A Class of Generalized Triangle Groups as Quotients of $PGL(2, Z)$

By

Imran Shahzad

Department of Mathematics
Quaid-i-Azam University
Islamabad, Pakistan
2020

A Class of Generalized Triangle Groups as Quotients of $PGL(2, Z)$

By

Imran Shahzad

Supervised By

Prof Dr. Qaiser Mushtaq

Department of Mathematics
Quaid-i-Azam University
Islamabad, Pakistan
2020

A Class of Generalized Triangle Groups as Quotients of $\boldsymbol{PGL(2,Z)}$

A thesis submitted in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

By

Imran Shahzad

Department of Mathematics
Quaid-i-Azam University
Islamabad, Pakistan
2020

Author's Declaration

I, **Imran Shahzad,** hereby state that my PhD thesis titled **A Class of Generalized Triangle Groups as Quotients of PGL(2,Z)** is my own work and has not been submitted previously by me for taking any degree from the Quaid-I-Azam University Islamabad, Pakistan or anywhere else in the country/world.

At any time if my statement is found to be incorrect even after my graduate the university has the right to withdraw my PhD degree.

Name of Student: **Imran Shahzad**

Date: **18 September 2020**

Plagiarism Undertaking

I solemnly declare that research work presented in the thesis titled "**A Class of Generalized Triangle Groups as Quotients of PGL(2,Z)**" is solely my research work with no significant contribution from any other person. Small contribution/help wherever taken has been duly acknowledged and that complete thesis has been written by me.

I understand the zero tolerance policy of the HEC and **Quaid-i-Azam University** towards plagiarism. Therefore, I as an Author of the above titled thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred/cited.

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even afterward of PhD degree, the University reserves the rights to withdraw/revoke my PhD degree and that HEC and the University has the right to publish my name on the HEC/University Website on which names of students are placed who submitted plagiarized thesis.

Student/Author Signature

Name: **Imran Shahzad**

A Class of Generalized Triangle Groups as Quotients of PGL(2,Z)

By

Imran Shahzad

CERTIFICATE

A THESIS SUBMITTED IN THE PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF THE

DOCTOR OF PHILOSOPHY IN MATHEMATICS

We accept this thesis as conforming to the required standard

1. Snadeem
Prof. Dr. Sohail Nadeem
(Chairman)

2. Qaiser Mushtaq
Prof. Dr. Qaiser Mushtaq
(Supervisor)

3. Akbar Azam
Prof. Dr. Akbar Azam
(External Examiner)

Department of Mathematics, COMSATS University, Park Road Chak Shahzad, Islamabad

4. ____________________
Dr. Asghar Khan
(External Examiner)

Department of Mathematics, Abdul Wali Khan University, Mardan.

Department of Mathematics
Quaid-I-Azam University
Islamabad, Pakistan
2020

Certificate of Approval

This is to certify that the research work presented in this thesis entitled **A Class of Generalized Triangle Groups as Quotients of PGL(2,Z)** was conducted by **Mr. Imran Shahzad** under the kind supervision of **Prof. Dr. Qaiser Mushtaq**. No part of this thesis has been submitted anywhere else for any other degree. This thesis is submitted to the Department of Mathematics, Quaid-i-Azam University, Islamabad in partial fulfillment of the requirements for the degree of Doctor of Philosophy in field of Mathematics from Department of Mathematics, Quaid-i-Azam University Islamabad, Pakistan.

Student Name: **Imran Shahzad** Signature: Imran

External committee:

a) **External Examiner 1**: Signature: Akbar Azam
Name: **Prof. Dr. Akbar Azàm**
Designation: Professor
Office Address: Department of Mathematics, COMSATS University, Park Road Chak Shahzad, Islamabad.

b) **External Examiner 2**: Signature:

Name: **Dr. Asghar Khan**
Designation: Associate Professor
Office Address: Department of Mathematics, Abdul Wali Khan University, Mardan.

c) **Internal Examiner** Signature: Qaiser Mushtaq
Name: **Prof. Dr. Qaiser Mushtaq**
Designation: Professor Emeritus
Office Address: Department of Mathematics, QAU Islamabad.

Supervisor Name: Signature: Qaiser Mushtaq
Prof. Dr. Qaiser Mushtaq

Signature: Nadeem

Name of Dean/ HOD

Prof. Dr. Sohail Nadeem

Dedicated

to

all those students of
Baluchistan who want to learn
but have less opportunities

Acknowledgements

Thanks to Almighty Allah who enable me to complete this thesis.

I am indebted to my supervisor, Prof. Dr. Qaiser Mushtaq for his invaluable discussions which empowered me to accomplish this thesis. I would never have been able to do this work without his continual guidance.

I am grateful to my family members especially my wife who provides me conducive environment for the completion of this task, my daughter whose smile refreshes me for research, my father who encouraged me continuously, and my mother who always kept me out from all kinds of stresses.

I am sincerely thankful to my research fellows especially Dr. Abdul Razaq for his time and a lot of valuable discussions, Dr. Iqtadar Hussain for his support, Dr. Irfan Younas and Shahid Saqlain were continuous shareholder of my stress during the entire period of my PhD and many other names including Syed Khurram Shahzad, Sir Ali Shahab, Shahzaib Haider and Mubashir Masood who always supported me the way they can. My acknowledgements will remain incomplete if I do not mention the names of my teachers Prof. Muhammad Abdullah, Prof. Ather Rasheed, Prof. Zeeshan Hashmi, Prof. Abdul Khaliq (late) and Prof. Irfan Ahmed Baig (S.I) who wished me success with satisfaction in my life.

Imran Shahzad

September 18, 2020

Preface

A Class of Generalized Triangle Groups as Quotients of *PGL(2, Z)*

It is well known that the modular group *PSL(2, Z)* is generated by the linear fractional transformations $x : z \rightarrow \frac{-1}{z}$ and $y : z \rightarrow \frac{z-1}{z}$ which satisfy the relations $x^2 = y^3 = 1$. An additional relation in a group converts it into a quotient of the group. If the additional relation is simply the power of the product of two generators x and y then it turns out to be a triangle group $\Delta(l,m,n) = < x, y\ ;\ x^l = y^m = (xy)^n = 1 >$. The triangle groups $\Delta(2,3,n)$ are especially important for being homomorphic images of the modular group *PSL(2,Z)*. If an additional relation is of the form $(w(x,y))^n$ where $w(x,y) = x^{p_1}y^{q_1}x^{p_2}y^{q_2}\ldots x^{p_k}y^{q_k}$ then the group converts into a generalized triangle group $\Delta^*(l,m,n) = < x, y\ ;\ x^l = y^m = (w(x,y))^n = 1 >$. It is known that the generalized triangle group is infinite when $\left(\frac{1}{l}+\frac{1}{m}+\frac{1}{n}\right) \leq 1$ and finite when $\left(\frac{1}{l}+\frac{1}{m}+\frac{1}{n}\right) > 1$. J. Howie, V. Metaftsis and R. M. Thomas proved a very important result about the classification of finite generalized triangle groups.

A word w is defined as a finite sequence $x_1^{\varepsilon_1}x_2^{\varepsilon_2}\ldots\ x_k^{\varepsilon_k}$, where for each $\boldsymbol{i}$, $\boldsymbol{x_i}$ belongs to the set of generators and each $\boldsymbol{\varepsilon_i}$ is either 1 or -1. The third relator leads to a word which is of special interest in this thesis.

Several group theorists discussed one relator quotients of various groups. A considerable number of them concentrated on one relator quotients of the modular group. M. D. E. Conder is one of them who found quotients of the modular group by inserting additional relations as *words* up to length 24. Y. T. Ulutas and I. N. Cangul, by using a different technique, investigated one relator quotients of the modular group by inserting additional relations as words up to length 21. Later on, a number of researchers followed both the techniques, but all were restricted by considering additional relations as words of finite lengths. In the entire discussion of one relator quotients, length of the additional relation as a word is the centre point of our concern.

In this dissertation, our aim is to study a class of generalized triangle groups as quotients of the modular group. Since, modular group is a two generator group, we insert an additional relation of the form $w(x,y) = x^{p_1}y^{q_1}x^{p_2}y^{q_2} \dots x^{p_k}y^{q_k}$ in the finite presentation of the group. We consider powers of the generators as terms of Fibonacci sequence of numbers. That is we consider groups $< x, y\,;\, x^2 = y^3 = w(x,y) = 1 >$ which are one relator quotient of the modular group and a class of generalized triangle groups. There are two major parts to investigate in this class of groups. Firstly, we determine additional relations for all lengths k, that is, the length of word $w(x,y)$-which varies from 1 to infinity. Secondly, we insert these (infinite) number of additional relations in finite presentation of the modular group and investigate the quotient groups thus obtained.

This thesis comprises five chapters. In chapter one, we mentions some basic concepts related to one relator quotients. This chapter contains finite presentations of groups, quotient of a group, group action on suitable sets, coset diagrams, projective general linear group, projective special linear group, triangle groups, generalized triangle groups, Fibonacci sequence, words, reduced words, equivalent words, syllable of a word, Tietze transformations, finite fields and projective lines over the finite fields.

In chapter two, there is a comprehensive survey of one relator quotients generally and one relator quotients of the modular group particularly. This study not only explains the results but also stresses upon the methodology adopted by various researchers. One relator quotients of the modular group are of special importance due to the interesting features of this group.

In chapter three, we generate words of all syllables. We use Fibonacci sequence of numbers in the powers of the generators in the additional relation for generating words of all syllables. We develop an algorithm by which we generate words. This algorithm gives four outputs; words of all syllables, reduced form of the words, count the number of x and y in words, and in their respective reduced forms. In the end, we divide words in classes on the basis of Fibonacci sequence.

In chapter four, we find one relator quotients of the modular group related to Fibonacci sequence of numbers. The words obtained in chapter three are used as additional relation in the modular group so that they can later be investigated as quotient groups. Finally, to identify these quotients we use Tietze transformation and in certain cases 'Groups, Algorithms and Programming' (GAP). It is a class of generalized triangle groups which we investigate as quotients of the modular group. Furthermore, from this class of quotients we choose one quotient, which is the alternating group of degree 4, that is, A_4 and by taking action of A_4 on the projective line over the finite field $F_{257,}$ that is $PL(F_{257})$ we construct an algebraic substitution box (S-box). By investigating the security strength parameters of this S-box, we conclude that this S-box is highly secure for the communication and highly preferable for cryptographic applications.

In chapter five, we determine number of all one relator quotients of the modular group for each syllable by considering all possible additional relations. Furthermore, we proved a number of results by which we find the number of cyclically reduced non-equivalent words for each syllable k. The one relator quotients corresponding to these cyclically reduced non-equivalent words are sufficient instead of finding all but equivalent quotients. In this chapter, we also view the additional relations as circuits (close paths) and find some interesting relationships between them. From the circuits point of view, if we consider all the possibilities of the additional relation then there are two types of circuits; one type consists of circuits having all triangles with one vertex inside or all triangles with one vertex outside of the circuit and the second type consists of circuits containing some (at least one) triangles with one vertex in side and some (at least one) triangles with one vertex outside the circuit. First type depicts triangle groups as quotients of the modular group and the other type depicts generalized triangle groups as quotients of the modular group. The study of one relator quotients provides a mechanism to determine all one relator quotients of any two-generator group.

Contents

Chapter 1

Definitions and Basic Concepts

This introductory chapter provides a background knowledge and general information in a formal way which enable the reader to go through this work without consulting the literature. We include only those definitions which are specifically related to generalized triangle groups and one relator quotients of a group. We adopt standard notations as used in text books. We begin the current chapter with a summary of basic concepts. References for further information are provided throughout.

Finite Presentation of a group

Let G be a group having generators $x_1, x_2, x_3, ...$ such that every element of G can be written as a product of some of these generators and their powers.

Let

$$X\left(x_1, x_2, x_3, ...\right), Y\left(x_1, x_2, x_3, ...\right), Z\left(x_1, x_2, x_3, ...\right), ...$$

be defining relations for G such that each of them defines the identity element of G and any other relator for G is obtained from these relators. Therefore, G is written as

$$G = \langle x_1, x_2, x_3, ... : \ X(x_1, x_2, x_3, ...), \ Y(x_1, x_2, x_3, ...), \ Z(x_1, x_2, x_3, ...), ...\rangle.$$

H. S. M. Coxeter and W. O. J. Moser [1] call a set of certain elements $x_1, x_2, x_3, ..., x_n$ of a group G, a set of generators if every element of G is expressible as a finite product of their powers (including negative powers). Such a group is conveniently denoted by the symbol $\langle x_1, x_2, ..., x_m\rangle$. When $m = 1$, we get a finite cyclic group $< x >$ denoted by C_n, where n is the order of the single generator x, that is $x^n = 1$, where 1 is a notation for the identity element of the group C_n. It is important to mention here that, the relation $x^n = 1$ means that the order of x is exactly n, and not merely divisor of n.

A presentation $< S, R >$ is called finitely generated if the set S is finite, and is finitely related if the set R is finite. A presentation $< S, R >$ is called finite if both S and R are finite; in that case $G =< S, R >$ is called finitely presented.

As we know there is no co-relation between cardinality of the set S and order of the group G. Our interest is mainly in the quotients of linear groups, therefore we refer to a wonderful paper by R. G. Swan [2] which discusses generators and relations for some linear groups. Some finite presentations of well known groups are given as follows.

$C_n =< x : x^n = 1 >$ cyclic group of order n

$S_3 =< x, y : x^2 = y^3 = (xy)^2 = 1 >$ is symmetric group of order 3!

$S_4 =< x, y : x^2 = y^3 = (xy)^4 = 1 >$ is symmetric group of order 4!

$A_4 =< x, y : x^2 = y^3 = (xy)^3 = 1 >$ is an alternating group of order $\frac{4!}{2}$

$A_5 =< x, y : x^2 = y^3 = (xy)^5 = 1 >$ is an alternating group of order $\frac{5!}{2}$

$D_{2n} =< x, y : x^2 = y^n = (xy)^2 = 1 >$ is a dihedral group of order $2n$

$D_\infty =< x, y : x^2 = (xy)^2 = 1 >$ is an infinite dihedral group

$Q_8 =< x, y : x^4 = 1,\ x^2 = y^2,\ yx = x^3y >$ or

$Q_8 =< x, y : yxy = x,\ xyx = y >$ quaternion group of order 8

$\mathbb{Z} \times \mathbb{Z} =< x, y : xy = yx >$ free product of $\mathbb{Z}$ and $\mathbb{Z}$

$C_2 \times C_3 =< x, y : x^2 = y^3 = 1 >$ is also known as the modular group or $PSL(2, \mathbb{Z})$.

Tietze Transformation

In group theory, to transform a given finite presentation of a group into another - often simpler- finite presentation of the same group is through Tietze transformations. These transformations are named after H. F. F. Tietze who introduced them in a paper in 1908.

Let S_3 have the finite presentation as $< x, y : x^3 = y^2 = (xy)^2 = 1 >$. By using Tietze transformations, let $xy = z$ then the new presentation of S_3 is $< y, z : (zy)^3 = y^2 = z^2 = 1 >$.

Finite Field

An integral domain which have finitely many elements is called a field. These are finite fields and have an important role in many branches of mathematics, especially in group theory. The most common examples of finite fields are $\mathbb{Z}_p$ for prime p or power of a prime p. Finite fields can be uniquely determined by the number of elements it contains. That is, for every prime p and integer $r > 0$ there exist a finite field having $q = p^r$ elements. Such fields are also expressed as $GF(q)$ or F_q and known as Galois field with $q = p^r$ elements.

The ring $\mathbb{Z}$ of integers when quotient by its ideal $n\mathbb{Z}$ induces $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ the integer modulo n. If n is a prime then $\mathbb{Z}_n$ is in fact a field under this structure.

The construction of a finite field is illustrated through the following example.

Example 1 *$GF(3^2)$ is constructed by choosing an irreducible polynomial $f(t) = t^2 + 2t + 2$ over $\mathbb{Z}_3$. The elements of $GF(3^2)$ are listed as below.*

Elements of $GF(3^2)$	*Elements of $GF(3^2)$ modulo $f(t)$*
0	0
t	t
t^2	$t+1$
t^3	$2t+1$
t^4	2
t^5	$2t$
t^6	$2t+2$
t^7	$t+2$
t^8	1

Table−1: Elements of $GF(3^2)$

Projective Lines over Finite Fields

The one-dimensional projective space is called a projective line. A projective line over the finite fields F_q, contains the elements of $GF(q)$ together with the additional point ∞. That is, $PL(F_q) = F_q \cup \{\infty\}$. Similarly, $PL(\mathbb{Q})$ means the projective lne over rational field and $PL(\mathbb{Q}(\sqrt{n}))$ is projective line over the rational quadratic field.

Remark 2 *An element $x \in F_q$ (where $q = p^r$) is said to be a non-zero square in F_q if $x \equiv a^2 (\mathrm{mod}\, p)$ for some non-zero element a in F_q.*

As an example, consider $F_{23} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22\}$ in which $24 \equiv (22)^2 (\mathrm{mod}\, 23)$. Thus, 24 is a non-zero square in F_{23}.

In chapter two, we use the concept of triangle groups and generalized triangle groups, so we are now defining these important concepts.

Triangle Group

The free product of two cyclic groups of order l and m is represented as $< x, y : x^l = y^m = 1 >$. If the third relation is defined as some power (say n) of the product of x and y then the new group is formed known as triangle group. The triangle groups are denoted by $\Delta(l, m, n)$ and represented as $\Delta(l, m, n) =< x, y : x^l = y^m = (xy)^n = 1 >$ where l, m and n are integers greater than or equal to 1. The finiteness of the triangle groups is describe in [1] on the basis of l, m and n. If $\left(\frac{1}{l} + \frac{1}{m} + \frac{1}{n}\right) > 1$ then $\Delta(l, m, n)$ are finite and infinite otherwise. The triangle groups $\Delta(2, 3, n)$ are infinite if and only if $n \geqslant 6$. Whereas, for $n \leq 5$ the triangle groups are finite.

Generalized Triangle Group

A group G is called a generalized triangle group if it can be presented in the form $< x, y : x^l = y^m = w^n = 1 >$, where l, m, n are integers greater than or equal to 1 and $w = x^{r_1} y^{s_1} x^{r_2} y^{s_2} ... x^{r_k} y^{s_k}$, $(k \geq 1,\ 0 < r_i < l,\ 0 < s_i < m)$ and w is not a proper power. The generalized triangle group is infinite whenever $\left(\frac{1}{l} + \frac{1}{m} + \frac{1}{n}\right) \leq 1$ but for $\left(\frac{1}{l} + \frac{1}{m} + \frac{1}{n}\right) > 1$ the generalized triangle group may be finite. J. Howie, V.

Metaftsis and R. M. Thomas in [3] discuss finite generalized triangle groups with their presentations. They prove a remarkable result about the classification of all finite generalized triangle groups. They classifies all finite generalized triangle groups as follows.

Theorem 3 *Let* $G = < x, y : x^l = y^m = w^n = 1 >$ *be a finite generalized triangle group, where* $w = x^{r_1}y^{s_1}x^{r_2}y^{s_2}...x^{r_k}y^{s_k}$, $0 < r_i < l$, $0 < s_i < m$, w *is not a proper power, and* $k \geq 2$ *then up to equivalence* G *is one of the following:*

1. $< x, y : x^2 = y^3 = (xyxyxy^2xy^2)^2 = 1 >$ is of order 576;
2. $< x, y : x^2 = y^3 = (xyxyxy^2)^3 = 1 >$ is of order 1440;
3. $< x, y : x^3 = y^3 = (xyxy^2)^2 = 1 >$ is of order 180;
4. $< x, y : x^3 = y^3 = (xyx^2y^2)^2 = 1 >$ is of order 288;
5. $< x, y : x^2 = y^5 = (xyxy^2)^2 = 1 >$ is of order 120;
6. $< x, y : x^2 = y^5 = (xyxyxy^4)^2 = 1 >$ is of order 1200;
7. $< x, y : x^2 = y^5 = (xyxyxy^2xy^4)^2 = 1 >$ is of order 1200;
8. $< x, y : x^2 = y^4 = (xyxyxy^3)^2 = 1 >$ is of order 192;
9. $< x, y : x^2 = y^3 = (xyxy^2)^2 = 1 >$ is of order 24;
10. $< x, y : x^2 = y^3 = (xyxyxy^2)^2 = 1 >$ is of order 48;
11. $< x, y : x^2 = y^3 = (xyxyxyxy^2)^2 = 1 >$ is of order 120;
12. $< x, y : x^2 = y^3 = (xyxyxy^2xyxy^2)^2 = 1 >$ is of order 720;
13. $< x, y : x^2 = y^3 = (xyxyxyxyxy^2xy^2)^2 = 1 >$ is of order 2880;

or possibly

14. $< x, y : x^2 = y^3 = (xyxyxyxy^2xyxy^2xy^2)^2 = 1 >$, and

15. $< x, y : x^2 = y^5 = (xyxyxyxy^2xy^2xyxy^2xy^2)^2 = 1 >$.

Thus, the afore mentioned theorem is almost a complete classification of finite generalized triangle groups. However, the last two groups listed in the above theorem remain undecided as to whether they are finite or infinite. L. Levai, G. Rosenberger and B. Souvignier [4] investigate these two groups seperately. They prove that the group $< x, y : x^2 = y^3 = (xyxyxyxy^2xyxy^2xy^2)^2 = 1 >$ is finite and order of this group is 424673280 while the group $< x, y : x^2 = y^5 = (xyxyxyxy^2xy^2xyxy^2xy^2)^2 = 1 >$ is infinite. Thus, they include the finite group in the list of thirteen finite generalized triangle groups and complete the list of fourteen finite generalized triangle groups.

H. S. M. Coexter and W. O. J. Moser [1] describe the geometry of triangle groups by determining the sum $\frac{1}{l} + \frac{1}{m} + \frac{1}{n}$. In terms of l, m and n there are following three cases.

If $\frac{1}{l} + \frac{1}{m} + \frac{1}{n} = 1$ it is an ‘Euclidean case’. In this case, the triangle groups are infinite symmetric groups such as $\Delta(2,3,6), \Delta(2,4,4)$ and $\Delta(3,3,3)$. If $\frac{1}{l} + \frac{1}{m} + \frac{1}{n} > 1$ it is a ‘spherical case’. In this case, the triangle groups are finite symmetric groups such as $\Delta(2,3,2), \Delta(2,3,3), \Delta(2,3,4), \Delta(2,3,5)$ and $\Delta(2,2,4)$. If $\frac{1}{l} + \frac{1}{m} + \frac{1}{n} < 1$ it is ‘hyperbolic case’. In this case, the triangle groups are infinite symmetric groups. For example, $\Delta(2,3,7)$ is an infinite symmetric group. One can see more about generalized triangle groups in [5, 6] and about the groups generated by two operators in [7].

Modular Group

The modular group $PSL(2,\mathbb{Z})$ is a discrete group of motions in the lobachevsky plane. It is therefore possible to express the modular group as a group generated by two linear fractional transformations $x : z \longmapsto \frac{-1}{z}$ and $y : z \longmapsto \frac{-1}{z+1}$ such that $x^2 = 1$ and $y^3 = 1$ are its defining relations. That is, $PSL(2,\mathbb{Z}) =< x, y : x^2 = y^3 = 1 >$. It is therefore $PSL(2,\mathbb{Z})$ is a free product of the cyclic group of order 2 and the cyclic group of order 3. The product of the generators xy is the translation $z \longmapsto z + 1$. The linear fractional transformation $t : z \longmapsto \frac{1}{z}$ inverts x and y, that is, $t^2 = (xt)^2 = (yt)^2 = 1$ and so extends the group $PSL(2,\mathbb{Z})$ to $PGL(2,\mathbb{Z})$. The extended modular group $PGL(2,\mathbb{Z})$ is then generated by x, y and t. Thereupon, $PGL(2,\mathbb{Z}) =< x, y, t : x^2 = y^3 = t^2 = (xt)^2 = (yt)^2 = 1 >$

The $PSL(2,\mathbb{Z})$ is a normal subgroup of index two in $PGL(2,\mathbb{Z})$. If $\mathbb{Z}$ is replaced by the finite field F_q in $PGL(2,\mathbb{Z})$ then the group $PGL(2,q)$ is obtained with the linear fractional transformations $z \longmapsto \frac{az+b}{cz+d}$ where $a, b, c, d \in F_q$ and $ad - bc \neq 0$. Furthermore, the group $PSL(2,q)$ is the subgroup of $PGL(2,q)$.

The concept of action of a group G on a set X is fundamental in group theory. In succeeding chapter we take the action of different groups on finite fields. Therefore, to illustrate the concept, we give an example of action of group on a set.

Example 4 *Consider* $SL(2,\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_{2\times 2},\ \textit{where } a, b, c, d \in \mathbb{R},\ ad - bc = 1 \right\}$, *acting on the upper half plane* $\mathbb{C}^+ = \{z : \mathrm{Im}(z) > 0\}$ *as* $z \longmapsto \frac{az+b}{cz+d}$, *where the transformation represents the matrix* $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$

To see that $SL(2,\mathbb{R})$ *acts on* $\mathbb{C}^+$, *let* $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL(2,\mathbb{R})$ *such that* $ad-bc=1$. *For* $z \in \mathbb{C}^+$, *define* $z^A = \frac{az+b}{cz+d}$, *where* $\mathrm{Im}(\frac{az+b}{cz+d}) > 0$.

For if $z = x+iy$, *then*

$$\begin{aligned}
\tfrac{az+b}{cz+d} &= \tfrac{a(x+iy)+b}{c(x+iy)+d} = \tfrac{(ax+b)+i(ay)}{(cx+d)+i(cy)} \\
&= \tfrac{[(ax+b)+i(ay)][(cx+d)-i(cy)]}{[(cx+d)+i(cy)][(cx+d)-i(cy)]} \\
&= \tfrac{[acx^2+(ad+bc)x+bd+acy^2]+i[acxy+ady-axy-bcy]}{(cx+d)^2+(cy)^2} \\
&= \tfrac{[acx^2+(ad+bc)x+bd+acy^2]+i[ad-bc]y}{(cx+d)^2+(cy)^2}
\end{aligned}$$

and $\quad \mathrm{Im}(\frac{az+b}{cz+d}) = (ad-bc)y > 0$, *as* $y > 0$ *and* $ad-bc=1$.

Take $B = \begin{bmatrix} e & g \\ f & h \end{bmatrix} \in SL(2,\mathbb{R})$. *Here* $e,f,g,h \in \mathbb{R}$ *and* $eh-fg=1$.

Consider

$$\begin{aligned}
(z^A)^B = (\tfrac{az+b}{cz+d})^B = \tfrac{e(\frac{az+b}{cz+d})+g}{f(\frac{az+b}{cz+d})+h} &= \tfrac{e(az+b)+g(cz+d)}{f(az+b)+h(cz+d)} \\
&= \tfrac{(ea+gc)z+(eb+gd)}{(fa+hc)z+(fb+hd)}.
\end{aligned}$$

As

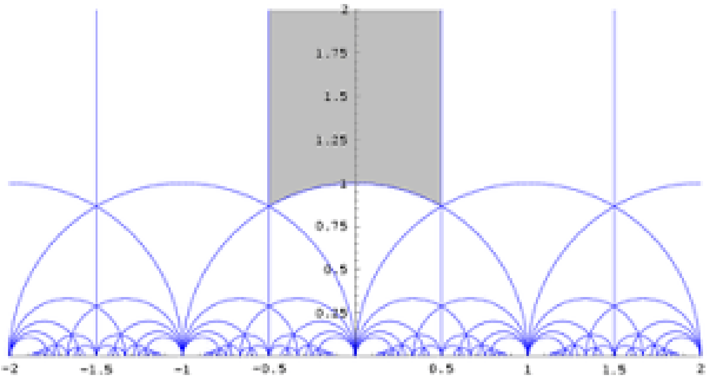
$$AB = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \begin{bmatrix} e & g \\ f & h \end{bmatrix} = \begin{bmatrix} ea+gc & fa+hc \\ eb+gd & fb+hd \end{bmatrix}$$

therefore $\quad (z^A)^B = z^{AB}$.

Since $\quad I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in SL(2,\mathbb{R})$,

therefore, it implies $\ \mathbb{Z}^I = \frac{1.\mathbb{Z}+0}{0.\mathbb{Z}+1} = \mathbb{Z}$.

The following diagram shows the fundamental domain for the action of $PSL(2,\mathbb{Z})$ on upper half plane.



Figure−1: *Fundamental Domain for the Action of* Modular Group on Upper half plane

Coset Diagrams

A. Cayley introduces the concept of a graph in relation with a group. He uses two different types of edges to present two generators of a finite group, namely S_3. The Cayley graph for a group represents the elements of the group. In fact, the vertices of the Cayley graph are the elements of the group. Whereas, O. Schreier generalizes this concept by introducing a graph whose vertices are the cosets of some subgroup of the group. Thus, in this way, Cayley diagrams become a special case of Schreier's coset diagram by taking trivial subgroup. H. S. M. Coxeter and W. O. J. Moser [1] use Cayley diagrams as well as Schreier's coset diagrams to prove some interesting results for finitely generated groups.

In 1970s, G. Higman introduces the concept of coset diagrams for the modular group in an interesting way. His doctoral student Q. Mushtaq discusses various actions of the modular group using these coset diagrams. Q. Mushtaq [8] gives a method known as Parametrization to draw a coset diagram of the triangle group $\Delta(2, 3, n)$ for $n \in \mathbb{N}$. He [9, 10] also discusses action of the modular group on real quadratic fields.

The coset diagram for $PSL(2,\mathbb{Z})$ is given below, in Figure-2. When $PSL(2,\mathbb{Z})$ acts on projective lines over the finite field, it means, there is a non-degenerate homomorphism from $PSL(2,\mathbb{Z})$ to $PSL(2,q)$. When either of the generator do not belong to the kernel of the homomorphism it is called non-degenerate homomorphism.

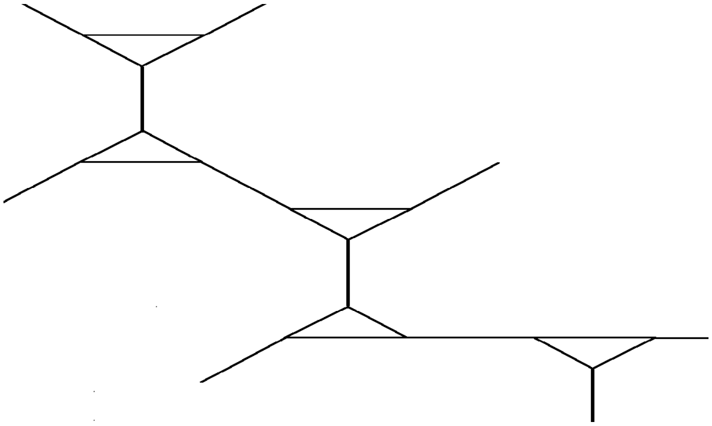


Figure 2: Coset Diagram for PSL(2,ℤ)

A coset diagram is connected if the corresponding action is transitive. That is, there exist only one orbit as a result of the action.

In $PSL(2,\mathbb{Z})$, the generator y (of order 3) represented by an edge of a triangle and so by y^3 it forms a triangle. Whereas, the generator x (of order 2) is represented by an edge. All directions are taken as counter clockwise. The fixed points of x or y, if they exist, are denoted by heavy dots. In $PGL(2,\mathbb{Z})$, the third generator t represents symmetry about the vertical axis.

For instance, consider the action of $PGL(2,\mathbb{Z})$ on $PL(F_{19})$. We find the permutation representations of $\overline{x}, \overline{y}$ and $\overline{t}$ from the linear transformations $x : z \longmapsto \frac{-1}{z}$, $y : z \longmapsto \frac{(z-1)}{z}$ and $t : z \longmapsto \frac{1}{z}$ respectively. Then,

$\overline{x}$: (1 18)(3 6)(0 ∞)(4 14)(7 8)(2 9)(10 17)(11 12)(5 15)(13 16)

$\overline{y}$: (2 10 18) (3 7 9) (0 ∞ 1) (4 15 6) (13 17 11) (5 16 14) (8) (12)

$\bar{t}$: (2 10) (4 5) (0 ∞) (6 16) (7 11) (3 13) (9 17) (14 15) (8 12) (1) (18)

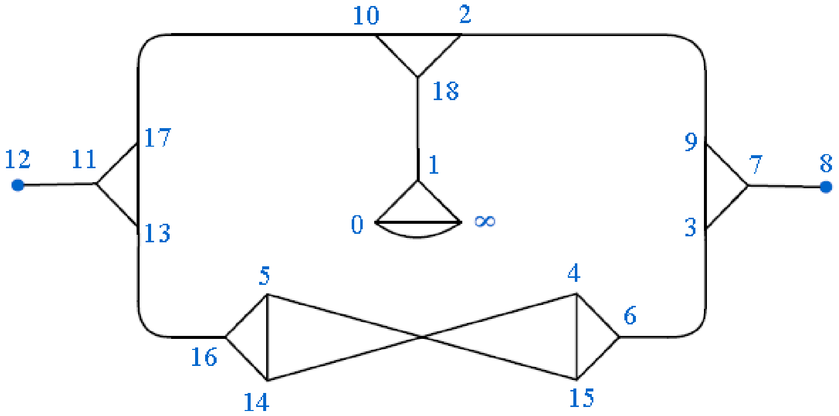


Figure 3: Action of PGL(2,$\mathbb{Z}$) on PL(F_{19})

Equivalent and non-equivalent words

A word w is defined as a finite sequence $x_1^{\epsilon_1}x_2^{\epsilon_2}...\ x_k^{\epsilon_k}$, where for each i, x_i belongs to the set of generators and each ϵ_i is either 1 or -1. Length of the word w is k in the above expression. 'Syllable' is a term also used by many researchers for the length of a word, but syllable of a word is particularly used for those words which are generated by the two generators. If a group is generated by two generators (say x and y) then for a word $w(x,y) = x^{r_1}y^{s_1}x^{r_2}y^{s_2}...x^{r_k}y^{s_k}$, the syllable is defined as the number of copies of $x^{p_i}y^{q_i}$ for $i \in \mathbb{N} \cup \{0\}$, appears in $w(x,y)$. In the word $w(x,y) = x^{r_1}y^{s_1}x^{r_2}y^{s_2}...x^{r_k}y^{s_k}$, syllable is k. We denote 'a word generated by x and y having syllable k' by $w_k(x,y)$.

Let w be a word, then by the deletion of all trivial relations (such as xx^{-1}, $x^{-1}x$, yy^{-1} and $y^{-1}y$) we get cyclically reduced form of the word. It is denoted by w^* in this dissertation. The cyclically reduced form of $w_k(x,y)$ is denoted by $w_k^*(x,y)$. In $PSL(2,\mathbb{Z})$, if $w\,(x,y)$ is a word generated by x and y then cyclically reduced form of the word is $w(x,y) = xy^{s_1}xy^{s_2}...xy^{s_k}, (k \geq 1,\ each\ s_i = 1\ or\ 2)$.

We need words generated by the generators of the modular group and their reduced forms in the upcoming chapters, so we are ellaborating these concepts here.

Example 5 *Let* $w = xy^2xyy^{-1}xx^2y^3$ *be a word. Then the reduced form of* w *in* $PSL(2,\mathbb{Z})$ *is* xy^2 *because*

$w = xy^2xyy^{-1}xx^2y^3 = xy^2x \cdot 1 \cdot x \cdot 1 \cdot 1 = xy^2x \cdot x = xy^2 \cdot 1 = xy^2.$

Example 6 *If* $w(x,y)$ *is a word generated by* x *and* y*, and the generators appear alternatively with powers of* y *as Fibonacci sequence then* $w_{57}(x,y)$ *is a word expressed as*

$$\begin{aligned} w_{57}(x,y) \;=\; & xyxyxy^2xy^3xy^5xy^8xy^{13}xy^{21}xy^{34}xy^{55}xy^{89}xy^{144}xy^{233}xy^{377}xy^{610}xy^{987} \\ & xy^{1597}xy^{2584}xy^{4181}xy^{6765}xy^{10946}xy^{17711}xy^{28657}xy^{46368}xy^{75025}xy^{121393} \\ & xy^{196418}xy^{317811}xy^{514229}xy^{832040}xy^{1346269}xy^{2178309}xy^{3524578}xy^{5702887} \\ & xy^{9227465}xy^{14930352}xy^{24157817}xy^{39088169}xy^{63245986}xy^{102334155}xy^{165580141} \\ & xy^{267914296}xy^{433494437}xy^{701408733}xy^{1134903170}xy^{1836311903}xy^{2971215073} \\ & xy^{4807526976}xy^{7778742049}xy^{12586269025}xy^{20365011074}xy^{32951280099}xy^{53316291173} \\ & xy^{86267571272}xy^{139583862445}xy^{225851433717}xy^{365435296162}. \end{aligned}$$

The reduced form of $w_{57}(x,y)$ *in the modular group is*

$$\begin{aligned} w^*_{57}(x,y) \;=\; & xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2 \\ & xyxyxy^2xy^2. \end{aligned}$$

According to J. Howie, V. Metaftsis and R. M. Thomas [3], two cyclically reduced words $w, w' \in \mathbb{Z}_p * \mathbb{Z}_q$ are equivalent if one is transformed to the other by (i) Automorphism of $\mathbb{Z}_p$ or of $\mathbb{Z}_q$ (ii) Cyclic permutation (iii) Inversion (iv) Interchanging the two free factors (if $p = q$).

According to Y. T. Ulutas and I. N. Cangul [11], 'two words w and w' are called equivalent if one of them (say w') is obtained from the word $w = x^{p_1}y^{q_1}x^{p_2}y^{q_2}\ldots\, x^{p_n}y^{q_n}$ by cutting some part from the beginning and pasting it at the end (or equivalently cutting some part from the end and pasting it in the beginning) in the same order.'

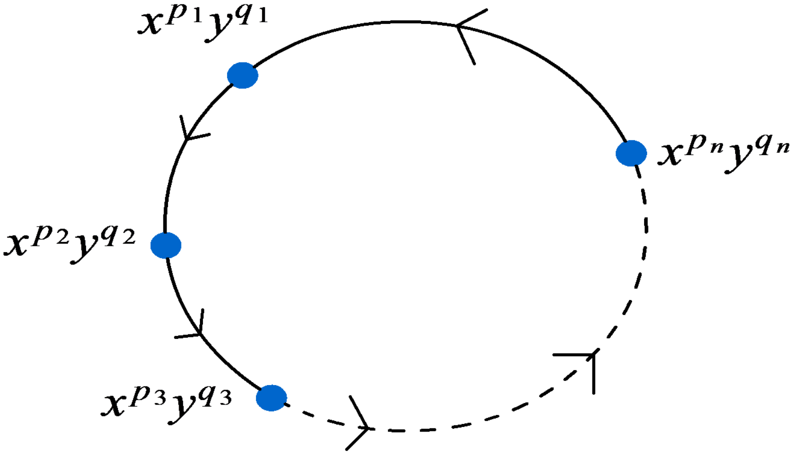


Figure 4: Cyclically Equivalent Words

In other words, if the word generated by the two generators x and y is of the form $w(x, y) = x^{r_1}y^{s_1}x^{r_2}y^{s_2}\ldots\, x^{r_k}y^{s_k}$, then any word start from $x^{r_i}y^{s_i}$ and ends at $x^{r_{i-1}}y^{s_{i-1}}$ is equivalent to the word $w(x, y)$, where i is the index of p and q in the word $w(x, y)$. For example, the words $x^{r_2}y^{s_2}x^{r_3}y^{s_3}\ldots\, x^{r_k}y^{s_k}x^{r_1}y^{s_1}$ and $x^{r_3}y^{s_3}x^{r_4}y^{s_4}\ldots x^{r_k}y^{s_k}x^{r_1}y^{s_1}x^{r_2}y^{s_2}$ are equivalent to $w(x, y) = x^{r_1}y^{s_1}x^{r_2}y^{s_2}\ldots\, x^{r_k}y^{s_k}$.Any two words which do not satisfy any of the above definitions are called non-equivalent words.

Example 7 *Let $w = xyxyxy^2xy^3$ be a word then the words $xy^3xyxyxy^2$, xy^2xy^3xyxy and $xyxy^2xy^3xy$ are equivalent to w. Whereas, the words $xyxy^2xyxy^3$, $xyxy^3xy^2xy$ and xy^3xyxy^2xy are non-equivalent to the word w.*

Quotient of a group

Let G be a group with finite presentation as $G =< S, R >$ where S be the set of generators and R the set of relations. If an additional relation, which is generated by the generators of G, inserted in the finite presentation of G then the new structure is called a quotient of the group.

If the group $PSL(2, \mathbb{Z})$ is finitely presented as $< x, y : x^2 = y^3 = 1 >$ and $w(x, y)$ is a word generated by x and y; the generators of $PSL(2, \mathbb{Z})$, then $< x, y : x^2 = y^3 = w(x, y) = 1 >$ is a quotient of the modular group.

Theorem 8 *If w and w' are two equivalent words then inclusion of w and w' in finite presentation of a group provides same quotients of the group.*

It is important to mention here that x and y, whenever they appear in this dissertation, varies from group to group. In particular, they are obviously not the generators of the modular group.

Chapter 2

Survey of One Relator Quotients

By inclusion of an additional relation in the existing relations of a group, we get a quotient of the group. In this chapter, we give a short but comprehensive survey of one relator quotients generally and one relator quotients of the modular group particularly. This study not only comprises on the results but also on the methodology adopted by different scholars in different times.

The study of one relator quotients of a group begins in 1901, while G. A. Miller [7] uses finite presentations for describing groups generated by two operators. These finite presentations gives a new dimension for the study of groups. G. A. Miller in his another significant paper [12] describes quotients of a two generator group where the additional relation is defined as some power of product of the two generators. In other words, G. A. Miller considers triangle groups as one relator quotients of two-generator groups. M. D. E. Conder [13] also investigates one relator quotients of the modular group.

M. Edjvet [14] discusses certain quotients of triangle groups defined as $(m, n, p; q) =<$

$x, y : x^m = y^n = (xy)^p = [x, y]^q = 1 >$. Here $[x, y]$ as usual is the commutator $x^{-1}y^{-1}xy$. This work is motivated by the work of J. Howie and R. M. Thomas who obtain necessary and sufficient condition for $(2, 3, p; q)$ to be finite, apart from two cases, $(2, 3, 13; 4)$ and $(2, 3, 7; 11)$. He obtains a necessary and sufficient condition for $(m, n, p; q)$ to be finite. He also discusses whether or not $(2, 3, 13; 4)$ and $(2, 3, 7; 11)$ are finite. In his main theorem of finite quotients of the triangle groups, five out of fourteen are two-relator quotients of the modular group.

V. Metaftsis and I. Miyamoto [15] investigate one relator quotients of the group defined by the product of two cyclic groups of order 3, that is, $< x, y : x^3 = y^3 = 1 >$. This work is greatly inspired by [13] and they follow the same scheme as in [13] for finding quotients of the group. They state: ‘In this paper we conduct a similar investigation on the abstract group $< x, y : x^3 = y^3 = 1 >$; we determine all possible equivalence classes of presentations for three relator quotients for a third relator of length at most 14 and we find order of all quotients. If the length of the third relator is increased to 16 the number of quotients is increased from 181 to 618 and it appears to be too great a task to present the results in the present paper.’ They also use a computer program to analyze the quotients. This program creates all possible combinations for all the different sizes of the third relator and then it reduces the list using the cyclic permutations of each additional relation and of automorphisms of $\mathbb{Z}_3 * \mathbb{Z}_3$. Specifically, this program compares each different word and its cyclic permutations with all the other words and chooses one presentation from each equivalence class. The well-known software CAYLEY and ‘Groups, Algorithms and Programming’ (GAP) are used for identification of quotients.

In two-generator groups, modular group is one of the most important and most studied group. Furthermore, in the documentation for the award of Abel Prize in 2009, modular group was described as an important group. One relator quotients of the modular group are of special importance due to the dynamic characteristics of the modular group. Also, the modular group is a two-generator group, so the addition of a relation converts it into a member of a class of generalized triangle groups. Therefore, the one relator quotients of the modular group can also be viewed as a class of generalized triangle groups.

Now the focus is-particularly-on one relator quotients of the modular group. For this we discuss three major approaches, namely:

1. Tietze Transformation Method
2. Ulutas and Cangul's approach
3. Allotrope of Carbon and Quotient of the Modular group

2.1 Tietze Transformation Method

Use of Tietze transformations is an important technique to find another presentation from one presentation of a group. M. D. E. Conder [13] use this technique to find quotients of the modular group by inserting one additional relation in the finite presentation of the group. He is of the view that if we determine order of the quotient then description of the quotient is not a difficult task. By using Tietze transformations as $u = xy$ and $v = xy^{-1}$ another presentation of the modular group is $< u, v : (vu^{-1}v)^2 = (u^{-1}v)^3 = 1 >$ where $x = xy^{-1}y^{-1}x^{-1}xy^{-1} = vu^{-1}v$ and

$y = y^{-1}x^{-1}xy^{-1} = u^{-1}v$, he looks up to the one relator quotients of the modular group in the form $< u, v : (vu^{-1}v)^2 = (u^{-1}v)^3 = w(u, v) = 1 >$ and he gives a complete list of one relator quotients of the modular group with length of $w(u, v)$ up to 24.

$L(w(u,v))$	Additional Relation	Group order	Description
1	u	1	$Trivial$
2	u^2	6	S_3
2	uv	6	C_6
3	u^3	12	A_4
3	u^2v	1	$Trivial$
4	u^4	24	S_4
4	u^3v	2	C_2
4	u^2v^2	18	$C_3 \times S_3$
4	$(uv)^4$	24	$C_2 \times A_4$
5	u^5	60	A_5
5	u^4v	3	C_3
5	u^3v^2	1	$Trivial$
5	u^2vuv	1	$Trivial$
6	u^6	$Infinite$	$Triangle\ group$
6	u^5v	2	C_2
6	u^4v^2	6	S_3

$L(w(u,v))$	Additional Relation	Group order	Description
6	u^3v^3	48	$C_4 \sim A_4$
6	u^3vuv	2	C_2
6	u^2v^2uv	42	$C_7 \sim C_6$
6	$(u^2v)^2$	48	$C_2 \sim S_4$
6	$(uv)^3$	$infinity$	$[3^+, 6]$
7	u^7	$infinite$	$Triangle\ group$
7	u^6v	1	$Trivial$
7	u^5v^2	3	C_3
7	u^4v^3	1	$Trivial$
7	u^4vuv	12	A_4
7	u^3v^2uv	1	$Trivial$
7	u^3vu^2v	3	C_3
7	$u^2v^2u^2v$	1	$Trivial$
7	u^2vuvuv	1	$Trivial$

Table 1: One Relator Quotients of PSL(2,Z) upto the Length 7

M. Conder, G. Havas and M. F. Newman [16] extend work of [13]. They investigate all such one relator quotients of the modular group where the additional relator is of length up to 36. Up to equivalence, there are 8296 more presentations and they determine the order of all except five of the quotients which are the following.

$$< u, v : (vu^{-1}v)^2 = (u^{-1}v)^3 = u^4vuv^4u^3vuv^3 = 1 >$$

$$< u, v : (vu^{-1}v)^2 = (u^{-1}v)^3 = u^4v^2u^2v^4u^2vuv^2 = 1 >$$

$$< u, v : (vu^{-1}v)^2 = (u^{-1}v)^3 = u^3vu^2vu^2v^2uv^2uv^3 = 1 >$$

$$< u, v : (vu^{-1}v)^2 = (u^{-1}v)^3 = u^3vu^2v^2uv^3u^2vuv^2 = 1 >$$

$$< u, v : (vu^{-1}v)^2 = (u^{-1}v)^3 = u^3vuvuv^3u^2vuvuv^2 = 1 > .$$

Most of their results are based on computer calculations. They use MAGMA which provides excellent facility in identifying groups.

Thus, by Tietze transformations approach, one relator quotients of the modular group are discussed with length up to 36 and five quotients are left without identification.

2.2 Ulutas and Cangul's Approach

Y. T. Ulutas and I. N. Cangul [17] investigate quotients of one of the Hecke group $H\left(\frac{1+\sqrt{5}}{2}\right) =< x, y : x^2 = y^5 = 1 >$ by inserting one additional relation. They consider the additional relation up to the length 25. Y. T. Ulutas and I. N. Cangul [11] find one relator quotients of $PSL(2, \mathbb{Z})$ by inserting additional relation up to the length 21. They use a different technique than that of [13]. However, their work of [17] and [11] are not comprehensive nor fully correct. In [11], they find number of one relator quotients of the modular group by developing two formulae. By considering k as number of x and l as number of y in $w(x, y)$, the number of cyclically reduced words are equal to $\begin{pmatrix} k \\ \\ l-k \end{pmatrix}$ and number of cyclically reduced non-equivalent words are equal to $\frac{1}{k}\left\{ \underset{d \mid (k,l-k)}{\Sigma} \left[\varphi(d) \begin{pmatrix} \frac{k}{d} \\ \\ \frac{l-k}{d} \end{pmatrix} \right] \right\}$. They consider generators x and y as white and black beads in a necklace and total number of possible ways to form a necklace for certain number of x and y is the number of cyclically reduced non-equivalent words.

H. B. Ozdemer, Y. T. Ulutas and I. N. Cangul [18] find normal subgroups of the Hecke group $H\left(\sqrt{2}\right) =< x, y : x^2 = y^4 = 1 >$ and also investigate one relator quotients of $H\left(\sqrt{2}\right)$. They use additional relations having length up to 19.

M. Aslam, A. Ali and R. Ahmad [19] investigate one relator quotients of another Hecke group $H\left(\sqrt{3}\right) =< x, y : x^2 = y^6 = 1 >$. They used the technique of [11] and gave a comprehensive list of the quotients. They insert additional relation up to the length 24. This completes the study of one relator quotients of well known Hecke groups. But the length of the additional relation is point of concern, which is finite in all above investigations.

2.3 Allotrope of Carbon and Quotient of the Modular group

P. E. Schupp and I. Kapovich [20] prove that quotients of the modular group satisfy a strong Mostow-type rigidity. The Cayley graph is the associated geometric structure of such a quotient. Furthermore, isometry of the Cayley graphs shows the corresponding quotients are isomorphic.

A. Torstensson [21] use coset diagrams to study quotients of finitely presented groups. In the first part, they describe couple of different applications of coset diagrams to study finitely presented groups. In the second part, they confine themselves to one relator quotients of the modular group. Thus, the diagrammatic study is also a useful aspect of the study of one relator quotients of the modular group.

Q. Mushtaq and A. Rafiq [22] consider the triangle group $\Delta(2,3,5)$ as an allotrope of carbon (Fullerene C_{60}) and they prove very interesting results. The coset diagrams for the action of $PSL(2,\mathbb{Z})$ on $PL(F_{5^n})$ depicts the diagrammatic analogs of the Fullerene C_{60}. By taking action of $PSL(2,\mathbb{Z})$ on $PL(F_{5^n})$ and using Burnside's lemma they count the number of blocks of the adjacency matrix seperately for n to be even or odd. Here, blocks of the adjancy matrix shows number of orbits occur in this action.

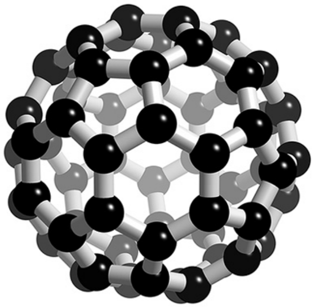


Figure 5: *Fullerene* C_{60}

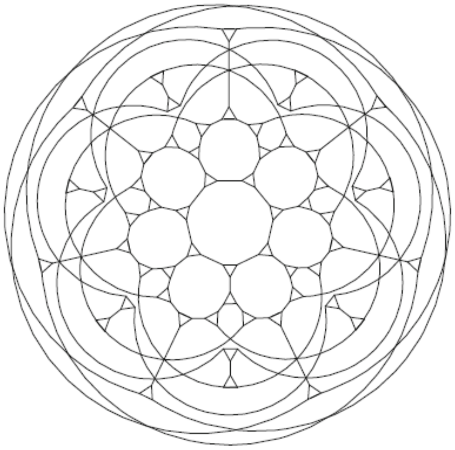
In Figure-5, the similarity of the Fullerene C_{60} and the triangle group $\Delta(2,3,5)$ is viewable easily. The black balls are considered as y^3 whereas the edges between the balls represent the generator x.

Q. Mushtaq and N. Mumtaz [23] investigate another triangle group $\Delta(2,3,7)$ whose structure is similar to another carbon allotrope $D168$ Shewarzite. They not only discuss the number of orbits of the action of $PSL(2,\mathbb{Z})$ on $PL(F_{7^n})$ but also some topological properties of the triangle group $\Delta(2,3,7)$. The action of $PSL(2,\mathbb{Z})$ on $PL(F_{7^n})$ gives the triangle group $\Delta(2,3,7)$ whose coset diagram is similar to the structure of $D168$. One of the important theorem of [23] in which authors describe the similarity of the structure $D168$ with the triangle group $\Delta(2,3,7)$ is given below.

Theorem 9 *If $PSL(2,\mathbb{Z})$ acts on $PL(F_{7^n})$, then*

$$\begin{aligned}\left|Orb_{PL(F_{7^n})}PSL(2,7)\right| &= 1+\frac{(7^n+1)-8}{168} \text{ if } n \text{ is odd}\\ \left|Orb_{PL(F_{7^n})}PSL(2,7)\right| &= 2+\frac{(7^n+1)-50}{168} \text{ if } n \text{ is even}\end{aligned}$$

The orbits of the coset diagram when $PSL(2,\mathbb{Z})$ acts on $PL(F_{7^n})$ for $n \geq 3$ are closely related to the structure of $D168$ Schwarzite. The transitive action of $PSL(2,\mathbb{Z})$ on $PL(F_7)$ gives an orbit γ_1 having 8 vertices. For $n = 2$, $PSL(2,\mathbb{Z})$ acts on $PL(F_{7^2})$ obtaining two orbits γ_1 and γ_2 where γ_2 have 42 vertices. When $PSL(2,\mathbb{Z})$ acts on $PL(F_{7^n})$ for $n \geq 3$, we obtain orbits γ_1, γ_2 and copies of γ_3. The orbit γ_3 and $D168$ Shwarzite both have genus 3, so these are topologically same.



Figure–6: Orbit γ_3 in the Action of PSL(2,Z) on $PL(F_{7^n})$

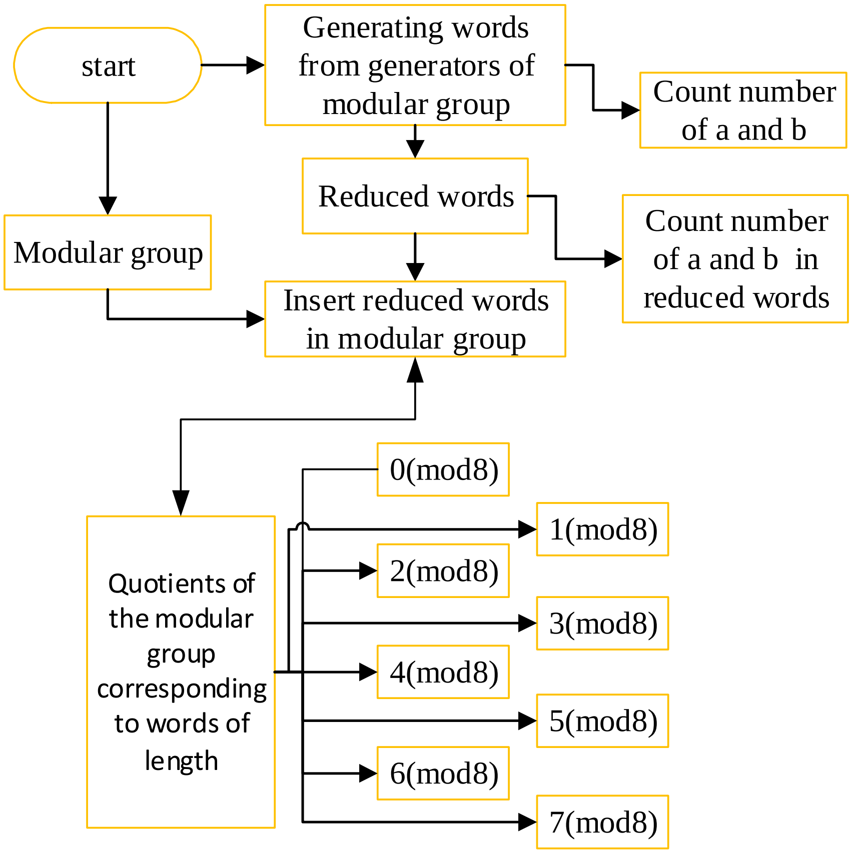
Thus, by summarizing the entire discussion, the triangle groups $\Delta(2,3,5)$ and $\Delta(2,3,7)$ are one relator quotients of the modular group which are viewed as isotopes of the carbon atom. Hence, the triangle group $\Delta(2,3,k)$ occurs as a useful subgroup of the homomorphic image of the modular group.

Conclusion 10 *In the entire discussion of one relator quotients of a group, syllable of the additional relation is the centre point of concern. By using different techniques, researchers find one relator quotients of different groups. But no one could find all one relator quotients of any group and particularly of the modular group. There is a limitation of the syllable of the additional relation while finding one relator quotients of the group. We try to deal with this limitation up to a certain level in this dessertation in the next chapters.*

Chapter 3

Additional Relation and The Fibonacci Sequence

Our aim is to study a class of generalized triangle groups as quotients of the modular group. Since, modular group is a two generator group, we insert an additional relation of the form $w(x,y) = x^{r_1}y^{s_1}x^{r_2}y^{s_2}...x^{r_k}y^{s_k}$ in the finite presentation of the group. By insertion of $w(x,y)$, the new presentation is $< x, y : x^2 = y^3 = w(x,y) = 1 >$ which is one relator quotient of the modular group as well as a class of generalized triangle groups. To study the above class of one relator quotients of the modular group, we divide the problem into two parts. Firstly, we find additional relations for all syllables. Secondly, we insert these (infinite) additional relations in the finite presentation of the modular group and investigate the quotients. In chapter three, we solve the first part of the problem while in chapter four, we investigate the later part of the problem. The following flowchart diagram shows the scheme of getting one relator quotients of $PSL(2,\mathbb{Z})$.


start
Generating words from generators of modular group
Count number of a and b
Reduced words
Count number of a and b in reduced words
Modular group
Insert reduced words in modular group
Quotients of the modular group corresponding to words of length
0(mod8)
1(mod8)
2(mod8)
3(mod8)
4(mod8)
5(mod8)
6(mod8)
7(mod8)

Flow Chart–1: Scheme for One Relator Quotients of Modular Group

The word $w(x, y)$ is the centre point of discussion. Without loss of generality, $w(x, y)$ begins from x and ends at y, That is $w(x, y) = x^{r_1}y^{s_1}x^{r_2}y^{s_2}...x^{r_k}y^{s_k}$ where r_i is 0 or 1 and s_i is $0, 1$ or 2. If $r_i = 0$ then x^{r_i} vanishes similarly if s_i= 0 then y^{s_i} vanishes. Thereupon, the choice we left for r_i is 1 and for s_i it is 1 or 2. Here, if we let $r_i = 1$ then $w(x, y)$ will be of the form $w(x, y) = xy^{s_1}xy^{s_2}...xy^{s_k}$. Since, it is matter of confusion that where we place $s_i = 1$ and where $s_i = 2$. So, in this situation, we use Fibonacci sequence and place the powers of y as terms of Fibonacci sequence in an order. Because of the relation $y^3 = 1$ the higher powers of y ultimately reduces to y^0, y^1 or y^2 and occurs on different places. Thus, instead of placing $0, 1, 2$ in powers of y by our own choice, Fibonacci sequence provides an arrangement. Therefore, the general form of $w(x,y)$ is $xy^1xy^1xy^2xy^3...xy^k$ where k is k^{th} term of Fibonacci sequence. Thus, we are inquiring the class of one relator quotients of the modular group which is of the form $< x, y : x^2 = y^3 = xy^1xy^1xy^2xy^3...xy^k = 1 >$ where k is the k^{th} term of the Fibonacci sequence**.** In this chapter our discussion is about $w(x,y) = xy^1xy^1xy^2xy^3...xy^k = 1$.

It is important to mention here that if we take all possible variations of powers of y (which are $0, 1, 2$) on all places, this will become a giant problem and beyond the scope of a PhD thesis. Also, we are discussing a class of generalized triangle groups so by Fibonacci sequence we get a class of generalized triangle groups as one relator quotients of the modular group. However, up to certain syllable we discuss $w(x,y)$ with all variations of powers of y in chapter 5 and obtain some interesting and worthy results. It is noteworthy that, now and onwards, whenever we write $w(x,y)$ it means the word is generated by the generators of the modular group.

3.1 Design of Algorithm for Generating Words of all Syllables

In this section, we generate words of all syllables. For this, we develop an algorithm by which we generate words. The algorithm is constructed in visual basic.net and we have used data type of maximum range, that is, 64 bits. The 64 bits have the range 0 to 18446744073709551615 which is a large number and it provides sufficiently large number of $w(x,y)$. This algorithm gives four outputs; words of all syllable, reduced form of the words, count of the number of generators x and y (as alphabets) in words and in their respective reduced forms. Finally, the words are divided into the classes up to the equivalence of their syllable. The sequence of Fibonacci numbers plays vital role in this classification of words.

Characteristics involved in the Algorithm

The algorithm is based on the following characteristics.

1. It starts constructing words with x^1y^1.

2. The strings of the words are of the form $w(x,y) = xy^1xy^1xy^2xy^3\ldots xy^k$ where powers of y are Fibonacci numbers.

3. The syllable of the string is any positive integer ‘n’.

4. If power of $x(=c)$ is more than 1, it uses $c(mod2)$ and if power of $y(=d)$ is more than 2 then $d(mod3)$.

5. It counts number of x and y in words.

6. It counts number of x and y in reduced form of the words.

Algorithm

```
Imports System.Numerics

Module Module1

Sub Main()

’ process(str)

Dim fstr As String = "x1y1"

’For i = 70 To 100

’ Console.WriteLine(i & " " & fibiter(i).ToString)
```

```
’Next
’Console.ReadKey()
Dim objWriter As New System.IO.StreamWriter("a.txt")
For i = 2 To 90
fstr = fstr & "," & "x1y" & fibiter(i).ToString
’Console.WriteLine("{0,3} {1}", i, fstr)
fstr = process(fstr, 0)
Dim orig = origstr(i)
Console.Write("{0,3} {1,-140}", i, output(fstr))
objWriter.Write("{0,3} {1,-140}", i, output(fstr))
Console.WriteLine("({0},{1}) -> ({2},{3})", CountCharacter(orig, "x"), countB(orig), CountCharacter(fstr, "x"), countB(fstr))
objWriter.WriteLine("({0},{1}) -> ({2},{3})", CountCharacter(orig, "x"), countB(orig), CountCharacter(fstr, "x"), countB(fstr))
’ objWriter.WriteLine("{0}", orig)
If (i + 2) Mod 4 = 0 Then
Console.WriteLine("")
objWriter.WriteLine(vbCrLf)
End If
Next
objWriter.Close()
’ output(fstr)
Console.ReadKey()
```

```
End Sub
Function fibiter(n As UInt64) As BigInteger
If n = 1 Or n = 2 Then
Return 1
Else
Dim num1, num2, sum As New BigInteger
num1 = 1
num2 = 1
sum = num1 + num2
Dim i As UInt64
For i = 3 To n
sum = num1 + num2
num1 = num2
num2 = sum
Next
Return sum
End If
End Function
Function origstr(n As UInt64)
Dim fstr = "x1y1"
Dim i As UInt64
For i = 2 To n
fstr = fstr & "," & "x1y" & fibiter(i).ToString
```

```
Next
Return fstr
End Function
Function countB(str As String) As BigInteger
Dim strtokens As String() = str.Split(",")
Dim y As BigInteger = 0
For Each tok As String In strtokens
Dim c As String = tok.Substring(3, tok.Length - 3)
y += BigInteger.Parse(c)
Next
Return y
End Function
Function output(str As String) As String
Dim strtokens As String() = str.Split(",")
Dim nstr As String = ""
For Each tok As String In strtokens
Dim c As String = tok.Substring(3, tok.Length - 3)
nstr += "xy" & If(c = "1", "", c)
Next
Return nstr
End Function
Public Function CountCharacter(ByVal value As String, ByVal ch As Char) As UInt64
```

```
Dim cnt As UInt64 = 0
For Each c As Char In value
If c = ch Then cnt += 1
Next
Return cnt
End Function
Function fibonacci(n As UInt64) As UInt64
If n = 1 Or n = 2 Then
Return 1
Else
Return fibonacci(n - 1) + fibonacci(n - 2)
End If
End Function
Function process(Str As String, op As Boolean) As String
Dim orig = Str
If op Then
Console.WriteLine("original: " & orig)
End If
Dim i As UInt64 = 0
”loop
Dim prev As String = ""
While (Not Str = prev)
prev = Str
```

```
”remlast
Dim strtokens As String() = Str.Split(",")
Dim c As BigInteger = BigInteger.Parse(strtokens(strtokens.Count - 1).Substring(3, strtokens(strtokens.Count - 1).Length - 3))
’Console.WriteLine("the value is {0}", c)
Str = Str.Substring(0, Str.Length - c.ToString().Length)
If (c Mod 3) = 0 Then
c = 3
Else
c = c Mod 3
End If
Str = Str + c.ToString()
”rem mid y
strtokens = Str.Split(",")
Dim newstr1 As String = ""
For i = 0 To strtokens.Count - 2
c = BigInteger.Parse(strtokens(i).Substring(3, strtokens(i).Length - 3))
c = c Mod 3
newstr1 = newstr1 & strtokens(i).Substring(0, 3) & c.ToString() & ","
Next
newstr1 = newstr1 & strtokens(strtokens.Count - 1)
Str = newstr1
Str = Str.Trim(",")
```

```
’
If op Then
Console.WriteLine("modding y: " & Str)
End If
”rem mid y0
strtokens = Str.Split(",")
newstr1 = ""
Dim d As UInt64
For i = 0 To strtokens.Count - 2
c = BigInteger.Parse(strtokens(i).Substring(3, strtokens(i).Length - 3))
If c = 0 Then
d = Convert.ToUInt64(strtokens(i).Substring(1, 1)) + Convert.ToUInt64(strtokens(i + 1).Substring(1, 1))
newstr1 = newstr1 & "x" & CStr(d) & "y" & Convert.ToUInt64(strtokens(i + 1).Substring(3, strtokens(i + 1).Length - 3)) & ","
i = i + 1
Else
newstr1 = newstr1 & strtokens(i) & ","
End If
Next
If Not i = strtokens.Count Then
newstr1 = newstr1 & strtokens(strtokens.Count - 1)
End If
```

```
Str = newstr1
Str = Str.Trim(",")
’
If op Then
Console.WriteLine("remvng y0: " & Str)
End If
”join mid x
strtokens = Str.Split(",")
newstr1 = ""
For i = 0 To strtokens.Count - 1
c = Convert.ToUInt64(strtokens(i).Substring(1, 1))
If c > 1 Then
c = c Mod 2
newstr1 = newstr1 & "x" & c.ToString() & strtokens(i).Substring(2, strtokens(i).Length
- 2) & ","
Else
newstr1 = newstr1 & strtokens(i) & ","
End If
Next
Str = newstr1
Str = Str.Trim(",")
’
If op Then
```

```
Console.WriteLine("modd x: " & Str)
End If
’rem x0
strtokens = Str.Split(",")
newstr1 = ""
For i = 0 To strtokens.Count - 2
c = Convert.ToUInt64(strtokens(i + 1).Substring(1, 1))
If c = 0 Then
d = Convert.ToUInt64(strtokens(i).Substring(3, strtokens(i).Length - 3)) + Convert.ToUInt64(strtokens(i + 1).Substring(3, strtokens(i + 1).Length - 3))
newstr1 = newstr1 & "x" & Convert.ToUInt64(strtokens(i).Substring(1, 1)) & "y" & d & ","
i = i + 1
Else
newstr1 = newstr1 & strtokens(i) & ","
End If
Next
If Not i = strtokens.Count Then
newstr1 = newstr1 & strtokens(strtokens.Count - 1)
End If
Str = newstr1
Str = Str.Trim(",")
’
```

```
If op Then
Console.WriteLine("remvng x0: " & Str)
End If
End While
Return Str
End Function
End Module
```

(This space is left due to a table on the next page)

The following Table-2 and Table-3 show the outcomes of the algorithm.

Syllable	Word
1	xy
2	$xyxy$
3	$xyxyxy^2$
4	$xyxyxy^2xy^3$
5	$xyxyxy^2xy^3xy^5$
6	$xyxyxy^2xy^3xy^5xy^8$
7	$xyxyxy^2xy^3xy^5xy^8xy^{13}$
8	$xyxyxy^2xy^3xy^5xy^8xy^{13}xy^{21}$
9	$xyxyxy^2xy^3xy^5xy^8xy^{13}xy^{21}xy^{34}$
10	$xyxyxy^2xy^3xy^5xy^8xy^{13}xy^{21}xy^{34}xy^{55}$
11	$xyxyxy^2xy^3xy^5xy^8xy^{13}xy^{21}xy^{34}xy^{55}xy^{89}$
12	$xyxyxy^2xy^3xy^5xy^8xy^{13}xy^{21}xy^{34}xy^{55}xy^{89}xy^{144}$
13	$xyxyxy^2xy^3xy^5xy^8xy^{13}xy^{21}xy^{34}xy^{55}xy^{89}xy^{144}xy^{233}$
14	$xyxyxy^2xy^3xy^5xy^8xy^{13}xy^{21}xy^{34}xy^{55}xy^{89}xy^{144}xy^{233}xy^{377}$
15	$xyxyxy^2xy^3xy^5xy^8xy^{13}xy^{21}xy^{34}xy^{55}xy^{89}xy^{144}xy^{233}xy^{377}xy^{610}$
16	$xyxyxy^2xy^3xy^5xy^8xy^{13}xy^{21}xy^{34}xy^{55}xy^{89}xy^{144}xy^{233}xy^{377}xy^{610}xy^{987}$
17	$xyxyxy^2xy^3xy^5xy^8xy^{13}xy^{21}xy^{34}xy^{55}xy^{89}xy^{144}xy^{233}xy^{377}xy^{610}xy^{987}xy^{1597}$
18	$xyxyxy^2xy^3xy^5xy^8xy^{13}xy^{21}xy^{34}xy^{55}xy^{89}xy^{144}xy^{233}xy^{377}xy^{610}xy^{987}xy^{1597}xy^{2584}$
19	$xyxyxy^2xy^3xy^5xy^8xy^{13}xy^{21}xy^{34}xy^{55}xy^{89}xy^{144}xy^{233}xy^{377}xy^{610}xy^{987}xy^{1597}xy^{2584}xy^{4181}$
20	$xyxyxy^2xy^3xy^5xy^8xy^{13}xy^{21}xy^{34}xy^{55}xy^{89}xy^{144}xy^{233}xy^{377}xy^{610}xy^{987}xy^{1597}xy^{2584}xy^{4181}xy^{6765}$

21	$xyxyxy^2xy^3xy^5xy^8xy^{13}xy^{21}xy^{34}xy^{55}xy^{89}xy^{144}xy^{233}xy^{377}xy^{610}xy^{987}xy^{1597}xy^{2584}xy^{4181}$
	$xy^{6765}xy^{10946}$
22	$xyxyxy^2xy^3xy^5xy^8xy^{13}xy^{21}xy^{34}xy^{55}xy^{89}xy^{144}xy^{233}xy^{377}xy^{610}xy^{987}xy^{1597}xy^{2584}xy^{4181}$
	$xy^{6765}xy^{10946}xy^{17711}$
23	$xyxyxy^2xy^3xy^5xy^8xy^{13}xy^{21}xy^{34}xy^{55}xy^{89}xy^{144}xy^{233}xy^{377}xy^{610}xy^{987}xy^{1597}xy^{2584}xy^{4181}$
	$xy^{6765}xy^{10946}xy^{17711}xy^{28657}$
24	$xyxyxy^2xy^3xy^5xy^8xy^{13}xy^{21}xy^{34}xy^{55}xy^{89}xy^{144}xy^{233}xy^{377}xy^{610}xy^{987}xy^{1597}xy^{2584}xy^{4181}$
	$xy^{6765}xy^{10946}xy^{17711}xy^{28657}xy^{46368}$
25	$xyxyxy^2xy^3xy^5xy^8xy^{13}xy^{21}xy^{34}xy^{55}xy^{89}xy^{144}xy^{233}xy^{377}xy^{610}xy^{987}xy^{1597}xy^{2584}xy^{4181}$
	$xy^{6765}xy^{10946}xy^{17711}xy^{28657}xy^{46368}xy^{75025}$
26	$xyxyxy^2xy^3xy^5xy^8xy^{13}xy^{21}xy^{34}xy^{55}xy^{89}xy^{144}xy^{233}xy^{377}xy^{610}xy^{987}xy^{1597}xy^{2584}xy^{4181}$
	$xy^{6765}xy^{10946}xy^{17711}xy^{28657}xy^{46368}xy^{75025}xy^{121393}$
27	$xyxyxy^2xy^3xy^5xy^8xy^{13}xy^{21}xy^{34}xy^{55}xy^{89}xy^{144}xy^{233}xy^{377}xy^{610}xy^{987}xy^{1597}xy^{2584}xy^{4181}$
	$xy^{6765}xy^{10946}xy^{17711}xy^{28657}xy^{46368}xy^{75025}xy^{121393}xy^{196418}$
28	$xyxyxy^2xy^3xy^5xy^8xy^{13}xy^{21}xy^{34}xy^{55}xy^{89}xy^{144}xy^{233}xy^{377}xy^{610}xy^{987}xy^{1597}xy^{2584}xy^{4181}$
	$xy^{6765}xy^{10946}xy^{17711}xy^{28657}xy^{46368}xy^{75025}xy^{121393}xy^{196418}xy^{317811}$
29	$xyxyxy^2xy^3xy^5xy^8xy^{13}xy^{21}xy^{34}xy^{55}xy^{89}xy^{144}xy^{233}xy^{377}xy^{610}xy^{987}xy^{1597}xy^{2584}xy^{4181}$
	$xy^{6765}xy^{10946}xy^{17711}xy^{28657}xy^{46368}xy^{75025}xy^{121393}xy^{196418}xy^{317811}xy^{514229}$
30	$xyxyxy^2xy^3xy^5xy^8xy^{13}xy^{21}xy^{34}xy^{55}xy^{89}xy^{144}xy^{233}xy^{377}xy^{610}xy^{987}xy^{1597}xy^{2584}xy^{4181}$
	$xy^{6765}xy^{10946}xy^{17711}xy^{28657}xy^{46368}xy^{75025}xy^{121393}xy^{196418}xy^{317811}xy^{514229}xy^{832040}$

Table 2: Words with Fibonacci Numbers as Powers

Syllable	Reduced Words
1	xy
2	$xyxy$
3	$xyxyxy^2$
4	$xyxyxy^2xy^3$
5	$xyxyxy$
6	$xyxyxyxy^2$
7	$xyxyxyxy^2xy$
8	$xyxyxyxy^2xyxy^3$
9	$xyxyxyxy^2xy^2$
10	$xyxyxyxy^2xy^2xy$
11	$xyxyxyxy^2xy^2xyxy^2$
12	$xyxyxyxy^2xy^2xyxy^2xy^3$
13	$xyxyxyxy^2xy^2xyxy$
14	$xyxyxyxy^2xy^2xyxyxy^2$
15	$xyxyxyxy^2xy^2xyxyxy^2xy$
16	$xyxyxyxy^2xy^2xyxyxy^2xyxy^3$
17	$xyxyxyxy^2xy^2xyxyxy^2xy^2$
18	$xyxyxyxy^2xy^2xyxyxy^2xy^2xy$
19	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxy^2$
20	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxy^2xy^3$
21	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxy$
22	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2$

23	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy$
24	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xyxy^3$
25	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2$
26	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xy$
27	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxy^2$
28	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxy^2xy^3$
29	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxy$
30	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2$
31	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy$
32	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xyxy^3$
33	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2$
34	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xy$
35	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxy^2$
36	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxy^2xy^3$
37	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxy$
38	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2$
39	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy$
40	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xyxy^3$
41	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2$
42	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xy$
43	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxy^2$
44	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxy^2xy^3$
45	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxy$

46	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2$
47	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy$
48	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xyxy^3$
49	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2$
50	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xy$
51	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxy^2$
52	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxy^2xy^3$
53	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxy$
54	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2$
55	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy$
56	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xyxy^3$
57	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2$
58	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xy$
59	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxy^2$
60	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxy^2$
	xy^3
61	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxy$
62	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxy$
	xy^2
63	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxy$
	xy^2xy
64	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxy$
	xy^2xyxy^3

65	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxy$
	$xy^2xy^2xyxyxy^2xy^2$
66	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxy$
	$xy^2xy^2xyxyxy^2xy^2xy$
67	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxy$
	$xy^2xy^2xyxyxy^2xy^2xyxy^2$
68	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxy$
	$xy^2xy^2xyxyxy^2xy^2xyxy^2xy^3$
69	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxy$
	$xy^2xy^2xyxyxy^2xy^2xyxy$
70	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxy$
	$xy^2xy^2xyxyxy^2xy^2xyxyxy^2$
71	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxy$
	$xy^2xy^2xyxyxy^2xy^2xyxyxy^2xy$
72	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxy$
	$xy^2xy^2xyxyxy^2xy^2xyxyxy^2xyxy^3$
73	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxy$
	$xy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2$
74	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxy$
	$xy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xy$
75	$xyxyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxy$
	$xy^2xy^2xyxyxy^2xy^2xyxyxy^2xy^2xyxy^2$

Table 3: Reduced Words

3.2 Classification of all Words

In Table-3, observe the pattern of the words and divide the words into eight classes corresponding to their syllables, that is, for each $i \in \{0, 1, 2, \ldots, 7\}$ there is a class of words having syllable $i(mod 8)$. Thereupon, eight classes of words emerge on the basis of equivalence of words. Furthermore, obtain words of the same class by adding number of copies of $xyxyxy^2xy^2$ after the first appearance of xy. For instance, $w_1(x, y) = xy, w_9\ (x, y) = xyxyxyxy^2xy^2$ and $w_{17}(x, y) = xyxyxyxy^2xy^2xyxyxy^2xy^2$. The following Table-4 summarizes all the eight classes of words in the form of relations:

Syllable of the word	*Additional relations*
$k \equiv 1(\text{mod } 8)$	$xy(xyxyxy^2xy^2)^\lambda = 1$
$k \equiv 2(\text{mod } 8)$	$xy(xyxyxy^2xy^2)^\lambda xy = 1$
$k \equiv 3(\text{mod } 8)$	$xy(xyxyxy^2xy^2)^\lambda xyxy^2 = 1$
$k \equiv 4(\text{mod } 8)$	$xy(xyxyxy^2xy^2)^\lambda xyxy^2xy^3 = 1$
$k \equiv 5(\text{mod } 8)$	$xy(xyxyxy^2xy^2)^\lambda xyxy = 1$
$k \equiv 6(\text{mod } 8)$	$xy(xyxyxy^2xy^2)^\lambda xyxyxy^2 = 1$
$k \equiv 7(\text{mod } 8)$	$xy(xyxyxy^2xy^2)^\lambda xyxyxy^2xy = 1$
$k \equiv 0(\text{mod } 8)$	$xy(xyxyxy^2xy^2)^\lambda xyxyxy^2xyxy^3 = 1$

Table 4: Classification of all Words

where λ is a non-negative integer for all the classes.

As the Fibonacci sequence $1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, \ldots$ appears in the powers of y, and because of the relation $y^3 = 1$ of the modular group, Fibonacci sequence reduces to the form $1, 1, 2, 0, 2, 2, 1, 0, 1, 1, 2, 0, 2, 2, 1, 0, \ldots$. Here, it is noteworthy that there is a repetition of terms after every eight syllables. Hence, this repetition continues up to infinity due to the pattern of Fibonacci sequence, that is, the method itself does not depend upon the range of 64 bits, because of the repetition of $1, 1, 2, 0, 2, 2, 1, 0$. Thus, by computer algorithm we get sufficiently large number of words $w(x, y)$ and after that the pattern of Fibonacci sequence generates $w(x, y)$ even for syllable greater than 2^{64}. That is, if $k = 2^{64} + 1 = 18,446,744,073,709,551,616 \equiv 0(mod 8)$ then $w_{2^{64}+1}(x, y)$ belongs to the class of syllable $0(mod 8)$ and thus $w_{2^{64}+1}(x, y) = xy(xyxyxy^2xy^2)^{2805843009213693951}xyxyxy^2xyxy^3$.

Correctness of the algorithm is also confirmed through analysis. Words of different syllables are obtained manually. They are then checked by using algorithm randomly for many values. Both; manual and algorithm, provide the same results. The GAP and the Tietze transformation are then used to identify the quotients for each $w(x, y)$ which also provide same quotients. This ensures correctness of the algorithm.

The advantage of this algorithm is that it provides $w(x, y)$ of sufficiently large syllable occurring in abundance, saving from chances of error and time. For the effective execution of the algorithm, processing power of the computer plays a vital role.

Number of x and y in Words and in their Reduced Forms

The word $w_k^*(x, y)$ is obtained from the word $w_k(x, y)$. But in order to generalize the notion of $w_k^*(x, y)$ for all syllables, formulae are devised for number of x and y appear in $w_k^*(x, y)$. Secondly, the pattern (position) of appearance of x and y in $w_k^*(x, y)$ needs to be observed. Thus, with this information, words of all syllables are generated. The symbols $N(x_{w_k})$ and $N(y_{w_k})$ are used for number of x and y in words respectively. Similarly, $N(x_{w_k^*})$ and $N(y_{w_k^*})$ are used for number of x and y in the reduced words respectively.

Theorem 11 *If syllable of the word $w(x, y)$ is k and k is any non-negative integer such that $k = 4p + r$ for some non-negative integers p and r then*

$$N\left(x_{w_k^*}\right) = \begin{cases} 2p+2 & if\ r = 0\ or\ 2 \\ 2p+1 & if\ r = 1 \\ 2p+3 & if\ r = 3 \end{cases}$$

Proof. Since syllable of the word $w(x, y)$ is k and k is a non-negative integer, divide all non-negative integers into subsets each subset containing four elements.

Let $\Im_1 = \{0, 1, 2, 3\}$, $\Im_2 = \{4, 5, 6, 7\}$,..., $\Im_k = \{4(k-1), 4(k-1)+1, 4(k-1)+2, 4(k-1)+3\}, \ldots$.

For $\Im_1$: If $k = 0$ then $0 = 4 \cdot 0 + 0$ implies that $N(x_{w_k^*}) = 2 \cdot 0 + 2 = 2$, that is, a word of syllable 0 have two x. In other words, $w(x, y) = x^2 = 1$ is the word of syllable 0 or the trivial word.

If $k = 1$, then $1 = 4 \cdot 0 + 1$ (where $r = 1$) implies that $N(x_{w_k^*}) = 2 \cdot 0 + 1 = 1$. Also $w_1(x, y) = xy$ shows $N(x_{w_1^*}) = 1$.

If $k = 2$, then $2 = 4 \cdot 0 + 2$ (where $r = 2$) implies that $N(x_{w_k^*}) = 2 \cdot 0 + 2 = 2$. Also $w_2(x, y) = xyxy$ shows $N(x_{w_2^*}) = 2$.

If $k = 3$, then $3 = 4 \cdot 0 + 3$ (where $r = 3$) implies that $N(x_{w_k^*}) = 2 \cdot 0 + 3 = 3$. Also $w_3(x, y) = xyxyxy^2$ shows $N(x_{w_3^*}) = 3$. Thus, the theorem holds for all elements of $\Im_1$.

For $\Im_n$: Since $\Im_n = \{4(n-1),\ 4(n-1)+1,\ 4(n-1)+2,\ 4(n-1)+3\}$, it is assumed that the result holds for $\Im_n$ and it requires only to be proved for the neighboring set; $\Im_{n+1} = \{4n, 4n+1, 4n+2, 4n+3\}$.

For $\Im_{n+1}$: As every $4th$ term of the Fibonacci sequence is multiple of 3 and these numbers appear in the power of y, so y vanishes at every 4th place. Then x on the left of y and x on the right of y multiply and gives x^2 which is equal to 1. Thus, in every 4 terms two x vanishes and only two x increases.

If $k = 4n$, then $N(x_{w_k^*}) =$ is equal to the number of x in $4(n-1)th$ term $+2$ $= 2n+2$.

If $k = 4n+1$, then $N(x_{w_k^*}) =$ number of x in $(4(n-1)+1)th$ term $+2 =$ $(2n-1)+2 = 2n+1$.

If $k = 4n+2$, then $N(x_{w_k^*}) =$ number of x in $(4(n-1)+2)th$ term $+2 = 2n+2$.

If $k = 4n+3$, then $N(x_{w_k^*}) =$ number of x in $(4(n-1)+3)th$ term $+2 =$ $(2n+1)+2 = 2n+3$. Thus, the theorem is proved for all elements of $\Im_{n+1}$, that is, the result holds for all non-negative integers. ■

Theorem 12 *If syllable of the word $w(x,y)$ is k and for some non-negative integers p and r, $k = 8p - r$ then*

$$N(y_{w_k^*}) = \left\{ \begin{array}{cc} 6p+3 & if\ r=0 \\ 6p & if\ r=1 \\ 6p-1 & if\ r=2 \\ 6p-3 & if\ r=3 \\ 6p+1 & if\ r=4 \\ 6p-2 & if\ r=5 \\ 6p-4 & if\ r=6 \\ 6p-5 & if\ r=7\ . \end{array} \right\}$$

Proof. Since syllable of the word $w(x,y)$ is k and k is a non-negative integer, the non-negative integers are divided into subsets, each containing eight elements.

Let $\Im_1' = \{0,1,2,3,4,5,6,7\}$, $\Im_2' = \{8,9,10,11,12,13,14,15\}$,..., $\Im_k' = \{8(k-1), 8k-7, 8k-6, 8k-5, 8k-4, 8k-3, 8k-2, 8k-1\}, \ldots$.

For $\Im_1'$: If $k=0$ then $0 = 8\cdot 0 - 0$ and so $N(y_{w_k^*}) = 6\cdot 0 + 3 = 3$, that is, a word of syllable 0 has three y. Hence, $w(x,y) = y^3 = 1$ is a word of syllable 0 or a trivial word.

If $k=1$, then $1 = 8\cdot 1 - 7$ and so $N(y_{w_k^*}) = 6\cdot 1 - 5 = 1$. That is $w(x,y) = xy$.

If $k=2$, then $2 = 8\cdot 1 - 6$ and so $N(y_{w_k^*}) = 6\cdot 1 - 4 = 2$. That is $w(x,y) = xyxy$.

If $k=3$, then $3 = 8\cdot 1 - 5$ and so $N(y_{w_k^*}) = 6\cdot 1 - 2 = 4$. That is $w(x,y) = xyxyxy^2$.

If $k=4$, then $4 = 8\cdot 1 - 4$ and so $N(y_{w_k^*}) = 6\cdot 1 + 1 = 7$. That is $w(x,y) = xyxyxy^2xy^3$.

If $k=5$, then $5 = 8\cdot 1 - 3$ and so $N(y_{w_k^*}) = 6\cdot 1 - 3 = 1$. That is $w(x,y) = xyxyxy$.

If $k = 6$, then $6 = 8 \cdot 1 - 2$ and so $N(y_{w_k^*}) = 6 \cdot 1 - 1 = 5$. That is $w(x, y) = xyxyxyxy^2$.

If $k = 7$. then $7 = 8 \cdot 1 - 1$ and so $N(y_{w_k^*}) = 6 \cdot 1 = 6$. That is $w(x, y) = xyxyxyxy^2xy$.

If $k = 8$, then $8 = 8 \cdot 1 - 0$ and so $N(y_{w_k^*}) = 6 \cdot 1 + 3 = 9$. That is $w(x, y) = xyxyxyxy^2xyxy^3$. Thus, the statement is true for all elements of $\Im_1^{'}$.

For $\Im_n^{'}$: Since $\Im_n^{'} = \{8(n-1), 8n-7, 8n-6, 8n-5, 8n-4, 8n-3, 8n-2, 8n-1\}$, we assume that the result holds for nth set. We prove it for the neighboring set.

For $\Im_{n+1}^{'}$: Since powers of y are from Fibonacci sequence

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, ... \tag{3.1}$$

By using the order of y which is 3, these terms reduce to the form

$$1, 1, 2, 0, 2, 2, 1, 0, 1, 1, 2, 0, 2, 2, 1, 0, ... \tag{3.2}$$

As each $\Im_i^{'}$ contains eight elements and every eight terms of the above sequence contains nine y, therefore, every $4th$ term of the above sequence is multiple of 3, that is, y vanishes at every $4th$ position. So, by addition of $3rd$ and $5th$ term, it reduces 3 y. Hence, in every eight terms the number of y increases to 6. Note that $\Im_{n+1}^{'} = \{8n, 8(n+1)-7, 8(n+1)-6, 8(n+1)-5, 8(n+1)-4, 8(n+1)-3, 8(n+1)-2, 8(n+1)-1\}$.

If $k = 8n$, then $N(y_{w_k^*}) =$ Number of y in $8(n-1)th$ term+6 $= (6n-3)+6 = 6n+3 = 6(n+1)-3$.

If $k = 8(n+1)-7$, then $N(y_{w_k^*}) =$ number of y in $(8n-7)th$ term+6 $= (6n-5)+6 = 6n+1 = 6(n+1)-5$.

If $k = 8(n+1)-6$, then $N(y_{w_k^*}) =$ number of y in $(8n-6)th$ term$+6 = (6n-4)+6 = 6n+2 = 6(n+1)-4$.

If $k = 8(n+1)-5$, then $N(y_{w_k^*}) =$ number of y in $(8n-5)th$ term$+6 = (6n-2)+6 = 6n+4 = 6(n+1)-2$.

If $k = 8(n+1)-4$, then $N(y_{w_k^*}) =$ number of y in $(8n-4)th$ term$+6 = (6n+1)+6 = 6n+7 = 6(n+1)+1$.

If $k = 8(n+1)-3$, then $N(y_{w_k^*}) =$ number of y in $(8n-3)th$ term$+6 = (6n-3)+6 = 6n+3 = 6(n+1)-3$.

If $k = 8(n+1)-2$, then $N(y_{w_k^*}) =$ number of y in $(8n-2)th$ term$+6 = (6n-1)+6 = 6n+5 = 6(n+1)-1$.

If $k = 8(n+1)-1$, then $N(y_{w_k^*}) =$ number of y in $(8n-1)th$ term$+6 = 6n+6 = 6n+6 = 6(n+1)$. Thus, the result holds for all elements of $\Im'_{n+1}$, that is for all non-negative integers. ■

For illustration of the above two theorems, the following example is given for different syllables.

Example 13 *(a) If syllable of the word* $w(x,y)$ *is* 56 *and* $56 = 4(14)+0$ *then by Theorem* 11, $p = 14$ *and* $r = 0$. *Therefore,* $N(x_{w_{56}^*}) = 2(14)+2 = 30$.

Also $56 = 8(7)-0$ *then by Theorem* 12, $N(y_{w_{56}^*}) = 6(7)+3 = 45$.

(b) If syllable of the word $w(x,y)$ *is* 57 *and* $57 = 4(14)+1$ *then by Theorem* 11, $p = 14$ *and* $r = 1$. *Therefore,* $N(x_{w_{57}^*}) = 2(14)+1 = 29$.

Also $57 = 8(8)-7$ *then by Theorem* 12, $N(y_{w_{57}^*}) = 6(8)-5 = 43$.

Number of x and y in $w(x,y)$ and in $w^*(x,y)$ are given in the following table.

Syllable	$(\mathbf{N}(\mathbf{x}_w), \mathbf{N}(\mathbf{y}_w))$	$(\mathbf{N}(\mathbf{x}_{w^*}), \mathbf{N}(\mathbf{y}_{w^*}))$	23	$(23, 75024)$	$(13, 18)$
1	$(01, 01)$	$(01, 01)$	24	$(24, 121392)$	$(14, 21)$
2	$(02, 02)$	$(02, 02)$	25	$(25, 196417)$	$(13, 19)$
3	$(03, 04)$	$(03, 04)$	26	$(26, 317810)$	$(14, 20)$
4	$(04, 07)$	$(04, 07)$	27	$(27, 514228)$	$(15, 22)$
5	$(05, 12)$	$(03, 03)$	28	$(28, 832039)$	$(16, 25)$
6	$(06, 20)$	$(04, 05)$	29	$(29, 1346268)$	$(15, 21)$
7	$(07, 33)$	$(05, 06)$	30	$(30, 2178308)$	$(16, 23)$
8	$(08, 54)$	$(06, 09)$	31	$(31, 3524577)$	$(17, 24)$
9	$(09, 88)$	$(05, 07)$	32	$(32, 5702886)$	$(18, 27)$
10	$(10, 143)$	$(06, 08)$	33	$(33, 9227464)$	$(17, 25)$
11	$(11, 232)$	$(07, 10)$	34	$(34, 14930351)$	$(18, 26)$
12	$(12, 376)$	$(08, 13)$	35	$(35, 24157816)$	$(19, 28)$
13	$(13, 609)$	$(07, 09)$	36	$(36, 39088168)$	$(20, 31)$
14	$(14, 986)$	$(08, 11)$	37	$(37, 63245985)$	$(19, 27)$
15	$(15, 1596)$	$(09, 12)$	38	$(38, 102334154)$	$(20, 29)$
16	$(16, 2583)$	$(10, 15)$	39	$(39, 165580140)$	$(21, 30)$
17	$(17, 4180)$	$(09, 13)$	40	$(40, 267914295)$	$(22, 33)$
18	$(18, 6764)$	$(10, 14)$	41	$(41, 433494436)$	$(21, 31)$
19	$(19, 10945)$	$(11, 16)$	42	$(42, 701408732)$	$(22, 32)$
20	$(20, 17710)$	$(12, 19)$	43	$(43, 1134903169)$	$(23, 34)$
21	$(21, 28656)$	$(11, 15)$	44	$(44, 1836311902)$	$(24, 37)$
22	$(22, 46367)$	$(12, 17)$	45	$(45, 2971215072)$	$(23, 33)$

Syllable	$(\mathbf{N}(\mathbf{x}_w),\mathbf{N}(\mathbf{y}_w))$	$(\mathbf{N}(\mathbf{x}_{w^*}),\mathbf{N}(\mathbf{y}_{w^*}))$	68	$(68,190392490709134)$	$(36,55)$
46	$(46,4807526975)$	$(24,35)$	69	$(69,308061521170128)$	$(35,51)$
47	$(47,7778742048)$	$(25,36)$	70	$(70,498454011879263)$	$(36,53)$
48	$(48,12586269024)$	$(26,39)$	71	$(71,806515533049392)$	$(37,54)$
49	$(49,20365011073)$	$(25,37)$	72	$(72,1304969544928656)$	$(38,57)$
50	$(50,32951280098)$	$(26,38)$	73	$(73,2111485077978049)$	$(37,55)$
51	$(51,53316291172)$	$(27,40)$	74	$(74,3416454622906706)$	$(38,56)$
52	$(52,86267571271)$	$(28,43)$	75	$(75,5527939700884756)$	$(39,58)$
53	$(53,139583862444)$	$(27,39)$	76	$(76,8944394323791463)$	$(40,61)$
54	$(54,225851433716)$	$(28,41)$	77	$(77,14472334024676220)$	$(39,57)$
55	$(55,365435296161)$	$(29,42)$	78	$(78,23416728348467684)$	$(40,59)$
56	$(56,591286729878)$	$(30,45)$	79	$(79,37889062373143905)$	$(41,60)$
57	$(57,956722026040)$	$(29,43)$	80	$(80,61305790721611590)$	$(42,63)$
58	$(58,1548008755919)$	$(30,44)$	81	$(81,99194853094755496)$	$(41,61)$
59	$(59,2504730781960)$	$(31,46)$	82	$(82,160500643816367087)$	$(42,62)$
60	$(60,4052739537880)$	$(32,49)$	83	$(83,259695496911122584)$	$(43,64)$
61	$(61,6557470319841)$	$(31,45)$	84	$(84,420196140727489672)$	$(44,67)$
62	$(62,10610209857722)$	$(32,47)$	85	$(85,679891637638612257)$	$(43,63)$
63	$(63,17167680177564)$	$(33,48)$	86	$(86,1100087778366101930)$	$(44,65)$
64	$(64,27777890035287)$	$(34,51)$	87	$(87,1779979416004714188)$	$(45,66)$
65	$(65,44945570212852)$	$(33,49)$	88	$(88,2880067194370816119)$	$(46,69)$
66	$(66,72723460248140)$	$(34,50)$	89	$(89,4660046610375530308)$	$(45,67)$
67	$(67,117669030460993)$	$(35,52)$	90	$(90,7540113804746346428)$	$(46,68)$

Table 5: Number of x and y in w(x,y) and w^*(x,y)

Chapter 4

A Class of Generalized Triangle Groups

In previous chapter, we discussed words $w(x, y)$, their reduced forms $w^*(x, y)$, formulae showing number of x and y in $w(x, y)$ and in $w^*(x, y)$, and finally we obtained eight classes of words and consequently of additional relations. In this chapter, we insert these $w^*(x, y) = 1$ in finite presentation of $PSL(2, \mathbb{Z})$ so that one-relator quotients of the modular group are obtained which are in the form $< x, y : x^2 = y^3 = w^*(x, y) = 1 >$. We take advantage of Tietze transformations and 'Groups, Algorithms and Programming' (GAP) for identification of these quotients. In second part of this chapter, we discuss some applications of quotients of $PSL(2, \mathbb{Z})$ in cryptography. The important non-linear component of cryptographic schemes is substitution box. The formation of substitution box have a variety of methods but here we use a quotient of $PSL(2, \mathbb{Z})$ and its coset diagram to have a strong and an efficient substitution box. This substitution box is not only have high non-linearity but also resistive against linear and differential attacks.

4.1 A Class of Generalized Triangle Groups as Quotients of the Modular Group

In this section we deal with one relator quotients of the modular group corresponding to the words generated in the previous chapter as expressed in Table–4 . We insert the additional relations in $PSL(2,\mathbb{Z})$ and then identify the one relator quotient of the modular group. The following is the main theorem in which quotients of the modular group are determined.

Theorem 14 *Let* $G =< x, y : x^2 = y^3 = w^*(x, y) = 1 >$ *be one relator quotient of* $PSL(2,\mathbb{Z})$ *where* $w^*(x, y)$ *is the reduced form of* $w(x, y) = x^{r_1}y^{s_1}x^{r_2}y^{s_2}\dots x^{r_k}y^{s_k}$ *and* $r_i s_i$ *are terms of the Fibonacci sequence. Then up to equivalence G is one of the eight groups; trivial group,* C_2*,* C_3*,* S_3*,* A_4*,* $C_3 \times S_3$*,* $((((C_2 \times D_8) : C_2) : C_3) : C_3) : C_2$ *and* $< x, y : x^2 = y^3 = (xyxyxy^2xy^2)^\lambda = 1 >$.

Proof. *As the words* $w(x, y) = x^{r_1}y^{s_1}x^{r_2}y^{s_2}\dots x^{r_k}y^{s_k}$ *are divided into eight classes with respect to their syllables, as shown in Table -4. Then, for each class of words having syllable* $i(mod8)$ *where* $i \in \{0, 1, 2, ..., 7\}$*, the quotients of* $PSL(2,\mathbb{Z})$ *are of the form:*

$G_1 =< x, y : x^2 = y^3 = xy(xyxyxy^2xy^2)^\lambda = 1 >$

$G_2 =< x, y : x^2 = y^3 = xy(xyxyxy^2xy^2)^\lambda xy = 1 >$

$G_3 =< x, y : x^2 = y^3 = xy(xyxyxy^2xy^2)^\lambda xyxy^2 = 1 >$

$G_4 =< x, y : x^2 = y^3 = xy(xyxyxy^2xy^2)^\lambda xyxy^2xy^3 = 1 >$

$G_5 =< x, y : x^2 = y^3 = xy(xyxyxy^2xy^2)^\lambda xyxy = 1 >$

$G_6 =< x, y : x^2 = y^3 = xy(xyxyxy^2xy^2)^\lambda xyxyxy^2 = 1 >$

$G_7 =< x, y : x^2 = y^3 = xy(xyxyxy^2xy^2)^\lambda xyxyxy^2xy = 1 >$

$G_0 =< x, y : x^2 = y^3 = xy(xyxyxy^2xy^2)^\lambda xyxyxy^2xyxy^3 = 1 >$

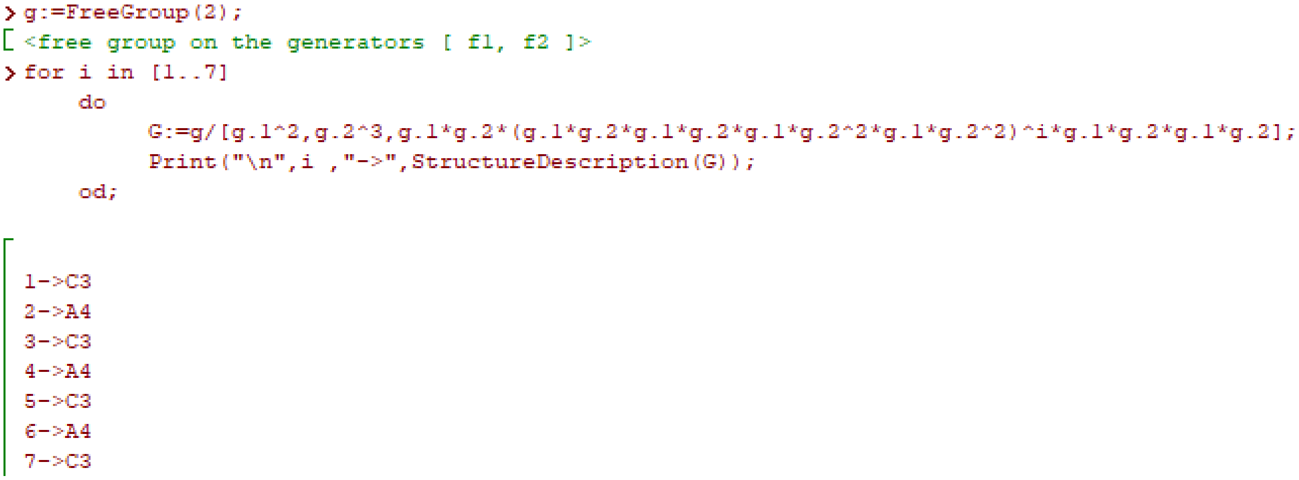
In all cases, λ is a non-negative integer and each quotient G_i,where $i \in \{0, 1, 2, \ldots, 7\}$, is associated with words of syllable $i(mod8)$.

First, the additional relation of G_1 is $xy(xyxyxy^2xy^2)^\lambda = 1$. For $\lambda = 0$, the additional relation is $xy = 1$ implying that $x = 1 = y$, and the quotient is a trivial group. For $\lambda = 1$, the additional relation is $xy(xyxyxy^2xy^2) = 1$ or $xyx = yxyxy^2xy^2$ or $xy^2x = 1$. It gives $x = 1 = y$. Thus, the quotient G_1 is a trivial group. Other values of λ similarly follow the pattern of $\lambda = 1$ because it increases the number of copies of $xyxyxy^2xy^2$. Thus, for all values of λ, quotient G_1 is a trivial group.

For G_2: The additional relation of G_2 is $xy(xyxyxy^2xy^2)^\lambda xy = 1$. For $\lambda = 0$, the additional relation is $xyxy = 1$. Thus, the quotient is $< x, y : x^2 = y^3 = (xy)^2 = 1 >$ which is S_3. For $\lambda = 1$, the additional relation is $xy(xyxyxy^2xy^2)xy = 1$ which implies that $yxyxy^2xy^2 = xy^2xy^2x$ or $(xy)^2 = 1$. Hence, the quotient is S_3. For other values of λ, in a similar way as for $\lambda = 1$ the quotient G_2 is S_3.

For G_3: The additional relation of G_3 is $xy(xyxyxy^2xy^2)^\lambda xyxy^2 = 1$. For $\lambda = 0$ it becomes $xyxyxy^2 = 1$. This implies that $xyx = yxy^2$ or $x = 1 = y$. This shows that the quotient is a trivial group. Hence, similarly for other values of λ, the quotient G_3 is trivial group.

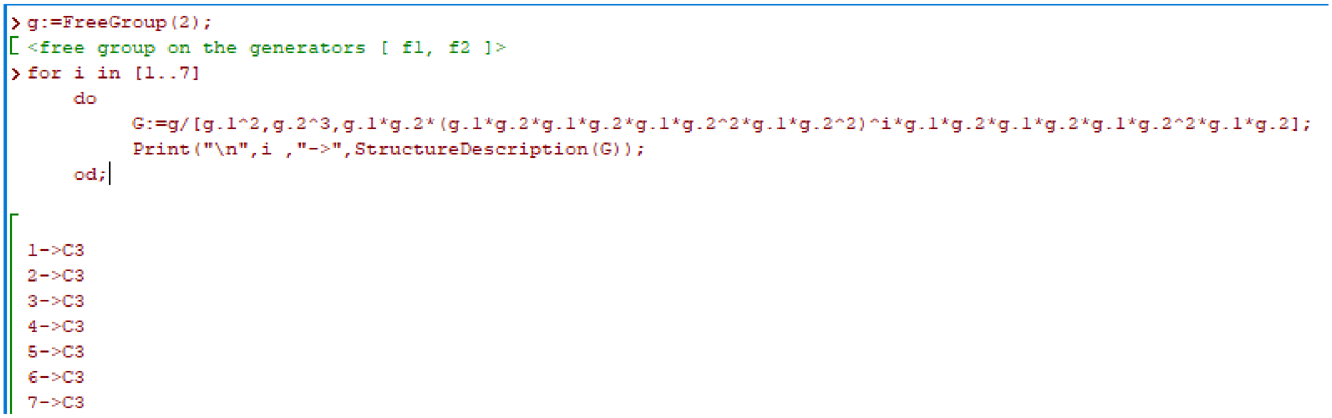
Similarly, By using GAP, we find G_5 and G_7 which are expressed in the following *pictures taken from GAP.*



```
> g:=FreeGroup(2);
[ <free group on the generators [ f1, f2 ]>
> for i in [1..7]
      do
           G:=g/[g.1^2,g.2^3,g.1*g.2*(g.1*g.2*g.1*g.2*g.1*g.2^2*g.1*g.2^2)^i*g.1*g.2*g.1*g.2];
           Print("\n",i ,"->",StructureDescription(G));
      od;

 1->C3
 2->A4
 3->C3
 4->A4
 5->C3
 6->A4
 7->C3
```

Group G_5



```
> g:=FreeGroup(2);
[ <free group on the generators [ f1, f2 ]>
> for i in [1..7]
      do
           G:=g/[g.1^2,g.2^3,g.1*g.2*(g.1*g.2*g.1*g.2*g.1*g.2^2*g.1*g.2^2)^i*g.1*g.2*g.1*g.2*g.1*g.2^2*g.1*g.2];
           Print("\n",i ,"->",StructureDescription(G));
      od;

 1->C3
 2->C3
 3->C3
 4->C3
 5->C3
 6->C3
 7->C3
```

Group G_7

Thus, by using Tietze transformation and by using GAP we find the other quotients and summarize the results in the following table.

	Syllable of the word	***Quotients of the Modular Group***
G_1	$k \equiv 1(\mathrm{mod}\, 8)$	*Trivial group*
G_2	$k \equiv 2(\mathrm{mod}\, 8)$	S_3
G_3	$k \equiv 3(\mathrm{mod}\, 8)$	*Trivial group*
G_4	$k \equiv 4(\mathrm{mod}\, 8)$	C_2
G_5	$k \equiv 5(\mathrm{mod}\, 8)$	$\begin{cases} C_3 & for\ \lambda = odd\ number \\ A_4 & for\ \lambda = even\ number \end{cases}$
G_6	$k \equiv 6(\mathrm{mod}\, 8)$	C_2
G_7	$k \equiv 7(\mathrm{mod}\, 8)$	C_3
G_0	$k \equiv 0(\mathrm{mod}\, 8)$	$\begin{cases} C_3 \times S_3 & for\ \lambda = 0 \\ \Big(\big(((C_2 \times D_8): C_2): C_3\big): C_3\Big): C_2 & for\ \lambda = 1 \\ < x, y: x^2 = y^3 = (xyxyxy^2xy^2)^2 & otherwise \end{cases}$

Table 6: A Class of Quotients of the Modular Group

Thus, we obtain a class of generalized triangle groups as quotients of $PSL(2,\mathbb{Z})$ *corresponding the word (of any syllable) and conclude that this class contains trivial group,* C_2*,* C_3*,* S_3*,* A_4*,* $C_3 \times S_3$*,* $((((C_2 \times D_8) : C_2) : C_3) : C_3) : C_2$ *and* $< x, y : x^2 = y^3 = (xyxyxy^2xy^2)^\lambda = 1 >$*. This completes the proof.* ∎

Remark 15 *It is pertinent to mention here that the group* $< x, y : x^2 = y^3 = (xyxyxy^2xy^2)^2 = 1 >$ *is described by J. Howie, V. Metaftsis and R. M. Thomas in [3] as one of the finite generalized triangle groups of order 576. Whereas, we identify the above-mentioned group as a quotient of* $PSL(2,\mathbb{Z})$ *and further the description of its structure is* $((((C_2 \times D_8) : C_2) : C_3) : C_3) : C_2$*.*

Remark 16 *It is worthwhile to note that there is a single quotient* G_i *corresponding to each class of syllable* $i(mod8)$ *except for* $i = 0$ *or* 5*.*

Remark 17 *Eight out of fourteen finite generalized triangle groups are one relator quotients of $PSL(2,\mathbb{Z})$. Our method/proposed scheme is applicable on all two generator groups. We can also view that all finite generalized triangle groups are two generator groups. So, the proposed method is sufficient to find one relator quotients of all finite generalized triangle groups. This study of quotients is comprehensive and provides a methodology to determine all one relator quotients of any two-generator group.*

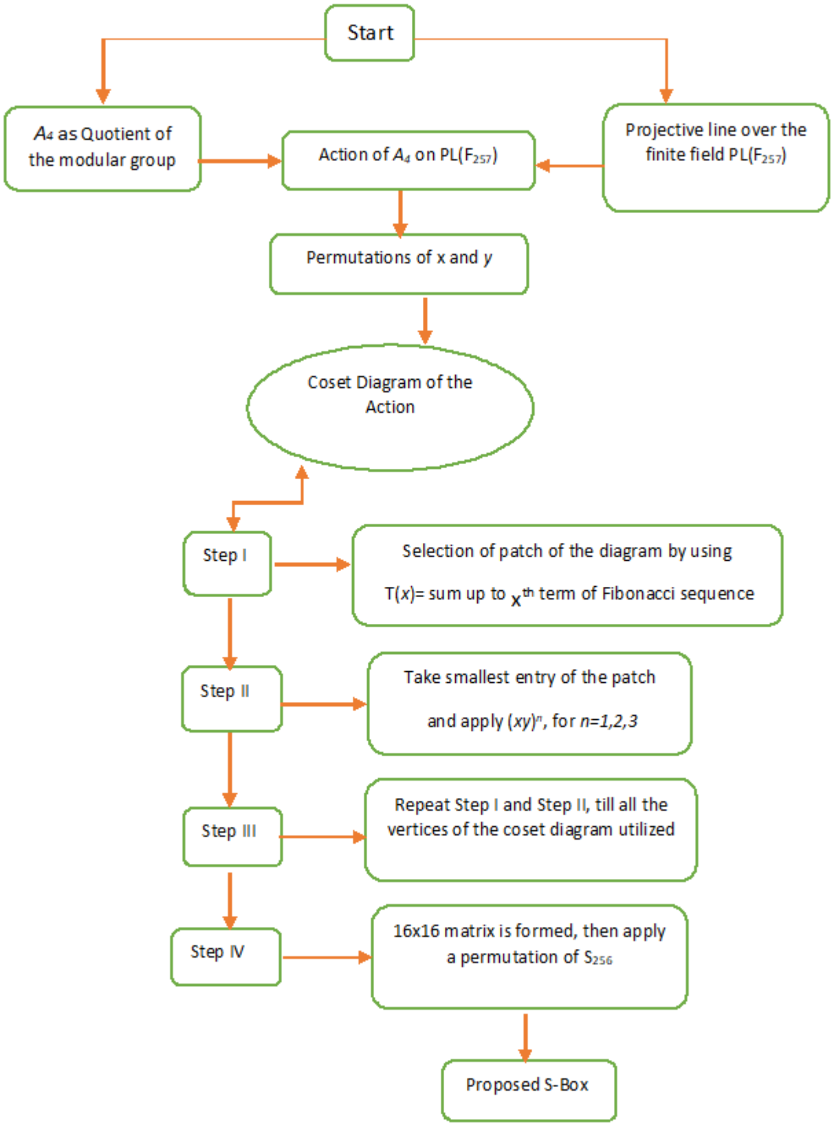
4.2 Quotients of the Modular Group and Algebraic Substitution Box

Historical Development

With rapid advancement in communication technology, the maintenance of data security has become a great challenge for cryptographers. In this regard, block encryption algorithm plays vital role in cryptographic systems. The important component of block encryption algorithm is the S-box. The security strength of the S-box determines the security strength of the entire cryptosystem. It is therefore established that the S-box plays an important role in the security of cryptographic schemes.

The DES [24] was proposed by a well-known computer production company in 1977, and the DES investigations drove the refinement in the cryptographic system enormously. Later, a group of university students broke the DES security. This led to the realization that of some other secure and efficient encryption method has to be evolved. In 2002, the Advanced Encryption Standard (AES) was created by J. Daemen and V. Rijmen [25] which is now the standard for the encryption. The S-box has a vital role in quality of encryption. Utilization of a weak S-box is tantamount to compromising on the security of encryption process. Therefore, before using an S-box in a cryptosystem, it is pertinent to assess its strength. The analyses for measuring strength include nonlinearity method (NL), linear approximation probability method (LAP), bit independence criterion (BIC), differential approximation probability method (DAP) and strict avalanche criterion (SAC). Some studies related to the construction of S-box and its strength are in [26, 27]. The analyses of S-box in image encryption based on majority logic criteria are investigated in [28, 29]. More investigation on the S-box based on a chaotic map is conducted in [30], hyperchaotic system-based S-box in [31], and chaotic neural network-based S-box in [32]. G. Chen, Y. Chen and X. Liao [33] described an S-box based on three-dimensional chaotic baker maps. U. Hayat and N. A. Azam [34] used elliptic curves to construct an S-box by considering the ordinate of the curve for this construction. Altaleb et al. [35] investigate the construction of an S-box by using the projective general linear group. Thus, various aspects of construction of an S-box are investigated to get a secure and better S-box which enables better encryption. For example, recently, attackers have been successful in breaking the loops of AES. Thus, the need for an efficient method to generate dynamic S-boxes exists. The construction of an S-box using the group graphs is presented as an alternative S-box design technique. It exponentially improved security and efficacy which is vividly visible in subsequent work in this section. We propose an efficient technique for the construction of an S-box by using action of a quotient of $PSL(2, \mathbb{Z})$ on $PL(F_{257})$. The permutations obtained in this way are used to draw a coset diagram. The vertices of the coset diagram are considered in a special way for constructing an S-box. The S-box generated in this way is highly secure, closely meeting the optimal values of the standard S-box. All the tests for the security strength are performed and compared with other S-boxes confirming that the proposed S-box is highly secure.

The purpose of this study is to establish a scheme for the construction of an S-box by taking action of one of the quotients of the modular group (e.g. we choose A_4) on the projective line over the finite field, that is $PL(F_{257})$. The proposed scheme is presented in the following flow chart.


Start
A_4 as Quotient of the modular group
Action of A_4 on PL(F_{257})
Projective line over the finite field PL(F_{257})
Permutations of x and y
Coset Diagram of the Action
Step I
Selection of patch of the diagram by using
T(x)= sum up to x th term of Fibonacci sequence
Step II
Take smallest entry of the patch
and apply $(xy)^n$, for n=1,2,3
Step III
Repeat Step I and Step II, till all the vertices of the coset diagram utilized
Step IV
16x16 matrix is formed, then apply a permutation of S_{256}
Proposed S-Box

Flow Chart 2: *Procedure for the Construction of S−Box*

4.2.1 S-Box Based on Action of a Group and Coset Diagrams

In the proposed scheme, firstly we take action of A_4 on $PL(F_{257})$, then in the second step, we draw a coset diagram of the action, and finally we construct an S-box by using vertices of the coset diagram. The action of the modular group on $PL(F_p)$ evolves a coset diagram in which each vertex is fixed by $(xy)^p$. In order to draw a coset diagram for $< x, y : x^2 = y^3 = (xy)^n = 1 >$, where n is of our own choice, there is a method given by Q. Mushtaq [8], known as parametrization method.

Action of A_4 on Projective Line over the Finite Field $PL(F_{257})$

The linear fractional transformations of the generators x and y act on each element of $PL(F_{257})$ produces the following permutation representations of $\overline{x}$ and $\overline{y}$.

$\overline{x}$: (055 00)(157 01)(019 002)(183 003)(004 20)(192 005)(006 150)(007 096)(008 024)(009 026)(029 010)(034 011)(012 044)(013 074)(014 inf)(211 015)(016 241)(251 017)(018 256)(021 189)(022 135)(023 093)(025 102)(027 128)(028 230)(203 030)(207 031)(032 182)(092 033)(035 158)(036 058)(037 179)(140 038)(039 063)(071 040)(041 126)(122 042)(043 136)(153 045)(237 046)(047 129)(048 239)(049 049)(098 050)(051 061)(052 053)(141 054)(056 086) (057 168)(184 059)(060 225)(062 077)(064 167)(164 065)(066 171)(067 105)(068 070)(069 083)(072 075)(073 209)(076 212)(078 254)(079 191)(080 200)(081 109)(082 255)(084 160)(085 205)(087 154)(088 166)(116 089)(090 162)(091 100)(094 206)(095 137)(165 097)(099 104)(226 101)(253 103)(106 248)(107 146)(108 161)(110 174)(175 111)(112 155)(113 138)(219 114)(115 133)(117 228)(118 221)(119 197)(188 120)(220 121)(123 195)(124 177)(125 201)(250 127)(130 173)(131 198)(132 240)(134 142)(139 178)(143 151)(144 231)(247 145)(147 172)(148 190)(149 242)(152 170)(156 238)(159 244)(243 163)(169 196)(176 204)(180 218)(181 186)(185 194)(235 187)(193 252)(199 229)(202 216)(208 223)(210 213)(214 245)(215 217)(222 246)(224 234)(227 249)(232 233)(236 236).

$\overline{y}$: (00 241 inf)(121 242 01)(256 120 240)(113 02 100)(239 128 141)(230 070 003)(171 011 238)(004 090 177)(151 237 064)(087 005 049)(236 154 192)(222 027

006)(214 019 235)(190 131 007)(110 051 234)(008 075 209)(166 233 302)(009 072 184)(169 232 057)(010 089 164)(152 231 077)(134 012 101)(229 107 140)(195 162 013)(079 046 228)(014 060 186)(181 227 055)(199 104 015)(137 042 226)(225 016 249)(148 105 017)(136 093 224)(189 084 018)(157 052 223)(074 020 050)(221 167 191)(132 033 021)(208 109 220)(022 115 206)(126 219 035)(145 174 023)(067 096 218)(059 024 045)(217 182 196) (163 056 025)(185 078 216)(153 073 026)(168 088 215)(111 085 028)(156 130 213)(179 029 040)(212 062 201)(095 044 030)(197 146 211)(175 183 031)(058 066 210)(173 034 036)(207 068 205)(116 037 097)(204 125 144)(119 099 038)(142 122 203)(129 039 243)(202 112 255)(147 041 248)(200 094 250)(043 061 247)(180 198 251)(047 102 159)(139 194 082)(150 048 253)(193 091 245)(149 081 053)(160 092 188)(103 054 246)(187 138 252)(086 063 244)(178 155 254)(165 071 065)(170 076 176)(127 133 069)(108 114 172)(135 080 083)(161 106 158)(124 123 098)(118 117 143).

The coset diagram for the action of A_4 on $PL(F_{257})$ consists of two types of the circuits, given below.

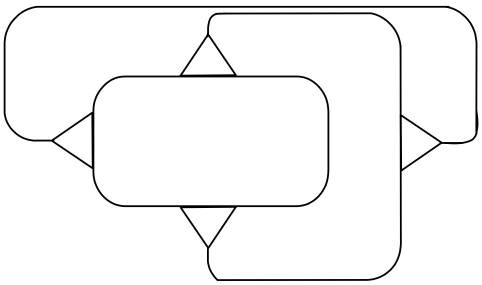


Figure 7: *Type−A Circuit*

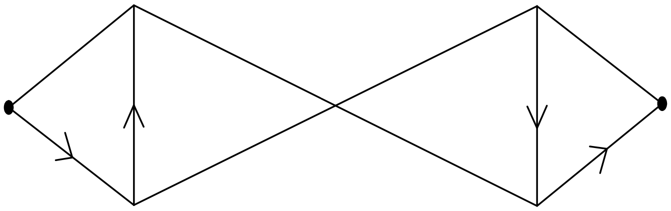


Figure 8: *Type−B Circuit*

(a) In Type-A circuit, there are four triangles and this type of circuit occurs twenty-one times in the coset diagram. There is no fix point of $\overline{x}$ nor of $\overline{y}$ in Type-A circuit. Thus, Type-A circuits use 252 vertices of the coset diagram.

(b) In type-B circuit, there are only two triangles and this type of circuit occurs only once in the coset diagram. In this circuit, there are two fixed points of $\overline{x}$. Thus, Type-B circuit utilized only six vertices of the coset diagram.

Construction of S-Box using Coset Diagram

After drawing the coset diagram, we proceed towards construction of S-box from the coset diagram. There are twenty-two circuits in the coset diagram, so the first step is how to choose a circuit. The second step is the selection of vertices of that circuit in a specific manner. Therefore, for the first part, instead of randomly choosing the circuits we choose the circuits by using a sequence, known as Fibonacci sequence $1, 1, 2, 3, 5, 8, ...$ We define mapping as $\beta : PL(F_{257}) \to PL(F_{257})$ by $\beta(k) =$ Sum of the first k terms of the Fibonacci sequence. Then, choose the circuit in which $\beta(x)$ occurs. By this mapping, we can easily and systematically choose the circuits one by one. For illustration, $\beta(1) = 1$, we pick the circuit of the coset diagram having 1 as the vertex, that is, the circuit shown in Figure-9. Similarly, for $\beta(0) = 0, \beta(2) = 1 + 1 = 2, \beta(3) = 1 + 1 + 2 = 4$, and so on. Secondly, after choosing the circuit of the coset diagram, now we select the vertices of that circuit in a special manner. We initiate from the vertex $\beta(1) = 1$ and apply $xy, (xy)^2$, and $(xy)^3$ (because of the third relator of A_4) on $\beta(1)$ and note the vertices, which are $(1, 52, 149)$. Then, in the same circuit we choose the smallest number from the remaining vertices of the circuit, which is 53, apply xy and its powers to get $(53, 223, 109)$. Continue the process by choosing the smallest from the remaining vertices of the circuit and apply xy and its powers so that all the vertices of the circuit are utilized. We can view the entries of the circuit containing $\beta(1) = 1$ in (starting from row 1 column 12 of) Table-7, except infinity. It is important to mention here that if $\beta(x)$ appears in the previous circuit then it means it is already utilized so move on. But, if $\beta(x)$ appears in the new circuit, then apply xy and its powers in the similar fashion and note the permutation. Continue the process till all the vertices of the coset diagram are exhausted yielding 258 entries in an order. Ignore ∞ and 256. Thus, a 16×16 S-box is constructed as shown in Table-7. It is important to mention here that whenever $\beta(x) > 256$ take modulo class 257. It seems easy to find $\beta(x)$ in modulo class 257 but this is not so. We use an online PowerMod Calculator for these calculations. The entire scheme of constructing an S-box is based on the action of a finite triangle group A_4, coset diagram, and Fibonacci sequence. These all inculcate the natural patterns in the scheme which gives a very suitable and effective S-box as a result.

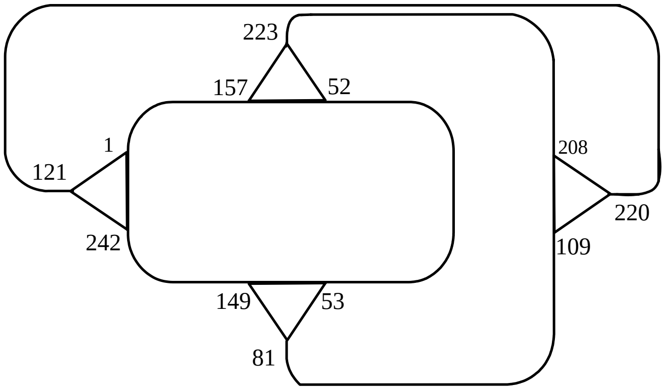


Figure 9: *A Circuit of the Coset Diagram Containing* $T(1)$

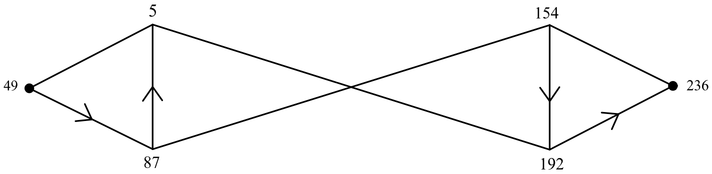


Figure 10: *Type B Circuit*

000	181	014	016	060	055	241	249	186	227	225	001	052	149	053	223
109	081	220	242	121	208	157	002	235	138	019	100	245	091	113	252
187	214	193	004	050	124	013	020	090	074	195	098	123	162	177	007
218	198	17	180	67	96	190	105	131	251	148	12	30	142	42	203
095	044	101	137	122	226	134	018	120	160	021	084	092	033	188	240
132	189	006	048	128	027	141	246	054	239	253	103	150	222	032	196
232	057	088	233	166	215	182	168	169	217	046	064	191	079	221	117
118	167	151	143	237	228	015	197	099	038	229	104	119	146	140	107
211	199	003	031	068	028	070	205	085	207	175	111	183	230	078	178
194	082	202	185	112	254	216	139	155	255	023	224	110	043	093	145
051	247	174	061	234	136	025	159	086	039	244	047	056	063	243	102
163	129	022	080	094	069	135	115	083	127	200	133	206	250	035	161
114	041	219	172	106	147	108	126	248	158	011	036	066	034	023	130
058	173	213	156	171	210	008	045	073	009	153	059	024	075	184	026
072	209	010	040	065	029	089	037	071	179	097	116	164	165	005	236
154	049	087	192	062	152	076	077	201	144	125	212	176	170	231	204

Table 7: 16×16 *Matrix Evolved from Coset Diagram*

For more variability, we apply one of the permutations from S_{256} on the outcome presented in Table-7 to change the positions of the elements. This permutation increases the randomness of the elements and gives the proposed S-box with high nonlinearity, as shown in Table-8. The permutation $\alpha \in S_{256}$ used here is as follows:

(001 195 199 236 194 185 207 251 082 026 096 155 104 175 052 132 197 030 149

216 233 167 043 118 024 011 221 146 047 241 171 140 090 148 248 121 242 069 008 055 240 042 045 200 143 162 021 142 190 157 131 074 184 161 127 062 218 211 124 208 097 153 039 087 202 041 100 066 072 170 232 178 065 010 073 007 015 059 238 231 122 058 234 182 023 219 061 086 133 051 247 018 048 222 137 098 077 125 228 014 029 220 165 094 214 166 003 244 130 209 112 189 203 169 033 243 187 076 113 145 070 255 053 037 168 107 223 226 224 116 108 044 006 114 068 054 180 103 046 204 201 111 147 159 013 213 181 129 225 078 177 152 115 016 093 019 109 079 227 229 085 192 176 188 057 212 235 063 193 249 105 173 164 102 084 040 253 210 237 239 080 217 099 071 134 034 110 049 135 089 035 032 009 036 215 128 092 191 139 117 138 252 038 245 163 246 160) (000 151 083 172 020 183 028 150 198 230 120 056 067 205 136 027 095 064 002 106 250 174) (005 088 179 141 156 050 154 060 081 158 123 101 025 254 031 012 126 196 091 186 075 206 144 022) (004) (017) (119).

(This space is left because of the table on the next page)

151	129	29	93	81	240	171	105	75	229	78	195	132	216	37	226
79	158	165	69	242	97	131	106	63	252	109	66	163	186	145	38
76	166	249	4	154	208	213	183	148	184	199	77	101	21	152	15
211	230	17	103	205	155	157	173	74	82	248	126	149	190	45	169
64	6	25	98	58	224	34	48	56	1	142	40	191	243	57	42
197	203	114	222	92	95	156	160	180	80	210	46	198	137	9	91
178	212	179	167	3	128	23	107	33	99	204	2	139	227	146	138
24	43	83	162	239	14	59	30	71	245	85	175	119	47	90	223
124	236	244	12	54	150	255	136	192	251	52	147	28	120	177	65
185	26	44	207	189	31	233	117	104	53	219	116	49	118	19	70
247	18	0	86	182	27	254	13	133	87	130	241	67	193	187	84
246	225	5	217	214	8	89	16	172	62	143	51	144	174	32	127
68	100	61	20	250	159	44	196	121	123	221	215	72	110	231	209
234	164	181	50	140	237	55	200	7	36	39	238	11	206	161	96
170	112	73	253	10	220	35	168	134	141	153	108	102	94	88	194
60	135	202	176	218	115	113	125	111	22	228	235	188	232	122	201

Table 8: Proposed S−Box

Analysis for Evaluating the Strength of S-box

The criteria generally selected to test the S-box are nonlinearity, strict avalanche criteria, bit independence criteria, linear approximation probability, and differential approximation probability. For testing the strength of the proposed S-box, we discuss each of them in the following. We also compare the results with recently developed S-boxes.

Non-Linearity

Nonlinearity (NL) is one of the significant criteria for the performance evaluation of the S-box which measures the randomness of the values of the S-box. The NL of proposed S-box is 110.50 which is higher than that of [36, 37, 38, 39, 40, 41, 42]. The higher the NL, the stronger the S-box. Hence, the NL of the proposed S-box guarantees a secure communication. The NL of the proposed S-box is expressed in Table-9 and comparison with [36, 37, 38, 39, 40, 41, 42] is in Table-12.

Function of S-box	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Non-Linearity	112	110	112	110	110	108	112	110

Table 9: Non−Linearity of the Proposed S−Box

Strict Avalanche Criteria

The concept of strict avalanche criteria (SAC) was introduced by Webster and Tavares [43] which measures the confusion creation of an S-box by measuring the change in output bits due to the change in input bits. The minimum and the maximum value of SAC of the proposed S-box are 0.40625 and 0.578125, whereas the average value is 0.503175 (Table-10) which is much closer to 0.5, the ideal value of SAC. The lesser deviation from 0.5, the stronger the S-box. The comparison of SAC of the proposed S-box with that of [36, 37, 38, 39, 40, 41, 42] is in Table-12, which depicts that the proposed S-box has better SAC performance.

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0.453125	0.546875	0.484375	0.453125	0.484375	0.515625	0.500000	0.500000
0.484375	0.484375	0.453125	0.484375	0.546875	0.531250	0.453125	0.515625
0.406250	0.515625	0.531250	0.500000	0.515625	0.500000	0.531250	0.56250
0.531250	0.515625	0.437500	0.515625	0.531250	0.421875	0.500000	0.546875
0.531250	0.531250	0.500000	0.515625	0.453125	0.500000	0.468750	0.531250
0.515625	0.515625	0.546875	0.453125	0.515625	0.546875	0.453125	0.515625
0.515625	0.531250	0.484375	0.578125	0.500000	0.453125	0.500000	0.546875
0.468750	0.515625	0.546875	0.484375	0.468750	0.531250	0.546875	0.484375

Table 10: *Strict Avalanche Criteria*

Differential Approximation Probability

Differential approximation probability (DAP) is a measure to analyse the resistance of the S-box against differential attacks. The smaller the DAP, the higher the resistance against attacks. The DAP of the generated S-box is 0.0234375 which is exceptionally good. This DAP value is near to the optimal value 0.0156. This reflects that the S-box generated by group action and using coset diagrams has the ability of high resistance against differential attacks. The comparison of DAP of proposed S-box with that of some other known S-boxes is given in Table-12.

Bit Independence Criteria

Bit independence criteria also measures the strength of the S-box. The BIC value of the generated S-box is 109.21 (Table-11). The comparison with that of [36, 37, 38, 39, 40, 41, 42] is in Table-12. This BIC value is sufficiently good and assures secure communication and better encryption in cryptographic application.

0	**1**	**2**	**3**	**4**	**5**	**6**
–	106	110	110	108	108	110
106	–	108	110	110	110	106
110	108	–	108	112	110	110
110	110	108	–	108	110	108
108	110	112	108	–	110	110
108	110	110	110	110	–	110
110	106	110	108	110	110	–

Table 11: *Bit Independence Criteria*

Linear Approximation Probability

Linear approximation probability (LAP) criteria measure the strength or resistance of the S-box against linear attacks. The smaller the LAP value, the higher the strength of security of the S-box. The LAP of the generated S-box is 0.0859375 which is smaller than that of [36, 37, 38, 39, 40, 41, 42]. This depicts that the proposed scheme has ability to generate a strong, efficient, and attack resistant S-box.

The comparison of NL, SAC, BIC, LAP, and DAP with other known S-boxes is given in Table-12. The NL and the BIC value of the proposed S-box are higher than that of the others. The least values of LAP and DAP show the proposed S-box is highly resistive against the linear as well as differential attacks. And the confusion/diffusion creation criteria SAC is also closer to the standard value 0.5000.

Hence, the perfect combination of all (NL, SAC, BIC, LAP, and DAP) shows the proposed S-box is a secure choice for encryption.

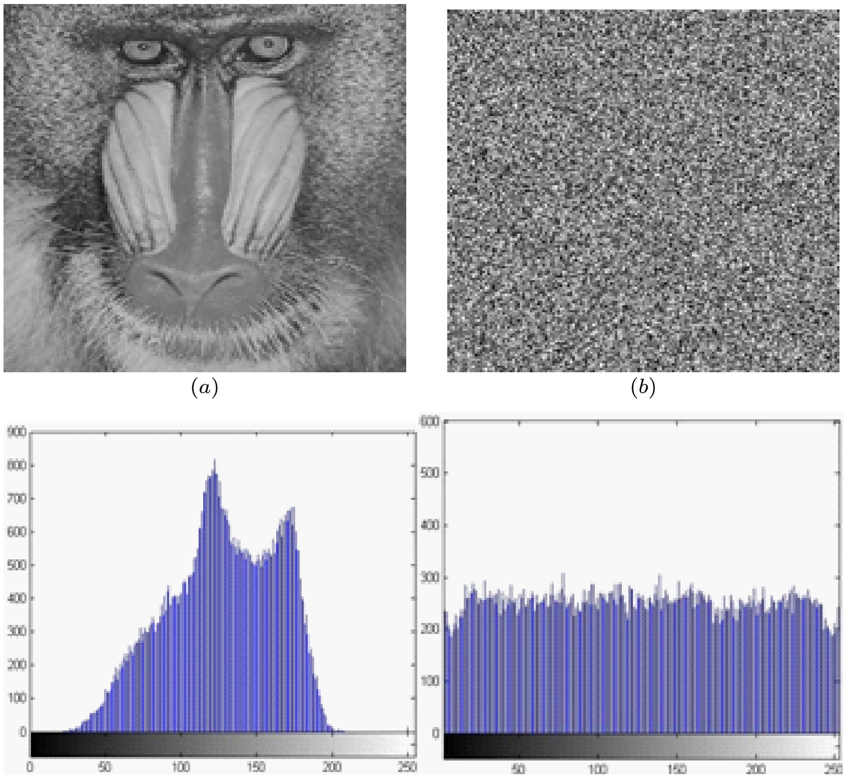
S-boxes	**Nonlinearity**	**SAC**	**BIC**	**LAP**	**DAP**
Proposed S-box	110.50	0.5031	109.21	0.0860	0.0234
Jakimoski and Kocarev [36]	103.25	0.5059	104.29	0.1250	0.0469
Tang et. al. [37]	104.88	0.4966	102.96	0.1328	0.0391
Belazi and Eilatif [38]	105.50	0.5000	103.78	0.1250	0.0468
Ullah et. al. [39]	106.00	0.5020	103.00	0.1250	0.0469
Wang et. al. [40]	110.00	0.4937	103.86	0.1250	0.0391
Razaq et. al. [41]	106.75	0.5032	103.64	0.1484	0.0469
Liu et. al. [42]	104.50	0.4980	104.64	0.1250	0.0469

Table 12: Strength Comparison of Proposed S−Box

Majority Logic Criteria

Majority logic criteria (MLC) measures image encryption strength of the S-box. Entropy, correlation, contrast, energy, and homogeneity are the components of MLC. We used JPEG image of a baboon for this analysis. Figures 11(a) and 11(c) show the original image and the histogram, while Figures 11(b) and 11(d) show the encrypted image and encrypted histogram. Specially, the entropy value which is 7.9832 is better than that of [25, 39, 41, 44, 45]. The entropy value is very close to the ideal value, which is 8. The values of contrast, correlation, energy, and homogeneity also indicate the proposed scheme provides a strong S-box which is suitable for encryption applications. The results of this analysis in comparison with well-known S-boxes are in

Table 13.



(*a*) (*b*)

(*c*) (*d*)

Figure−11: image Encryption with Proposed S−BOX

Baboon Image	Entropy	Energy	Contrast	Homogeneity	Correlation
Daemen and Rijmen [25]	7.9325	0.0211	7.2240	0.4701	0.0815
Proposed S-box	7.9832	0.0157	10.4027	0.3909	0.00073
Ullah et.al.[39]	7.9824	0.0172	8.7348	0.4074	−0.0043
Razak et.al.[41]	7.9551	0.0174	8.5267	0.4088	0.00044
Khan et.al.[44]	7.9612	0.0210	8.1213	0.4011	−0.0512
Belazi et.al.[45]	7.9252	0.0222	8.0391	0.4428	0.0119

Table 13: Majority Logic Criteria Comparision

Result Discussion

The nonlinearity of the proposd S-box is very high which shows the security strength of the S-box. The resistance against the linear attacks and the differential attacks is measured by the LAP value and the DAP value. Both the values of the proposed S-box are very small which is suitable and better for the strength of an S-box. Furthermore, the SAC of the proposed S-box is 0.503 which is very close to 0.5, perfect value of SAC. Similarly, the BIC value of the proposed S-box is better than the other well known S-boxes. Table-12 shows the comparison of all the values. This means, the proposed S-box is an excellent choice for the cryptographic applications because it is a perfect combination of NL, SAC, LAP, DAP and BIC. The image of babon is used for MLC. The values of contrast, energy, homogeneity, correlation and entropy shows that the proposed S-box is suitable for image encryption.

Conclusion

In this chapter, we found one relator quotients of the modular group related to Fibonacci sequence of numbers. The words obtained in chapter three are now utilised as additional relation in the modular group and then the resultant quotients are investigated. Finally, to identify these quotients we used Tietze transformations and on some places ‘Groups, Algorithms and Programming’ (GAP). This is a class of generalized triangular group which we investigated as quotients of the modular group. Furthermore, from this class of quotients we choose one quotient, which is A_4, and by taking action of A_4 on $PL(F_{257})$ we construct an algebraic S-box. By investigating the security strength parameters of this S-box, we conclude this S-box is highly secure for the communication and highly preferable for cryptographic applications.

Chapter 5

All one Relator Quotients of the Modular Group

Since one relator quotients of the modular group are of the form $< x, y : x^2 = y^3 = w(x, y) = 1 >$ where $w(x, y) = x^{r_1}y^{s_1}x^{r_2}y^{s_2}...x^{r_k}y^{s_k}$. In chapter three, we fixed the powers of the generators as Fibonacci sequence of numbers and found one relator quotients of the modular group. To find one relator quotients of the modular group with all variations of powers of x and y and for all syllable of $w(x, y)$ is a gigantic problem. A step towards this problem, we find number of cyclically reduced non-equivalent words with all variations of powers of x and y and for all syllable of $w(x, y)$. By this we come to know that how many one relator quotients of the modular group exists corresponding to each syllable k. Thus, by considering all variations of powers of the generators in $w(x, y)$ we are able to count the number of one relator quotients of the modular group. For this goal, we prove some important results in this chapter.

5.1 Number of One-Relator Quotients of the Modular Group

Number of one relator quotients of the modular group are equal to the number of cyclically reduced non-equivalent words for every k; the syllable of $w(x, y)$. Therefore, firstly we find all the possibilities for the additional relator $w(x, y) = 1$ for each syllable k then find number of cyclically reduced non-equivalent words. In the following theorem we obtain a formula for the number of all possible words for any syllable k.

Theorem 18 *Let $w(x, y) = xy^{s_1}xy^{s_2}...xy^{s_k}$ be the word generated by x and y then for a specific syllable k, there are exactly 2^k words generated by x and y.*

Proof. *In $w(x, y)$, positions and powers of x are fixed. Therefore, it is sufficient to count the possibilities of $y^{s_1}y^{s_2}...y^{s_k}$. By using the multiplication rule of counting, if k objects each have two possibilities then there are exactly 2^k arrangments of the objects. Thus, there are 2^k words having syllable k generated by x and y.* ■

As an illustration, we choose a fix k and find all the words of syllable k which are generated by x and y.

Let $k = 5$ then by Theorem-18 there are $2^5 = 32$ total words.

$N(x_w)$	$N(y_w)$	*cyclically reduced words*
5	5	$xyxyxyxyxy$
5	6	$xyxyxyxyxy^2$
5	6	$xyxyxyxy^2xy$
5	6	$xyxyxy^2xyxy$
5	6	$xyxy^2xyxyxy$
5	6	$xy^2xyxyxyxy$
5	7	$xyxyxyxy^2xy^2$
5	7	$xyxyxy^2xy^2xy$
5	7	$xyxy^2xy^2xyxy$
5	7	$xy^2xy^2xyxyxy$
5	7	$xy^2xyxyxyxy^2$
5	7	$xyxyxy^2xyxy^2$
5	7	$xyxy^2xyxy^2xy$
5	7	xy^2xyxy^2xyxy
5	7	$xyxy^2xyxyxy^2$
5	7	$xy^2xyxyxy^2xy$
5	8	$xyxyxy^2xy^2xy^2$
5	8	$xyxy^2xy^2xy^2xy$
5	8	$xy^2xy^2xy^2xyxy$
5	8	$xy^2xy^2xyxyxy^2$
5	8	$xy^2xyxyxy^2xy^2$
5	8	$xyxy^2xy^2xyxy^2$
5	8	$xy^2xy^2xyxy^2xy$
5	8	$xy^2xyxy^2xyxy^2$
5	8	$xyxy^2xyxy^2xy^2$
5	8	$xy^2xyxy^2xy^2xy$
5	9	$xyxy^2xy^2xy^2xy^2$
5	9	$xy^2xy^2xy^2xy^2xy$
5	9	$xy^2xy^2xy^2xyxy^2$
5	9	$xy^2xy^2xyxy^2xy^2$
5	9	$xy^2xyxy^2xy^2xy^2$
5	10	$xy^2xy^2xy^2xy^2xy^2$

Table 14: *All words of length* 5

We extend this table with other variations of $N(x_w)$ and $N(y_w)$ which are infinite in number.

From Table-14, it is very clear that ${}^5C_0$ words having five y and no y^2, ${}^5C_1$ words having four y and one y^2, ${}^5C_2$ words having three y and two y^2, ${}^5C_3$ words having two y and three y^2 and ${}^5C_4$ words having one y and four y^2, and ${}^5C_5$ words having no y

and five y^2. Thus, in general, ${}^kC_i$ represents the number of words having syllable k with y^2 appearing i times and y appears $k-i$ times.

5.2 Additional Relations in view of Circuits

In the discussion of all possible non-equivalent words for each syllable k, firstly we eliminate the cyclically equivalent words. Figure-4 is an easy way to understand cyclically equivalent words. Secondly, there exist inverses of the words. Inverses are just the conversion of inside triangles to outside triangles and outside triangles of the circuit to inside. Thus, algebraically words and their inverses play the same role. We therefore eliminate the inverses. One can view this in the following figures-12 and figure-13.

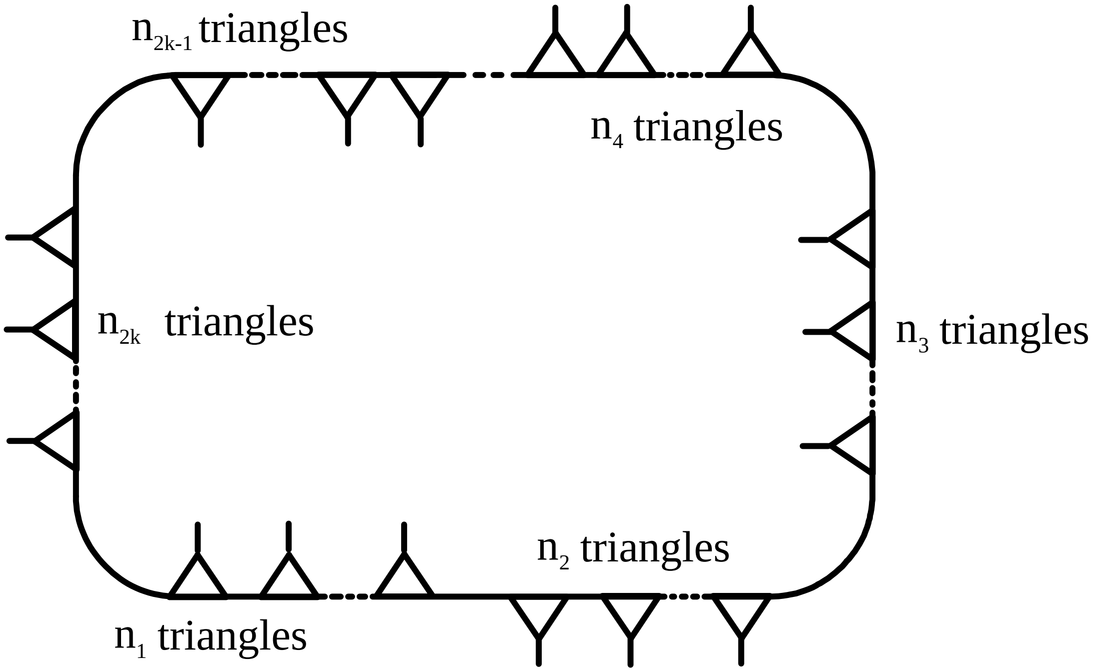


Figure 12: Ci*rcuit of the type* $(n_1, n_2, \ldots, n_{2k})$

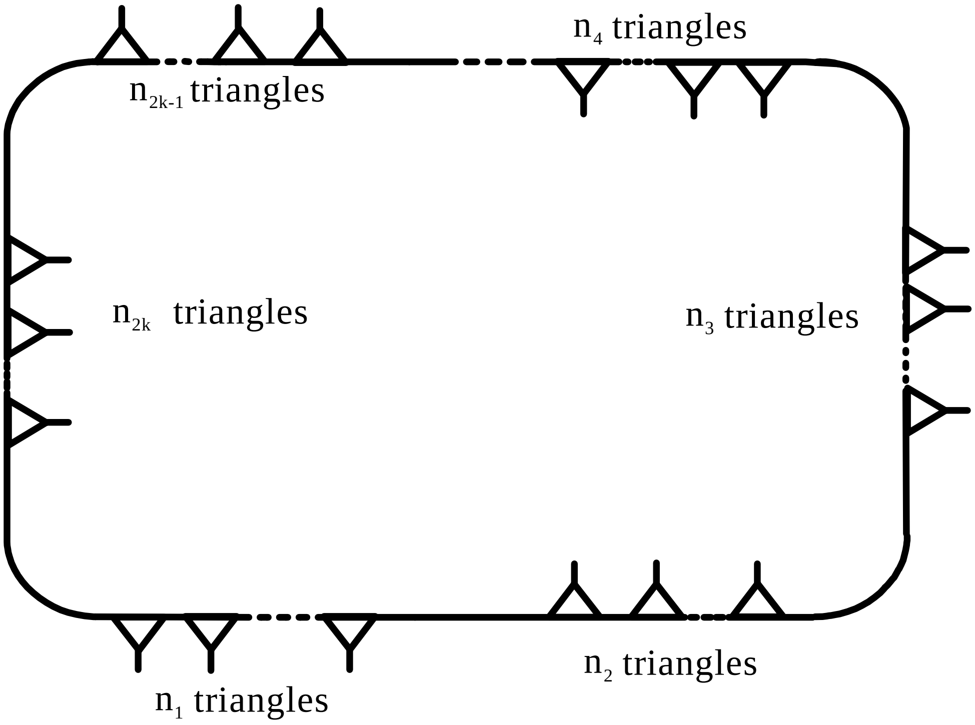


Figure 13: *Inverse of the* Ci*rcuit* $(n_1, n_2, \ldots, n_{2k})$

Now we discuss non-equivalent words. For any syllable k, we prove the result for number of non-equivalent words. These non-equivalent words contain x, y and y^2. There are two types of circuits corresponding to additional relations.

Type-I These circuits consists of all triangles with one vertex inside or all triangles with one vertex outside of the main frame of the circuit. This type of circuits exists only when the word is of the form $(xy)^k$ or $(xy^2)^k$. It is pertinent to mention here that addition of such words gives triangle groups as quotient of the modular group. For different values of k, geometry of the triangle groups is discussed in chapter 1. For $k > 6$, the triangle groups are of infinite order and finite for other values of k.

Type-II These circuits consists of some triangles with one vertex inside and some triangles with one vertex out side of the main frame of the circuits. These circuits are always of even length. Length of the circuit is the number of variations from inside triangles to outside triangles and outside triangles to inside triangles. A Circuit of length two is represented by (a, b) with a number of triangles inside and b number of triangles outside of the main frame of the circuit. A theorem of Q. Mushtaq [47] which assures there exists a real quadratic irrational number of the type $\alpha = \frac{a+\sqrt{n}}{c}$ where n is square free positive integer, in the circuit of the orbit of $PSL(2, \mathbb{Z})$ acting on $PL(F_q)$. The length of the circuits also depends upon the syllable of the word. For illustration, let $k = 6$ and consider all cyclically reduced non-equivalent words. The word $xyxyxyxyxyxy$ or $(xy)^6$ shows that all the triangles are inside the circuit (so of Type-I) and gives the triangle group $\Delta(2, 3, 6)$. The word $xyxyxyxyxyxy^2$ depicts that five triangles are inside the circuit while one triangle is outside the circuit and the circuit is is of the form $(5, 1)$. Similarly, the circuit for the word $xyxyxyxyxy^2xy^2$ is $(4, 2)$ and for $xyxyxyxy^2xy^2xy^2$ is $(3, 3)$. The circuit corresponding to the word $xyxyxyxy^2xyxy^2$ consists of three triangles inside, one triangle outside, one triangle inside and one triangle outside, that is, circuit is of the type $(3, 1, 1, 1)$ and length of the circuit is four. Same is the case with $xyxyxy^2xyxyxy^2$, $xyxyxy^2xyxy^2xy^2$ and $xyxyxy^2xy^2xyxy^2$. Now the only remaining word is $xyxy^2xyxy^2xyxy^2$. Here, the circuit is of the form $(1, 1, 1, 1, 1, 1)$, that is, six triangles alternatively inside and outside of the main frame of the circuit.

On the other hand, due to different combinations of circuit types one can reversely find cyclically reduced non-equivalent words. Precisely, all the combinations of making 6 (in even combinations) are $6 = 6 + 0 = 5 + 1 = 4 + 2 = 3 + 3 = 1 + 1 + 1 + 3 = 1 + 2 + 1 + 2 = 1 + 1 + 2 + 2 = 2 + 2 + 1 + 1 = 1 + 1 + 1 + 1 + 1 + 1$. These nine combinations provide nine cyclically reduced non-equivalent words.

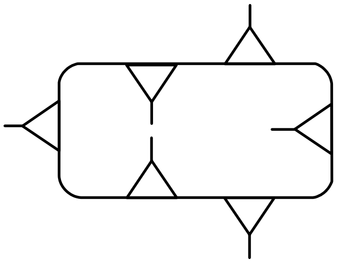


Figure 14(*a*): *Circuit* (1,1,1,1,1,1)

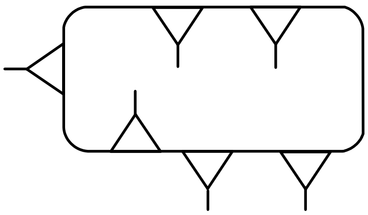


Figure 14(*b*): *Circuit* (1,2,2,1)

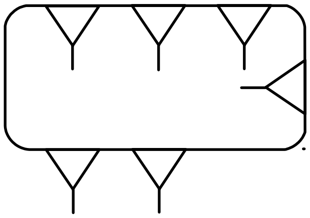


Figure 14(*c*): *Circuit* (4,2)

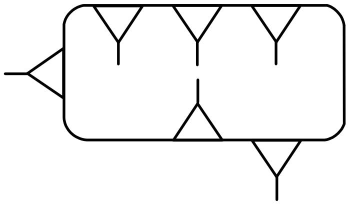


Figure 14(*d*): *Circuit* (1,1,1,3)

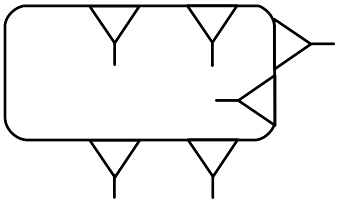


Figure 14(*e*): *Circuit* (1,1,2,2)

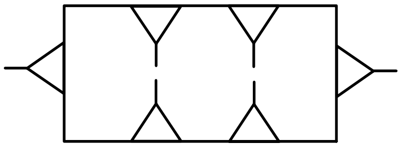


Figure 14(*f*): *Circuit* (1,2,1,2)

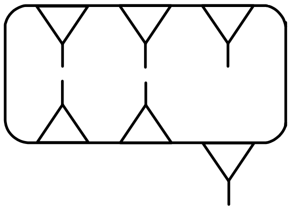


Figure 14(*g*): *Circuit* (5,1)

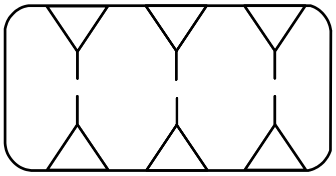


Figure 14(*h*): *Circuit* (6,0)

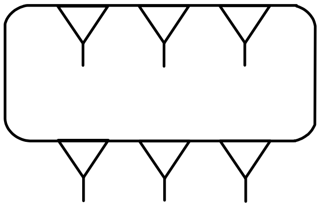


Figure 14(*i*): *Circuit* (3,3)

5.3 Number of Cyclically Reduced Non-Equivalent Words

If two words w and $w^{'}$ are equivalent by definition then the corresponding quotients are isomorphic. So, there is a need to identify the equivalent words which we eliminate from the total possibilities to get a small list of non-equivalent words and consequently quotients of the modular group.

Remark 19 *Let $w(x,y) = xy^{s_1}xy^{s_2}...\ xy^{s_k}$ be a word and all $s_{i's}$ are same in $w(x,y)$ then no other word is equivalent to $w(x,y)$.*

Proof. Obvious from the definition. ■

Remark 20 *Let $w(x,y) = xy^{s_1}xy^{s_2}...\ xy^{s_k}$ be a word and $s_{i'_s}$ are alternatively 1 and 2. Then the words equivalent to $w(x,y)$ are either 1 or 2. If $s_1 = s_k$ then there are two equivalent words while otherwise only one equivalent word.*

Proposition 21 *If $w(x,y) = xy^{s_1}xy^{s_2}...\ xy^{s_k}$ be a word then the words which are equivalent to $w(x,y)$ are at the most $k-1$.*

The following theorem is important because it gives the number of non-equivalent words for a fixed syllable k.

Theorem 22 *If k is the syllable of a word $w(x,y)$ then number of cyclically non-equivalent words are $2+\sum\limits_{i=1}^{k-1} t_i$, where $t_i = \left\lceil \frac{{}^kC_i}{k} \right\rceil$ for $1 \leq i \leq k-1$.*

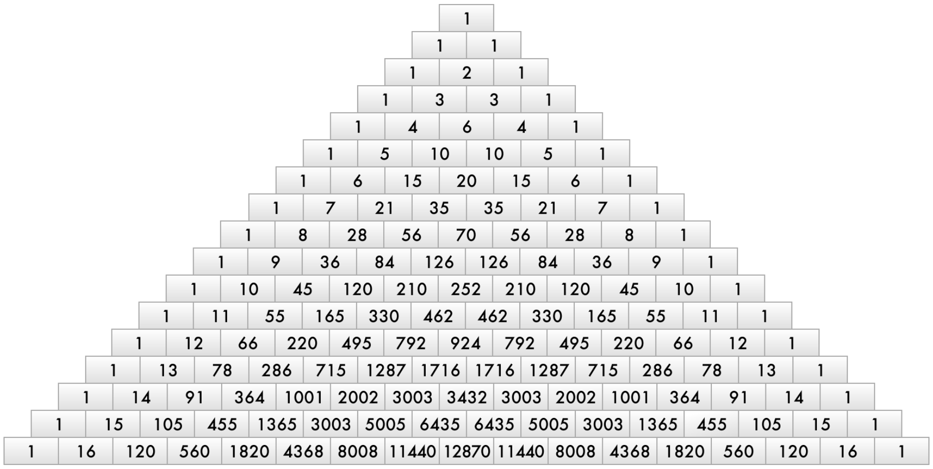
Proof. If syllable of $w(x,y) = k$, then by Theorem-18 there are exactly 2^k words of syllable k which are distributed in $k+1$ classes as $2^k{=}\sum\limits_{i=0}^{k} {}^kC_i$. Also each row of the Pascal triangle satisfies $2^k{=}\sum\limits_{i=0}^{k} {}^kC_i$. Therefore, there is a relationship between rows of the Pascal triangle and the number of cyclically non-equivalent words. Thereupon, we utilize the similarity of rows of the Pascal triangle with syllable of the words. The k^{th} row of Pascal triangle is associated with the words of syllable k. And each element ${}^kC_i$ (for $1 \leq i \leq k$) of the row k represents i number of y^2 appear in $w_k^*(x,y)$, that is, $N(y^2_{w_k^*}) = i$. Clearly, ${}^kC_0$ and ${}^kC_k$ represent $(xy)^k$ and $(xy^2)^k$. These words have no other equivalent words by Remark 19. For the remaining ${}^{k}C_1$ to ${}^{k}C_{k-1}$, we represents each class having ${}^{k}C_i$ words by Ψ_i. Every class Ψ_i is non-empty so there exists a word say $w^1(x,y) \in \Psi_i$. Then by proposition-21, there are $k-1$ other words must exist which are equivalent to $w^1(x,y)$. If ${}^{k}C_i > k$, then there exists another word say $w^2(x,y) \in \Psi_i$ and by proposition-21 there exist $k-1$ more words which are equivalent to $w^2(x,y)$. Similarly, If ${}^{k}C_i > 2k$, then there exist some $w^3(x,y) \in \Psi_i$ and the process continues until, one reaches on a point where $kt \leq {}^{k}C_i < k(t+1)$ with t a non-negative integer. Thus, there are exactly t words each have $k-1$ number of equivalent words. Along with those, there is a unique word having less than $k-1$ equivalent words and the existence of such words is discussed in remark 20. Thus, the total number of cyclically non-equivalent words for each Ψ_i are $t_i = \left\lceil \frac{{}^{k}C_i}{k} \right\rceil$. Hence, number of cyclically non-equivalent words are $2 + \sum_{i=1}^{k-1} t_i$. This completes the proof.

■

In cyclically non-equivalent words another important property exists. That is, some words and their inverses both exist in cyclically non-equivalent words. According to J. Howie, V. Metaftsis and R. M. Thomas [3] words and their inverses are equivalent especially in the case when they are treated as additional relation in a group. Furthermore, by Theorem-8, if the equivalent words are inserted in a group as additional relation then the corresponding quotients are same. Thus, there is a need to identify and then eliminate either words or their inverses from the cyclically non-equivalent words, to get a precise list of non-equivalent words. In this connection, firstly we establish a result for the number of non-equivalent words (by eliminating inverses of the words) for each syllable k. After that, we discuss some prperties of words and their inverses which help to identify equivalent and non-equivalent quotients.

Theorem 23 *If k is the syllable of a word $w(x,y)$ then number of non-equivalent words are $1+\sum\limits_{i=1}^{\left[\frac{k}{2}\right]} t_i$ where $t_i = \left\lceil \frac{{}^kC_i}{k} \right\rceil$ for $1 \leq i \leq k-1$ and $\left[\frac{k}{2}\right]$ is the greatest integer function.*

Proof. If syllable of $w(x,y) = k$, then by Theorem-18, there are exactly 2^k words of syllable k which are distributed in $k+1$ classes as $2^k{=}\sum\limits_{i=0}^{k} {}^kC_i$. Also the sum of each row of the Pascal triangle also satisfies $2^k{=}\sum\limits_{i=0}^{k} {}^kC_i$. So, there is a relationship between rows of the Pascal triangle and the number of cyclically reduced non-equivalent words for corresponding syllable. Theorem 22 gives cyclically non-equivalent words. Now by eliminating inverse of each word we get number of cyclically reduced non-equivalent words. As, inverses can be get by replacing y to $y^2$and y^2 to y in $w(x,y)$. Therefore, avoiding the inverses we consider number of y greater than number of y^2 in $w(x,y)$, or otherwise. That is, this divides the Pascal triangle in to two equal halves vertically.



1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1
1 6 15 20 15 6 1
1 7 21 35 35 21 7 1
1 8 28 56 70 56 28 8 1
1 9 36 84 126 126 84 36 9 1
1 10 45 120 210 252 210 120 45 10 1
1 11 55 165 330 462 462 330 165 55 11 1
1 12 66 220 495 792 924 792 495 220 66 12 1
1 13 78 286 715 1287 1716 1716 1287 715 286 78 13 1
1 14 91 364 1001 2002 3003 3432 3003 2002 1001 364 91 14 1
1 15 105 455 1365 3003 5005 6435 6435 5005 3003 1365 455 105 15 1
1 16 120 560 1820 4368 8008 11440 12870 11440 8008 4368 1820 560 120 16 1

Figure 15: Pascal Triangle Division for Non−Equivalent Words

Therefore, we now only consider cyclically reduced words having 0 to $\frac{k}{2}$ number of ones in power of y. By using Theorem-22, it becomes ${}^{k}C_0 + \sum_{i=1}^{\left[\frac{k}{2}\right]} t_i$ where t_i is number of cyclically reduced words in each Ψ_i. This completes the proof. ■

Proposition 24 *Let $N(x_w) = k_1$, $N(y_w) = k_2$ be the two possible numbers then the number of cyclically reduced non-equivalent words for $[k_1, k_2]$ and for $[k_1, 3k_1 - k_2]$ are equal.*

As an illustration of all the above discussion, we provide the following example.

Example 25 *Consider Table-14 of all words of length 5. Then by Theorem 8, Theorem 18, Theorem 22, Theorem 23 and Proposition 24 we have the following Table-15 of cyclically reduced non-equivalents words which give different quotients.*

$N(x_w)$	$N(y_w)$	$Cyclically\ reduced\ non-equivalent\ words$
5	5	$xyxyxyxyxy$
5	6	$xyxyxyxyxy^2$
5	7	$xyxyxyxy^2xy^2$
5	7	$xyxyxy^2xyxy^2$

Table 15: Cyclically Reduced Non−Equivalent words

Thus, the classification of all one relator quotients of the modular group on the basis of equivalent and non-equivalent words is presented. It gives a method (in the form of Theorem 8, Theorem18, Theorem 22, Theorem 23 and Proposition 24) to find a precise list of quotients which is sufficient instead of inquiring all the quotients of the modular group for that syllable.

Now we discuss some other relationship between the equivalent words which helps us to investigate non-equivalent words and consequencelly quotients of the modular group. By using the inversion, one can easily prove xy^r is equivalent to xy^{3-r} where r

is either 1 or 2. By using this fact, the words $xy^{r_1}xy^{r_2}$ and $xy^{3-r_2}xy^{3-r_1}$ are also equivalent and consequently by adding these words in $PSL(2,\mathbb{Z})$, the resultant quotients are also same. Similarly, we can extend this for the words of higher syllables.

Proposition 26 *Let $PSL(2,\mathbb{Z}) =< x,y : x^2 = y^3 = 1 >$ be the modular group then the one-relator quotients $Q_1 =< x,y : x^2 = y^3 = xy^{r_1}xy^{r_2}xy^{r_3}...xy^{r_k} = 1 >$ and $Q_2 =< x,y : x^2 = y^3 = xy^{3-r_k}xy^{3-r_{k-1}}...xy^{3-r_1} = 1 >$ are isomorphic where for each i, r_i is either 1 or 2.*

Concluding the entire discussion, we are now giving a brief table presenting number of words for each syllable and number of cyclicall reduced non-equivalent words for each syllable.

Syllable of the words	Total number of words	Number of cyclically reduced non-equivalent words
1	2	1
2	4	2
3	8	2
4	16	4
5	32	4
6	64	9
7	128	10
8	256	22
9	512	30
10	1024	66
11	2048	84
12	4096	212
13	8192	316
14	16384	711
15	32768	1095
16	65536	2453
17	131072	3856
18	262144	8636
19	524288	57558
20	1048576	30837
21	2097152	49935
22	4194304	111061
23	8388608	182362
24	16777216	405867
25	33554432	671091

Table−16: Number of non−equivalent words

By using the Theorem-23, one can extend the table-16 of non-equivalent words upto any syllable k.

Conclusion

Firstly we discussed number of all possible words for any syllable $k \in \mathbb{N}$. For this, Pascal triangle gives number of all such possible combinations. Secondly, we eliminated the cyclically equivalent words from the total possible words. A formula was established in this regard. Furthermore, we reduced the list by eliminating the inverses of the words and established a formula for cyclically reduced non-equivalent words for each syllable $k \in \mathbb{N}$. Thus, in consequence of Theorem-22 and Theorem-23**,** a precise list for number of cyclically reduced non-equivalent words was obtained. Thus, in this chapter, we discussed number of one relator quotients of the modular group with no limits on syllable of the aditional relation.

REFERENCES

[1] H. S. M. Coexter and W. O. J. Moser, Generators and Relations for Discrete Groups, 2nd Edition, Springer, 1965.

[2] R. G. Swan, Generators and Relations for certain Special Linear Groups, Advances in Mathematics, $6(1971), 1-77$.

[3] J. Howie, V. Metaftsis and R. M. Thomas, Finite Generalized Triangle Groups, Transactions of the American Mathematical Society, $347(1995), 3613-3623$.

[4] L. Levai, G. Rosenberger and B. Souvignier, All Finite Generalized Triangle Groups, Transactions of the American Mathematical Society, $347(1995), 3625-3627$.

[5] G. Baumslag, J. W. Morgan and P. B. Shalen, Generalized Triangle Groups, Mathematical Proceedings of the Cambridge Philosophical Society, 102(1987), $25-31$.

[6] B. Fine and G. Rosenberger, A Note on Generalized Triangle Groups, Abhandlungen aus dem Mathematischen Seminar der Universitat Hamburg, $56(1986), 233-244$.

[7] G. A. Miller, On the Groups Generated by Two Operators, Bulletin of the American Mathematical Society, $7(1901), 424-426$.

[8] Q. Mushtaq, A Condition for the existance of a fragment of a coset diagram, The Quarterly Journal of Mathematics, $1(1988), , 81-95$

[9] Q. Mushtaq, Modular Group Acting on Real Quadratic Fields, Bulletin of the Australlian Mathematical Society, 37(1988), $303-309$.

[10] G. Higman and Q. Mushtaq, Coset Diagrams and Relations for $PSL(2,\mathbb{Z})$, Arab Gulf Journal of Scientific Research, $1(1983), 159-164$.

[11] Y. T. Ulutas and I. N. Cangul, One Relator Quotients of the Modular Group, Bulletin of the Institute of Mathematics Academia Sinica, $32(2004), 291-296$.

[12] G. A. Miller, Groups Defined by the Orders of two Generators and the Order of their Product, American Journal of Mathematics, $24(1902), 96-100$.

[13] M. Conder, Three-Relator Quotients of the Modular Group, Quarterly Journal of Mathematics, Oxford, $38(1987), 427-447$.

[14] M. Edjvet, On certain Quotients of the Triangle Groups, Journal of Algebra, $169(1994), 367-391$.

[15] V. Metaftsis and I. Miyamoto, One-Relator Product of two Groups of Order three with Short Relators, Kyushu Journal of Mathematics, $52(1998), 81 - 97$.

[16] M. Conder, G. Havas and M. F. Newman, On One-Relator Quotients of the Modular Group, Groups St Andrews, 11(2009), $183 - 197$.

[17] Y. T. Ulutas and I. N. Cangul, One Relator Quotients of the Hecke Group $H(\frac{1+\sqrt{5}}{2})$, Bulletin of the Institute of Mathematics Academia Sinica, $31(2003), 59 - 74$.

[18] H. B. Ozdemir, Y. T. Ulutas and I. N. Cangul, Normal Subgroups of the Hecke Group $H(\sqrt{2})$ Corresponding to One-Relator Quotients of small Order, International Journal of Contemporary Mathematical Sciences, $1(2006), 15-23$.

[19] M. Aslam, A. Ali and R. Ahmad, One-Relator Quotients of the Hecke Group $H(\sqrt{3})$, Quasigroups and Related Systems, $19(2011), 173 - 182$.

[20] I. Kapovich and P. E. Schupp, Random Quotients of the Modular Group are Rigid and Essentially Incompressible, Journal Reine Angewandte Mathematik, $628(2009), 91 - 119$.

[21] A. Torstensson, Coset Diagrams in the Study of Infinitly Presented Groups with an Application to Quotients of the Modular Group, Journal of Commutative Algebra, $2(2010), 501 - 514$.

[22] Q. Mushtaq and A. Rafiq, Adjacency Matrices of $PSL(2, 5)$ and Resemblance of its Coset Diagrams with Fullerene C_{60}, Algebra Colloquium, $4(2013), 541 - 552$.

[23] Q. Mushtaq and N. Mumtaz, $PSL(2, 7)$ and Carbon Allotrope D168 Schwarzite, Journal of Mathematical Chemistry, 56(2018), DOI No. $10.1007/s10910 - 018 - 0900 - y$.

[24] D. E. Standard, National Bureau of Standards, NBS FIPS PUB 46, US Department of Commerce, Gaithersburg, MD, USA, 1977.

[25] J. Daemen and V. Rijmen, The Design of Rijndael: AES-The Advanced Encryption Standard, Springer Science & Business Media, Berlin, Germany, 2013.

[26] L. Cui and Y. Cao, A New S-box Structure Named Affine-Power-Affine, International Journal of Innovative Computing, Information and Control, $3(2007), 751 - 759$.

[27] E. Biham and A. Shamir, Differential Cryptanalysis of DES-Like Cryptosystems, Journal of Cryptology, $1(1991), 3 - 72$.

[28] T. Shah, I. Hussain, M. A. Gondal and H. Mahmood, Statistical Analysis of S-box in Image Encryption Applications Based on Majority Logic Criterion, International Journal of Physical Sciences, $16(2011), 4110 - 4127$.

[29] I. Hussain, T. Shah, H. Mahmood, M. A. Gondal and U. Y. Bhatti, Some Analysis of S-box based on Residue of Prime Number, Proceedings of the Pakistan Academy of Sciences, $2(2011), 111 - 115$.

[30] D. Lambic, A Novel Method of S-box Design Based on Chaotic Map and Composition Method, Chaos Solitons & Fractals, $58(2014), 16 - 21$.

[31] E. Al Solami, M. Ahmad, C. Volos, M. N. Doja and M. M. S. Beg, A New Hyperchaotic System-Based Design for Efficient Bijective Substitution-Boxes, Entropy, 7(2018), DOI No. $10.3390/e20070525$.

[32] Y. Wang, L. Yang, M. Li and S. Song, A Method for Designing S-box Based on Chaotic Neural Network, Proceedings of the 2010 6th International Conference on Natural Computation, $2(2010), 1033 - 1037$.

[33] G. Chen, Y. Chen and X. Liao, An Extended Method for Obtaining S-boxes Based on Three Dimensional Chaotic Baker Maps, Chaos Solitons & Fractals, $3(2007), 571 - 579$.

[34] U. Hayat and N. A. Azam, A Novel Image Encryption Scheme Based on an Elliptic Curve, Signal Processing, $155(2019), 391 - 402$.

[35] A. Altaleb, M. S. Saeed, I. Hussain and M. Aslam, An Algorithm for the Construction of Substitution Box for Block Ciphers Based on Projective General Linear Group, AIP Advances, 3(2017), DOI No. 10.1063/1.4978264.

[36] G. Jakimoski and L. Kocarev, Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps, IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, $2(2001), 163 - 169$.

[37] G. Tang, X. Liao and Y. Chen, A Novel Method for Designing S-boxes Based on Chaotic Maps, Chaos Solitons & Fractals, $2(2005), 413 - 419$.

[38] A. Belazi and A. A. A. El-latif, A Simple yet Efficient S-box Method Based on Chaotic Sine Map, Optik, $130(2017), 1438 - 1444$.

[39] A. Ullah, S. S. Jamal and T. Shah, A Novel Construction of Substitution Box using a Combination of Chaotic Maps with improved Chaotic Range, Nonlinear Dynamics, $4(2017), 2757 - 2769$.

[40] Y. Wang, P. Lei and K. W. Wong, A Method for Constructing Bijective S-box with High Non-Linearity Based on Chaos and Optimization, International Journal of Bifurcation and Chaos, 10(2015), DOI No. $10.1142/S0218127415501278$.

[41] A. Razaq, A. Awais, U. Shuaib, N. Siddiqui, A. Ullah and A. Waheed, A Novel Construction of Substitution Box Involving Coset Diagram and a Bijective Map, Security and Communication Networks, 2017, DOI No. 10.1155/2017/5101934.

[42] L. Liu, Y. Zhang and X. Wang, A Novel Method for Constructing the S-box Based on Spatiotemporal Chaotic Dynamics, Applied Sciences, 12(2018), DOI No. 10.3390/app8122650.

[43] A. F. Webster and S. E. Tavares, On the Design of S-boxes, Proceedings of the 1985 Conference on the Theory and Application of Cryptographic Techniques, Springer, $1985, 523 - 534$.

[44] M. Khan, T. Shah and S. I. Batool, Construction of S-box Based on Chaotic Boolean Functions and its Application in Image Encryption, Neural Computing and Applications, $3(2016), 677 - 685$.

[45] A. Belazi, M. Khan, A. A. A. El-Latif and S. Belghith, Efficient Cryptosystem Approaches: S-boxes and Permutation Substitution-based Encryption, Nonlinear Dynamics, $1(2017), 337 - 361$.

[46] I. Younas and M. Khan, A New Efficient Digital Image Encryption Based on Inverse Left Almost Semi group and Lorenz Chaotic System, Entropy, 913(2018), DOI No. 10.3390/e20120913.

[47] Q. Mushtaq, On Word Structure of the Modular Group over Finite and Real Quadratic Fields, Discrete Mathematics, $178(1998), 155 - 164$.

turnitin Turnitin Originality Report

A Class of Generalized Triangle Groups as Quotients of PGL(2,Z). by Imran Shahzad .

From DRSM (DRSM L)

- Processed on 29-Sep-2020 09:57 PKT
- ID: 1400034103
- Word Count: 19702

Confirmed.
Qaiser Mushtaq
30.09.2020

Similarity Index
16%
Similarity by Source

Internet Sources:
8%
Publications:
13%
Student Papers:
6%

Focal Person (Turnitin)
Quaid-i-Azam University
Islamabad

sources:
1

1% match (Internet from 26-Oct-2017)

http://staff.itee.uq.edu.au/havas/ORQMG/orqmgw.pdf
2

1% match (student papers from 17-Jan-2017)

Submitted to Higher Education Commission Pakistan on 2017-01-17
3

1% match (student papers from 09-Jul-2015)

Submitted to Higher Education Commission Pakistan on 2015-07-09
4

< 1% match (student papers from 01-Nov-2014)

Submitted to Higher Education Commission Pakistan on 2014-11-01
5

< 1% match (Internet from 07-Mar-2016)

http://prr.hec.gov.pk/Chapters/1880S-1.pdf
6

< 1% match (publications)

Marston Conder. "The genus of compact riemann surfaces with maximal automorphism group", Journal of Algebra, 1987