Some properties of subgroup counting function

Sucharit Sarkar

April 26, 2004

1 Introduction

Let C_p denote the cyclic subgroup of order p. Let $G = C_{p_1} * C_{p_2} * \cdots * C_{p_k}$ and let M_n be the number of subgroups of G of index n. We will study a few properties of M_n modulo some primes. If $p_1 = p_2 = 2$, then $M_n = 1(2)$. Also if $G = C_{p_1} * C_{p_2}$, $p_1 = 1(q)$ and $n \neq 1, p_2(q)$, then $M_n = 0(q)$.

2 Graphical representation

Subgroups of index n in $G = C_{p_1} * C_{p_2} * \cdots * C_{p_k}$ are in 1-1 correspondance with subgroups of index n in $F[x_1, x_2, \ldots, x_k]$, the free group on k generators, containing the normal subgroup generated by $\{x_1^{p_1}, x_2^{p_2}, \ldots, x_k^{p_k}\}$.

Such subgroups in turn are in 1-1 correspondance with connected directed graph on n vertices, with a basepoint, with edges coloured in k colours, such that each vertex has 1 incoming and 1 outgoing edge of each colour and the colour j cycles are either loops or p_j cycles. This correspondance is given by the fundamental group of the graph w.r.t the basepoint.

So for $G = C_{p_1} * C_{p_2}$, subgroups of index n correspond to bi-coloured (say with colours red and blue) graphs, such that red cycles are either loops or p_1 cycles and blue cycles are either loops or p_2 cycles.

3 $G = C_{p_1} * C_{p_2}$

We want to count M_n modulo a prime q which divides $p_1 - 1$. If n is not congruent to 1 or p_2 modulo q, it turns out that q divides M_n.

Theorem 1 *If $G = C_{p_1} * C_{p_2}$, $p_1 = 1(q)$ and $n \neq 1, p_2(q)$, then $M_n = 0(q)$.*

Proof The main idea of the proof is make C_q act in some way on a subset of the set of all legal graphs on n vertices, such that there will be no fixed graph. This implies the number of graphs in this subset was divisible by q, so $M_n(q)$ depends on the remaining graphs. Then we will make C_q act freely (i.e. without any fixed points) in another way on a subset of the remaing graphs, and then concentrate on the ones still remaining. Continuing in this way, after a finite

stage, we will still have a few graphs left, and no natural way of making C_q act freely on any subset of them. Then we will have another type of action of C_q on these graphs, and look at all the fixed points. Then there will be another action of C_q on these fixed points and we will look at the fixed points of that also. Contuining in this fashion we will find that unless $n = 1, p_2(q)$, there cannot exist a graph which is a fixed point of all the actions. This will conclude the proof.

Given a legal graph, by it's blue skeleton (with a basepoint) we mean the new graph (not necessarily connected) obtained by deleting all the red edges. Clearly different graphs can have the same blue skeleton. The way we will define the actions, the blue skeleton of a graph will not be changed.

Given any red p_1 cycle with one of the vertices being labelled as loopbase, we can number each vertex by the minimum number of the directed red edges to be traversed from loopbase to reach that vertex. For example the loopbase will be numbered 0, and it's 2 adjacent vertices will be numbered as 1 and $p_1 - 1$.

As $p_1 = 1(q)$, so $C^*_{p_1}$, the (cyclic) mutiplicative group on $\{1, 2, \ldots, p_1 - 1\}$, has a unique (cyclic) subgroup of order q. Let the subgroup be generated by $r \in C_{p_1}$. All our actions by C_q will be of the following type.

We will take some red p_1 cycle with a fixed loopbase, and number all the vertices in the manner as described above. Under the action of $t \in C_q$ on the graph, we will delete all the red edges of just this red cycle, and make new edges from $r^t j$ to $r^t(j + 1)$ $\forall j \in C_{p_1}$. The old loopbase will still be a called as the loopbase, and the other vertices will be numbered accordingly. (Note, for $t \neq 0$, all the vertices except the loopbase will be renumbered). It is easy to see that this is a well defined action.

Let A be the basepoint vertex of the whole graph, and let $\mathcal{A}$ be the set of vertices connected to A in the blue skeleton, i.e. by blue edges. Let a be the number of vertices in $\mathcal{A}$ ($a = 1, p_2$). Let us number each vertex of $\mathcal{A}$ by the minimum number of directed blue edges to be traversed to reach the vertex from A. (The important thing is to number the vertices in such a way that the numbering depends only on the blue edges of $\mathcal{A}$).

Let us consider all the legal graphs where some 2 distinct vertices of $\mathcal{A}$ are connected without using any blue edge of $\mathcal{A}$ (all graphs in this set necessarily having $a = p_2$). We make C_q act freely on this set as follows.

Let us consider all possible pairs of vertices in $\mathcal{A}$, where both vertices of the pair are connected without the blue edges of $\mathcal{A}$. Let us choose the vertex with the minimum number which occurs in some pair. Then we choose the red cycle (necessarily a p_1 cycle) passing through that vertex and call the vertex as it's loopbase, and make C_q act on the graph as described above. It is not difficult to see that this is a well defined action without a fixed point.

So graphs which are remaining do not have any 2 distinct vertices of $\mathcal{A}$ connected without the blue edges of $\mathcal{A}$. So if exactly $\widetilde{a}$ vertices in $\mathcal{A}$ have red p_1 cycles (the rest have red loops), we number these $\widetilde{a}$ cycles from 1 to $\widetilde{a}$, based on the numbering of the corresponding vertex in $\mathcal{A}$.

Consider the red cycle numbered j, and call it's (unique) vertex in $\mathcal{A}$ as it's loopbase and number the rest of the vertices accordingly. Let $\mathcal{B}_j$ be the set of

all vertices connected in the blue skeleton to the $p_1 - 1$ vertices of the red cycle except the loopbase, and call this red cycle as the defining cycle of $\mathcal{B}_j$. There is a natural ordering of the vertices of $\mathcal{B}_j$ as follows.

The vertices of the defining cycle are already numbered from 1 to $p_1 - 1$. So for each blue cycle in $\mathcal{B}_j$, consider the smallest vertex (say vertex numbered k) of the defining red cycle which is also in this blue cycle, and call it the blue-loopbase and number all the vertices of this cycle by minimum number (say l) of directed blue edges to be traversed to go to that vertex from the blue-loopbase. This numbers all the vertices in $\mathcal{B}_j$ by the pair (k, l), and gives an ordering based on the dictionary ordering.

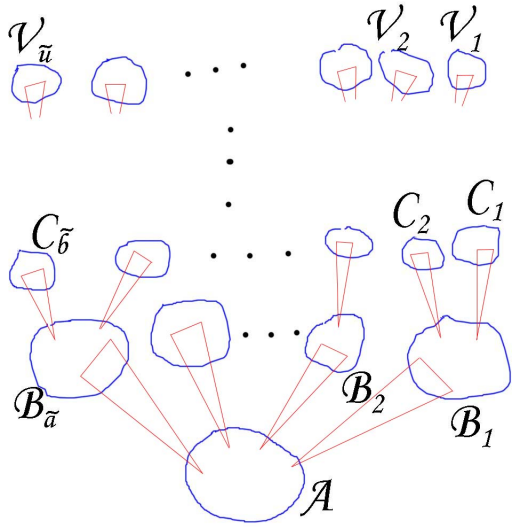
If there is a total of b vertices in $\bigcup \mathcal{B}_j$, then there is again a natural numbering of these vertices from 1 to b. Vertices in $\mathcal{B}_i$ will be numbered lower than the vertices in $\mathcal{B}_j$ for $i < j$. And in a particular $\mathcal{B}_j$, vertices are ordered as desribed above. (Here also the numbering of the vertices depends only on the blue edges of $\mathcal{A}$, $\mathcal{B}_j$ and their red defining cycles).

Now among the remaining graphs, consider all the graphs which have 2 distinct vertices of some $\mathcal{B}_j$ connected without using the blue edges of $\mathcal{B}_j$ or it's defining cycle. We will make C_q act freely on this set in a very similar fashion as the first one.

Consider all the pair of vertices in $\bigcup \mathcal{B}_j$ such that they are connected without using the blue egdes of any $\mathcal{B}_j$ or it's defining cycle, and choose the minimum vertex occuring in some pair. We choose the red (p_1) cycle passing through that vertex and call that vertex it's loopbase, and make C_q act in the manner already described. A similar proof as before will show that this is well defined and cannot have any fixed points.

Now we look at the graphs that are still remaining and proceed similarly. If exactly $\widetilde{b}$ vertices in $\bigcup \mathcal{B}_j$ have red p_1 cycles, we number each of these cycles from 1 to $\widetilde{b}$ (based on the numbering of the b vertices of $\bigcup \mathcal{B}_j$. In the red cycle numbered k, define the vertex in $\bigcup \mathcal{B}_j$ as the loopbase and number the other vertices in the red cycle accordingly. Then define $\mathcal{C}_k$ to be the set of vertices connected in the blue skeleton to $p_1 - 1$ vertices of this red cycle except the loopbase and call this cycle to be the defining cycle for $\mathcal{C}_k$. There will be a natural ordering for the vertices of $\mathcal{C}_k$ which in turn will give a numbering of the c vertices in $\bigcup \mathcal{C}_k$ from 1 to c (again the ordering depending only on the blue edges upto $\mathcal{C}_k$ and the red defining cycles upto this stage). We will look at the all the graphs where some 2 distinct vertices of some $\mathcal{C}_k$ are connected without using the blue edges or the red defining cycle of $\mathcal{C}_k$. We will choose a particular red cycle with a loopbase based on our numbering and make C_q act freely using this red cycle. We will then look at the remaining graphs.

However as M_n is finite, this process cannot continue indefinitely, and we have to stop somewhere. Take any legal graph which is left out and assume all it's vertices are partitioned into $\mathcal{A}, \mathcal{B}_j, \ldots, \mathcal{V}_t$, such that in $\mathcal{V}_t$ all the red cycles other than it's defining cycle are loops.



Now we will make C_q act in a different way on these remaining graphs. Call the sequence $\{\widetilde{a}, \widetilde{b}, \ldots\}$ as the signature of a graph. It is a sequence of 0 after some point. In the graph in the previous paragraph, we assumed that it is 0 after $\widetilde{u}$. The sequence of actions we define now will preserve the signature of the graph and for every signature, there cannot be any graph fixed by all actions if $n \neq 1, p_2(q)$.

Take a particular signature (say one where the last non-zero entry is $\widetilde{u}$). All the $\widetilde{u}$ defining cycles of $\bigcup \mathcal{V}_t$ have fixed loopbase, and hence have numbered vertices. We make C_q act on the graph by making C_q act on all the defining red cycles (with loopbases) simultaneously. It is clearly well defined and preserves signature. If a graph is fixed, it is not difficult to see that it must be fixed if C_q just acted on the red defining cycle of 1 particuar $\mathcal{V}_t$.

But then $\mathcal{V}_t$ must look the same after the action of C_q. But when we ordered the vertices of $\mathcal{V}_t$, we assigned a pair of numbers to any given vertex as (the minimum vertex in the red defining cycle $\bigcap$ the blue cycle containing the given vertex, the minimum number of directed blue edges to be traversed to reach the given vertex from the minimum vertex). Under the action of a non-zero element of C_q, all the $p_1 - 1$ vertices of the red defining cycle in $\mathcal{V}_t$ are renumbered, and hence each vertex in $\mathcal{V}_t$ is renumbered (by another pair of numbers). This induces a free action of C_q on the vertices of $\mathcal{V}_t$ (we are using the fact that $\mathcal{V}_t$ looks same after action of C_q on the defining cycle, hence if some vertex is numbered (k, l) in $\mathcal{V}_t$, then after the action by some element of C_q and the consequent renumbering, some vertex in $\mathcal{V}_t$ will be numbered as (k, l)). Thus there must be $0(q)$ vertices in $\mathcal{V}_t$, hences $0(q)$ vertices in $\bigcup \mathcal{V}_t$.

Now let us look at all the graphs that are fixed of the given signature (all such graphs having $0(q)$ vertices in $\bigcup \mathcal{V}_t$). We now make C_q act on these graphs by making it act on all the $\widetilde{t}$ defining cycles of $\bigcup \mathcal{U}_i$. A similar reasoning shows

each $\mathcal{U}_i$ and hence $\bigcup \mathcal{U}_i$ has $0(q)$ vertices.

Proceeding similarly, we find for a graph to be fixed by all such C_q actions, the number of vertices in each $\mathcal{B}_j, \mathcal{C}_k, \ldots, \mathcal{U}_i, \mathcal{V}_t$ must have $0(q)$ vertices. But then n, the total number of vertices must be $a = 1, p_2(q)$, which is not possible. Thus there is no fixed graph, and hence $M_n = 0(q)$.

4 $G = C_2 * C_2 * C_{p_3} * \cdots * C_{p_k}$

We will prove that $M_n = 1(2)\ \forall n$. The case $p_j = 2\ \forall j$ has already been settled by Newman and Grady for $k \geq 4$, and by Sury for $k = 3$. Without loss of generality, we can assume that p_k is an odd prime.

Before embarking on the actual proof, let us prove a few simple lemmas.

Lemma 1 $\frac{1}{2^l}\frac{(2l)!}{l!} = 1(2), \binom{2m}{m} = 0(2)$ *and* $\binom{2m}{2l} = \binom{m}{l}(2)$.

Proof We know the exact power of 2 dividing $n!$ is $\{[\frac{n}{2}]+[\frac{n}{4}]+\cdots\}$. So the exact power of 2 dividing $\frac{(2l)!}{l!}$ is $\{l + [\frac{l}{2}] + \cdots\} - \{[\frac{l}{2}] + \cdots\} = l$. Similarly the exact power of 2 dividing $\binom{2m}{m}$ is $\{m+[\frac{m}{2}]+\cdots\}-2\{[\frac{m}{2}]+\cdots\} = m-\{[\frac{m}{2}]+\cdots\}$. But $\{[\frac{m}{2}]+\cdots\} \leq \{\frac{m}{2}+\cdots\} = m$ and equality cannot hold throughout, thus proving $\binom{2m}{m} = 0(2)$. Similarly the exact power of 2 dividing $\binom{2m}{2l}$ is $\{m + [\frac{m}{2}] + \cdots\} - \{l + [\frac{l}{2}] + \cdots\} - \{m - l + [\frac{m-l}{2}] + \cdots\} = \{[\frac{m}{2}] + \cdots\} - \{[\frac{l}{2}] + \cdots\} - \{[\frac{m-l}{2}] + \cdots\}$ which is the exact power of 2 dividing $\binom{m}{l}$.

Lemma 2 $\sum_{l=0}^{m} \#\{\bar{s} \in \mathbb{N}^m \mid \sum_{i=1}^{m} s_i = r\}\binom{2m}{2l}\frac{1}{2^l}\frac{(2l)!}{l!} = 0(2)$, *where* $\#S$ *denotes the cardinality of the set* S.

Proof Using $\frac{1}{2^l}\frac{(2l)!}{l!} = 1(2)$ and $\binom{2m}{2l} = \binom{m}{l}(2)$, the given sum simplifies to $\sum_l \#\{\bar{s} \in \mathbb{N}^m \mid \sum_{i=1}^{m} s_i = r\}\binom{m}{l}$. But as $\binom{m}{l} = \binom{m}{m-l}$, so the given sum with $l \neq m - l$ is $0(2)$. Now if $m = 1(2)$, $l = m - l$ is not possible, hence the whole sum is $0(2)$. While on the other hand, if $m = 0(2)$, then the required sum is $\#\{\bar{s} \in \mathbb{N}^m \mid \sum_{i=1}^{m} s_i = r\}\binom{m}{m/2} = 0(2)$ as $\binom{m}{m/2} = 0(2)$.

With these 2 lemmas in hand, let us state and prove our theorem.

Theorem 2 *If* $G = C_2 * C_2 * C_{p_3} * \cdots * C_{p_k}$, *then* $M_n = 1(2)$.

Proof We use induction on k, the number of colours in our graphical reperesentation. It is clearly true for $k = 2$. As argued earlier, we can assume $p_k = 1(2)$. In the graphical representation, we are working with k coloured graphs, and let green be the colour corresponding to p_k. Thus the green cycles are either loops or p_k cycles. Let us call any other colour in the graph as grey. The graph obtained by deleting all the green edges is called the grey skeleton. In a manner very similar to the previous section, we will be using free action of C_2 on a subset of graphs, and count the remaining graphs.

If N_r denotes the number of subgroups of index r in $G = C_2 * C_2 * C_{p_3} * \cdots * C_{p_{k-1}}$, then by induction hypothesis $N_r = 1(2)$.

We define a special graph to be a connected legal graph of the above type (on n vertices and with k colours), such that the only cycle at the basepoint that is not a loop is the green cycle (i.e. the grey connected component of the basepoint is itself), and also that green cycle is the only green cycle that is not a loop (the other green cycles are loops). First we prove there are even number of special graphs for any n.

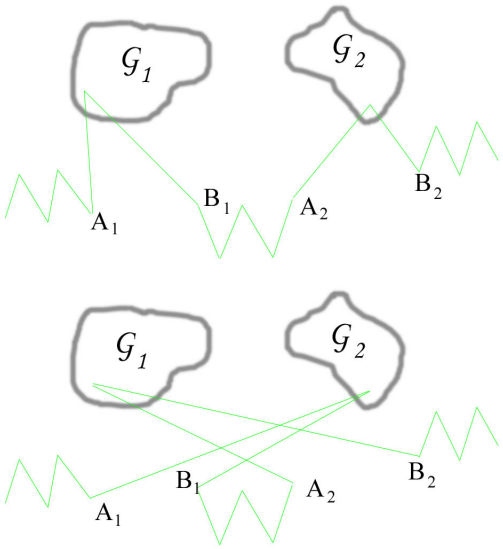
In a special graph, the vertices of the green cycle are very naturally numbered from 0 to $p_k - 1$, with the basepoint (treated as a loopbase) being numbered 0. Call the grey connected components of the $n-1$ vertices (i.e all vertices except the basepoint) to be proper grey components. For each proper grey connected component, call the minimum vertex of the green cycle in that grey component to be the greybase of the component. The ordering of the vertices in the green cycle, naturally orders the proper grey components based on their greybases.

Take the set of all special graphs which have at least 3 vertices of the green cycle, in some grey connected component, and we will make C_2 act freely on this set as follows.

Let $\mathcal{G}$ be the first grey connected component that has atleast 3 vertices from the green cycle. Let A, A_1, A_2 be the first 3 vertices of the green cycle in $\mathcal{G}$ (A being the greybase). If l_i denotes the green edge incident on A_i from the vertex B_i (not necessarily in $\mathcal{G}$), and if m_i denote the green edge leaving A_i to C_i (again need not be in $\mathcal{G}$), then we delete these 4 green edges l_1, l_2, m_1, m_2 and put 4 new green edges from B_1 to A_2, B_2 to A_1, A_1 to C_2 and A_2 to C_1. This is easily seen to be a well defined free action of C_2 on this set of special graphs.

Let $p_k - 1 = 2m$. There must be even number of proper grey components containing exactly 1 vertex each of the green cycle, for the other grey components have exactly 2 vertices each from the green cycle, and the total number of vertices in the green cycle is $2m = 0(2)$. So let $2m - 2l$ be the number of grey connected components with exactly one vertex each (just the greybase) from the green cycle. Based on the ordering of all the $2m$ vertices, these $2m - 2l$ vertices are naturally ordered. Now each of these proper grey components corresponds to a subgroup of $G = C_2 * C_2 * C_{p_3} * \cdots * C_{p_{k-1}}$ after treating it's greybase as a basepoint. Pair up these subgroups (which are also ordered) as first 2, next 2, next 2 and so on. Look at the all the special graphs from the ones that are remaining where the 2 subgroups of at least 1 such pair does not correspond to the same subgroup of $G = C_2 * C_2 * C_{p_3} * \cdots * C_{p_{k-1}}$. We make C_2 act freely on this set as follows.

Number the pairs from 1 to $m - l$ based on the ordering of the grey components. Choose the first pair, where the 2 subgroups are different. Let $\mathcal{G}_1$ and $\mathcal{G}_2$ be the 2 proper grey components corresponding to these 2 subgroups. As before let A_i be the greybase in $\mathcal{G}_i$, let l_i be the green incoming edget to A_i from B_i and m_i be the green outgoing edge from A_i to C_i. We delete the 4 green edges l_1, l_2, m_1, m_2 and put 4 new green edges from B_1 to A_2, B_2 to A_1, A_1 to C_2 and A_2 to C_1.



Now we actually count the number of special graphs that are still remaining in terms of N_r.

The $2m-2l$ greybases can be chosen from $2m$ vertices in $\binom{2m}{2l}$ ways. Let t_i be the number of vertices in either of the 2 grey connected component in the pair numbered i. The index t_i subgroup of $G = C_2 * C_2 * C_{p_3} * \cdots * C_{p_{k-1}}$ corresponding to each of these 2 pairs can be chosen in N_{t_i} ways. The remaining $2l$ vertices have to be partioned in l groups of 2 vertices each (corresponding to the vertices belonging to the same proper grey component), and this partioning can be done in precisely $\frac{1}{2^l}\frac{(2l)!}{l!}$ ways. Let these l grey components be numbered from 1 to l based on the ordering of their greybases. Let u_i be the number of vertices in the grey component numbered 1. These grey components also correspond to subgroups of $G = C_2 * C_2 * C_{p_3} * \cdots * C_{p_{k-1}}$, and so there are N_{u_i} choices for a grey component with u_i vertices. After that the second vertex of the green cycle (the vertex other than the greybase) in that grey component can be chosen in $u_i - 1$ ways.

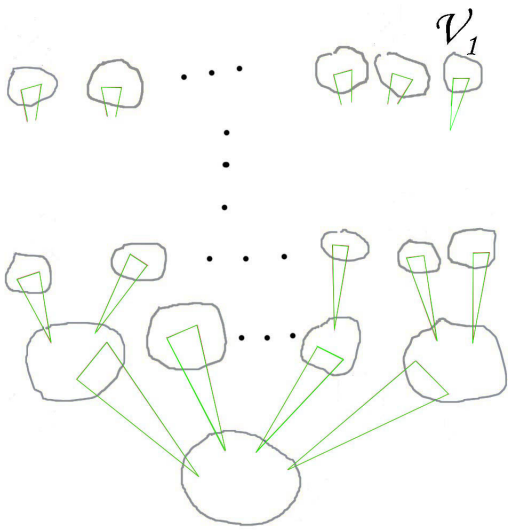
So for a given l, and fixed u_i and t_i, the number of special graphs remaining is $\binom{2m}{2l}\frac{1}{2^l}\frac{(2l)!}{l!}\prod_{i=1}^{m-l} N_{t_i}\prod_{i=1}^{l} N_{u_i}(u_i-1)$. Using the fact $N_r = 1(2)$, this expression simplifies to $\binom{2m}{2l}\frac{1}{2^l}\frac{(2l)!}{l!}\prod_{i=1}^{l}(u_i-1)$. Now if any of the $u_i = 1(2)$, this expression is $0(2)$. For this expression to be non-zero, all u_i are even, say $u_i = 2s_i$. Then the expression becomes $\binom{2m}{2l}\frac{1}{2^l}\frac{(2l)!}{l!}$. But total number of vertices is given by $n-1 = \sum_{i=1}^{l} 2s_i + \sum_{i=1}^{m-l} 2t_i$. So if $n = 0(2)$, we do not have any non-zero expression, and hence the whole sum is $0(2)$. Else $n = 2r+1$, and then s_i, t_i satisfy $r = \sum_{i=1}^{l} s_i + \sum_{i=1}^{m-l} t_i$. The number of such solutions is $\#\{\bar{s} \in \mathbb{N}^m \mid \sum_{i=1}^{m} s_i = r\}$. So the total number of such special graphs is $\sum_{l=0}^{m} \#\{\bar{s} \in \mathbb{N}^m \mid \sum_{i=1}^{m} s_i = r\}\binom{2m}{2l}\frac{1}{2^l}\frac{(2l)!}{l!} = 0(2)$.

Now we prove that there are odd number of legal graphs on n vertices in k

colours using the fact that there are even number of special graphs of the same type. For this part, we will closely follow the method of the previous section with green taking the role of red, grey for blue, and 2 instead of q.

Let $\mathcal{A}$ be the grey connected component containing basepoint. If there are a vertices in $\mathcal{A}$, we number the vertices from 0 to $a-1$, in such a way that the numbering depends only on the grey edges of $\mathcal{A}$. We can make C_2 act freely on the set of all graphs where some 2 vertices of $\mathcal{A}$ are connected without using the grey edges. We now concentrate on the remaining graphs. If exactly $\widetilde{a}$ vertices of $\mathcal{A}$ have non-loop green cycles, then after numbering these vertices and green cycles from 1 to $\widetilde{a}$ and calling them the loopbases for the corresponding green cycles, we define $\mathcal{B}_j$ to be the set of vertices grey connected to the p_k-1 vertices (except loopbase) of the green cycle numbered j and call this cycle as it's green defining cycle. It is not difficult to convince oneself that the vertices of $\bigcup \mathcal{B}_j$ can also be ordered such that the ordering depends only on grey edges of $\mathcal{A}$ and $\mathcal{B}_j$ and their green defining cycles. Now consider all the graphs where some 2 vertices of $\mathcal{B}_j$ can be connected without using the grey edges of $\mathcal{B}_j$ and we can make C_2 act freely on this set, and proceed with the remaining graphs.

Being a finite graph, we have to stop somewhere. We take 2 cases, $\mathcal{A}$ covers the whole graph, or else it does not. If it does not, then as in the previous section, let $\widetilde{u}$ be the last non-zero entry in the signature $\{\widetilde{a}, \widetilde{b}, \ldots\}$. If there are v_1 vertices in $\mathcal{V}_1$, then by keeping the rest of the graph fixed, and considering different grey skeletons for $\mathcal{V}_1$, we conclude that there are even number of such possibilities (as each grey skeleton of $\mathcal{V}_1$ corresponds to a special graph on v_1+1 vertices with it's defining cycle playing the role of the unique green cycle of the special graph). Thus there are even number of graphs with $\mathcal{A}$ not being the whole of the graph.



But if $\mathcal{A}$ is the whole of the graph, then every green cycle is a loop and the grey skeleton of the whole graph is connected. Number of such graphs is clearly N_n, hence odd. This completes the induction step and proves that $M_n = 1(2)$.

5 Conclusion

The result we proved in the previous section is true in a bigger generality. Newman and Grady proved for $p > 3$, that if $p_1 = p_2 = p$ and $p_j \geq p \ \forall j$, then $M_n(p)$ satisfies a recurrance relation (independent of k or other p_j) of length p. But since the first $p-1$ values of $M_n(p)$ are $\{1, 0, 0, \ldots, 0\}$ for all such groups, hence $M_n(p)$ is same for all such groups $\forall n$. What we proved in the previous section is the case for $p = 2$. The case $p = 3$ is still open.