathbb{Z}/k\mathbb{Z})^\times$ is generated by a single element.

Remark 6. If k is not prime, then the sets $\{0\}$ and $(\mathbb{Z}/k\mathbb{Z})^\times$ does not cover the whole $\mathbb{Z}/k\mathbb{Z}$.

If $a \in (\mathbb{Z}/k\mathbb{Z})^\times$, then the subgroup $\langle a \rangle$ of $(\mathbb{Z}/k\mathbb{Z})^\times$ is a cycle of M_k^a, and $(\mathbb{Z}/k\mathbb{Z})^\times$ is a sum of cycles of period $o_k(a)$. $(\mathbb{Z}/k\mathbb{Z}) \setminus (\mathbb{Z}/k\mathbb{Z})^\times$ is also a sum of cycles, but it is difficult in general to determine their periods. The periodic structure can be detected through reductions $M_k^a \Rightarrow M_{k/d}^a$ for all divisors d of k.

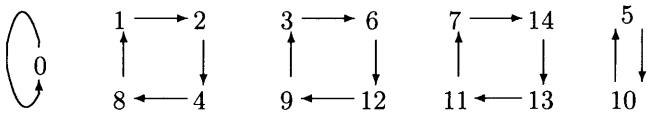
If $a \notin (\mathbb{Z}/k\mathbb{Z})^\times$, then the connected component $\mathcal{F}(0; M_k^a)$ is a pseudo-tree. The periodic structure can be detected through a reduction $M_k^a \Rightarrow M_{k/d}^a$, where $d = (a, k)$.

Remark 7. Assume that there are 2 cycles C' and C'' in M_k^a. Put $s = p(C')$ and $t = p(C'')$, then $\overline{a^s v} = \overline{v}$ and $\overline{a^t w} = \overline{w}$ for any $v \in C'$ and $w \in C''$. Then $\overline{a^{ns} v} = \overline{v}$ and $\overline{a^{nt} w} = \overline{w}$ for any positive integer n. Therefore $O^+(\overline{v + w})$ becomes a cycle whose period is the least common multiple of s and t. Denote this cycle by $C' \oplus_{(v,w)} C''$, and call it the amalgamation of C' and C'' at (v, w). Note that $C' \oplus_{(v,w)} C''$ may not be identical with $C' \oplus_{(v',w)} C''$ for different pairs (v, w) nad (v', w').

For example, consider M_{15}^2, and the reduction scheme

$$\begin{array}{ccc} M_{15}^2 & \Longrightarrow & M_5^2 \\ \Downarrow & & \Downarrow \\ M_3^2 & \Longrightarrow & M_1^2 = M_1^0 = C_1 \end{array}$$

M_{15}^2 is of cycle type. $\mathcal{F}(0)$ comes from M_1^2 as $E_{15}(M_1^2)$. $\mathcal{F}(3)$ comes from M_5^2 as $E_3(\mathcal{F}(1; M_5^2))$ and $\mathcal{F}(5)$ comes from M_3^2 as $E_5(\mathcal{F}(1; M_3^2))$. And other cycles are obtained by amalgamation: $\mathcal{F}(1) = \mathcal{F}(3) \oplus_{(3,5)} \mathcal{F}(5)$ and $\mathcal{F}(11) = \mathcal{F}(3) \oplus_{(3,10)} \mathcal{F}(5)$.



Remark 8. For general $k > 1$, the pseudo-tree structure of the connected component $\mathcal{F}(0; M_k^a)$ and periodic structures of M_k^a can be detected through the reduction scheme

$$M_k^a \Rightarrow M_{k/d}^a \Rightarrow \cdots \Rightarrow M_{k_1}^a \Rightarrow M_{k_1/d_1}^a \Rightarrow \cdots \Rightarrow M_{k_\ell}^a$$

where $d = (k, a)$, $m = \max\{n > 0 \mid d^n | k\}$, $k_1 = k/d^m$, $d_1 = (k_1, a)$, $m_1 = \max\{n > 0 \mid d_1^n | k_1\}$, $k_2 = k_1/d_1^{m_1}$, $\ldots$, $k_\ell = k_{\ell-1}/d_{\ell-1}^{m_{\ell-1}}$, $(k_\ell, a) = 1$. The pseudo-tree structure of $\mathcal{F}(0; M_k^a)$ is the same as $\mathcal{F}(0; M_{k/k_\ell}^a)$. The reduction scheme is parallel to the above:

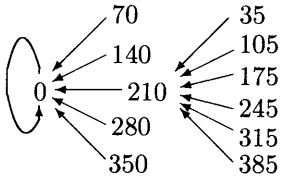
$$M_{k/k_\ell}^a \Rightarrow M_{k/k_\ell d}^a \Rightarrow \cdots \Rightarrow M_{k_1/k_\ell}^a \Rightarrow M_{k_1/k_\ell d_1}^a \Rightarrow \cdots \Rightarrow M_1^a = M_1^0$$

and the periodic structure M_k^a is same as $M_{k_\ell}^a$.

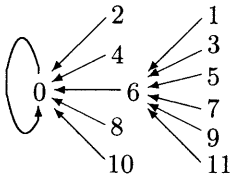
Example. $k = 420,\ a = 6,\ d = (k,a) = 6,\ k_1 = 70,\ d_1 = (k_1,a) = 2,\ k_2 = 35,\ \ell = 2,\ d/d_\ell = 12.$

$$M^6_{420} \Rightarrow M^6_{70} \Rightarrow M^6_{35}\,, \qquad M^6_{12} \Rightarrow M^6_2 \Rightarrow M^6_1 = M^0_1$$

$\mathcal{F}(0; M^6_{420})$:



M^6_{12} :



The periodic structures of M^6_{35} can be detected through the reduction scheme:

$$\begin{array}{ccc} M^6_{35} & \Longrightarrow & M^6_5 = M^1_5 \\ \Downarrow & & \Downarrow \\ M^6_7 & \Longrightarrow & M^6_1 = M^0_1 = C_1 \end{array}$$

Five C_1's arise as $E_7(M^6_5)$. One $C_1 = \mathcal{F}(0; M^6_{35})$ comes also as $E_7(\mathcal{F}(0; M^6_5)) = E_5(\mathcal{F}(0; M^6_7))$. Three C_2's arise as $E_5(M^6_7 \setminus \{0\})$. Other 12 C_2's are obtained by amalgamation of C_2 and C_1 besides $\{0\}$. See §7..5 in detail.

In the following, we will consider pseudo-tree structures of the connected components $\mathcal{F}(0)$ and periodic structures in the individual cases.

§5..1 Case of $k = p$: prime

Let $k = p$ be a prime number. M^0_p is the constant graph $K^0_p \cong B^1_p$ (p-nary pseudo-tree of height 1). For $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, M^a_p is of cycle type. From the remark after Theorem 1,

$$M^a_p \cong \begin{cases} K^0_p & (a = 0) \\ pC_1 & (a = 1) \\ C_1 \cup tC_s & (a > 1, s = o_p(a), t = (p-1)/s) \end{cases}$$

The values of $s(a)$ may run throught the set of all divisors of $p-1 = \varphi(p) = |(\mathbb{Z}/p\mathbb{Z})^\times|$. Hence the number $m(p)$ of the isomorphism classes among M^a_p is $1 + \delta(p-1)$, where $\delta(p-1)$ is the number of divisors of $p-1$.

In particular, if t and $p-1 = \varphi(p)$ is coprime, then a is also a generator, $o(a) = p-1$ and $\langle a \rangle = (\mathbb{Z}/p\mathbb{Z})^\times$.

Here we list divisors s of $p-1$ and $m(p)$ for prime numbers $p \leqq 131$. For any s in the column of p, there exists an integer $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ with $o_p(a) = s$. Then $\langle a \rangle$ is a subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$ of order s, and the coset decomposition of the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ gives the all connected components of M^a_p. More precisely, $\mathcal{F}(0) = \{0\}$, $\mathcal{F}(1) = \mathcal{F}(a) = \langle a \rangle \cong C_s$ and $M^a_p \cong C_1 \cup dC_s$.

p	2	3	5	7	11	13	17	19	23	29
$p-1$	1	2	4	6	10	12	16	18	22	28
s	1	1, 2	1,2, 4	1,2, 3,6	1, 2, 5,10	1, 2, 3, 4, 6, 12	1, 2, 4, 8, 16	1, 2, 3, 6, 9, 18	1, 11, 22	1, 2, 4, 7, 14, 28
$m(p)$	2	3	4	5	5	7	6	7	4	7

p	31	37	41	43	47	53	59
$p-1$	30	36	40	42	46	52	58
s	1, 2, 3, 5, 6, 10, 15, 30	1, 2, 3, 4, 6, 9, 12,18,36	1, 2, 4, 5, 8, 10, 20, 40	1, 2, 3, 6, 7, 14, 21, 42	1, 2, 23, 46	1, 2, 4, 13, 28, 52	1, 2, 29, 58
$m(p)$	9	10	9	9	5	7	5

p	61	67	71	73	79	83	89
$p-1$	60	66	70	72	78	82	88
s	1,2,3, 5,6,10, 15, 20, 30, 60	1, 2, 3, 6,11, 22, 33, 66	1,2,5, 7,10, 14,35, 70	1,2,3,4, 6, 8, 9, 12, 18, 36, 72	1, 2, 3, 6, 13, 26, 39, 78	1,2, 41, 82	1,2, 4,8, 11,22, 44,88
$m(p)$	11	9	9	12	9	5	9

p	97	101	103	107	109	113	127	131
$p-1$	96	100	102	106	108	112	126	130
s	1,2,3, 4,6,8, 12, 16, 24, 32, 48, 96	1,2,4, 5,10, 20,25, 50, 100	1,2,3, 6,17, 34, 51, 102	1,2, 53, 106	1,2,3, 4,6,9, 12,18, 27,36, 54,108	1,2,4, 7,8, 14,16, 28,56, 112	1,2,3, 6,7,9, 14,18, 21,42, 63,126	1,2,5, 10,13, 26,75
$m(p)$	13	10	9	5	13	11	13	8

Proposition 3 (1) *The number of cycle of of odd degree is even.*

(2) *For any $s \geq 1$, there exist multiplicative dynamical graphs with cycles of period s.*

Proof. (1) In fact, $M_2^1 = 2C_1$ for $p = 2$. An odd prime p can be written as $p = 4n \pm 1$, therefore $p - 1 = 4n$, $4n - 2 = 2(2n - 1)$ is even.

(2) The famous Dirichlet's theorem states that if $(a, q) = 1$, there exist an infinite number of primes of the form $a + nq$ $(n \geq 1)$. Hence there exits a number $n \geqq 1$ such that $ns + 1$ is prime. Then $\varphi(ns+1) = ns$, and there is a number $a \in (\mathbb{Z}/(ns+1)\mathbb{Z})^\times$ with order $s = o_{ns+1}(a)$. *qed.*

Here we list the smallest primes $p(s) = ns + 1$ $(n \geq 1)$ for $s \leqq 100$.

s	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$p(s)$	3	7	5	10	13	29	17	19	11	23	13	53	29	31	17	103	19

s	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
$p(s)$	191	41	43	23	47	97	101	79	109	29	59	31	311	97	67

s	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
$p(s)$	103	71	73	149	191	79	41	83	43	173	89	181	47	283	97

s	49	50	51	52	53	54	55	56	57	58	59	60	61
$p(s)$	197	101	103	53	106	109	331	113	229	59	709	61	367

s	62	63	64	65	66	67	68	69	70	71	72	73	74
$p(s)$	311	127	193	131	67	269	137	139	71	569	73	293	149

s	75	76	77	78	79	80	81	82	83	84	85	86	87
$p(s)$	151	457	463	79	317	241	163	83	167	337	1021	173	349

s	88	89	90	91	92	93	94	95	96	97	98	99	100
$p(s)$	89	179	91	547	277	373	83	659	97	389	197	199	101

§5..2 Case of $k = 2^m$ $(m > 0)$

For $m > 0$, put $K_m = (\mathbb{Z}/2^m\mathbb{Z})^\times$, then $|K_m| = \varphi(2^m) = 2^{m-1}$. Recall Theorem 1 (3).

Let $0 \leq a < 2^m$. The multiplicative dynamical graph $M^a_{2^m}$ is of cycle type in the case $a \not\equiv 0 \pmod 2$, is a pseudo-tree otherwise($a \equiv 0 \pmod 2$).

Assume $(a, 2^m) = 2^q > 1$. Let $m = nq + r$ $(n \geq 1,\ 0 \leq r < q)$, then the reduction scheme is

$$M^a_{2^m} \Longrightarrow M^a_{2^{m-q}} \Longrightarrow \cdots \Longrightarrow M^a_{2^{m-nq}} = M^a_{2^r} = M^0_{2^r} \cong K^0_{2^r},$$

and $M^a_{2^m}$ is a pseudo-tree. In this case, we get

$$M^a_{2^{nq+r}} \cong \begin{cases} L_0 \vee_0 (2^q - 1)(L_1 \vee_1 B^{n-1}_{2^q}) & (r = 0) \\ L_0 \vee_0 \left((2^q - 2^r)(L_1 \vee_1 B^{n-1}_{2^q}) \cup (2^r - 1)(L_1 \vee_1 B^n_{2^q})\right) & (r > 0) \end{cases}$$

Proof. Factor a as $a = 2^q b$, where $(b, 2) = 1$. Then $1 \leqq b < 2^{nq}$. Consider the reduction $M^a_{2^{q+r}} \Longrightarrow M^0_{2^r}$ and the subgraph $G' = E_{2^q}(M^0_{2^r})$ of $M^a_{2^{q+r}}$. We get the set $V(G') = \{2^q i \mid 0 \leq i \leq 2^r - 1\}$ of verteces of G', the set $\mathcal{L}(G'; 1) = \{2^q i \mid 1 \leq i \leq 2^r - 1\}$ of leaves of G' and the limit cycle $\mathcal{L}(G'; \infty) = \{0\}$.

Let $\bar{b} = b \pmod{2^q}$, then $1 \leq \bar{b} < 2^q$, $b = \bar{b} + 2^q\beta$ and $(\bar{b}, 2) = 1$. Hence there are $c, d \in \mathbb{Z}$ satisfying $\bar{b}c + 2^q d = 1$. Here we may assume $1 \leq c < 2^q$. For i with $1 \leq i \leq 2^r - 1$, let $j = 2^{q-r}ci \pmod{2^q}$, then $j = 2^{q-r}ci + 2^q\alpha$ and

$$\begin{aligned} aj &= 2^r bj = 2^r b(2^{q-r}ci + 2^q\alpha) = 2^q bci + 2^{r+q}\alpha \\ &\equiv 2^q(\bar{b} + 2^q\beta)ci = 2^q\bar{b}ci \equiv 2^q(1 - 2^q d)i \equiv 2^q i \pmod{2^{q+r}}. \end{aligned}$$

Thus $j \longrightarrow 2^q i$ and also $j + 2^r h \pmod{2^{q+r}} \longrightarrow 2^q i$. Since

$$|\{j + 2^r h \pmod{2^{q+r}} \mid h \geqq 0\}| = |\{j + 2^r h \pmod{2^{q+r}} \mid 0 \leqq h \leqq 2^q - 1\}| = 2^q,$$

the pseudo-tree $2^q L_1 (= B^1_{2^q}$: 2^q-nary pseudo-tree of height 1) is attached at every vertex $2^q i (1 \leq i \leq 2^r - 1)$.

Consider the gate $W(0)$ to the fixed point $\{0\}$. $\{2^r k \mid 1 \leqq k \leqq 2^q - 1\} \longrightarrow 0$, since $2^r b \cdot 2^r k = 2^{q+r} bk \equiv 0 \pmod{2^{q+r}}$. However $\{2^q k' \mid 1 \leqq k'\} \subset \mathcal{L}(G'; 1)$. Let $2^r k = 2^q k'$, then $k = 2^{q-r}k' \leq 2^q - 1$, so $k' \leq 2^r - \dfrac{1}{2^{q-r}}$, that is $k' \leq 2^r - 1$. Thus $(2^q - 2^r)L_1$ is attached newly to $\{0\}$, hence

$$M^a_{2^{q+r}} \cong L_0 \vee_0 \left((2^q - 2^r)(L_1) \cup (2^r - 1)(L_1 \vee_1 B^1_{2^q})\right),$$

and $|\mathcal{L}(M^a_{2^{q+r}}; 1)| = (2^r - 1)2^q + (2^q - 2^r) = 2^{q+r} - 2^r$.

Next, consider tghe reduction $M^a_{2^{2q+r}} \Longrightarrow M^a_{2^{q+r}}$ and the subgraph $G'' = E_{2^q}(M^a_{2^{q+r}})$, then

$$\begin{aligned} \mathcal{L}(G''; 1) &= \{2^q(j + 2^r h) \mid 1 \leq j \leq 2^r - 1,\ 0 \leq h \leq 2^q - 1\} \\ &\quad \cup \left(\{2^{q+r}k \mid 1 \leq k \leq 2^q - 1\} \setminus \{2^{2q}k' \mid 1 \leq k' \leq 2^r - 1\}\right) \end{aligned}$$

is the set of leaves of G''.

For every point $v \in \mathcal{L}(G''; 1)$, there is a vertex $w \in M^a_{2^{2q+r}}$ such that $v = \overline{aw} = \overline{2^q bw}$ $(w \to v)$, and as before $w + 2^r h \to v$, $v \vee_v 2^q L_1 \subset M^a_{2^{2q+r}}$. Hence we get

$$M^a_{2^{2q+r}} \cong L_0 \vee_0 \left((2^q - 2^r)(L_1 \vee_1 B^1_{2^q}) \cup (2^r - 1)(L_1 \vee_1 B^2_{2^q})\right).$$

It is similarly proved for higher m. *qed.*

For $a \in (\mathbb{Z}/2^m\mathbb{Z})^\times$, define the sequence $\mathbf{a}(a) = (a_m = a, a_{m-1}, \ldots, a_1)$ by $a_i = a \pmod{2^i} \in (\mathbb{Z}/2^i\mathbb{Z})^\times$ and let $s_i = o_{2^i}(a_i)$, $\mathbf{s}(a) = (s_m, s_{m-1}, \ldots, s_1)$, then

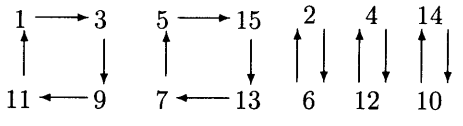
$$M^a_{2^m} \cong C_1 \cup \bigcup_{i=1}^{m} \frac{2^{i-1}}{s_i} C_{s_i}.$$

Here s_i is a power of 2, since $\varphi(2^i) = 2^{i-1}$. Periods of any cycles in $M^a_{2^m}$ are of the form 2^n $(0 \le n \le m-1)$. Note the sequence of orders satisfy the condition $s_i = s_{i-1}$ or $2s_{i-1}$.

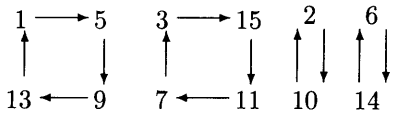
Example. $m = 4$. We list all MDG $M^a_{2^4}$ of cycle type:

a	$\mathbf{a}(a)$	$\mathbf{s}(a)$	M^a_{16}
1	(1,1,1,1)	(1,1,1,1)	$16C_1$
3	(3,3,3,1)	(4,2,2,1)	$2C_1 \cup 3C_2 \cup 2C_4$
5	(5,5,1,1)	(4,2,1,1)	$4C_1 \cup 2C_2 \cup 2C_4$
7	(7,7,3,1)	(2,2,2,1)	$2C_1 \cup 7C_2$
9	(9,1,1,1)	(2,2,2,1)	$2C_1 \cup 7C_2$
11	(11,3,3,1)	(4,2,2,1)	$2C_1 \cup 3C_2 \cup 2C_4$
13	(13,5,1,1)	(4,2,1,1)	$4C_1 \cup 2C_2 \cup 2C_4$
15	(15,7,3,1)	(2,2,2,1)	$2C_1 \cup 7C_2$

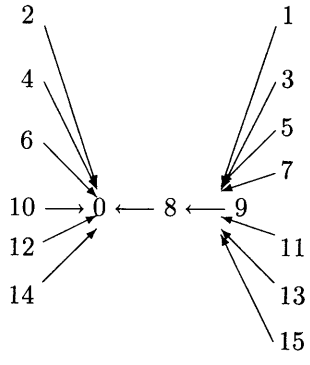
M^3_{16} : $\{0, 8\}$ are fixed points.



M^5_{16} : $\{0, 4, 8, 12\}$ are fixed points.



M^8_{16} : $\{0\}$ is a fixed point.



§5..3 Case of $k = p^2$ (p: odd prime)

Let $K = (\mathbb{Z}/p^2\mathbb{Z})^\times$ and $\bar{K} = (\mathbb{Z}/p\mathbb{Z})^\times$. Then the order of K is $|K| = \varphi(p^2) = p^2 - p = p(p-1)$, and its divisor is a divisor s of $p-1$ or its p multiple ps, since p is prime.

For $a \in K$, put $\bar{a} = a \pmod p$, then $\bar{a} \in \bar{K}$. Put $\bar{s} = o_{\bar{K}}$, then $s = o_K(a) = \bar{s}$ or $p\bar{s}$.

In fact, if $a^s \equiv 1 \pmod{p^2}$, then there exist poistive integers q, r and $\bar{a} \in \bar{K}$ such that $a^s - 1 = qp^2$ and $a = \bar{a} + rp$. Hence

$$0 \equiv qp^2 = (\bar{a} + rp)^s - 1 \equiv \bar{a}^s - 1 \pmod p,$$

thus $s = \bar{s}$ for the case $s < p$.

Let $p \leq s$, then $\bar{s} = s/p$ devides $p-1$. In fact, $\bar{a}^{p-1} \equiv 1 \pmod p$ by the little theorem of Fermat(Theorem 1 (5)). So

$$\bar{a}^s - 1 = \bar{a}^{p\bar{s}} - 1 = (\bar{a}^p)^{\bar{s}} - 1 \equiv \bar{a}^{\bar{s}} - 1 \equiv 0 \pmod p.$$

Thus

$$M^a_{p^2} \cong \begin{cases} K^0_{p^2} & (a = 0) \\ L_0 \vee_0 (p-1)B^1_p & (p|a) \\ p^2 C_1 & (a = 1) \\ pC_1 \cup (p-1)C_p & (a \in \mathbb{Z}^\times_{p^2} \text{ and } o(a) = p) \\ C_1 \cup tC_s & (a \in \mathbb{Z}^\times_{p^2} \text{ and } s = o(a) < p, t = (p^2-1)/s) \\ C_1 \cup tC_{s/p} \cup tC_s & (a \in \mathbb{Z}^\times_{p^2} \text{ and } s = o(a) > p, t = p(p-1)/s) \end{cases}$$

Let $a = kp + 1$ $(0 < k < p)$, then $o(a) > 1$ and $p|o(a)$, and thus $o(a) = p$. In fact,

$$a^p = (kp+1)^p \equiv {}_pC_1 \cdot kp + {}_pC_0 \cdot 1 \equiv 1 \pmod{p^2}.$$

Let $a = p^2 - 1$, then $o(a) = 2$ and

$$M^a_{p^2} = C_1 \cup \frac{p-1}{2} C_2 \cup \frac{p^2-p}{2} C_2 = C_1 \cup \frac{p^2-1}{2} C_2.$$

$$M^a_{p^2} = C_1 \cup \frac{p-1}{2} C_2 \cup \frac{p^2-p}{2} C_2 = C_1 \cup \frac{p^2-1}{2} C_2.$$

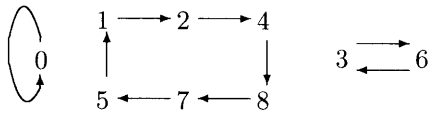
Any divisors of $\varphi(p^2) = p(p-1)$ can be periods of cycles of some $M^a_{p^2}(0 < a < p^2)$. The number $m(p^2)$ of the isomorphism classes among $M^a_{p^2}$ is $1 + 1 + \delta(p(p-1)) = 2(1 + \delta(p-1)) = 2m(p)$, where $\delta(d)$ is the number of divisors of d.

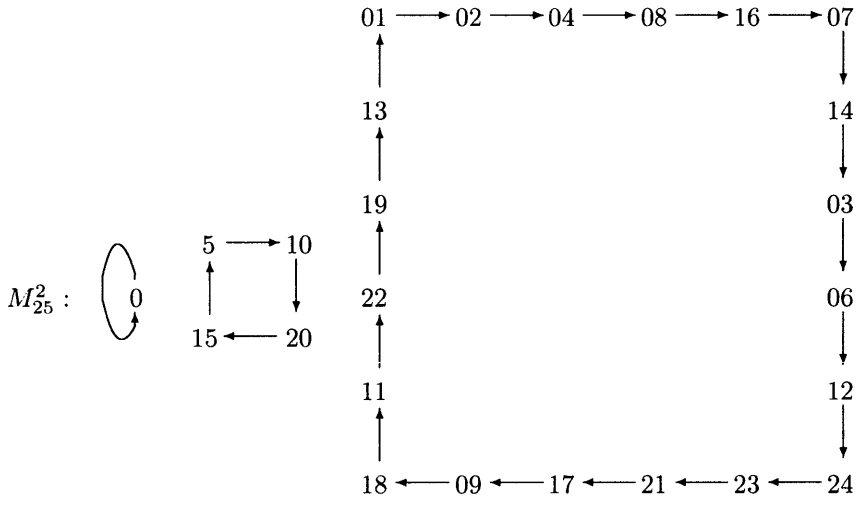
Now, we list maximal periods and $m(p^2)$ of $M^a_{p^2}(0 < a < p^2)$:

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43
$\varphi(p^2)$	2	6	20	42	110	156	272	342	506	812	930	1332	1649	1806
$m(p^2)$	4	6	8	10	10	14	12	14	8	14	18	20	18	18

From this list, we know the case where the values k for which cycles of period s appear in MDG M^a_k are lower than $p(s)$ in the subsection §7..1. For example, a cycle of peirod 6, 20 or 55 appears in M^2_9, M^2_{25} or M^2_{121} respectively.

M^2_9 :





§5..4 Case of $k = p^m$ $(m > 0, p$:prime)

Let p be an odd prime and $K_m = (\mathbb{Z}/p^m\mathbb{Z})^\times$ for $m > 1$, then $|K_m| = \varphi(p^m) = p^{m-1}(p-1)$. Let $0 \leq a < p^m$, then the multiplicative dynamical graph $M_{p^m}^a$ is of cycle type in the case $a \not\equiv 0 \pmod p$, is a pseudo-tree otherwise($a \equiv 0 \pmod p$).

Assume $(a, p^m) = p^q > 1$. Let $m = nq + r$ $(n \geq 1,\ 0 \leq r < q)$, then the reduction scheme is

$$M_{p^m}^a \Longrightarrow M_{p^{m-q}}^a \Longrightarrow \cdots \Longrightarrow M_{p^{m-nq}}^a = M_{p^r}^a = M_{p^r}^0 \cong K_{p^r}^0,$$

and $M_{p^m}^a$ is a pseuodo-tree. In this case, we get

$$M_{p^{nq+r}}^a \cong \begin{cases} L_0 \vee_0 (p^q - 1)(L_1 \vee_1 B_{p^q}^{n-1}) & (r = 0) \\ L_0 \vee_0 \left((2^q - 2^r)(L_1 \vee_1 B_{p^q}^{n-1}) \cup (2^r - 1)(L_1 \vee_1 B_{p^q}^{n})\right) & (r > 0) \end{cases}$$

Proof. Factor a as $a = p^q b$, where $(b, p) = 1$. Then $1 < b < p^{nq}$. Consider the reduction $M_{p^{q+r}}^a \Longrightarrow M_{p^r}^0$ and the subgraph $G' = E_{p^q}(M_{p^r}^0)$ of $M_{p^{q+r}}^a$. We get the set $V(G') = \{p^q i \mid 0 \leq i \leq p^r - 1\}$, the set $\mathcal{L}(G'; 1) = \{p^q i \mid 1 \leq i \leq p^r - 1\}$ of leaves of G' and the limit cycle $\mathcal{L}(G'; \infty) = \{0\}$.

Let $\bar{b} = b \pmod{p^q}$, then $1 \leq \bar{b} < p^q$, $b = \bar{b} + p^q\beta$, $(\bar{b}, p) = 1$. Hence there are $c, d \in \mathbb{Z}$ satisfying $\bar{b}c + p^q d = 1$. Here we may assume $1 \leq c < p^q$. For i with $1 \leq i \leq p^r - 1$, let $j = p^{q-r}ci \pmod{p^q}$, then $j = p^{q-r}ci + p^q\alpha$ and,

$$\begin{aligned} aj &= p^r bj = p^r b(p^{q-r}ci + p^q\alpha) = p^q bci + p^{r+q}\alpha \\ &\equiv p^q(\bar{b} + p^q\beta)ci = p^q\bar{b}ci \equiv p^q(1 - p^q d)i \equiv p^q i \pmod{p^{q+r}}. \end{aligned}$$

Thus $j \longrightarrow p^q i$ and also $j + p^r h \pmod{p^{q+r}} \longrightarrow p^q i$. Since

$$|\{j + p^r h \pmod{p^{q+r}} \mid h \geqq 0\}| = |\{j + p^r h \pmod{p^{q+r}} \mid 0 \leqq h \leqq p^q - 1\}| = p^q,$$

the pseudo-tree $p^q L_1$ $(= B_{p^q}^1$: p^q-nary pseudo-tree) is attached at every vertex $p^q i (1 \leq i \leq p^r - 1)$.

Consider the gate $W(\{0\})$ of the fixed point $\{0\}$. $W(\{0\})$ contains $\{p^r k \mid 1 \leqq k \leqq p^q - 1\}$, since $p^r b \cdot p^r k = p^{q+r}bk \equiv 0 \pmod{p^{q+r}}$, that is, $p^r k \longrightarrow 0$. However $\{p^q k' \mid 1 \leqq k'\} \subset \mathcal{L}(G'; 1)$. Let $p^r k = p^q k'$, then

$k = p^{q-r}k' \leqq p^q - 1$, so $k' \leq p^r - \dfrac{1}{p^{q-r}}$, that is, $k' \leqq p^r - 1$. Thus $(p^q - p^r)L_1$ is newly attached at $\{0\}$, hence

$$M^a_{p^{q+r}} \cong L_0 \vee_0 \left((p^q - p^r)(L_1) \cup (p^r - 1)(L_1 \vee_1 B^1_{p^q})\right),$$

and $|\mathcal{L}(M^a_{p^{q+r}}; 1)| = (p^r - 1)2^q + (p^q - p^r) = p^{q+r} - p^r$.

Next consider the reduction $M^a_{p^{2q+r}} \Longrightarrow M^a_{p^{q+r}}$ and the subgraph $G'' = E_{p^q}(M^a_{p^{q+r}})$, then

$$\begin{aligned}\mathcal{L}(G''; 1) &= \{p^q(j + 2^r h) \mid 1 \leq j \leq p^r - 1,\ 0 \leq h \leq p^q - 1\} \\ &\quad \cup \left(\{p^{q+r}k \mid 1 \leq k \leq p^q - 1\} \setminus \{p^{2q}k' \mid 1 \leq k' \leq p^r - 1\}\right)\end{aligned}$$

is the set of leaves of G''.

For every point $v \in \mathcal{L}(G''; 1)$, there is a vertex $w \in M^a_{p^{2q+r}}$ such that $v = \overline{aw} = \overline{p^q bw}$ $(w \to v)$, and as before $w + p^r h \to v$, $v \vee_v p^q L_1 \subset M^a_{p^{2q+r}}$. Hence we get

$$M^a_{p^{2q+r}} \cong L_0 \vee_0 \left((p^q - p^r)(L_1 \vee_1 B^1_{p^q}) \cup (p^r - 1)(L_1 \vee_1 B^2_{p^q})\right).$$

It is similarly proved for higher m. *qed.*

Proposition 4 *Let $m \geq 2$. For $a \in (\mathbb{Z}/p^m\mathbb{Z})^\times$, define the sequence $\mathbf{a}(a) = (a_m = a, a_{m-1}, \ldots, a_1)$ as $a_i = a \pmod{p^i} \in (\mathbb{Z}/p^i\mathbb{Z})^\times$.*

(1) *$s_i = ps_{i-1}$ or s_{i-1} for $i \geq 2$.*

(2) *Let $i \leq m - 1$. If $s_i = ps_{i-1}$, then $s_{i+1} = ps_i$.*

Proof. (1) For $a \in (\mathbb{Z}/p^i\mathbb{Z})^\times$, put $\bar{a} = a \pmod{p^{i-1}}$ and $s = o_{p^{i-1}}(\bar{a})$, then there are $e, f \in \mathbb{Z}$ such that $\bar{a}^s = 1 + e \cdot p^{i-1}$, $a = \bar{a}1 + f \cdot p^{i-1}$, hence

$$a^{ps} = ((\bar{a} + f \cdot p^{i-1})^p)^s \equiv (\bar{a}^p)^s = (\bar{a}^s)^p \equiv (1 + e \cdot p^{i-1})^p \equiv 1 \pmod{p^i}$$

and $s \leqq s_i = o_{p^i}(a) \leqq ps$, $s_i | ps$. Therefore $s_i = s$ or ps, since p is prime.

(2) It is sufficient to show $a_{i+1}^{s_i} \not\equiv 1 \pmod{p^{i+1}}$. We use notations $a = a_i, \bar{a} = a_{i-1}$ as in the proof of (1), then $a^{ps} \equiv 1$, $a^s \not\equiv 1 \pmod{p^i}$ and $\bar{a}^s \equiv 1 \pmod{p^{i-1}}$ Hence $a^s = (\bar{a} + f \cdot p^{i-1})^s \equiv \bar{a}^s + fsp^{i-1} \equiv 1 + hp^{i-1} \pmod{p^i}$. Here $h = h' + fs$ and $(h, p) = 1$. In fact, if $(h, p) > 1$, then $(h, p) = p$ and $a^s \equiv 1 \pmod{p^i}$. Thus $a^s = 1 + h''p^i + hp^{i-1}$, where h'' is an integer.

Write a_{i+1} as $a_{i+1} = a + h'p^i$, then $a_{i+1}^{s_i} = (a + h'p^i)^{sp} = ((a + h'p^i)^p)^s \equiv (a^p)^s = (a^s)^p = (1 + h''p^i + hp^{i-1})^p \equiv 1 + hp^i \not\equiv 1 \pmod{p^{i+1}}$ となる. *qed.*

For $a \in (\mathbb{Z}/p^m\mathbb{Z})^\times$, take sequences $\mathbf{a}(a)$ and $\mathbf{s}(a) = (s_m, s_{m-1}, \ldots, s_1)$ as Proposition 5, then

$$M^a_{p^m} \cong C_1 \cup \bigcup_{i=1}^{m} \frac{p^{i-1}(p-1)}{s_i} C_{s_i}.$$

As for s_1, any divisors of $p - 1$ actually apear, but from the proposition above, the order sequences $\mathbf{s}(a)$ of a may occur in the very restricted form, such as $(p^{m-i}s, \ldots, ps, s, \ldots, s)$, where s is a divisor of $p - 1$. Thus the number of isomorphism classes of MDG $M^a_{p^m}$ of cycle type is $m\delta(p - 1)$, where $\delta(p - 1)$ is the number of divisors of $p - 1$.

Example 1. $k = 27$, $p = 3$, $m = 3$. We list here all M^a_{27} of cycle type.

a	$\mathbf{a}(a)$	$\mathbf{s}(a)$	M_{27}^a
1	$(1,1,1)$	$(1,1,1)$	$27C_1$
2	$(2,2,2)$	$(18,6,2)$	$C_1 \cup C_2 \cup C_6 \cup C_{18}$
4	$(4,4,1)$	$(9,3,1)$	$3C_1 \cup 2C_3 \cup 2C_9$
5	$(5,5,2)$	$(18,6,2)$	$C_1 \cup C_2 \cup C_6 \cup C_{18}$
7	$(7,7,1)$	$(9,3,1)$	$3C_1 \cup 2C_3 \cup 2C_9$
8	$(8,8,2)$	$(6,2,2)$	$C_1 \cup 4C_2 \cup 3C_6$
10	$(10,1,1)$	$(3,1,1)$	$9C_1 \cup 6C_3$
11	$(11,2,2)$	$(18,6,2)$	$C_1 \cup C_2 \cup C_6 \cup C_{18}$
13	$(13,4,1)$	$(9,3,1)$	$3C_1 \cup 2C_3 \cup 2C_9$
14	$(14,5,2)$	$(18,6,2)$	$C_1 \cup C_2 \cup C_6 \cup C_{18}$
16	$(16,7,1)$	$(9,3,1)$	$3C_1 \cup 2C_3 \cup 2C_9$
17	$(17,8,2)$	$(6,2,2)$	$C_1 \cup 4C_2 \cup 3C_6$
19	$(19,1,1)$	$(3,1,1)$	$9C_1 \cup 9C_2$
20	$(20,2,2)$	$(18,6,2)$	$C_1 \cup C_2 \cup C_6 \cup C_{18}$
22	$(22,4,1)$	$(9,3,1)$	$3C_1 \cup 2C_3 \cup 2C_9$
23	$(23,5,2)$	$(18,6,2)$	$C_1 \cup C_2 \cup C_6 \cup C_{18}$
25	$(25,7,1)$	$(9,3,1)$	$3C_1 \cup 2C_3 \cup 2C_9$
26	$(26,8,2)$	$(2,2,2)$	$C_1 \cup 13C_2$

Thus there are 6 possible sequnces of orders such as $(1,1,1),(3,1,1),(9,3,1)$, $(2,2,2),(6,2,2),(18,6,2)$, and the 6 possible period charateristic as $27\mathbb{k}_1$, $9\mathbb{k}_1+6\mathbb{k}_3$, $3\mathbb{k}_1+2\mathbb{k}_3+3\mathbb{k}_9$, $\mathbb{k}_1+13\mathbb{k}_2$, $\mathbb{k}_1+4\mathbb{k}_2+3\mathbb{k}_6$, $\mathbb{k}_1+\mathbb{k}_2+\mathbb{k}_6+\mathbb{k}_{18}$ respectively.

Example 2. $k=81$, $p=3$, $m=4$. We list here all M_{81}^a of cycle type. There are 8 possible sequnces of orders such as $(1,1,1,1),(3,1,1,1),(9,3,1,1)$, $(27,9,3,1)$, $(2,2,2,2),(6,2,2,2),(18,6,2,2),(54,18,6,2)$, and the 8 possible period charateristic as $81\mathbb{k}_1$, $27\mathbb{k}_1+18\mathbb{k}_3$, $9\mathbb{k}_1+6\mathbb{k}_3+6\mathbb{k}_9$, $3\mathbb{k}_1+2\mathbb{k}_3+2\mathbb{k}_9+2\mathbb{k}_{27}$, $\mathbb{k}_1+40\mathbb{k}_2$, $\mathbb{k}_1+13\mathbb{k}_2+9\mathbb{k}_6$, $\mathbb{k}_1+4\mathbb{k}_2+3\mathbb{k}_6+3\mathbb{k}_{18}$, $\mathbb{k}_1+\mathbb{k}_2+\mathbb{k}_6+\mathbb{k}_{18}+\mathbb{k}_{54}$ respectively.

The sets of a with $s(a)$ are given as

$\{a\in I_{81} \mid s(a)=(1,1,1,1)\}=\{1\}$, $\{a\in I_{81} \mid s(a)=(2,2,2,2)\}=\{80\}$,

$\{a\in I_{81} \mid s(a)=(3,1,1,1)\}=\{28,55\}$,

$\{a\in I_{81} \mid s(a)=(6,2,2,2)\}=\{26,53\}$,

$\{a\in I_{81} \mid s(a)=(9,3,1,1)\}=\{10,19,37,46,64,73\}$,

$\{a\in I_{81} \mid s(a)=(18,6,2,2)\}=\{8,17,35,44,62,71\}$,

$\{a\in I_{81} \mid s(a)=(27,9,3,1)\}=\{4,7,13,16,22,25,31,34,40,43,49,52,58,61,67,70,76,79\}$,

$\{a\in I_{81} \mid s(a)=(54,18,6,2)\}=\{2,5,11,14,20,23,29,32,38,41,44,47,50,56,59,65,68,74,77\}$,

We observe that

$\{a\in I_{81} \mid s(a)=(1,1,1,1)\}=-\{a\in I_{81} \mid s(a)=(2,2,2,2)\}$,

$\{a\in I_{81} \mid s(a)=(3,1,1,1)\}=-\{a\in I_{81} \mid s(a)=(6,2,2,2)\}$,

$\{a\in I_{81} \mid s(a)=(9,3,1,1)\}=-\{a\in I_{81} \mid s(a)=(18,6,2,2)\}$,

$\{a\in I_{81} \mid s(a)=(27,9,3,1)\}=-\{a\in I_{81} \mid s(a)=(54,18,6,2)\}$,

and there hold similar relations also Example 1.

§5..5 Case of Composite Numbers k

The case where k is a composite number, is very comlicate to describe the structures of multiplication DG M_k^a's. If $(k,a) > 1$, then by Remark 8 after Proposition 3, the pseudo-tree structure of M_k^a can be detected through the reduction scheme

$$M_k^a \Rightarrow \cdots \Rightarrow M_{k'}^a,$$

where $(k',a) = 1$, and the periodic structures of M_k^a and $M_{k'}^a$ are same: $\mathbb{P}(M_k^a) = \mathbb{P}(M_{k'}^a)$.

Hence for the purpose to investigate periodic structures of MDG's, we may assume that $(k,a) = 1$. Decompose k as $k = pq$, the composition of mutually prime numbers p, q. Consider the reduction scheme

$$\begin{array}{ccc} M_{pq}^a & \Longrightarrow & M_p^a \\ \Downarrow & & \\ M_q^a & & \end{array}$$

Then M_p^a and M_q^a are also of cyclic type, since $(p,a) = (q,a) = 1$. If we know their periodic structures, then the cycles of M_{pq}^a are obtained as the extensions $E_q(M_p^a)$ and $E_p(M_q^a)$, and their amalgamtions.

Given k explicitely, one may carry out these procedures inductively on the size k of MDG's.

In this subsection, we treat the case where these factors p and q are prime themselves. Let $0 \leqq a < pq$.

Case 1. $a = 0$. $M_{pq}^0 \cong K_{pq}^0$ is the constant graph.

Case 2. $(a,pq) = p$. Decompose a as $a = bp$ $(1 \leq b < q)$, then by Euclid's Algorithm, there are c, α with $c, \alpha \in \mathbb{Z}, 1 \leqq c < q$, satisfying $bc = 1 + \alpha q$.

Consider the reduction $M_{pq}^a = M_{pq}^{bp} \Longrightarrow M_q^{bp}$, then M_q^{bp} is of cycle type, since $(bp,q) = 1$. The structure of M_q^{bp} is determined in §7..1, and the extension $E_p(M_q^{bp})$ is also of cyclic type with the same periodic characteristic: $\mathbb{P}(M_{pq}^{bp}) = \mathbb{P}(E_p(M_q^{bp}))$. Its vertex set is $V(E_p(M_q^{bp})) = \{ip \mid 0 \leq i < q\}$.

Then define the numbers j with $1 \leqq j < q$ as $j \equiv ci \pmod q$, then $j \longrightarrow ip$ in M_{pq}^a. In fact, there is an integer $\beta \in \mathbb{Z}$ satisfying $j = ci + \beta q$ and

$$aj = bpj = bp(ci + \beta q) \equiv bcpi = (1 + \alpha q)pi \equiv ip \pmod{pq}.$$

Moreover, it is obvious that $\{j + \ell q \mid 1 \leq \ell < p\} \longrightarrow ip$, and we know the gate to the vertex ip, hence we get

$$M_{pq}^a = E_p(M_q^{bp}) \bigvee_{i=0}^{q-1} \left(\vee_{ip} K_p^0\right),$$

and

$$\mathbb{P}(M_{pq}^a) = \mathbb{P}(M_q^a),\ \mathbb{V}(M_{pq}^a) = p\mathbb{P}(M_q^a),\ \mathbb{D} = (p-1)q\Bbbk_0 + q\Bbbk_p.$$

Case 3. $(a,pq) = q$. Similarly as in the case 2.

Case 4. $(a,pq) = 1$. Then $a \in \mathbb{Z}_k^\times = \mathbb{Z}_{pq} \cong \mathbb{Z}_{p-1} \oplus \mathbb{Z}_{q-1}$, and M_{pq}^a is of cycle type. Put $s = o_k(a)$, then

$$M_{pq}^a = E_p(M_q^a) \cup E_q(M_p^a) \cup \frac{(p-1)(q-1)}{s} C_s \setminus C_1.$$

Here the reason why we delete one C_1, is that $C_1 = \{0\}$ is included both in $E_p(M_q^a)$ and $E_q(M_p^a)$.

Note that we may take s as any divisors of $\varphi(pq) = (p-1)(q-1)$. Put $\bar{a}_p = a \pmod p$ and $\bar{a}_q = a \pmod q$.

Case 4-1. $s|(p-1), s \not|(q-1)$.

$$M_p^{\bar{a}_p} = C_1 \cup \frac{p-1}{s},\ M_q^{\bar{a}_q} = qC_1,\ M_{pq}^a = qC_1 \cup \frac{q(p-1)}{s} C_s.$$

Case 4-2. $s \nmid (p-1), s \mid (q-1)$.

$$M_q^{\bar{a}_q} = C_1 \cup \frac{q-1}{s},\ M_p^{\bar{a}_p} = pC_1,\ M_{pq}^{a} = pC_1 \cup \frac{p(q-1)}{s}C_s.$$

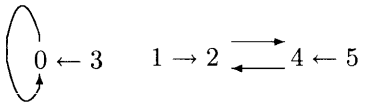
Case 4-3. $s \mid (p-1), s \mid (q-1)$.

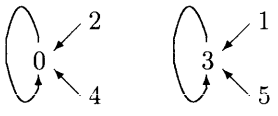
$$M_p^{\bar{a}_p} = C_1 \cup \frac{p-1}{s},\ M_q^{\bar{a}_q} = C_1 \cup \frac{q-1}{s},\ M_{pq}^{a} = C_1 \cup \frac{pq-1}{s}C_s.$$

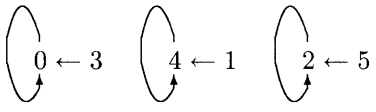
Case 4-4. $s \nmid (p-1), s \nmid (q-1)$

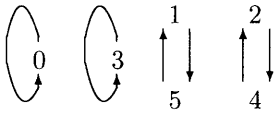
$$M_p^{\bar{a}_p} = pC_1,\ M_q^{\bar{a}_q} = qC_1\ M_{pq}^{a} = (p+q-1)C_1 \cup \frac{(p-1)(q-1)}{s}C_s.$$

Example 1. $k = 2 \cdot 3$, $a = 2, \ldots, 5$.

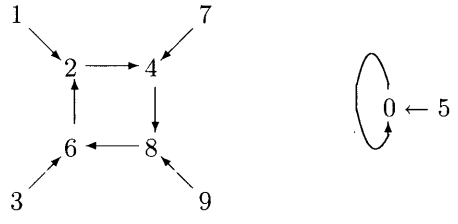
M_6^2 : 

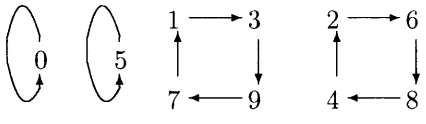
M_6^3 : 

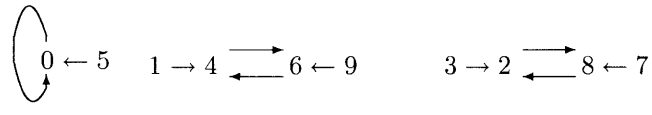
M_6^4 : 

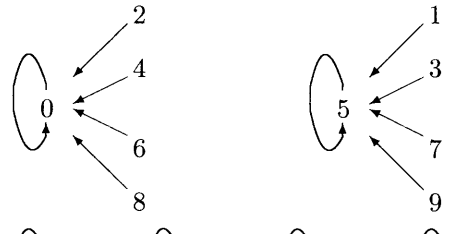
M_6^5 : 

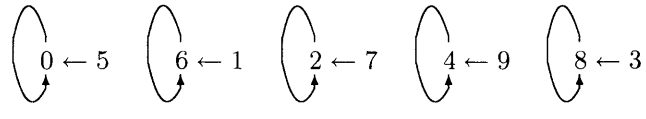
Example 2. $k = 10 = 2 \cdot 5$, $a = 2, \ldots . 9$.

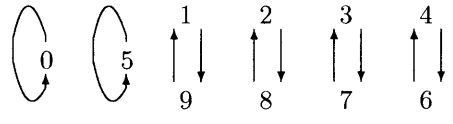
$M_{10}^2 (= (M_{10}^8)^{-1})$: 

$M_{10}^3 (= (M_{10}^7)^{-1})$: 

M_{10}^4 : 

M_{10}^5 : 

M_{10}^6 : 

M_{10}^9 : 

§5..6 Miscellaneous Cases

Here we list miscellaneous cases($k \leqq 100$), which may serve good exercises.

Case 1:$k = 2^m q$. One may take $k = 12, 20, 24, 28, 40, 44, 48, 52, 56, 68, 76, 80, 88, 92$.

Case 2:$k = p^2 q$, *p:odd prime*. One may take $k = 18, 45, 50, 63, 75, 99$.

Case 3:$k = p^2 q^2$, *p, q:prime*. $k = 36, 100$.

We list orders $o_{100}(a)$ for $a \in \mathbb{Z}_{100}^{\times}$.

a	1	3	7	9	11	13	17	19	21	23	27	29	31	33
$o(a)$	1	20	4	10	10	20	20	10	5	20	20	10	10	20

a	37	39	41	43	47	49	51	53	57	59	61	63	67
$o(a)$	20	10	5	4	20	2	2	20	4	10	5	20	20

a	69	71	73	77	79	81	83	87	89	91	93	97	99
$o(a)$	10	10	20	20	10	5	20	20	10	10	4	20	2

$\mathbb{Z}_{100}^{\times} \cong \mathbb{Z}_4^{\times} \times \mathbb{Z}_{25}^{\times} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_5$ and any divisors of $20 = 4 \cdot 5$ may occur as orders.

Case 4:$k = pqr$, *p, q, r:prime*. One may take $k = 30, 42, 66, 70, 78$.

Referennce

[1] A. Baker, A Concise Introduction to the Theory of Numbers, Cambridge Uni-versity Press (1984).

[2] Yuhihiro Kaine, *Towards Clinical Mathematics Education*, Bull. of the Fac. of Education, Mie University (Educational Science), 52 (2001), 101-105 (in Japanese).

[3] ——, *Games of Number Structures I*, Bull. of the Fac. of Education, Mie University (Educational Science), 52(2001), 107-118 (in Japanese).

[4] ——, *Dynamical Graphs and Strategy Games — Roles of Materials in Clinical Mathematics Education*, Bull. of the Fac. of Education, Mie University (Natural Science), 53 (2002), 73-83 (in Japanese).

[5] ——, *Games of Number Structures II (Reversed Di. erence)*, Bull. of the Fac. of Education, Mie University (Natural Science), 53 (2002), p.7-26.

[6] ——, *Remmendation of Clinical Mathematica Education*, Sugaku Seminar, extra number "Making Education of Mat hematics" (2002. 10. 30), 147-163 (in Japanese).

[7] ——, *Dynamical Graphs on ten Verteces, at the begining of Mathematical Association of Japan*, Journal of Mathematical Culture, vol.0, no. 1 (2002.12), p.75-94 (in Japanese).

[8] ——, *Classification of Dynamical Graphs with Vertex Number* $\leqq$ 10, Bull. of the Fac. of Education, Mie University (Natural Science), 53 (2004), p.9-43.

[9] ——, *Dynamical Graphs: A Mathematical Theory of Graphical Illustration to Arithmetics*), in prep.

[10] T. Takagi, Lectures on Elementary Number Theory, the 2nd ed., Kyoritu Publ.(1971)(in Japanese).