ON GROUPS OF ODD ORDER WITH EXACTLY TWO NON-CENTRAL CONJUGACY CLASSES OF EACH SIZE

Thesis submitted in partial fulfillment of the requirement for

The award of the degree of

Masters of Science

In

Mathematics and Computing

Submitted by

Sakshi

Roll no. - 30703018

Under

the guidance of

Dr. Deepak Gumber

JULY 2009

School of Mathematics and Computer Applications

Thapar University

Patiala-147004 (PUNJAB)

INDIA

Dedicated to
God,
Parents and Teachers

CERTIFICATE

*I hereby certify that the work which is being presented in the thesis entitled "**On Groups of Odd Order with Exactly Two Non-central Conjugacy Classes of Each Size** " in partial fulfillment of the requirements for the award of degree of Master of Science , School of Mathematics and Computer Applications, Thapar University, Patiala is an authentic record of my own work carried out under the supervision of Dr. Deepak Gumber.*

The matter presented in this thesis has not been submitted for the award of any other degree of this or any other university.

Sakshi
(Sakshi)

(Registration No. 30703018)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(Dr. Deepak Gumber)
Assistant Professor
SMCA, Thapar University
Patiala

Countersigned by:

Dr. S.S. Bhatia 13.7.09
(Professor & Head)
School of Mathematics & Computer Applications
Thapar University, Patiala.

Dr. R.K. Sharma 24/7/09
Dean of Academic Affairs
Thapar University
Patiala.

ACKNOWLEDGEMENT

I feel privileged to express my sincere regards and gratitude to my supervisor Dr. Deepak Gumber for their expert guidance, cool temperament, valuable suggestions, support, advice and continuous encouragement throughout the course of my thesis work.

I am highly obliged to Prof. S.S. Bhatia, Head SMCA, Thapar University, Patiala, for their motivation and inspiration that trigged me for thesis work.

I would like to thank all the staff members and my co-students who were always there at the need of the hour and provided with all the help and facilities, which I required for the completion of my thesis.

I am also thankful to the authors whose works I have consulted and quoted in this work.

Last but not the least I would like to thank God for not letting me down at the time of crisis and showing me the silver lining in the dark clouds.

(Sakshi)

TABLE OF CONTENTS

Chapter-1

Introduction

Understanding conjugacy classes is essential to the investigation of groups. One of the first major results regarding conjugacy classes is due to Landau [6], who showed that for some given natural number r, the equation

$$1 = \sum_{i=1}^{r} \frac{1}{m_i}$$

when m_r are natural numbers, has a finite number of solutions. By setting $m_i = o(C_G(g_i))$ where g_i are representatives of the conjugacy classes of a finite group *G*, then the class equation

$$1 = \sum_{i=1}^{r} \frac{1}{o(C_G(g_i))}$$

is such an equation. Therefore, for given *r*, the number of finite groups with *r* conjugacy classes is bounded.

An interesting family of question arises: In what way does the numerical information about conjugacy classes of a finite group (the number of classes and their sizes) affect its structure?

We give some examples of such results:

* Burnside [2] has the following results:

1) A simple group has no conjugacy class of prime power size.

2) A classification of all groups G with a conjugacy class of size o(G)/2.

3) A classification of all groups with up to 5 conjugacy classes.

* Poland [9] extends Burnside's work and classifies all groups with upto 8 conjugacy classes.

* In 1973, F.M.Markel [7,8] studied finite solvable groups in which distinct conjugacy classes have distinct sizes.

A well known open conjecture states that S_3 is the only non-abelian finite group with conjugacy classes of distinct sizes. For solvable groups, this conjecture was proved by Zhang in [10] and independently by Knor, Lempken and Thielcke in [5]. As shown in [1], if G is a finite group, then the two conditions: (i) the conjugacy classes of G are of distinct sizes, and (ii) the non-central conjugacy classes of G are of distinct sizes, are equivalent to each other. In this note we give a shorter proof of this result (see Corollary 3.3).

If G is a finite group of odd order, then each size of a non-central conjugacy class of G appears an even number of times (see Lemma 3.1). Therefore, the corresponding problem for groups of odd order is to determine all such groups with exactly two non-central conjugacy classes of each size. The main aim of this thesis is to solve this problem.

It is interesting to notice that the proof of this problem uses only very elementary results in group theory and in number theory. In particular, we do not use the famous result of Feit and Thompson [3] about the solvability of groups of odd order.

Chapter-2

Notations and Preliminaries

Throughout this thesis G denotes a finite group unless stated otherwise. We first define some terms and prove some results which are used in this thesis.

Definition 2.1 (Order of a set) The cardinality of set X is called the order of the set X and it is denoted by $o(X)$.

Definition 2.2 (Permutation) Let X be a non-empty set. A one-one and onto function $f : X \to X$ is called a permutation on X.

Definition 2.3 (Symmetric group) Let X be a non empty set. The group of all permutations on X under the composition of mappings is called the symmetric group on X and is denoted by S_X.
If $o(X) = n$, S_X is denoted by S_n and called the symmetric group of degree n and order $n!$.

Definition 2.4 (Order of an element) Let G be a group and let $a \in G$. The least positive integer m such that $a^m = e$ is called the order of a. If no such

positive integer exists, then *a* is said to be of infinite order. The order of a is denoted as $o(a)$.

Theorem 2.5 Let *G* be a finite group and let $a \in G$ be an element of order *n*. Then $a^m = e$ if and only if *n* is a divisor of *m.*

Proof: Firstly, let *n* is a divisor of *m,* where $o(a) = n$. So there exists a positive integer *q* such that $m = nq$. Now $a^m = a^{nq} = (a^n)^q = e^q = e$.

Conversely, let $a^m = e$, where $o(a) = n$. Suppose *m* is not divisible by *n.* Dividing *m* by *n,* $m = nq + r$ where $q, r \in I$ and $o \le r < n$.

Thus $e = a^m = a^{nq+r} = a^{nq}.a^r = (a^n)^q.a^r = e^q.a^r = a^r$, a contradiction, since $o(a) = n$. Thus *r*=0 and hence *m* is divisible by *n.*

Theorem 2.6 Let *G* be a group and let $a \in G$ be an element of order *m*. Then $o(a^k) = \frac{m}{(m,k)}$ where $k \in N$.

Proof: Let $o(a^k) = t$. Now $a^{kt} = (a^k)^t = e$, but $o(a) = m$. Thus by theorem 2.5, $m \mid kt$. Let $d = (m,k)$. Thus $d \mid m$ and $d \mid k$. Let $m = m_1 d$ and $k = k_1 d$ where $(m_1, k_1) = 1$. So $\frac{m}{d} = m_1$. Thus we need to prove $m_1 = t$. Now $m \mid kt$, so $m_1 d \mid k_1 dt$. Thus $m_1 \mid k_1 t$, but $(m_1, k_1) = 1$.

Hence $m_1 \mid t$. ---------- (1)

Again $(a^k)^{m_1} = a^{km_1} = a^{k_1 dm_1} = a^{k_1 m} = (a^m)^{k_1} = e$, but $o(a^k) = t$.

Thus $t \mid m_1$. ---------- (2)

From (1) and (2), we get $m_1 = t$. This proves the theorem.

Definition 2.7 (Center of a group) The center of a group *G*, written *Z* (*G*), is the set of those elements of *G* that commute with every element in *G*, i.e. $$Z(G) = \{a \in G \mid ax = xa \forall x \in G\}$$

Remark *G* is abelian if and only if *Z*(*G*)=*G*.

Definition 2.8 (Normalizer or centralizer of an element)

Let *G* be a group, $a \in G$ be any element. Then the subset $N_G(a) = C_G(a) = \{x \in G \mid xa = ax\}$ is called the normalizer or centralizer of *a* in *G*.

Definition 2.9 (Cosets) Let *H* be a subgroup of G. Given $a \in G$, the set $aH = \{ah \mid h \in H\}$ is called the left coset of *H* determined by *a* and the set $Ha = \{ha \mid h \in H\}$ is called the right coset of *H* determined by *a*.

The set of all left cosets of *H* in *G* is written as G/H and $G/H = \{xH \mid x \in G\}$.

Definition 2.10 (Right congruence modulo a subgroup) Let *G* be a group and *H* be a subgroup of *G*. Given $a, b \in G$, *a* is said to be right congruent to *b* *modulo H* {symbolically $a \equiv_r b (\mathrm{mod}\, H)$ } if and only if $ab^{-1} \in H$.

Theorem 2.11 If *G* is a group and *H* is a subgroup of *G*. Then the relation $\equiv_r$ of right congruence modulo *H* is an equivalence relation on *G*. Further for any $a \in G$ the set $\{ha \mid h \in H\}$ is the equivalence class to which *a* belongs.

Proof: Let $a, b \in G$ and *e* be the identity of *H*.

1) Reflexivity: Since $aa^{-1} = e \in H$, $a \equiv_r a (\mathrm{mod}\, H)$.

2) Symmetry: Let $a \equiv_r b (\mathrm{mod}\, H)$, so $ab^{-1} \in H$. Thus $(ab^{-1})^{-1} = ba^{-1} \in H$. Hence $b \equiv_r a (\mathrm{mod}\, H)$.

3) Transitivity: Let $a \equiv_r b (\mathrm{mod}\, H)$ and $b \equiv_r c (\mathrm{mod}\, H)$. So $ab^{-1} \in H$ and $bc^{-1} \in H$. Thus $ac^{-1} = (ab^{-1})(bc^{-1}) \in H$. Hence $a \equiv_r c (\mathrm{mod}\, H)$.

Thus the relation of right congruence modulo *H* is an equivalence relation on *G.* Let *cl(a)* denote the equivalence class to which *a* belongs i.e. $cl(a) = \{b \in G \mid b \equiv_r a (\mathrm{mod}\, H)\}$. Let *Ha* denote the set $\{ha \mid h \in H\}$.Now $b \in cl(a)$ gives $b \equiv_r a (\mathrm{mod}\, H)$. So $ba^{-1} \in H$. Thus $b = (ba^{-1})a \in Ha$. Hence $cl(a) \subseteq Ha$. Again $c \in Ha$ gives $c = ha$ for some $h \in H$. Thus $ca^{-1} = h \in H$. So $c \equiv_r a (\mathrm{mod}\, H)$ and hence $c \in cl(a)$. Therefore, $Ha \subseteq cl(a)$. Thus $Ha = cl(a)$.

Theorem 2.12 (Lagrange) The order of any subgroup of a finite group divides the order of the group.

Proof: Let *G* be a finite group and *H* be a subgroup of *G.* Suppose $o(H) = n$. For any $a \in G$, define $f : H \to Ha$ such that $f(h) = ha$. This mapping is onto as each member of *Ha* is of type $ha, h \in H$. Further for any two elements $h_1, h_2 \in H$, let $f(h_1) = f(h_2)$. So $h_1 a = h_2 a$. Then by right cancellation law, $h_1 = h_2$. Hence *f* is a 1-1 mapping of *H* onto *Ha.* This means that $o(H) = o(Ha)$. Let $Ha_1, Ha_2, ..., Ha_t$ be the totality of distinct right cosets of *H* in *G.* Then these *t* right cosets constitute the totality of distinct equivalence classes in *G* determined by the relation of right congruence modulo *H*, by theorem 2.11. Thus $Ha_1, Ha_2, ..., Ha_t$ are disjoint subsets of *G* and $G = Ha_1 \cup Ha_2 \cup ... \cup Ha_t$.

As seen above $o(Ha_i) = o(H) = n \ \ \forall i = 1,2,...,t$. Therefore $o(G) = nt$. Hence $o(H) \mid o(G)$.

Definition 2.13 (Index of a subgroup) Let *G* be a group and *H* be a subgroup of *G*. Then the number of right (left) cosets of *H* in *G* is called the index of *H* in *G*. It is denoted by [*G:H*].

Theorem 2.14 If *a, b* be any elements of a group *G* such that $ab = ba$ and $(o(a), o(b)) = 1$. Then $o(ab) = o(a)o(b)$.

Proof: Let $o(a) = m$ and $o(b) = n$, where $(m,n) = 1$. Let $o(ab) = k$. To show that *k*=*mn*, where $ab = ba$. Now

$$e = (ab)^{nk} = a^{nk}b^{nk} = a^{nk}(b^n)^k = a^{nk}e^k = a^{nk}e = a^{nk}$$

i.e. $a^{nk} = e$, but $o(a) = m$. Thus by theorem 2.5, $m \mid nk$, but $(m,n) = 1$.

Therefore, $m \mid k$. ……. (1)

Similarly, $b^{mk} = e$, but $o(b) = n$. Thus, $n \mid mk$, but $(m,n) = 1$.

Thus, $n \mid k$. ……. (2)

From (1) and (2), we get $[m,n] \mid k$ …… (3)

But $[m,n] \cdot (m,n) = mn$, so $[m,n] \cdot 1 = mn$. From (3), we have $mn \mid k$. …..(4)

Again $(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n (b^n)^m = e^n e^m = ee = e$, but $o(ab) = k$.

Thus $k \mid mn$. …….(5)

From (4) and (5), we get $k = mn$. Hence, $o(ab) = o(a)o(b)$.

Definition 2.15 (Euler function $\phi(n)$) For any positive integer *n*, $\phi(n)$ is defined as follows:

$\phi(1)=1$ and for $n>1$, we have $\phi(n)$ =The number of positive integers less than n and co prime to n .If p is a prime number, then $\phi(p)=p-1$.

Definition 2.16 (Cyclic group) A group G is called a cyclic group if there exists $a \in G$ such that each element of G can be written as an integral power of a. We write, $G=\langle a \rangle$, i.e. G is generated by a.

Theorem 2.17 A finite group of order n is cyclic if and only if it has an element of order n.

Proof: Let G be a cyclic group of order n and let a be generator of G. Put $H=\{a^i \mid i \in Z\}$. Clearly H is a subgroup of G. As G is finite, a can not be of infinite order. Let $o(a)=m$. We claim that H has m elements. Now $a, a^2, ..., a^{m-1}, a^m = e$ all belong to H and no two of them are equal as $o(a)=m$. Hence H has at least m elements. Let $x \in H$ and $x=a^j, j \in Z$. Now $j=mk+r,\ 0 \le r < m$, k and r are integers. Then $x=a^j=(a^m)^k a^r=a^r$. So any element of H is one of $a, a^2, ..., a^{m-1}, a^m$. Hence $H=\{a, a^2, ...a^m\}$. This proves our claim. Since $G=\langle a \rangle, G \subseteq H$. In other words G=H and so $n=o(G)=o(H)=m=o(a)$.

Conversely, let G be a group of order n and $b \in G$ be of order n. As before $K=\{b^r \mid r \in Z\}$ is a subgroup of G having n elements as $o(b)=n$. Since $K \subseteq G$ and $o(K)=n=o(b), K=G$. Consequently G is a cyclic group generated by b.

Remark Now let G be any group and $a \in G$. Let $H=\{a^n \mid n \in Z\}$. Consider any two elements $x=a^n, y=a^m$ in H. We find that $xy^{-1}=a^n a^{-m}=a^{n-m} \in H$.

This implies that *H* is a subgroup of *G*. Clearly *H* is a cyclic group generated by *a*. This subgroup is called a ***cyclic subgroup*** of *G* generated by *a* and we write $H = \langle a \rangle$.

Theorem 2.18 If *G* is a finite group then order of any element of *G* divides the order of *G.*

Proof: Let *G* be a finite group and $a \in G$. Let $H = \langle a \rangle$ be a cyclic subgroup of *G* generated by *a*. Then by theorem 2.17, $o(H) = o(a)$. By Lagrange's theorem, $o(H) \mid o(G)$. Hence $o(a) \mid o(G)$.

Theorem 2.19 Every cyclic group is abelian.

Proof: Consider a cyclic group generated by a. Let $x, y \in G$ be arbitrary elements. Then $x = a^n$ and $y = a^m$ for some *n* and *m.* Consider $xy = a^n a^m = a^{n+m} = a^{m+n} = a^m a^n = yx$. Thus *G* is an abelian group.

Theorem 2.20 If *p* is prime and *o*(*G*)=*p,* then G is a cyclic group.

Proof: Take $a \in G$ with $a \neq 1$. Then the cyclic subgroup $\langle a \rangle$ has more than one element (it contains *a* and 1), and its order $o(\langle a \rangle) > 1$ is a divisor of *p*. Since *p* is prime, $o(\langle a \rangle) = p = o(G)$, and so $\langle a \rangle = G$.

Theorem 2.21 The number of generators of a finite cyclic group of order *n* is $\phi(n)$.

Proof: Let *G* be a cyclic group of order *n* generated by *a*.Thus $o(G) = n = o(a)$. Also any element of *G* is of the form a^k for some integer *k.*

Thus by theorem 2.6, we have $o(a^k) = \frac{n}{(n,k)}$ ---------- (1)

Also, we know that the order of the generator of a cyclic group is equal to the order of the group. So if a^k is to be the generator of *G*, then $o(a^k) = n$. Thus from (1), $(n,k) = 1$. So the number of positive integers less than *n* and relatively prime to *n* will satisfy the above relation.

Hence number of generators of *G* is $\phi(n)$.

Definition 2.22 (Centralizer of a subgroup) If *H* is a subgroup of a group *G*, denoted as $H \leq G$, then the centralizer of *H* in *G* is

$$C_G(H) = \{x \in G \mid xh = hx \ \forall \ h \in H\} .$$

Definition 2.23 (Normalizer of a subgroup) If $H \leq G$, the normalizer of *H* in *G*, denoted by $N_G(H)$ is

$$N_G(H) = \{a \in G \mid aH = Ha\}.$$

Definition 2.24 (Conjugate element) An element $b \in G$ is called a conjugate of $a \in G$ if there exists some $g \in G$ such that $b = gag^{-1}$.

Definition 2.25 (Conjugacy class) Let *G* be a group and let $x \in G$. Then the set $x^G = \{gxg^{-1} \mid g \in G\}$ is called the conjugacy class of *x* in *G*.

Lemma 2.26 The relation of conjugacy in a group *G* is an equivalence relation.

Proof: Let *a, b, c* be any arbitrary elements of *G*.

1) Reflexive: Since $a = eae^{-1}$, thus $a \sim a$.

2) Symmetric: Let $a \sim b$. So there exist $g \in G$ such that $a = gbg^{-1}$.

Thus $g^{-1}ag = b$. Hence $b \sim a$.

3) Transitive: Let $a \sim b$ and $b \sim c$. So, there exist $g, h \in G$ such that $a = gbg^{-1}$ and $b = hch^{-1}$.

Consider $a = gbg^{-1} = g(hch^{-1})g^{-1} = ghc(gh)^{-1}$. Hence $a \sim c$. This proves the lemma.

Lemma 2.27 Let G be a group. Then the set of conjugacy classes of G is a partition of G.

Proof: Define a relation $\sim$ on G as follows:

$a \sim b$ if $a = gbg^{-1}$ for some $g \in G$.

By lemma 2.26, it is an equivalence relation on G. The equivalence class of a in G is then the set $\{gag^{-1} \mid g \in G\}$, which is also the conjugacy class of a.

Thus, the set of conjugacy classes of G is a partition of G.

Lemma 2.28 Let G be a group. Then $o(a^G) = [G : N(a)]$.

Proof: Let $a \in G$. Then the mapping $\sigma : a^G \to G/N(a)$ given by $\sigma(xax^{-1}) = xN(a)$ is trivially onto.

The mapping is one-one: Let $x, y \in G$. Then $xN(a) = yN(a)$ gives $y^{-1}x \in N(a)$.

Thus $y^{-1}xa = ay^{-1}x$ and hence $xax^{-1} = yay^{-1}$.

Therefore, σ is a bijection, proving $o(a^G) = o(G/N(a)) = [G : N(a)]$.

Theorem 2.29 (The Class Equation)

Let G be a finite group and let $g_1, g_2, ..., g_r$ be the representatives of the distinct conjugacy classes of G not contained in the center $Z(G)$ of G. Then

$$o(G) = o(Z(G)) + \sum_{i=1}^{r} [G : N(g_i)]$$

Proof: Let $x \in Z(G)$. Then, $cl(x) = \{x\}$, since then $gxg^{-1} = x \forall g \in G$.

So $\{x\}$ is a conjugacy class of order 1.

Let $Z(G) = \{1, z_2, ..., z_m\}$ and let $K_1, K_2, ..., K_r$ be the distinct conjugacy classes of G not contained in the center and g_i be the representative of K_i for each i. Then the full set of conjugacy classes of G is given by

$$\{1\}, \{z_2\}, ..., \{z_m\}, K_1, K_2, ..., K_r$$

Since by lemma 2.27,these partition G, we have

$$o(G) = \sum_{i=1}^{m} 1 + \sum_{i=1}^{r} o(K_i)$$

$$= o(Z(G)) + \sum_{i=1}^{r} [G : N(g_i)]$$

This proves the class equation.

Definition 2.30 (p-group) A finite group G is called a p-group (p is prime), if order of every element of G is a power of p. i.e. if $x \in G$, then $o(x) = p^m$ for some $m \geq 0$.

Theorem 2.31 Let G be a finite group of order p^n, where p is a prime and $n>0$. Then G has a non-trivial center Z.

Proof: Consider the class equation of G,

$$o(G) = o(Z) + \sum_{x \in C} [G : N(x)]$$

where C contains exactly one element from each conjugacy class containing more than one element.

As $N(x) \leq G$, by Lagrange's theorem, $o(N(x)) \mid o(G)$. If $x \notin Z$, then $o(N(x)) < p^n$. Thus, $[G : N(x)] > 1$. So $[G : N(x)] = p^r; 1 \leq r \leq n$. Hence, $p \mid [G : N(x)] \ \forall x \notin Z$. Therefore, $p \mid \sum_{x \in C} [G : N(x)]$. Also, $p \mid o(G)$. Thus, $p \mid \left(o(G) - \sum_{x \in C} [G : N(x)] \right)$ which gives $p \mid o(Z)$. Hence Z is non-trivial.

Lemma 2.32 If p is a prime, then every group G of order p^2 is abelian.

Proof: Let G be a group of order p^2. Then by theorem 2.31, center of G, say Z, is non-trivial. Since $o(Z) \mid p^2$, $o(Z) = p \text{ or } p^2$. If $o(Z) = p^2$, then $G=Z$ and hence abelian. Let $o(Z) = p$. Consider the quotient group G/Z. Clearly, $o(G/Z) = \frac{p^2}{p} = p$. Thus, by theorem 2.20, G/Z is cyclic.

Let $G/Z = \langle xZ \rangle$.

Let $a, b \in G$, then $aZ, bZ \in G/Z$. Thus, $aZ = x^m Z, bZ = x^n Z$ for some $m, n \geq 0$.

Hence, $a = x^m z_1, b = x^n z_2$ for some $z_1, z_2 \in Z$. Now

$$ab = x^m z_1 x^n z_2 = x^m x^n z_1 z_2 = x^{m+n} z_1 z_2 = x^{n+m} z_1 z_2 = x^n x^m z_2 z_1$$
$$= x^n z_2 x^m z_1 = ba .$$

Thus G is abelian.

Lemma 2.33 (Cauchy's theorem for abelian groups) Let G be a finite abelian group and let p be a prime. If $p \mid o(G)$, then G has an element of order p.

Proof: We prove the result by induction on $o(G) = n$. Assume result is true for all abelian groups of order less than n. If $o(G) = p$ or G is cyclic, then G has an element of order p. So, suppose that $\exists b(\neq e) \in G$ such that $\langle b \rangle \neq G$. If $p \mid o(\langle b \rangle)$, then we are done. So, let p does not divide $o(\langle b \rangle)$, but $p \mid o(G)$. So $p \mid \frac{o(G)}{o(\langle b \rangle)}$ i.e. $p \mid o\left(G/\langle b \rangle\right)$. By induction hypothesis, $G/\langle b \rangle$ has an element say $\bar{a}$ of order p. So $(\bar{a})^p = \langle b \rangle$. Thus $\overline{a^p} = \langle b \rangle$. Let $o(a) = k$. Then $a^k = 1$. Thus $\overline{a^k} = \bar{1} = \langle b \rangle$ i.e. $(\bar{a})^k = \langle b \rangle$. So $p \mid k(= o(a))$. Therefore $p \mid o(\langle a \rangle)$. Hence $\langle a \rangle$ has and hence G has an element of order p.

Definition 2.34 (Sylow p-subgroup) Let G be a finite group. Let p be a prime such that $p^m \mid o(G)$ but p^{m+1} does not divide $o(G)$.A subgroup of G of order p^m is called a sylow p-subgroup of G.

Example: $o(S_3) = 6 = 2 \cdot 3$

$\{1,(12)\}, \{1,(13)\}, \{1,(23)\}$ are sylow 2-subgroups of S_3.

Definition 2.35 (Subnormal series) A sequence $\{e = G_0, G_1, ..., G_r = G\}$ of subgroups of a group G is called a subnormal series of G if $G_i \triangleleft G_{i+1},\ 0 \leq i \leq r$

.

Definition 2.36 (Solvable series) A subnormal series of a group G with abelian factor groups is called a solvable series. A group G is said to be ***solvable*** if it has a solvable series.

Definition 2.37 (Homomorphism) Let $(G,*)$ and $(H,\cdot)$ be two groups. A function $f: G \to H$ is a homomorphism if $\forall a,b \in G$

$$f(a*b) = f(a)\cdot f(b)$$

An ***Isomorphism*** is a homomorphism that is also a bijection.

Definition 2.38 Let $f: G \to H$ be a homomorphism and define

$$\text{Kernel } f = \{a \in G \mid f(a) = 1\} \text{ and}$$

$$\text{Image } f = \{h \in H \mid h = f(a) \text{ for some } a \in G\}$$

We usually write Ker f instead of kernel f and im f instead of image f. It is easy to verify that Ker f and im f are subgroups of G and H respectively.

Theorem 2.39 Ker f is a normal subgroup of G.

Proof: Let $f: G \to H$ be a homomorphism. Let $a \in Ker\ f$, then $f(a) = 1$.

Let $g \in G$. Consider $f(gag^{-1}) = f(g)f(a)f(g)^{-1} = f(g)f(g)^{-1} = 1$.

Thus, $gag^{-1} \in Ker\ f$. Hence, $g(Ker\ f)g^{-1} \leq Ker\ f \ \ \forall g \in G$. Therefore, $Ker\ f \lhd G$.

Theorem 2.40 (First Isomorphism Theorem) Let $f: G \to H$ be a homomorphism with kernel K. Then K is a normal subgroup of G and $G/K \cong im\ f$.

Proof: As seen above, $K \lhd G$. Define $\phi: G/K \to H$ by $\phi(aK) = f(a)$.

To see that ϕ is well-defined, assume that $aK = bK$ *i.e.* $a^{-1}b \in K$. Then $1 = f(a^{-1}b) = f(a)^{-1} f(b)$. Thus $f(a) = f(b)$; it follows that $\phi(aK) = \phi(bK)$, as desired.

ϕ is a homomorphism:

$\phi(aKbK) = \phi(abK) = f(ab) = f(a)f(b) = \phi(aK)\phi(bK)$**.**

Clearly, $im\ \phi = im\ f$. Finally, we show that ϕ is an injection.

If $\phi(aK) = \phi(bK)$, then $f(a) = f(b)$; hence $f(ab^{-1}) = 1$ i.e. $ab^{-1} \in K$. Thus $aK = bK$. Hence $G/K \cong im\ f$.

<u>Lemma 2.41 (N/C Lemma)</u> If H is a subgroup of a group G, then $C_G(H) \lhd N_G(H)$ and $N_G(H)/C_G(H)$ can be embedded in $Aut(H)$.

<u>Proof</u>: If $a \in G$, let γ_a denote conjugation by a. i.e. $\gamma_a : G \to G$ by $\gamma_a(x) = axa^{-1}$. Define $\phi : N_G(H) \to Aut(H)$ by $\phi(a) = \sigma_a$ where $\sigma_a = \gamma_a|_H$, γ_a restricted to H. Now $\sigma_a(h) = aha^{-1} \in H$ since $a \in N_G(H)$. Thus $\sigma_a : H \to H$ is an automorphism and hence $\sigma_a \in Aut(H)$.

ϕ is a homomorphism: Consider

$$\sigma_{ab}(h) = abh(ab)^{-1} = abhb^{-1}a^{-1} = a\sigma_b(h)a^{-1} = \sigma_a(\sigma_b(h)) = (\sigma_a\sigma_b)(h)$$

Thus $\phi(ab) = \sigma_{ab} = \sigma_a\sigma_b = \phi(a)\phi(b)$.

Now we will prove $\ker\phi = C_G(H)$. Now $a \in \ker\phi$, so $\phi(a) \equiv \sigma_a \equiv I$. Thus, $\sigma_a(h) = I(h) \forall h \in H$ i.e. $aha^{-1} = h \forall h \in H$. Hence $a \in C_G(H)$. Therefore, $\ker\phi \subseteq C_G(H)$.

By reversing the steps, we will get $C_G(H) \subseteq \ker\phi$. Thus $\ker\phi = C_G(H)$.

By theorem 2.40, $C_G(H) \triangleleft N_G(H)$ and $N_G(H)/C_G(H) \cong im\phi \leq Aut(H)$.This proves the lemma.

Definition 2.42 (Exponent) Let *G* be a group. The least positive integer *n* such that $x^n = 1 \; \forall x \in G$ is called the exponent of *G*. If no such *n* exists, then we say exponent of *G* is infinite. It is denoted as *exp(G)*.

Definition 2.43 (Unit) If *R* is a ring with identity 1, then a unit is an element *x* of *R* which has both a right inverse *y* and a left inverse *z*. These are then equal, since $z = z \cdot 1 = zxy = 1y = y$.

Theorem 2.44 If *R* is a ring with identity 1, then the set *U* of units of *R* is a group under multiplication.

Proof: U is non-empty since $1 \cdot 1 = 1$. So $1 \in U$. Let $x \in U$ and $y \in U$. Then $(xy)(y^{-1}x^{-1}) = x1x^{-1} = xx^{-1} = 1$,

$(y^{-1}x^{-1})(xy) = y^{-1}1y = y^{-1}y = 1$. Hence $xy \in U$. Since $1 \cdot x = x \cdot 1 = x \;\; \forall x \in U$,1 is the identity for *U*. If $x \in U$, then $xx^{-1} = x^{-1}x = 1$, so $x^{-1} \in U$. Also, x^{-1} is an inverse for *x*. Hence *U* is a group.

Theorem 2.45 The multiplicative group of non-zero elements of a finite field is cyclic.

Proof: Let *F* be a finite field of order *q* and let $F^* = F \setminus \{0\}$. Then F^* is an abelian group of order *q-1*. Let $\exp(F^*) = n$. Clearly $n \leq q-1$. Then $x^n = 1 \; \forall x \in F^*$. Now $x^n - 1$ can have at most *n* roots in F^* but it has *q-1* roots in F^*. So $q - 1 \leq n$. Hence *n=q-1*.

Since $\exp(F^*) = n$, there must be an element $a \in F^*$ such that $o(a) = n = q-1$. So F^* is cyclic generated by *a*.

Definition 2.46 (Congruence class) The Congruence class of an integer *a* *mod n* is given by

$$[a] = \{b \in Z : b \equiv a \bmod n\} = \{a + kn : k \in Z\}.$$

The set Z_n of all the congruence classes mod n is called the set of integers modulo n; it is an abelian group when equipped with the operation: $[a]+[b]=[a+b]$; here $e=[0]$ and $[-a]+[a]=[0]$. Z_n is even a commutative ring with "one" as [1] and multiplication is defined by $[a][b]=[ab]$.

Remark We know, $Z_n = \{[0],[1],...,[n-1]\}$.

By theorem 2.44, the set Z_n^* of units of this ring forms a multiplicative group.

Example: If *n=12*, then $Z_n = \{[0],[1],...,[11]\}$ and $Z_n^* = \{[1],[5],[7],[11]\}$.

Theorem 2.47 If $n \geq 2$, then

$$Z_n^* = \{[m] \mid 0 < m < n, (m,n) = 1\}$$

$$Z_n^* = \{[m] \mid o([m]) = n \ \ in \ \ (Z_n, +)\}.$$

Proof: Clearly, $[0] \notin Z_n^*$. Let 0 < m < n. If $[m] \in Z_n^*$, then $\exists\, r$ such that $[m][r]=[1]$ i.e. $(m+nZ)(r+nZ) = 1+nZ$. So $mr+nZ = 1+nZ$ i.e. $mr \in 1+nZ$. Let $mr = 1-ns$ where $-s \in Z$. Thus $\exists$ - $s \in Z$ such that $mr+sn=1$. Hence $(m,n)=1$. If $(m,n)=1$, then $\exists\, r \in Z$ and $s \in Z$ such that $mr+ns=1$ i.e. $mr=1-ns$. Hence $mr \equiv 1 (\bmod n)$. If $o([m]) = t \ in \ Z_n$, then $t[m]=[0]$. Now $t[m] = [m]+[m]+...+[m]$ $= [m+m+...+m] = [tm]$. Thus $[tm]=[0]$. Hence $tm \equiv 0 (\bmod n)$. Therefore,

$t \equiv t \cdot 1 \equiv t(mr) \equiv (tm)r \equiv 0 (\mathrm{mod}\, n)$.

Hence $t \geq n$. Also $n \geq t$. Thus $t = n$.

Finally, if $o([m]) = n \text{ in } Z_n$, then the *n* elements $[m], 2[m], ..., n[m]$ are all distinct.

Hence $\exists\, t$ such that $t[m] = [1]$, so that $[t][m] = [1]$. Therefore $[m] \in Z_n^*$.

Theorem 2.48 Z_p is a field, where *p* is prime.

Proof: We know Z_p is a commutative ring with unity. If 0 < m < p, then $(m, p) = 1$. Therefore, Z_p^* consists of all non-zero elements of Z_p, by theorem 2.47. Thus all non-zero elements of Z_p are invertible. Hence Z_p is a field.

Result Let $T : G \to G$ be one-one homomorphism and $a \in G$ be such that $o(a) = n$. Then $o(a) = o(T(a))$.

Proof: Now $o(a) = n$ so $a^n = 1$. Consider $[T(a)]^n = T(a^n) = T(1) = 1$. Thus $o(T(a)) \mid n$. Suppose $o(T(a)) = m < n$. Thus $(T(a))^m = 1$ i.e. $T(a^m) = 1$. Since *T* is one-one, so $a^m = 1$, which is a contradiction. Hence $o(a) = o(T(a))$.

Theorem 2.49 $Aut(Z_n) \cong Z_n^*$, if $n \geq 2$.

Proof: For all $T \in Aut(Z_n)$, let $f(T) = T[1]$. Now by above result $o(T[1]) = o([1]) = n.$ Therefore, by theorem 2.47, *f* is a function from $Aut(Z_n)$ into Z_n^*. If also $U \in Aut(Z_n)$ and $T[1] = U[1]$, then $T[i] = U[i]$ $\forall i$, so that *T*=*U*. This means that *f* is 1-1. Let $[i] \in Z_n^*$, consider the function $T : Z_n \to Z_n$ given by $T[j] = [ij]$. Clearly it is onto.

***T* is a homomorphism:**

Now $T([j]+[k]) = T([j+k]) = [i(j+k)] = [ij+ik] = [ij]+[ik] = T[j]+T[k]$.

***T* is one-one:**

Suppose $T[j] = T[k]$ i.e. $[ij] = [ik]$. So $ij + nZ = ik + nZ$. Thus

$ij - ik = i(j-k) \in nZ$. Let $i(j-k) = nr$ for some $r \in Z$. Then $[i(j-k)] = [0]$ i.e.

$[i][j-k] = [0]$. Since $[i] \in Z_n^*$, so it is invertible. Thus we have

$[i]^{-1}[i][j-k] = [0]$ i.e. $[j]-[k] = [0]$. Hence $[j] = [k]$.

Thus T is an automorphism of Z_n and $f(T) = T[1] = [i]$. Thus f is onto Z_n^*.

Finally, if $T[1] = [i]$ and $U[1] = [k]$ with T and U in $Aut(Z_n)$, then

$TU[1] = T[k] = T(k[1]) = kT[1] = k[i] = [k][i] = [i][k] = T[1]U[1]$.

Hence $f(TU) = f(T)f(U)$. Therefore f is an isomorphism of $Aut(Z_n)$ onto Z_n^*.

<u>Definition 2.50 (Mobius function)</u> The Mobius function $\mu(n)$ is defined as follows:

$$\mu(1) = 1 \ ;$$

If $n>1$, write $n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$, where p_i are distinct primes and $a_i \geq 1$ are integers. Then

$$\mu(n) = (-1)^k \text{ if } a_1 = a_2 = \ldots = a_k = 1,$$

$$\mu(n) = 0 \quad \text{otherwise.}$$

Note that $\mu(n) = 0$ if and only if n has a square factor greater than 1.

Here is a short table of values of $\mu(n)$:

n:	1	2	3	4	5	6	7	8	9	10
$\mu(n)$:	1	-1	-1	0	-1	1	-1	0	0	1.

Theorem 2.51 If $n \geq 1$ we have $\sum_{d|n} \mu(d) = \left[\frac{1}{n}\right] = \begin{cases} 1 \ \textit{if} \ n = 1 \\ 0 \ \textit{if} \ n > 1 \end{cases}$.

Proof: The formula is clearly true if $n = 1$. Assume, then, that $n > 1$ and write $n = p_1^{a_1} p_2^{a_2} \ldots . p_k^{a_k}$. In the sum $\sum_{d|n} \mu(d)$ the only non-zero terms come from $d = 1$ and from those divisors of *n* which are products of distinct primes. Thus

$$\sum_{d|n} \mu(d) = \mu(1) + \mu(p_1) + \ldots + \mu(p_k) + \mu(p_1 p_2) + \ldots + \mu(p_{k-1} p_k) + \ldots + \mu(p_1 p_2 \ldots p_k)$$

$$= 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \ldots + \binom{k}{k}(-1)^k = (1-1)^k = 0 .$$

Theorem 2.52 If $n \geq 1$ we have $\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$.

Proof: We know $\phi(n) = \sum_{k=1}^{n}{}' 1$, where the $'$ indicates that the sum is extended over those *k* relatively prime to *n*. This sum can be rewritten in the form $\phi(n) = \sum_{k=1}^{n} \left[\frac{1}{(n,k)}\right]$, where now *k* runs through all integers less than or equal to *n*. Now we use theorem 2.51 with *n* replaced by (n,k) to obtain

$$\phi(n) = \sum_{k=1}^{n} \sum_{d|(n,k)} \mu(d) = \sum_{k=1}^{n} \sum_{\substack{d|n \\ d|k}} \mu(d) .$$

For a fixed divisor *d* of *n* we must sum over all those *k* in the range $1 \leq k \leq n$ which are multiples of *d*. If we write $k = qd$ then $1 \leq k \leq n$ if and only if $1 \leq q \leq n/d$. Hence the last sum for $\phi(n)$ can be written as

$$\phi(n) = \sum_{d|n} \sum_{q=1}^{n/d} \mu(d) = \sum_{d|n} \mu(d) \sum_{q=1}^{n/d} 1 = \sum_{d|n} \mu(d) \frac{n}{d} .$$

This proves the theorem.

Lemma 2.53 For $n \geq 1$, $\phi(n) = n\prod_{p|n}\left(1-\frac{1}{p}\right)$.

Proof: For *n=1* the product is empty since there are no primes which divide 1. In this case it is understood that the product is to be assigned the value 1. Suppose, then, that *n>1* and let $p_1, p_2, ...p_r$ be the distinct prime divisors of *n*. The product can be written as

$$\prod_{p|n}\left(1-\frac{1}{p}\right) = \prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right) = 1 - \sum\frac{1}{p_i} + \sum\frac{1}{p_i p_j} - \sum\frac{1}{p_i p_j p_k} + ... + \frac{(-1)^r}{p_1 p_2 \cdots p_r} \quad \ldots(1)$$

On the right, in a term such as $\sum\frac{1}{p_i p_j p_k}$ it is understood that we consider all possible products $p_i p_j p_k$ of distinct prime factors of *n* taken three at a time. Note that each term on the right of (1) is of the form $\pm 1/d$ where *d* is a divisor of *n* which is either 1 or a product of distinct primes. The numerator ± 1 is exactly $\mu(d)$. Since $\mu(d) = 0$ if *d* is divisible by the square of any p_i, we see that the sum in (1) is exactly the same as $\sum_{d|n}\frac{\mu(d)}{d}$, but from theorem 2.52, $\frac{\phi(n)}{n} = \sum_{d|n}\frac{\mu(d)}{d}$ and thus $\phi(n) = n\prod_{p|n}\left(1-\frac{1}{p}\right)$.

Theorem 2.54 $\phi(mn) = \phi(m)\phi(n)(d/\phi(d))$**,** where $d = (m,n)$.

Proof: By Lemma 2.53, $\frac{\phi(n)}{n} = \prod_{p|n}\left(1-\frac{1}{p}\right)$.

Next we note that each prime divisor of *mn* is either a prime divisor of *m* or of *n* , and those primes which divide both *m* and *n* also divide (*m,n*). Hence

$$\frac{\phi(mn)}{mn} = \prod_{p|mn}\left(1-\frac{1}{p}\right) = \frac{\prod_{p|m}\left(1-\frac{1}{p}\right)\prod_{p|n}\left(1-\frac{1}{p}\right)}{\prod_{p|(m,n)}\left(1-\frac{1}{p}\right)} = \frac{\frac{\phi(m)}{m}\frac{\phi(n)}{n}}{\frac{\phi(d)}{d}}$$

So $\frac{\phi(mn)}{mn} = \frac{\phi(m)\phi(n)d}{mn\,\phi(d)}$. Thus $\phi(mn)=\phi(m)\phi(n)(d/\phi(d))$.

Theorem 2.55 $\phi(mn)=\phi(m)\phi(n)$ if $(m,n)=1$.

Proof: By theorem 2.54, $\phi(mn)=\phi(m)\phi(n)$.

Lemma 2.56 If p is a prime and α be any positive integer, then $\phi(p^\alpha)=p^\alpha-p^{\alpha-1}$.

Proof: By Lemma 2.53, $\phi(n)=n\prod_{p|n}\left(1-\frac{1}{p}\right)$. Taking $n=p^\alpha$.

$$\phi(p^\alpha)=\prod_{p|p^\alpha}p^\alpha\left(1-\frac{1}{p}\right)=\prod_{p|p^\alpha}p^{\alpha-1}(p-1)=p^{\alpha-1}(p-1).$$

Thus, $\phi(p^\alpha)=p^\alpha-p^{\alpha-1}$.

Theorem 2.57 $\phi(n)$ is even for $n\geq 3$. Moreover, if n have r distinct odd prime factors, then $2^r \mid \phi(n)$.

Proof: If $n=2^\alpha, \alpha\geq 2$, then Lemma 2.56 shows that $\phi(n)$ is even. If n has at least one odd prime factor, we write

$$\phi(n)=n\prod_{p|n}\frac{p-1}{p}=\frac{n}{\prod_{p|n}p}\prod_{p|n}(p-1)=c(n)\prod_{p|n}(p-1),$$

where $c(n)$ is an integer. The product multiplying $c(n)$ is even, so $\phi(n)$ is even.

Moreover, each odd prime p contributes a factor 2 to this product, so $2^r \mid \phi(n)$ if n have r distinct odd prime factors.

Definition 2.58 If G is a finite group, then $\Pi(G)$ denotes the set of primes dividing $o(G)$.

Chapter-3

Main Result

We now prove our main result: to identify finite groups of odd order with exactly two non-central conjugacy classes of each size. All the results in this section have appeared in [4].

Lemma 3.1 If G is a finite group of odd order, then each size of a non-central conjugacy class of G appears an even number of times.

Proof: As Z is a subgroup of G, so by Lagrange's theorem $o(Z)$ divides $o(G)$. Thus $o(Z)$ is odd. We know,

$$o(x^G) = [G : C_G(x)] = \frac{o(G)}{o(C_G(x))}$$

which gives $(o(x^G))(o(C_G(x))) = o(G)$.

Thus, $o(x^G) \mid o(G)$. Hence $o(x^G)$ is odd.

Since order of an element of a group divides order of the group, so order of x should be odd and hence it can-not be 2. So no $x \in G$ can satisfy $x^2 = 1$.

Thus, $x \neq x^{-1}$. Suppose $x \sim x^{-1}$. Then $x, x^{-1} \in x^G$. If b is any other element in x^G, then $b = g^{-1}xg$ for some $g \in G$. Now $b^{-1} = g^{-1}x^{-1}g$, which is a conjugate of x^{-1}. Since $x^{-1} \in x^G$ and we know conjugacy is an equivalence relation, therefore $b^{-1} \in x^G$.

So $o(x^G)$ is even, which is a contradiction as $o(x^G)$ is odd. Hence, x is not conjugate to x^{-1}. Thus, we have two conjugacy classes x^G and $\left(x^{-1}\right)^G$. Now if

$b \in x^G$ then $b = g^{-1}xg$ for some $g \in G$. Thus, $b^{-1} = g^{-1}x^{-1}g \in \left(x^{-1}\right)^G$. So if $b \in x^G$, then $b^{-1} \in \left(x^{-1}\right)^G$. Thus $o(x^G) = o((x^{-1})^G)$. This proves the lemma.

Proposition 3.2 Let G be a finite non-abelian group and suppose that G contains at most two non-central conjugacy classes of each size. Moreover, suppose that $o(x^G) = o(y^G)$ for $x, y \in G - Z(G)$ implies that $o(x) = o(y)$, then $Z(G) = 1$.

Proof: Denote $Z(G) = Z$ and $C_G(x) = C(x)$ for $x \in G$.

We shall assume that $Z > 1$ and we shall reach a contradiction.

Let $p \in \Pi(Z)$, the set of primes dividing $o(Z)$, and let $z \in Z$ be of order p. Let $x \in G - Z$ be of order m.

Now $C_G(zx) = C(zx) = \{g \in G \mid g(zx) = (zx)g\}$ and

$C_G(x) = C(x) = \{g \in G \mid gx = xg\}$. Let $g \in C(x)$. So $gx = xg$. Since

$g(zx) = z(gx) = z(xg) = (zx)g$, therefore $g \in C(zx)$. Hence $C(x) \subset C(zx)$.

Let $g \in C(zx)$, then $g(zx) = (zx)g$ i.e. $z(gx) = z(xg)$. Thus $gx = xg$ i.e. $g \in C(x)$. Hence, $C(zx) \subset C(x)$. Thus, $C(x) = C(zx)$.

By lemma 2.28, $o(x^G) = [G : C(x)]$ and $o((zx)^G) = [G : C(zx)]$. Since $C(x) = C(zx)$, therefore $o(x^G) = o((zx)^G)$. So, by our assumptions $o(zx) = o(x) = m$. Now $o(zx) = m$. So $(zx)^m = 1$ i.e. $z^m x^m = 1$. Thus $z^m = 1$.

Hence $1 = x^m = z^m$. It follows from theorem 2.5 that $p \mid m$.

Let $q \in \Pi(G) - \{p\}$ and $Q \in syl_q(G)$. So $o(Q) = q^m$ for some $m \geq 1$. Let $y \in Q - Z$, then $o(y) = q^r$ for some $r \geq 1$. So, $p \mid o(y) = q^r$. Thus $p \mid q$, which

is a contradiction. Thus, $y \in Z$ and hence, $Q \leq Z$. Now $o\left(\frac{G}{Z}\right) = \frac{o(G)}{o(Z)} = p^l$, because every $q \neq p$ divides $o(Z)$. Hence, G/Z is a p-group.

But if such a q exists, then by similar arguments (by starting with an element $z \in Z$ of order q) we can prove that G/Z is a q-group, a contradiction. Hence G is a p-group.

If $o(G) = p$, then G is cyclic and hence abelian, but G is non-abelian. So $o(G) \neq p$. If $o(G) = p^2$, then G is abelian by lemma 2.32, which is a contradiction. So $o(G) \neq p^2$. Hence $o(G) = p^n \geq p^3$.

If $o(Z) = p^n = o(G)$, then G is abelian, a contradiction. So $o(Z) \neq p^n$.

If $o(Z) = p^{n-1}$, then $o\left(\frac{G}{Z}\right) = p$ and thus, by theorem 2.20, G/Z is cyclic.

Let $G/Z = \langle xZ \rangle$.

Let $a, b \in G$, then $aZ, bZ \in G/Z$. Thus, $aZ = x^m Z, bZ = x^n Z$ for some $m, n \geq 0$.

Hence, $a = x^m z_1, b = x^n z_2$ for some $z_1, z_2 \in Z$. Now

$$ab = x^m z_1 x^n z_2 = x^m x^n z_1 z_2 = x^{m+n} z_1 z_2 = x^{n+m} z_1 z_2 = x^n x^m z_2 z_1$$
$$= x^n z_2 x^m z_1 = ba \ .$$

Thus G is abelian, which is a contradiction. So $o(Z) \neq p^{n-1}$. Thus $o(Z) \leq p^{n-2}$.

Also, we know center of a p-group is non-trivial. So $o(Z) \geq p$. Hence, $p \leq o(Z) \leq p^{n-2}$.

Since $Z \subseteq C_G(x)$ and $x \in C_G(x) \setminus Z$, therefore $o(C_G(x)) > o(Z) \geq p$. Thus $o(C_G(x)) \geq p^2$. So, we have $o(x^G) = \frac{o(G)}{o(C_G(x))} \leq \frac{p^n}{p^2} = p^{n-2}$.

Hence, both Z and the sizes of the non-central conjugacy classes of G are bounded by p^{n-2} from above.

Let there exist $x \in G$ with a conjugacy class of size p^{n-2}. Now

$$o(x^G) = [G : C_G(x)] = \frac{o(G)}{o(C_G(x))}.$$

Thus we have $o(C_G(x)) = \frac{o(G)}{o(x^G)} = \frac{p^n}{p^{n-2}} = p^2$. Also $Z \subset_{\neq} C_G(x)$ and

$o(C_G(x)) = p^2$, therefore $o(Z) = p$.

Hence, it follows from our assumptions and class equation that

$$p^n \leq p + 2p + 2p^2 + \ldots + 2p^{n-2} = p + 2p\left(1 + p + \ldots + p^{n-3}\right)$$

$$= p + 2p\left(\frac{p^{n-2} - 1}{p - 1}\right) \leq p + 2p^{n-1} - 2p = 2p^{n-1} - p$$

$$\leq 2p^{n-1} < p^n$$

a final contradiction. This proves the proposition.

As an immediate corollary we obtain

Corollary 3.3 Let G be a non-abelian finite group with non-central conjugacy classes of distinct sizes. Then $Z(G) = 1$ .In particular, all conjugacy classes of G are of distinct sizes.

Proof: Since G has non-central conjugacy classes of distinct sizes, so the first hypothesis of proposition 3.2 is satisfied. Suppose $o(x^G) = o(y^G)$ for $x, y \in G - Z(G)$ and since G has only one conjugacy class of each size, so x and

y are in the same conjugacy class and hence $o(x)=o(y)$. Thus second hypothesis of proposition 3.2 is also satisfied and hence $Z(G)=1$.

Theorem 3.4 Let G be a non-abelian finite group of odd order and suppose that G contains exactly two non-central conjugacy classes of each size. Then G is the non-abelian group of order 21.

Proof: Let $x, y \in G - Z(G)$ and $o(x^G) = o(y^G)$. Since G is of odd order, so $o(x^G) = o((x^{-1})^G)$. Also G contains exactly two non-central conjugacy classes of each size. So y is conjugate in G to x or to x^{-1}. Thus $o(x)=o(y)$.

Hence, by proposition 3.2, $Z(G)=1$.

Let $x \in G - \{1\}$ be of order $n \geq 3$.

Let $S = \{x^i \mid 1 \leq i \leq n, (i,n)=1\}$, $H = \langle x \rangle$, and $K = N_G(H)$. Clearly $o(S) = \phi(n)$, an even number by theorem 2.57.

Now $o(x) = n$, so $x^n = 1$ which gives $x^{n-1} = x^{-1}$. Also $(n-1, n) = 1$. Thus, $x^{n-1} = x^{-1} \in S$. Also G is of odd order, so x is not conjugate to x^{-1}.

Now $H = \langle x \rangle = \{1, x, x^2, ..., x^{n-1}\}$. Since H is a finite cyclic group of order n, so by theorem 2.21 number of generators of H is $\phi(n)$ and S contains all the generators of H.

Let $y \in S$, so $H = \langle y \rangle$. It is clear that any element of G which commutes with y will commute with whole of H. Thus $C_G(y) = C_G(H)$.

Let $y_1, y_2 \in S$. So $C_G(y_1) = C_G(y_2) = C_G(H)$.Now $o((y_1)^G) = [G : C_G(y_1)]$ and $o((y_2)^G) = [G : C_G(y_2)]$. Thus $o((y_1)^G) = o((y_2)^G)$. Thus if $y \in S$, then $o(y^G) = o(x^G) = o((x^{-1})^G)$.

But G contains exactly two non-central conjugacy classes of each size. So $y \in S$ is either conjugate to x or to x^{-1}. Hence every element of S is either conjugate to x or to x^{-1}.

Suppose $x^i, x^j \in S$ and $x^i \sim x^j$ in G. So, $g^{-1}x^i g = x^j$ for some $g \in G$ i.e. $g^{-1}x^i g \in H$. Then, $\left(g^{-1}x^i g\right)^n \in H \ \ \forall n \geq 1$. So $g^{-1}Hg \in H$. Hence $g \in N_G(H) = K$. Thus if $x^i \sim x^j$ in G, then $x^i \sim x^j$ in K. If $x^i \in S$, then $x^{-i} = x^{n-i} \in S$. Also, if $x^i \sim x$, then $x^{-i} \sim x^{-1}$.

Hence, S is partitioned into two sets of equal size $\phi(n)/2$, consisting of elements which are conjugate in K to x or to x^{-1} respectively.

Consider x^K. Any element of x^K is of the form $k^{-1}xk$, where $k \in K$. Since $K = N_G(H),\ k^{-1}xk \in H$. Let $k^{-1}xk = x^r$ for some r. Suppose $o(x^r) = m < n$. Then $(k^{-1}xk)^m = (x^r)^m = 1$. This gives $k^{-1}x^m k = 1$ and hence $x^m = 1$, a contradiction. So $o(x^r) = n$ and thus $k^{-1}xk \in S$. Thus x^K and similarly $(x^{-1})^K$ are in S. Therefore $o(x^K) = \dfrac{\phi(n)}{2} = [K : C_K(x)]$.

We know $C_G(x) = \{g \in G \mid gx = xg\}$ and $C_K(x) = \{k \in K \mid kx = xk\}$. Clearly $C_K(x) \subset C_G(x)$.

Let $g \in C_G(x)$. So $gx = xg$. Thus $gx^i = x^i g \ \ \forall i$. So $gH = Hg$. Thus $g \in K$ and hence $C_G(x) \subset C_K(x)$. Thus $C_G(x) = C_K(x)$

Hence $\dfrac{\phi(n)}{2} = [K : C_G(x)]$ --------- (1)

and since $\phi(n)/2$ is the order of the conjugacy class of x in K, so it will divide order of K and also $o(K) \mid o(G)$. Thus $\phi(n)/2$ is a divisor of $o(G)$, an odd

integer. The case $n = pq$ for distinct odd primes *p* and *q* is impossible, since $\frac{\phi(pq)}{2} = \frac{(p-1)(q-1)}{2}$ is even.

Hence *G* contains no elements of order divisible by more than one prime and consequently all elements of *G* are of prime power order. We prove that $o(C_G(x))$ are also of prime power. Suppose the contrary that $o(C_G(x))$ is not of prime power. Let *p, q* be the primes such that they divide $o(C_G(x))$. Suppose $x, y \in C_G(x)$, then by Cauchy's theorem $o(x) = p$ and $o(y) = q$. So by theorem 2.14, $o(xy) = o(x)o(y) = pq$, which is a contradiction as $xy \in G$. Let $p \in \Pi(G)$ and let $x \in G$ be of order *p*. Let $H = \langle x \rangle$. By equation(1),

$$o\left(\frac{N_G(H)}{C_G(x)}\right) = o\left(\frac{N_G(H)}{C_G(H)}\right) = \frac{\phi(p)}{2} = \frac{p-1}{2}.$$

By N/C lemma, $N_G(H)/C_G(H)$ can be embedded in $Aut(H)$. Since *H* is cyclic of order *p,* therefore $H \cong Z_p$. By theorem 2.49, $Aut(H) \cong Aut(Z_p) \cong Z_p^*$. But Z_p is a field, therefore by theorem 2.45, Z_p^* is cyclic. Thus $Aut(H)$ is cyclic and hence $N_G(H)/C_G(H)$ is cyclic. Let $N_G(H)/C_G(H) = \langle \alpha C_G(H) \rangle$, where $\alpha \in N_G(H) \leq G$. Since $o(\alpha)$ is a prime power, therefore $o(\alpha C_G(H))$ is also of prime power. Hence $o\left(N_G(H)/C_G(H)\right)$ is a prime power.

Thus $\frac{(p-1)}{2} = o\left(N_G(H)/C_G(H)\right)$ is either 1or it is a power of $q \in \Pi(G), q < p$.

Thus either $p = 3$ or $p = 2q^i + 1$ for some $q < p, i \in N$ and q^i dividing $o(G)$. Let *p* be the smallest prime dividing $o(G)$. Since $(p-1)/2$ divides $o(G)$, we must have $p = 3$, since p is the smallest prime and $q < p$.

If $\Pi(G)=\{3\}$, then $o(G)=3^n$ i.e. G is a p-group and we know center of a p-group is non-trivial i.e. $Z(G)\neq 1$, but $Z(G)=1$. Hence the case $\Pi(G)=\{3\}$ is impossible.

Let q be the smallest prime in $\Pi(G)-\{3\}$. Then $\frac{q-1}{2}=3^i$ for some $i\in N$. Thus $q=2.3^i+1$. We prove that $2.q^j+1\equiv 0(\mathrm{mod}\,3)\ \forall j\in N$ by mathematical induction.

Let $j=1$, then $2q+1=2(2.3^i+1)+1=4.3^i+3=3(1+4.3^{i-1})\equiv 0(\mathrm{mod}\,3)$.

Let result is true for $j=k$ i.e. $2.q^k+1\equiv 0(\mathrm{mod}\,3)$. We will prove for $j=k+1$.

$2q^{k+1}+1=2q^kq+1=2q^k(2.3^i+1)+1=4q^k.3^i+2q^k+1\equiv 4q^k.3^i(\mathrm{mod}\,3)\equiv 0(\mathrm{mod}\,3)$

Hence, $2.q^j+1\equiv 0(\mathrm{mod}\,3)\ \forall j\in N$.

Thus no prime in $\Pi(G)$ is equal to $2.q^j+1$.

Let r be the smallest prime in $\Pi(G)-\{3,q\}$. So $\frac{r-1}{2}=3^i$ or $\frac{r-1}{2}=q^j$ for some $i,j\in N$. Thus $r=2.3^i+1$ or $r=2.q^j+1$.

But as proved above , $2.q^j+1\equiv 0(\mathrm{mod}\,3)$. So this case will not arise. When $r=2.3^i+1$, then $2.r^j+1\equiv 0(\mathrm{mod}\,3)\ \forall j\in N$.

Thus no prime in $\Pi(G)$ is equal to $2.r^j+1$ and the same argument applied to other $r\in\Pi(G)$, one by one, and according to their increasing order, implies that all primes in $\Pi(G)$ are of the form 2.3^i+1 for some $i\in N$ and 3^i dividing $o(G)$.

Suppose first that $o(C_G(x))=3$ for some $x\in G$. Then 3 is the highest power of 3 dividing $o(G)$ and it generates only the prime $2.3+1=7$.

Hence $o(G)=3.7^j$ for some $j\in N$. If $j\geq 2$, then $o(C_G(y))\neq 7$ for all $y\in G$.

Now the class equation is

$$o(G) = o(Z) + \sum [G : C_G(x)] = o(Z) + 2\left(\frac{o(G)}{o(C_G(x))} + \frac{o(G)}{o(C_G(y))} + \ldots \right)$$

$$1 = \frac{1}{o(G)} + 2\left(\frac{1}{o(C_G(x))} + \frac{1}{o(C_G(y))} + \ldots \right)$$

$$\leq \frac{1}{3.7^j} + \frac{2}{3} + 2\left(\frac{1}{7^2} + \frac{1}{7^3} + \ldots \right) \leq \frac{1}{3.7^2} + \frac{2}{3} + 2\left(\frac{1/7^2}{1-1/7} \right)$$

$$= \frac{1}{3.7^2} + \frac{2}{3} + \frac{1}{21} < 1$$

a contradiction. Hence $j=1$ and $o(G) = 3 \cdot 7 = 21$, as required.

It remains only to drive a contradiction in the case when $o(C_G(x)) \neq 3$ for all $x \in G$. In this case

$$1 \leq \frac{1}{o(G)} + 2\left(\frac{1}{3^2} + \frac{1}{3^3} + \ldots \right) + 2\sum_{i=1}^{\infty} \left(\frac{1}{2.3^i + 1} + \frac{1}{\left(2.3^i + 1\right)^2} + \ldots \right)$$

$$\leq \frac{1}{3^2} + 2\left(\frac{1/3^2}{1-1/3} \right) + 2\sum_{i=1}^{\infty} \left(\frac{1/\left(2.3^i + 1\right)}{1-1/\left(2.3^i + 1\right)} \right) = \frac{1}{3^2} + \frac{1}{3} + \sum_{i=1}^{\infty} \left(\frac{1}{3^i} \right)$$

$$= \frac{1}{3^2} + \frac{1}{3} + \frac{1/3}{1-1/3} = \frac{1}{3^2} + \frac{1}{3} + \frac{1}{2}$$

$$< 1$$

a final contradiction. This proves the theorem.

References

[1] M. Bianchi, A. Gillio and M. Herzog, Groups with non-central classes of distinct lengths. *Istit. Lombardo (Rend. Sc.)* A **124** (1990) 157-160.

[2] W. Burnside, Theory of groups of finite order, 2nd ed., Dover, New York, 1955.

[3] W. Feit and J. G. Thompson, Solvability of groups of odd order. *Pacific J. Math.* **13** (1963) 775-1029.

[4] M. Herzog and J. Schonheim, On groups of odd order with exactly two non-central conjugacy classes of each size. *Arch. Math.* **86** (2006) 7-10.

[5] R. Knor, W. Lempken and B. Thielcke, The S_3 conjecture for solvable groups. *Israel J. Math.* **91** (1995) 61-76.

[6] Landau, Uber die Klassenzahl der binaren quadratischen Formen Von negatives Discriminante, *Math. Ann.* **56** (1903) 671-676.

[7] F. M. Markel, Conjugacy class problems for finite groups, PhD Thesis, University of Toronto, 1973.

[8] F. M. Markel, Groups with many conjugate elements, *J. Algebra* **26** (1973) 69-74.

[9] J. Poland, Finite groups with a given number of conjugate classes, *Canad. J. Math*. **20** (1968) 456-464.

[10] J. P. Zhang, Finite groups with many conjugate elements. *J. Algebra* **170** (1994) 608-624.