Structures of Elementary Dynamical Graphs

Yukihiro Kanie

Contents

§ 1. Brief Reviews of Finite Dynamical Graphs ............................................. 2
  § 1.1 Cycles and invertible DG ................................................................. 3
  § 1.2 Degrees and Size and Period Characteristic ....................................... 4
  § 1.3 Attaching ......................................................................................... 4
  § 1.4 p-nary Pseudo-tree ......................................................................... 5

§ 2. Realization of Dynamical Graphs .............................................................. 6
  § 2.1 Shifts and Extension ......................................................................... 6
  § 2.2 Elementary DG .................................................................................. 6

§ 3. Facts from Elementary Number Theory .................................................. 6
  § 3.1 The Group of Reduced Residue Classes ............................................. 6
  § 3.2 Quadratic Residues .......................................................................... 8

§ 4. Addition Graph $A_k$ ............................................................................ 8

§ 5. Multiplication Graph $M_k$ .................................................................... 9
  § 5.1 Case of $k = p$: prime ................................................................. 13
  § 5.2 Case of $k = p^m (m > 0)$ ............................................................. 15
  § 5.3 Case of $k = p^1 (p: odd prime)$ ..................................................... 17
  § 5.4 Case of $k = p^m (m > 0, p: prime)$ .............................................. 18
  § 5.5 Case of Composite Numbers $k$ ....................................................... 21
  § 5.6 Miscellaneous Cases ....................................................................... 23

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 $k \leq 10$. 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.
§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 vertex $w$ 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 $D(V)$ 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 $\varphi : V \to W$ satisfying the equality

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

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

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 $D(V)$ the set of all dynamical graphs on $V$, and by $D'(V)$ 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 $G$.

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 vertices 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 $(v)$. For any subset $U \subset V$, denote by $(U)$ the DG generated by $U$.

For a vertex $v \in V$, the set of all 'ancestors' 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 $n \geq 0$, denote by $G^{(n)}$ the subgraph $G(f|_{f^{-1}(V)}) = (f^n(V))$ 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

$$V = f^0(V) \supseteq f^1(V) \supseteq \cdots \supseteq f^h(V) = f^{h+1}(V) = \cdots$$
for some $h > 0$. Introduce the set

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

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

A DG $G$ is called connected, if $(v) \cap (w) \neq \emptyset$ 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) vertices satisfies

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

then the subgraph $(C)$ 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 $C$, $C = (v) = V^-(v)$. 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 $\mathcal{F}(C) \supseteq C$. 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 connected 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 $(v)$ 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 $O^-(v) \supseteq W$. And consider two number, the width $w(v) = \#W(v) = \deg v - 1$ and the weight $w^t(v) = \#O^-(v)$ 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

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

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

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

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

— 3 —
§1.2 Degrees and Size and Period Characteristic

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 \( D_i(G) = \{ v \in V \mid \deg(v) = i \} \), then \( D_0 = L_1 \) is the set of all leaves.

Put \( D_i(G) = \sharp D_i(G) \) and \( D(G) = (D_0, D_1, \ldots) = \sum_{i \geq 0} D_i k_i \), then there holds the degree equation:

\[
s(G) = \# E = \sum_{v \in V} \deg v = \sum_{i \geq 0} D_i = \sum_{i \geq 1} i D_i.
\]

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, \( \mathbb{D}(G) = s(G) k_1 = 1^{s(G)} \).
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 vertices \( v \), 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 \( (s(G) - c) k_0 + c k_d \), where \( cd = s(G) \).

Let \( G = G(f) \) be a finite DG, and \( c = c(G) \) be the connectivity \( c = c(G) \). Let \( \{ G^1, \ldots, G^c \} \) be the set of connected components of \( G \), \( C^i \) be the unique cycle of \( G^i (1 \leq i \leq c) \). In this situation, \( G \) is written as a disjoint sum \( G = \bigcup_{i=1}^{c} G^i \) of all connected components, and \( L_\infty(G) = \bigcup_{i=1}^{c} C^i \) is the sum of all limit cycles.

Now introduce the size characteristic \( \mathbb{S}(G) = (s^1, \ldots, s^c) \) and the period characteristic \( \mathbb{P}(G) = (p^1, \ldots, p^c) \) 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 convenience sake, we use the following notation for sets \( \mathbb{S} = \{ s_1, \ldots, s_c \} \) of \( c \) natural numbers. Let \( n_j = \# \{ s_i \mid s_i = j \} \), then write \( \mathbb{S} = \sum_{j \geq 0} n_j j = \prod_{j \geq 1} j^{n_j} \). Then we get

\[
\sum_{j=1}^{c} s_j = \sum_{j \geq 1} n_j j, \quad c = \sum_{j \geq 1} n_j.
\]

If every \( G^i (1 \leq i \leq c) \) is isomorphic to a graph \( \overline{G} \), then we use the abbreviation \( c \overline{G} \) for \( \bigcup_{i=1}^{c} G^i \). 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, \( \mathbb{S}(C_p) = k_p, \mathbb{P}(C_p) = k_p, \mathbb{D}(C_p) = pk_1 \).

§1.3 Attaching

Given a graph \( G = G(f) \in \mathbb{D}(V) \), a vertex \( v \in V \), a pseudo-tree \( T = G(t) = (U, F) \in T \) with the root \( u \in U \), then define the dynamical graph \( G(h) \in \mathbb{D}(V') \) 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
Any connected dynamical graphs can be expressed as a cycle $C$ with pseudo-trees $T_i$ attached at gates $v_i$ $(i = 1, \cdots, g)$: $G = C \lor v_1 T_1 \cdots v_g T_g$. Then the size of $G$ is given as
\[
s(G) = p(G) + \sum_{i=1}^{g} \text{wt}(T_i).
\]
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 $L_w$ with linear pseudo-trees $L_{w_i}$ attached at branch points $v_i$ $(i = 1, \cdots, b(T))$: $T = (\cdots(L_{w_0} \lor v_i L_{w_i}) \cdots) \lor v_g L_{w_g}$. Then $s(T) = 1 + \sum_{i=0}^{b} w_i$.

In particular, $L_0 = K_0 = C_1$, and attaching $L_0$ does not change any graph: $G \lor v L_0 = G$ for any $v \in V$.

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

1.4 $p$-nary Pseudo-tree

Fix $(p, \ell) (p > 1, \ell > 0)$, we define $p$-nary pseudo-trees $B^\ell_p$ inductively on $\ell$ as follows: At first let $B^0_p = L_0$, and put
\[
B^{\ell+1}_p = L_0 \lor 0 p(L_1 \lor 1 B^\ell_p).
\]
Then $B^\ell_p$ is a pseudo-tree of height $\ell$, $\#L_1(B^\ell_p) = p^\ell$ (the number of leaves), and
\[
s(B^\ell_p) = \sum_{i=1}^{\ell} p^i = \frac{p^{\ell+1} - 1}{p - 1}, \quad \text{wt}(B^\ell_p) = \frac{p^\ell - 1}{p - 1}, \quad \mathcal{D}_0(B^\ell_p) = p^\ell k_0 + \frac{p^\ell - 1}{p - 1} k_p.
\]
In fact, we can verify inductively
\[
\text{wt}(B^{\ell+1}_p) = p \left( 1 + \frac{p^\ell - 1}{p - 1} \right) = \frac{p^{\ell+1} - 1}{p - 1}.
\]
$B^1_p$ is a linear pseudo-tree $L_\ell$ of weight $\ell$, and $B^1_p$ is called a binary pseudo-tree of height $\ell$.

The multiplication graph $M^p_2$ is expressed as $L_1 \lor 1 B^1_p$, and in general the multiplication graph $M^p_\ell$ is expressed as $L_0 \lor 0 (p - 1)(L_1 \lor 1 B^{\ell-1}_p)$. Its size can be computed as
\[
s(M^p_\ell) = 1 + \text{wt}(M^p_\ell) = 1 + (p - 1)(1 + \frac{p^\ell - 1}{p - 1} - 1) = p^k.
\]

2. Realization of Dynamical Graphs

For explicit realizations of dynamical graphs, fix the size $k$, and take the $k$-skelton of $N$ :
\[
I_k = \left\{ i \in \mathbb{N} \mid 0 \leq i < k \right\} = \left\{ 0, 1, 2, \ldots, k - 1 \right\} \quad (k : \text{finite})
\]
\[
I_k = \left\{ i \in \mathbb{N} \mid 0 \leq i \right\} \quad (k = \infty)
\]
as a set of vertices. 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 $\mathcal{D}_k$ and $\mathcal{D}'_k$ by $\mathcal{D}(I_k)$ and $\mathcal{D}'(I_k)$ respectively. We know easily that $\#\mathcal{D}_k = k^k$, $\#\mathcal{D}'_k = k!$ and $\#\mathcal{D}'_k = p(k)$, where $p(k)$ is the partition number of $k$. By [8], we know the number $\delta_k = \#\mathcal{D}_k$ as follows.

<table>
<thead>
<tr>
<th>$k$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\delta_k$</td>
<td>1</td>
<td>3</td>
<td>7</td>
<td>18</td>
<td>46</td>
<td>130</td>
<td>343</td>
<td>951</td>
<td>2615</td>
<td>7207</td>
</tr>
</tbody>
</table>
Thus there are so many different nonisomorphic DG's, even if the number of vertices is small as 10. For an educational purpose, we want to clarify the structures of DG's at least with the size \( \leq 100 \), then we must restrict ourselves to small groups of DG's such as elementary dynamical graphs (EDG).

### §2.1 Shifts and 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 \( \varphi(i) = \bar{i} + b \). If \( \varphi f = f \varphi \), then the \( \varphi \)-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 \( T_b G' \) is a DSG of \( G \). And if \( G' \) is a connected component or a cycle of \( G \), then \( T_b G' \) is also a connected component or a cycle respectively.

For an integer \( b > 0 \), define the injection \( p : I_k \to I_{bk} \) defined by \( p(i) = \bar{i} \). Then we denote the \( p \)-transfer operation \( p * G \) on the subset \( \{ bi \mid i \in I_k \} \) of \( I_{bk} \) by \( E_c G \), 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, \( (x^2)_2 = (x)_2, (x^3)_3 = (x)_3 \), \( (x^4)_4 = (x^2)_4, (x^5)_5 = (x)_5, (x^3)_6 = (x)_6, (x^7)_7 = (x)_7 \), \( (x^8)_8 = (x^4)_8 \), \( (x^9)_9 = (x^3)_9 \), \( (x^{10})_10 = (x)_{10} \).

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 \( S(K_k^a) = k_k \), \( P(K_k^a) = k_1 \), \( D(K_k^a) = (k - 1)k_0 + k_k \).

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, \( S(A_k^a) = \mathbb{P}(A_k^a) = k_k \), \( D(A_k^a) = k_1k_1 \). In particular, \( S(K_k^a) = \mathbb{P}(K_k^a) = D(K_k^a) = 1_k = k_1 \).

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, \( (a, k) = 1 \).

\( A_k^0 = M_k^1 = kK_k^1 \) is the identity graph w.r.t. the pointwise product in \( D_k \).

### §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, \( nx = 0 \pmod{k} \).
(Here, the same statement holds, even if $x$ is an integer. So we sometimes use the notation $x$ for the set $\mathbb{Z}/k\mathbb{Z}$ of congruence classes modulo $k$.) It is well-known that $\alpha_k(x) = k/d$, where $d$ is the greatest common divisor $d = (x, k)$ of $x$ and $k$, and $\{ix | 0 \leq i < k\} = \{ix | 0 \leq i < k/d\}$. In particular, if $(x, k) = 1$, then $\{ix | 0 \leq i < k\} = \mathbb{Z}/k\mathbb{Z}$. The additive subgroup $\langle x \rangle$ generated by $x$ coincides with the set $\{ix | 0 \leq i < k/d\}$.

In this note, we will use the notation $K$ for the set $\{x | (x, k) = 1, 0 < x < k\}$. $K$ 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 $K$ is also obtained as the set of units (invertible elements) of the ring $\mathbb{Z}/k\mathbb{Z}$. For an element $a \in K$, define the multiplicative order $\omega_k(a)$ of $a$ as the minimal positive integer $n$ such that $a^n \equiv 1 \pmod{k}$. In other words, $\omega_k(a) = \#(a)$ as multiplicative subgroups. If $K = \langle a \rangle$, then $a$ is a generator and is called a primitive root modulo $k$.

Define the Euler’s function $\varphi(k)$ by $\varphi(k) = \#K$. By Lagrange’s theorem, $\omega_k(a)$ 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 $(\mathbb{Z}/p^n\mathbb{Z})^\times \cong \mathbb{Z}_{p-1} \oplus \mathbb{Z}_{p-1} \oplus \cdots \oplus \mathbb{Z}_{p-1}$. Here consider a multiplication group on the left hand side, and an additive group on the right hand side.

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

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

(5) (Euler’s Theorem) If $(a, n) = 1$ (that is, $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$), 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

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

**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 $(\mathbb{Z}/p_1^{e_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{e_2}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/q_l^{e_l}\mathbb{Z})^\times$. 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 $\omega_k(a)$ 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, there 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 $M_1^t \cong pC_1$. Let $t > 0$. If $d = (t, p-1)$, then $o_a(p) = (p-1)/d$ and $M_n^t \cong C_1 \cup dC_{(p-1)/d}$. 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

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

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's 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)

\[
\left( \frac{-1}{p} \right) = (-1)^{(p-1)/2}, \quad \left( \frac{2}{p} \right) = (-1)^{(p^2-1)/8}
\]

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 \( A_k^{-a} \). As for isomorphism classes, it is necessary to consider \( A_k^a \) with \( a (1 \leq a \leq \frac{k}{2}) \), since \( A_k^{a+k} = A_k^a \) and \( A_k^a = kK_k^a \). More precisely,

**Theorem 4** Let \( k > 0 \). For any \( a (0 \leq a < k) \), \( A_k^a \) is of cycle type, and \( \mathbb{S}(A_k^a) = \mathbb{P}(A_k^a) \) and \( \mathbb{D}(A_k^a) = 1^k = k k_1 \). In particular, there are no leaves: \( L_1(A_k^a) = \emptyset \).

1. If \( (a, k) = 1 \), then \( A_k^a \) is a cycle of period \( k \). \( A_k^a \cong C_k \). \( \mathbb{P}(A_k^a) = k k_1 \).
2. If \( (a, k) = d > 1 \), then \( A_k^a = \bigcup_{i=0}^{d-1} T_i(E_d(A_k^a)) \cong dE_d(A_k^a) \cong dC_{dk'}, \) where \( k' = k/d \). \( \mathbb{P}(A_k^a) = dk k' \).

There are distinct \( \delta \) 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 characteristic, that is \( \mathbb{P}(G) = c k_p \) for some \( c, p > 0 \), can be realized as an addition DG, for example, \( \mathbb{P}(A_{cp}^c) = c k_p \).

**Proof.** (1) By elementary number theory, \( \# \{ i a \mid 0 \leq i < k \} = k \).

(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...
§5. Multiplication Graph \( M_k^a \)

Fix an integer \( k > 0 \). In this section, we consider multiplication 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. \( M_k^a = M_k^{\alpha + k} \), for any integer \( \alpha \).
2. If \( (a, k) = 1 \), then \( M_k^a \) is of cycle type. \( \mathcal{S}(M_k^a) = \mathcal{P}(M_k^a), \mathcal{D}(M_k^a) = k \cdot k_1. \)

In the following, assume that \( (a, k) = d > 1 \). Put \( k' = k/d \).
3. \( M_k^a \) is not of cycle type, and the connected component \( \mathcal{F}(0) \) is a pseudo-tree \( T \) of a positive height \( h \). \( M_k^a \) is isomorphic to \( \tilde{C}(M_k^a) \) attached at all vertices by \( T \):

\[
M_k^a \cong \tilde{C}(M_k^a) \cup_{v \in \tilde{C}} T.
\]

In particular, the width and weight of all vertices \( v \) of \( \tilde{C} \) are given as

- \( w(v) = w(0) = d - 1 \),
- \( \text{wt}(v) = \text{wt}(0) \).

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

\[
O^-(v) = \{ w + f^n(v) \mid w \in T, n = \text{ht}(w) \},
\]

where \( f^n(v) \) is the \( n \)-th cyclic past of \( v \).

5. The degrees of all vertices \( v \notin \mathcal{L}_1(M_k^a) \) are the same: \( \deg(0) = d \). Moreover, \( D_d = k' \).
6. The set \( \mathcal{L}_1(M_k^a) \) of all leaves is \( \{ w \in I_k \mid f^w \} \), and so its cardinality is \( k - k' \). Hence \( \mathcal{D}(M_k^a) = (k - k') \cdot k_0 + k' \cdot k_d \).

**Proof.** (1) and (2) is obvious. (4) implies immediately (3). (3) Since \( n = \text{ht}(w), f^n(w) = a^n w \equiv 0 \) (mod \( k \)) and \( v = f^n(f^n(v)) = a^n f^n(v) \), therewith \( f^n(w + f^n(v)) = a^n(w + f^n(v)) \equiv 0 + v = v \) (mod \( k \)). Since \( f(w) \in T \) and \( \text{ht}(f(w)) = n - 1, w + f^n(v) \rightarrow f(w) + f^{n+1}(v) \in O^-(v) \).
(5) implies (6). (5) $v \to 0 \iff av \equiv 0 \pmod{k} \iff dv \equiv 0 \pmod{k}$, since $a = a'd$, $(a',k) = 1$. Put $k' = k/d$. For every $i \ (0 \leq i < d-1)$, $0 \leq ik' < k$ and $ik' - a ik' = a'dk' = a'ik = 0$. Hence deg(0) $\geq d$.

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 $v \geq d$.

On the other hand, $k - k/a \geq 0$. For every $i \ (0 \leq i < k-1)$, $0 \leq ik < k$ and $ik - a ik = a'ik = 0$. Hence deg(0) $\geq d$.

Now we will show the special cases of MDG.

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

Pseudo-tree of height 1. $P = k_1$, $D = (k-1)k_0 + k_k$

(2) Two special cases of cyclic type:

(2-1) $M_k^a = kK_0^a \cong kC_1$:

(2-2) $M_k^{a+k-1}$:

\[ M_k^{a+k-1} = \begin{cases} C_1 \cup \frac{k-1}{2}C_2 & (k : odd) \\ 2C_1 \cup \left(\frac{k}{2} - 1\right)C_2 & (k : even) \end{cases} \]

$P(M_k^{a+k-1}) = \begin{cases} k_1 + \frac{k-1}{2}k_2 & (k : odd) \\ 2k_1 + \left(\frac{k}{2} - 1\right)k_2 & (k : even) \end{cases}$

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

(3-1) If $c = a$, then $d = a$, $k' = a^{n-1}$, $M_{c^n}^a$ is a pseudo-tree of height $n$, and $M_{c^n}^a \cong L_0 \lor (a-1)(L_1 \lor (B_{c^n}^{a+1}))$. $D(M_{c^n}^a) = a^{n-1}(a-1)k_0 + a^{n-1}k_a$.

\[ \mathcal{L}_j(M_{c^n}^a) = \begin{cases} \{i \in I_{c^n} | a^{j-1}i, a^j i \} & (1 \leq j \leq n) \\ \{0\} & (j = \infty) \end{cases} \]

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

(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 $\mathbb{Z}_k^\times = \mathbb{Z} \setminus \{0\}$ and $\varphi(p) = p - 1$. The coset decomposition by $\langle a \rangle$ gives a connected component decomposition of the MDG $M_k^a$.

(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) $a^n v \equiv 0 \pmod{c^d}$ for any $v \in I_k$. Assume $(b,c) = 1$. Consider the reduction scheme:

\[ M_{c^n}^a \implies M_{c^n}^{a+1} \implies \cdots \implies M_{c^n}^{a/k} \implies M_c^a = M_c^b = K_c^0 \]
$M_c^a$ is obtained from $E_c(M_c^a)$ by attaching $K_c^0$ at each leaves of $E_c(M_c^0)$. In fact, $(b,c) = 1$, hence $b \in \mathbb{Z}_c^*$ 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 $cv (1 \leq v < c)$ of $E_c(M_c^0)$, take vertices $\{w + ci \mid 0 \leq i < c\}$, then
\[
 w + ci \rightarrow a(w + ci) \equiv bc(xv + ci) = cvbx + (cb)ci = cv(1 - yc) + c^2bi
\]
and the number of these new vertices is $(c - 1)c = c^2 - c$, so no other vertices remain in $M_c^a$.

By induction on $n$, we will show $M_c^a \cong L_0 \vee_0 (c - 1)(L_1 \vee_1 B_c^{n-1})$. Assume $M_c^{a-1} \cong L_0 \vee_0 (c - 1)(L_1 \vee_1 B_c^{n-2})$. As for the case $n = 2$, $L_1(E_c(M_c^{a-1})) = \{cv \mid 1 \leq v < c\}$. Consider the set $\{w + ci \mid 0 \leq i < c\}$, 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 $cv$ determined also as modulo $c^a$.

**Examples for (3-2).**

1. $M_{16}^6$, $c = 2, n = 4, a = 6, (c^n, a) = c$. $D(M_{16}^6) = 8k_0 + 8k_2$, $L_1 = \mathcal{D}_0 = \{v \mid (v, 2) = 1\}$, $L_2 = \{v \mid 2v, 4 \mid v\}$, $L_3 = \{v \mid 4v, 8 \mid v\}$, $L_4 = \{v \mid 8v, 16 \mid v\} = \{8\}$, $L_\infty = \{0\}$.

   \[\begin{array}{cccc}
   & & 6 & \\
   & 4 & 14 & \\
   0 & 9 & 13 & \\
   12 & 2 & 11 & \\
   & 10 & 7 & \\
   8 & & & \\
   \end{array}\]

2. $M_{36}^6$, $c = 6, n = 2, a = 12, (c^n, a) = a = 2c$. $D(M_{36}^6) = 33k_0 + 3k_2$, $L_1 = \mathcal{D}_0 = I_{36} \setminus \mathcal{L}_\infty$, $\mathcal{L}_\infty = \{0\}$, $\mathcal{D}_1 = \{0, 12, 24\}$.
   $W(0) = \{3v \mid 1 \leq v < 12\} \subset E_3(M_{12}^0)$, $O^{-}(12) = \{3v + 1 \mid 0 \leq v < 12\} = 1 + E_3(M_{12}^0)$, $O^{-}(24) = \{3v + 2 \mid 0 \leq v < 12\} = 2 + E_3(M_{12}^0)$.

**Remark 1.** By Theorem 5 (6), if $(k, a) = (k, b)$, then the degree characteristic coincide: $D(M_k^a) = D(M_k^b)$, but they are not necessarily isomorphic with each other. For example, $M_{12}^9 \not\cong M_{12}^3$, since $P(M_{12}^9) = 2k_1 + k_2$, $P(M_{12}^3) = 4k_1$.

M_{12}^3: \[\begin{array}{cccc}
   & & 4 & \\
   & 6 & 10 & \\
   0 & 2 & 9 & \\
   8 & & & \\
   \end{array}\]

M_{12}^9: \[\begin{array}{cccc}
   & & 4 & \\
   & 3 & 11 & \\
   0 & 7 & 10 & \\
   8 & & & \\
   \end{array}\]

**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 $(\mathbb{Z}/p^2\mathbb{Z})^\times$ for some primes $p$. 

---

---
$e > 0$. 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 $\mathbb{P}(M^a_p) = k_0 + k_{p-1}$ is equivalent with that $a$ is a generator of $(Z/pZ)^\times$.

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

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

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

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

For example, consider $M^2_{15}$, and the reduction scheme

$$
\begin{align*}
M^2_{15} & \Rightarrow M^2_5 \\
\downarrow & \downarrow \\
M^2_3 & \Rightarrow M^2 = M^0_1 = C_1
\end{align*}
$$

$M^2_{15}$ is of cycle type. $\mathcal{F}(0)$ comes from $M^2_2$ as $E_{15}(M^2_1)$. $\mathcal{F}(3)$ comes from $M^2_3$ as $E_3(\mathcal{F}(1; M^2_2))$ and $\mathcal{F}(5)$ comes from $M^2_5$ as $E_5(\mathcal{F}(1; M^2_2))$. 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 $\mathcal{F}(0; M^a_k)$ and periodic structures of $M^a_k$ can be detected through the reduction scheme

$$
M^a_k \Rightarrow M^a_{k/d} \Rightarrow \cdots \Rightarrow M^a_{k_1} \Rightarrow M^a_{k_1/d_1} \Rightarrow \cdots \Rightarrow M^a_{k_1}
$$

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

$$
M^a_{k_1} \Rightarrow M^a_{k_1/k_t} \Rightarrow \cdots \Rightarrow M^a_{k_1/k_t} \Rightarrow M^a_{k_1/k_t d_1} \Rightarrow \cdots \Rightarrow M^a_1 = M^0_1
$$

and the periodic structure $M^a_k$ is same as $M^a_{k_t}$.

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

\[
M_{420}^6 \Rightarrow M_{70}^6 \Rightarrow M_{35}^6, \quad M_{12}^6 \Rightarrow M_2^6 \Rightarrow M_1^6 = M_1^0
\]

The periodic structures of \( M_{35}^6 \) can be detected through the reduction scheme:

\[
M_{35}^6 \quad \Rightarrow \quad M_5^6 = M_5^1
\]

\[
\downarrow \quad \downarrow
\]

\[
M_2^6 \quad \Rightarrow \quad M_1^6 = M_1^0 = C_1
\]

Five \( C_1 \)'s arise as \( E_7(M_5^6) \). One \( C_1 = \mathcal{F}(0; M_{35}^6) \) comes also as \( E_7(\mathcal{F}(0; M_5^6)) = E_5(\mathcal{F}(0; M_5^6)) \). Three \( C_3 \)'s arise as \( E_5(M_5^6 \setminus \{0\}) \). 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. \( M_p^0 \) is the constant graph \( K_p^0 \cong B_p^1 \) (\( p \)-nary pseudo-tree of height 1). For \( a \in (\mathbb{Z}/p\mathbb{Z})^* \), \( M_p^a \) is of cycle type. From the remark after Theorem 1,

\[
M_p^a \cong \begin{cases} 
K_p^0 & (a = 0) \\
pC_1 & (a = 1) \\
C_1 \cup tC_s & (a > 1, s = o_p(a), t = (p - 1)/s)
\end{cases}
\]

The values of \( s(a) \) may run thrown the set of all divisors of \( p - 1 = \varphi(p) = |(\mathbb{Z}/p\mathbb{Z})^*| \). Hence the number \( m(p) \) of the isomorphism classes among \( M_p^a \) 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 \( \langle a \rangle = (\mathbb{Z}/p\mathbb{Z})^* \).

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

<table>
<thead>
<tr>
<th>( p )</th>
<th>2</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
<th>23</th>
<th>29</th>
</tr>
</thead>
<tbody>
<tr>
<td>( p - 1 )</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>10</td>
<td>12</td>
<td>16</td>
<td>18</td>
<td>22</td>
<td>28</td>
</tr>
<tr>
<td>( s )</td>
<td>1</td>
<td>1, 2, 3, 6</td>
<td>1, 2</td>
<td>1, 2, 3, 4, 6, 12</td>
<td>1, 2, 4, 8, 16</td>
<td>1, 2, 3, 4, 6, 9, 18, 22, 28</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( m(p) )</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>7</td>
<td>6</td>
<td>7</td>
<td>4</td>
<td>7</td>
<td>14</td>
</tr>
</tbody>
</table>
### Proposition 3

1. The number of cycle 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 exists a number $n \geq 1$ 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 $s = o_{ns+1}(a)$.

\[ \text{qed.} \]

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

<table>
<thead>
<tr>
<th>$s$</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>17</th>
<th>18</th>
</tr>
</thead>
<tbody>
<tr>
<td>$p(s)$</td>
<td>3</td>
<td>7</td>
<td>10</td>
<td>13</td>
<td>17</td>
<td>19</td>
<td>23</td>
<td>29</td>
<td>31</td>
<td>37</td>
<td>41</td>
<td>43</td>
<td>47</td>
<td>53</td>
<td>59</td>
<td>61</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$s$</th>
<th>19</th>
<th>20</th>
<th>21</th>
<th>22</th>
<th>23</th>
<th>24</th>
<th>25</th>
<th>26</th>
<th>27</th>
<th>28</th>
<th>29</th>
<th>30</th>
<th>31</th>
<th>32</th>
<th>33</th>
</tr>
</thead>
<tbody>
<tr>
<td>$p(s)$</td>
<td>191</td>
<td>41</td>
<td>43</td>
<td>23</td>
<td>47</td>
<td>97</td>
<td>101</td>
<td>79</td>
<td>109</td>
<td>29</td>
<td>59</td>
<td>31</td>
<td>311</td>
<td>97</td>
<td>67</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$s$</th>
<th>34</th>
<th>35</th>
<th>36</th>
<th>37</th>
<th>38</th>
<th>39</th>
<th>40</th>
<th>41</th>
<th>42</th>
<th>43</th>
<th>44</th>
<th>45</th>
<th>46</th>
<th>47</th>
<th>48</th>
</tr>
</thead>
<tbody>
<tr>
<td>$p(s)$</td>
<td>103</td>
<td>71</td>
<td>73</td>
<td>149</td>
<td>191</td>
<td>79</td>
<td>41</td>
<td>83</td>
<td>43</td>
<td>173</td>
<td>89</td>
<td>181</td>
<td>47</td>
<td>283</td>
<td>97</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$s$</th>
<th>49</th>
<th>50</th>
<th>51</th>
<th>52</th>
<th>53</th>
<th>54</th>
<th>55</th>
<th>56</th>
<th>57</th>
<th>58</th>
<th>59</th>
<th>60</th>
<th>61</th>
</tr>
</thead>
<tbody>
<tr>
<td>$p(s)$</td>
<td>197</td>
<td>101</td>
<td>103</td>
<td>53</td>
<td>106</td>
<td>109</td>
<td>331</td>
<td>113</td>
<td>229</td>
<td>59</td>
<td>709</td>
<td>61</td>
<td>367</td>
</tr>
</tbody>
</table>
§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 \( M_{2^m}^a \) is of cycle type in the case \( a \equiv 0 \pmod{2} \), is a pseudo-tree otherwise (\( a \equiv 0 \pmod{2} \)).

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

\[
M_{2^m}^a \Rightarrow M_{2^{m-nq}}^a \Rightarrow \cdots \Rightarrow M_{2^{m-nq}}^a = M_{2^r}^a = K_{2^r}^0,
\]

and \( M_{2^m}^a \) is a pseudo-tree. In this case, we get

\[
M_{2^{m+r}}^a \cong \begin{cases} 
L_0 \cup_0 \left( (2^r-1)(L_1 \cup_0 B_{2^q-1}^n) \right) & (r = 0) \\
L_0 \cup_0 \left( \left( (2^r-2^i)(L_1 \cup_0 B_{2^q-1}^n) \right) \cup \left( 2^r-1 \right) \cup_0 \left( L_1 \cup_0 B_{2^q-1}^n \right) \right) & (r > 0)
\end{cases}
\]

Proof. Factor \( a \) as \( a = 2^b k \), where \( (b, 2) = 1 \). Then \( 1 \leq b < 2^a \). Consider the reduction \( M_{2^{m+r}}^a \Rightarrow M_{2^r}^0 \) and the subgraph \( G' = E_{2^r}(M_{2^r}^0) \) of \( M_{2^{m+r}}^a \). We get the set \( V(G') = \{ 2^i | 0 \leq i \leq 2^r-1 \} \) of vertices of \( G' \), the set \( \mathcal{L}(G' ; 1) = \{ 2^i | 1 \leq i \leq 2^r-1 \} \) of leaves of \( G' \) and the limit cycle \( \mathcal{L}(G' ; \infty) = \{ 0 \} \).

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

\[
M_{2^{m+r}}^a \cong L_0 \cup_0 \left( \left( (2^r-2^r)(L_1 \cup_0 B_{2^q-1}^n) \right) \cup \left( 2^r-1 \right) \cup_0 \left( L_1 \cup_0 B_{2^q-1}^n \right) \right).
\]

The set of leaves of \( G' \)

\[
\mathcal{L}(M_{2^{m+r}}^a ; 1) = \left( (2^r-1)2^r + (2^r-2^r) = 2^{r+r} - 2^r \right).
\]

Next, consider the reduction \( M_{2^{m+r}}^a \Rightarrow M_{2^{m+r}}^a \) and the subgraph \( G'' = E_{2^r}(M_{2^{m+r}}^a) \), then

\[
\mathcal{L}(G'' ; 1) = \left( \{ 2^r(3+j+2^r h) | 1 \leq j \leq 2^r-1 \}, 0 \leq h \leq 2^r-1 \} \right.
\]

is the set of leaves of \( G'' \).
For every point \( v \in \mathcal{L}(G'; 1) \), there is a vertex \( w \in M_{2q+1}^a \) such that \( v = \overline{aw} = 2^b w \), and as before \( w + 2^b h \to v, v \lor v 2^b L_1 \subset M_{2q+1}^a \). Hence we get

\[
M_{2q+1}^a \cong L_0 \lor_0 ((2^{2q} - 2^r)(L_1 \lor_1 B_{2^q}^1) \cup (2^r - 1)(L_1 \lor_1 B_{2^q}^2)).
\]

It is similarly proved for higher \( m \).

\[\text{qed.}\]

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

\[
M_{2m}^a \cong C_1 \cup \bigcup_{i=1}^{m} \frac{2^{i-1}}{s_i} C_{s_i}.
\]

Here \( s_i \) is a power of 2, since \( \varphi(2^i) = 2^{i-1} \). Periods of any cycles in \( M_{2m}^a \) are of the form \( 2^a (0 \leq a \leq m - 1) \).

Note the sequence of orders satisfy the condition \( s_i = s_{i-1} \) or \( 2s_{i-1} \).

**Example.** \( m = 4 \). We list all MDG \( M_{2^4}^a \) of cycle type:

<table>
<thead>
<tr>
<th>( a )</th>
<th>( a(a) )</th>
<th>( s(a) )</th>
<th>( M_{16}^a )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(1, 1, 1, 1)</td>
<td>(1, 1, 1, 1)</td>
<td>16C_1</td>
</tr>
<tr>
<td>3</td>
<td>(3, 3, 3, 1)</td>
<td>(4, 2, 2, 1)</td>
<td>2C_1 \cup 3C_2 \cup 2C_4</td>
</tr>
<tr>
<td>5</td>
<td>(5, 5, 1, 1)</td>
<td>(4, 2, 1, 1)</td>
<td>4C_1 \cup 2C_2 \cup 2C_4</td>
</tr>
<tr>
<td>7</td>
<td>(7, 7, 3, 1)</td>
<td>(2, 2, 2, 1)</td>
<td>2C_1 \cup 7C_2</td>
</tr>
<tr>
<td>9</td>
<td>(9, 1, 1, 1)</td>
<td>(2, 2, 1, 1)</td>
<td>2C_1 \cup 7C_2</td>
</tr>
<tr>
<td>11</td>
<td>(11, 3, 3, 1)</td>
<td>(4, 2, 2, 1)</td>
<td>2C_1 \cup 3C_2 \cup 2C_4</td>
</tr>
<tr>
<td>13</td>
<td>(13, 5, 1, 1)</td>
<td>(4, 2, 1, 1)</td>
<td>4C_1 \cup 2C_2 \cup 2C_4</td>
</tr>
<tr>
<td>15</td>
<td>(15, 7, 3, 1)</td>
<td>(2, 2, 2, 1)</td>
<td>2C_1 \cup 7C_2</td>
</tr>
</tbody>
</table>

\( M_{16}^{3^*} \) : \( \{0, 8\} \) are fixed points.

\[
1 \to 3 \quad 5 \to 15 \quad 2 \quad 4 \quad 14
\]

\( M_{16}^{5^*} \) : \( \{0, 4, 8, 12\} \) are fixed points.

\[
1 \to 5 \quad 3 \to 15 \quad 2 \quad 6
\]

\( M_{16}^{7^*} \) : \( \{0\} \) is a fixed point.

\[
10 \to 0 \quad 8 \to 9 \quad 11 \quad 13 \quad 15
\]
§5.3 Case of $k = p^2$ ($p$: odd prime)

Let $K = (\mathbb{Z}/p^2\mathbb{Z})^\times$ and $\hat{K} = (\mathbb{Z}/p\mathbb{Z})^\times$. 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 $\bar{a} \in \hat{K}$. Put $s = o_K(a) = \bar{s}$ or $ps$.

In fact, if $a^s \equiv 1 \pmod{p^2}$, then there exist positive integers $q, r$ and $\bar{a} \in \hat{K}$ 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 $s = s/p$ devides $p - 1$. In fact, $\bar{a}^p - 1 \equiv 1 \pmod{p}$ by the little theorem of Fermat (Theorem 1 (5)). So

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

Thus

$$M_{p^2}^a \equiv \begin{cases} K_{p^2}^0 & (a = 0) \\ L_0 \vee \langle p-1 \rangle B_p^1 & (p|a) \\ p^2C_1 & (a = 1) \\ pC_1 \cup \langle p-1 \rangle C_p & (a \in \mathbb{Z}_{p^2}^\times \text{ and } o(a) = p) \\ C_1 \cup tC_s & (a \in \mathbb{Z}_{p^2}^\times \text{ and } s = o(a) < p, t = (p^2 - 1)/s) \\ C_1 \cup tC_{s/p} \cup tC_s & (a \in \mathbb{Z}_{p^2}^\times \text{ and } s = o(a) > p, t = p(p - 1)/s) \\ \end{cases}$$

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

$$a^p = (kp + 1)^p \equiv pC_1 \cdot kp + C_0 \cdot 1 \equiv 1 \pmod{p^2}.$$  

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

$$M_{p^2}^a = C_1 \cup \frac{p - 1}{2} C_2 \cup \frac{p^2 - p}{2} C_2 = C_1 \cup \frac{p^2 - 1}{2} C_2.$$  

Any divisors of $\varphi(p^2) = p(p - 1)$ can be periods of cycles of some $M_{p^2}^a (0 < a < p^2)$. The number $m(p^2)$ of the isomorphism classes among $M_{p^2}^a$ 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 $M_{p^2}^a (0 < a < p^2)$:

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

From this list, we know the case where the values $k$ for which cycles of period $s$ appear in MDG $M_k^a$ are lower than $p(s)$ in the subsection §7.1. For example, a cycle of period 6, 20 or 55 appears in $M_9^2$, $M_{23}^2$, or $M_{121}^2$, respectively.
§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 $M^a_{p^m}$ 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

$$M^a_{p^m} \Rightarrow M^a_{p^{m-q}} \Rightarrow \cdots \Rightarrow M^a_{p^{m-nq}} = M^a_{p^{r+q}} \equiv K_0^0,$$

and $M^a_{p^{r+q}}$ is a pseudo-tree. In this case, we get

$$M^a_{p^{r+q}} \equiv \begin{cases} L_0 \cup_0 (p^q - 1)(L_1 \cup_1 B_{p^r}^{n-1}) & (r = 0) \\ L_0 \cup_0 ((2^q - 2)(L_1 \cup_1 B_{p^r}^{n-1}) \cup (2^q - 1)(L_1 \cup_1 B_{p^r}^{n-1})) & (r > 0) \end{cases}$$

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

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,

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

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

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

the pseudo-tree $p^q L_1 = (B_{p^q}^1)$ 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 $\{p^q k \mid 1 \leq k \leq p^q - 1\}$, since $p^q b \cdot p^q k = p^{q+r}bk \equiv 0 \pmod{p^{q+r}}$, that is, $p^q k \rightarrow 0$. However $\{p^q k' \mid 1 \leq k' \leq p^q - 1\} \subset L(G'; \infty)$. Let $p^q k = p^q k'$, then
$k = p^a r k' \leq p^a - 1$, so $k' \leq p^r - \frac{1}{p^a r}$, that is, $k' \leq p^r - 1$. Thus $(p^a - p^r)L_1$ is newly attached at $\{0\}$, hence

$$M_{p^a+r}^{s+r} \cong L_0 \cup (p^a - p^r)(L_1 \cup (p^r - 1)(L_1 \cup B_{p^r}^1)),$$

and $|L(M_{p^a+r}^{s+r}:1)| = (p^r - 1)2^a + (p^a - p^r) = p^{a+r} - p^r$.

Next consider the reduction $M_{p^a+r}^{s+r} \rightarrow M_{pr}^{s+r}$ and the subgraph $G'' = E_{p^r}(M_{pr}^{s+r})$, then

$$L(G'';1) = \{p^h(j + 2^r h) \mid 1 \leq j \leq p^r - 1, 0 \leq h \leq p^a - 1\}$$

$$\cup \{\{p^{r+k}k \mid 1 \leq k \leq p^a - 1\} \setminus \{p^{2k}k' \mid 1 \leq k' \leq p^r - 1\}\}$$

is the set of leaves of $G''$.

For every point $v \in L(G'';1)$, there is a vertex $w \in M_{p^a+r}^{s+r}$ such that $v = \overline{vw} = \overline{prw}$ ($w \rightarrow v$), and as before $w + p^r h \rightarrow v$, $v \vee v p^r L_1 \subset M_{p^a+r}^{s+r}$. Hence we get

$$M_{p^a+r}^{s+r} \cong L_0 \cup (p^a - p^r)(L_1 \cup B_{p^r}^1) \cup (p^r - 1)(L_1 \cup B_{p^r}^2).$$

It is similarly proved for higher $m$.

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

(1) $a_i = a \pmod{p^i}$ in $(\mathbb{Z}/p^m\mathbb{Z})^*$.

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

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

\textbf{Proof.} (1) For $a \in (\mathbb{Z}/p^m\mathbb{Z})^*$, put $\tilde{a} = a \pmod{p^{i-1}}$ and $s = o_{p-1}(\tilde{a})$, then there are $e, f \in \mathbb{Z}$ such that

$$\tilde{a}^s = 1 + e \cdot p^{i-1}, a = \tilde{a}1 + f \cdot p^{i-1},$$

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

(2) It is sufficient to show $a_{i+1}^s \equiv 1 \pmod{p^{i+1}}$. We use notations $a = a_i, \tilde{a} = a_{i-1}$ as in the proof of (1), then $a_{i-1}^s \equiv 1, a_i^s \equiv 1 \pmod{p^i}$ and $\tilde{a}^s \equiv 1 \pmod{p^{i-1}}$. Hence $a^s = (\tilde{a}1 + f \cdot p^{i-1})^s \equiv \tilde{a}^s + fsp^{i-1} \equiv 1 + hp^{i-1}$ (mod $p^i$). 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 $a_{i+1}^s = (a + h'p^i)^s = ((a + h'p^i)p)^s = (a^s)^p = 1 + h'p^i + hp^{i+1}) \equiv 1 + hp^i \equiv 1$ (mod $p^{i+1}$) となる。

\text{Example 1.} $k = 27, p = 3, m = 3$. We list here all $M_{27}^a$ of cycle type.

\text{Proposition 5} Let $m \geq 2$. For $a \in (\mathbb{Z}/p^m\mathbb{Z})^*$, take sequences $a(a)$ and $s(a) = (s_m, s_{m-1}, \ldots, s_1)$ as Proposition 5, then

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

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

\text{Example 1.} $k = 27, p = 3, m = 3$. We list here all $M_{27}^a$ of cycle type.
Thus there are 6 possible sequences 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 characteristic as $27k_1, 9k_1 + 6k_3, 3k_1 + 2k_3 + 3k_9, k_1 + 13k_2, k_1 + 4k_2 + 3k_6, k_1 + k_2 + k_6 + k_{18}$ respectively.

**Example 2.** $k = 81$, $p = 3$, $m = 4$. We list here all $M_{81}^a$ of cycle type. There are 8 possible sequences 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 characteristic as $81k_1, 27k_1 + 18k_3, 9k_1 + 6k_3 + 6k_9, 3k_1 + 2k_3 + 3k_9 + 2k_{27}, k_1 + 40k_2, k_1 + 13k_2 + 9k_6, k_1 + 4k_2 + 3k_6 + 3k_{18}, k_1 + k_2 + k_6 + k_{18} + k_{54}$ respectively.

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

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

\[
\{a \in I_{81} \mid s(a) = (3, 1, 1, 1)\} = \{28, 55\}, \quad \{a \in I_{81} \mid s(a) = (6, 2, 2, 2)\} = \{26, 53\},
\]

\[
\{a \in I_{81} \mid s(a) = (9, 3, 1, 1)\} = \{10, 19, 37, 46, 64, 73\}, \quad \{a \in I_{81} \mid s(a) = (18, 6, 2, 2)\} = \{8, 17, 35, 44, 62, 71\},
\]

\[
\{a \in I_{81} \mid s(a) = (27, 9, 3, 1)\} = \{4, 7, 13, 16, 22, 25, 31, 34, 40, 43, 49, 52, 58, 61, 67, 70, 76, 79\}, \quad \{a \in I_{81} \mid s(a) = (54, 18, 6, 2)\} = \{2, 5, 11, 14, 20, 23, 29, 32, 38, 41, 44, 47, 50, 56, 59, 65, 68, 74, 77\}.
\]

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 complicated to describe the structures of multiplication $DG$ $M_k^n$'s. If $(k, a) > 1$, then by Remark 8 after Proposition 3, the pseudo-tree structure of $M_k^n$ can be detected through the reduction scheme

$$M_k^n \Rightarrow \cdots \Rightarrow M_k^{n'}.$$ 

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

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

$$M_{pq}^a \Rightarrow M_p^a \downarrow \Rightarrow M_q^a.$$ 

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 amalgamations.

Given $k$ explicitly, 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 $0 \leq a < pq$.

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 $c, \alpha$ with $c, \alpha \in \mathbb{Z}, 1 \leq c < q$, satisfying $bc = 1 + \alpha q$.

Consider the reduction $M_{pq}^a = M_{pq}^{bp} \Rightarrow M_q^{bp}$, 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: $P(M_{pq}^{bp}) = P(E_p(M_q^{bp}))$. Its vertex set is $V(E_p(M_q^{bp})) = \{ i p \mid 0 \leq i < q \}$.

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

$$a_j = bpj = bp(ci + \beta q) \equiv bcpi = (1 + \alpha q)(1 + \alpha q) \equiv ip \pmod pq.$$ 

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

$$M_{pq}^a = E_p(M_q^{bp}) \bigvee_{i=0}^{q-1} (\vee_{ip} K_{pq}^0).$$ 

and

$$P(M_{pq}^a) = P(M_q^a), \ V(M_{pq}^a) = pP(M_q^a), \ D = (p - 1)qk_0 + qk_p.$$ 

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

Case 4. $(a, pq) = 1$. Then $a \in \mathbb{Z}_k = \mathbb{Z}_{pq} \cong \mathbb{Z}_{p-1} \oplus \mathbb{Z}_{q-1}$, 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 $a_p = a \pmod p$ and $a_q = a \pmod q$.

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

$$M_{pq}^a = C_1 \cup \frac{p - 1}{s}, \ M_q^a = qC_1, \ M_p^a = qC_1 \cup \frac{q(p - 1)}{s} C_s.$$
Case 4-2. \( s \nmid (p-1), s \nmid (q-1) \).

\[
M_q^{\alpha_q} = C_1 \cup \frac{q-1}{s}, \quad M_p^{\alpha_p} = pC_1, \quad M_{pq}^a = pC_1 \cup \frac{p(q-1)}{s}C_s.
\]

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

\[
M_p^{\alpha_p} = C_1 \cup \frac{p-1}{s}, \quad M_q^{\alpha_q} = C_1 \cup \frac{q-1}{s}, \quad M_{pq}^a = C_1 \cup \frac{pq-1}{s}C_s.
\]

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

\[
M_p^{\alpha_p} = pC_1, \quad M_q^{\alpha_q} = qC_1, \quad M_{pq}^a = (p+q-1)C_1 \cup \frac{(p-1)(q-1)}{s}C_s.
\]

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

\[
M_6^a : \begin{cases} 
0 \rightarrow 3 & 1 \rightarrow 2 \\
4 \leftarrow 5 & 0 \leftarrow 2 
\end{cases}
\]

\[
M_6^b : \begin{cases} 
0 \rightarrow 3 & 4 \leftarrow 1 \\
2 \leftarrow 5 & 0 \leftarrow 3
\end{cases}
\]

\[
M_6^c : \begin{cases} 
0 \rightarrow 4 & 2 \leftarrow 1 \\
3 \leftarrow 5 & 0 \leftarrow 2
\end{cases}
\]

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

\[
M_{10}^{a\alpha} = (M_{10}^a)^{-1} : \begin{cases} 
0 \rightarrow 5 & 1 \rightarrow 2 \\
4 \leftarrow 6 & 0 \leftarrow 2 
\end{cases}
\]

\[
M_{10}^{b\alpha} = (M_{10}^b)^{-1} : \begin{cases} 
0 \rightarrow 5 & 4 \leftarrow 6 \\
2 \rightarrow 8 & 0 \rightarrow 2 
\end{cases}
\]

\[
M_{10}^{c\alpha} : \begin{cases} 
0 \rightarrow 5 & 1 \rightarrow 2 \\
4 \leftarrow 6 & 0 \rightarrow 2 
\end{cases}
\]

\[
M_{10}^{d\alpha} : \begin{cases} 
0 \rightarrow 5 & 4 \leftarrow 6 \\
2 \rightarrow 8 & 0 \rightarrow 2
\end{cases}
\]

\[
M_{10}^{e\alpha} : \begin{cases} 
0 \rightarrow 5 & 1 \rightarrow 2 \\
4 \leftarrow 6 & 0 \rightarrow 2
\end{cases}
\]
§5.6 Miscellaneous Cases

Here we list miscellaneous cases $(k \leq 100)$, 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 $a \in \mathbb{Z}_{100}^\times$.

<table>
<thead>
<tr>
<th>$a$</th>
<th>1</th>
<th>3</th>
<th>7</th>
<th>9</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
<th>21</th>
<th>23</th>
<th>27</th>
<th>29</th>
<th>31</th>
<th>33</th>
</tr>
</thead>
<tbody>
<tr>
<td>$o(a)$</td>
<td>1</td>
<td>20</td>
<td>4</td>
<td>10</td>
<td>10</td>
<td>20</td>
<td>20</td>
<td>10</td>
<td>10</td>
<td>20</td>
<td>10</td>
<td>10</td>
<td>20</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$a$</th>
<th>37</th>
<th>39</th>
<th>41</th>
<th>43</th>
<th>47</th>
<th>49</th>
<th>51</th>
<th>53</th>
<th>57</th>
<th>59</th>
<th>61</th>
<th>63</th>
<th>67</th>
</tr>
</thead>
<tbody>
<tr>
<td>$o(a)$</td>
<td>20</td>
<td>10</td>
<td>5</td>
<td>4</td>
<td>20</td>
<td>2</td>
<td>2</td>
<td>20</td>
<td>4</td>
<td>10</td>
<td>5</td>
<td>20</td>
<td>20</td>
</tr>
</tbody>
</table>

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

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

Reference


