

International Journal of Statistics and Applied Mathematics



ISSN: 2456-1452
 Maths 2018; 3(2): 127-132
 © 2018 Stats & Maths
 www.mathsjournal.com
 Received: 21-01-2018
 Accepted: 22-02-2018

Imrosepreet Singh
 Assistant Professor P.G.
 Department of Mathematics
 A.S. College for Women Khanna,
 Punjab, India

Classification of simple groups upto order 200

Imrosepreet Singh

Abstract

In this paper the focus is on simple groups up to order 200. After explaining the basic notions of a group, abelian groups, subgroup, p-subgroup, sylow p-subgroup various result/theorems that can be used to test that a group is simple or not are given. While we are talking about the simple groups a the main thing which is to be kept in mind that group of prime order is always simple. So as we discuss about the classification of simple groups it should be clear that we will discuss only groups of Composite order as a group of prime order is always simple. All the results which are to be used are proved mainly using sylow's theorems. So after proving sylow theorem and using them to derive all the results that are to be used. we arrive at the conclusion that the only simple groups up to order 200 are only of order 60,168. Rest of the groups of Composite order are not simple by one way or another.

Keywords: Simple groups, order 200

Introduction

Basic Terminology

Group: In mathematics, a group is an algebraic structure consisting of a set of elements equipped with an operation that combines any two elements to form a third element. The operation satisfies four conditions called the group axioms, namely closure, associativity, identity and invertibility.

Mathematically A group is a set, G , together with an operation \bullet (called the *group law* of G) that combines any two elements a and b to form another element, denoted $a \bullet b$ or ab . To qualify as a group, the set and operation, (G, \bullet) , must satisfy four requirements known as the *group axioms*

Closure property

For all a, b in G , the result of the operation, $a \bullet b$, is also in G .

Associative property

For all a, b and c in G , $(a \bullet b) \bullet c = a \bullet (b \bullet c)$.

Identity element

There exists an element e in G , such that for every element a in G , the equation $e \bullet a = a \bullet e = a$ holds. Such an element is unique and thus one speaks of *the* identity element.

Inverse element

For each a in G , there exists an element b in G , commonly denoted a^{-1} (or $-a$, if the operation is denoted "+"), such that $a \bullet b = b \bullet a = e$, where e is the identity element.

The result of an operation may depend on the order of the operands. In other words, the result of combining element a with element b need not yield the same result as combining element b with element a .

Abelian Group: A group G is said to be abelian if $ab = ba$ for all $a, b \in G$.

Subgroup: Let G be a group, and let H be a subset of G . Then H is called a subgroup of G if H is itself a group, under the operation induced by G .

Correspondence
Imrosepreet Singh
 Assistant Professor P.G.
 Department of Mathematics
 A.S. College for Women Khanna,
 Punjab, India

Normal Subgroup. In abstract algebra, a normal subgroup is a subgroup which is invariant under conjugation by members of the group of which it is a part. In other words, a subgroup H of a group G is normal in G if and only if $gH = Hg$ for all g in G; i.e., the sets of left and right cosets coincide.

Simple group: In mathematics, a simple group is a nontrivial group whose only normal subgroups are the trivial group and the group itself. A group that is not simple can be broken into two smaller groups, a normal subgroup and the quotient group, and the process can be repeated.

p-subgroup: When P is a prime number, then a p-group is a group, all of whose elements have order some power of P or equivalent definition is that whose is order is some power of p

Sylow p-subgroup: If P^k is the highest power of a prime P dividing the order of a finite group G, then any subgroup of order P^k is called a Sylow P -subgroup of G.

Theorem 1.1 A group of prime order is always simple.

Proof: As we know that a prime number has namely two divisors that are only 1 and prime number itself. So as by Lagrange's theorem the order of subgroup must divide the order of group so if at all a group of prime order has a subgroup it must be of order 1 or p {where $p = o(G)$ }. In fact these are the only subgroups which a group of prime order has and these are also the normal subgroups as we know that every group has two normal subgroups. So a group of prime order does not have any proper normal subgroup so it is not simple. Thus whenever we are talking of checking whether the group is simple or not we must consider only groups of Composite order as aa the group of prime order are always simple.

Theorem 1.2 An abelian group G of composite order can not be simple

Proof: As we know that every subgroup of an abelian group G is a normal subgroup Also the converse of lagrange's theorem holds for finite abelian groups. Therefore if we have a abelian group of composite order say n it must have a proper divisor say k so by converse of lagrange,s theorem it must have subgroup of order k. Also since it is abelian therefore that subgroup of order k is normal also. Thus we have a proper normal subgroup of G. Thus G is not simple.

Theorem 2.1 Sylow's First theorem: If G is a finite group of order p^nq ($n \geq 1$), where is a prime number and q is any positive integer such that $(p,q) = 1$. Then for each i ($1 \leq i \leq n$), G has at least one subgroup of order p^i i.e a sylow p-subgroup. Thus Sylow's first theorem shows the existence of sylow p- subgroups.

Theorem 2.2 Sylow's Second theorem: Any two Sylow p-subgroups of a finite group are conjugate to each other

Theorem 2.3 Sylow's third theorem: The number of Sylow p-subgroups of G is of the form $1+kp$, where k is a non-negative integer such that $1+kp \mid o(G)$

Proof: Let $o(G) = p^nq$, where $(p,q) = 1$.

Let P be a Sylow p-subgroup of G so that $o(P) = p^n$

We have, $G = \cup_{a \in G} P a P \dots \dots \dots \dots \dots \dots \dots (1)$

Now $a \in N(P) \Rightarrow Pa = aP \Rightarrow PPa = PaP \Rightarrow Pa = P a P$

$\Rightarrow \cup_{a \in N(P)} P a P = \cup_{a \in N(P)} P a = N(P)$

[Because P is subgroup of N (P) therefore $\cup_{a \in N(P)} P a = N(P)$]

And $a \notin N(P) \Rightarrow Pa \neq aP \Rightarrow P = aPa^{-1} \Rightarrow o(aPa^{-1}) = p^m$ where $m < n$

$\Rightarrow O(PaP) = \frac{o(P)o(P)}{o(P \cap aPa^{-1})} = p^{2n-m}$

From equation (1) we get $o(G) = o(N(P)) + \sum_{a \notin N(P)} p^{2n-m}$

$$\Rightarrow \frac{o(G)}{o(N(P))} = 1 + \sum_{a \notin N(P)} \frac{p^{2n-m}}{o(N(P))}$$

$$\Rightarrow \frac{o(G)}{o(N(P))} = 1 + \frac{p^{n+1}}{o(N(P))} \sum_{a \notin N(P)} p^{n-m-1}$$

$$\Rightarrow \frac{o(G)}{o(N(P))} = 1 + \frac{p^{n+1} t}{o(N(P))} : t \in N$$

Since L.H.S is a positive integer

$$\text{Therefore } \frac{p^{n+1}t}{o(N(P))} = s = \text{a non negative integer ... (2)}$$

$$\Rightarrow p^{n+1}t = sv$$

Again P is a subgroup of N (P) therefore $o(P) \mid o(N(P)) \Rightarrow o(N(P)) = p^n v$ where $v \in \mathbb{N}$
 From equation (2) we have

$$p^{n+1}t = sp^n v \Rightarrow pt = sv \Rightarrow p \mid sv \Rightarrow p \mid s \text{ or } p \mid v \text{ as } p \text{ is a prime number}$$

$$\text{If } p \mid v \text{ then } p^{n+1} \mid p^n v \Rightarrow p^{n+1} \mid o(N(P)) \text{ and } o(N(P)) \mid o(G) \Rightarrow p^{n+1} \mid o(G)$$

Which is a contradiction.

$$\text{Hence } p \mid s \Rightarrow s = pk \Rightarrow \frac{s}{p} = k \text{ where } k \text{ is a non negative integer}$$

$$\Rightarrow \frac{t}{v} = k [\because pt = sv]$$

$$\text{Therefore number of sylow } p\text{-subgroups} = o(G)/o(N(P)) = 1 + p^{n+1}t/p^n v = 1 + p t/v = 1 + pk$$

Corollary 2.3.1 : Since we can always write the order of group in the form $p^n q$ where $(p, q) = 1$ then by above theorem the number of sylow p -subgroups is $1 + kp$ where $1 + kp \mid o(G)$ i.e. $1 + kp \mid p^n q$ and $(p, q) = 1$ i.e. $1 + kp \mid q$. Thus to conclude by using sylow third theorem the number of sylow p -subgroups is $1 + kp$ where $1 + kp \mid q$.

Theorem 2.4 If there is only one Sylow p -subgroup of a group then it is always normal subgroup of that group

Proof: Let $o(G) = p^n q$ where $(p, q) = 1$ Let P be the only Sylow p -subgroup of G so that

$o(G) = p^n$. Now $g^{-1}Pg$ is also a subgroup of $G \forall g \in G$ and $o(g^{-1}Pg) = o(P)$ thus $g^{-1}Pg$ is also a Sylow p -subgroup but as we are already given that there is only one Sylow p -subgroup so both must coincide. Thus $g^{-1}Pg = P \forall g \in G \Rightarrow Pg = gP \forall g \in G$

Corollary 2.5 Thus by combining the results of 2.3.1 and 2.4 we conclude that once the number of Sylow p -subgroups found by 2.3.1 is only one i.e. a unique Sylow p -subgroup then it will always be normal subgroup by using 2.4. So if we have only one Sylow p -subgroup for a particular prime p in a group that will be a normal subgroup so that group can not be simple. This result can be used to show that groups of order 21, 33, 35, 39, 40, 46, 51, 54, 55, 57, 58, 62, 69, 74, 77, 82, 84, 85, 86, 87, 88, 91, 92, 93, 94, 95, 98, 99, 102, 104, 106, 110, 111, 114, 115, 116, 118, 119, 122, 123, 126, 129, 133, 134, 135, 136, 140, 141, 142, 143, 145, 146, 152, 153, 154, 155, 156, 158, 159, 161, 165, 166, 170, 171, 174, 175, 176, 177, 178, 183, 184, 187, 188, 189, 190, 194, 195, 198.

Theorem 2.6 Sylow Test for Non Simplicity: Let G be a group of Composite order such that $p \mid o(G)$ where p is a prime number. If 1 is the only divisor of $o(G)$ that is congruent to 1 mod p , then G is not simple.

Proof: We have two cases

Case I. $o(G) = p^n$ since $o(G) = p^n$ therefore $Z(G) \neq \{e\}$

Thus $Z(G)$ is a proper normal subgroup of G . Hence G is not simple.

Case II. $o(G) = p^n q$

By Sylow's third theorem number of sylow p subgroups is $1 + kp$ where $1 + kp \mid o(G)$

Since 1 is the only divisor of that is congruent to 1 mod p therefore $1 + kp = 1$

Thus there is a unique sylow p subgroup which is normal in G . Hence G is not simple.

Sylow Test for Non Simplicity serves an important tool for testing the simple groups up to order 200. After applying Sylow Test for Non Simplicity the only possible simple groups having composite order are of order 12, 24, 30, 36, 48, 56, 60, 72, 80, 90, 96, 105, 108, 112, 120, 132, 144, 150, 160, 168, 180, 192.

Theorem 2.7

If G is a group such that $o(G) = pq$ where $p < q$, p, q are primes and $p \nmid q-1$. Then G is cyclic

Proof: By Sylow's First Theorem G has atleast one Sylow p -subgroup and one Sylow q -subgroup.

By Sylow's Second Theorem, the number of Sylow p -subgroup is $1 + kp$ where $1 + kp \mid q$

Thus $1 + kp = 1$ or q

If $1 + kp = 1$ then sylow p -subgroup is unique hence normal in G hence G has a proper Normal subgroup thus G is not simple then we are through Again by Sylow's Second Theorem, the number of Sylow q -subgroup is $1 + kq$ where $1 + kq \mid p$

Thus $1 + kq = 1$ or p If $1 + kq = 1$ then sylow q -subgroup is unique hence normal in G hence G has a proper Normal subgroup thus G is not simple again we are through If $1 + kq = p$ then $kq = p - 1$ which means that $q \mid p - 1$ which is not true.

Now $o(H) = p$, $o(K) = q$, and $H \cap K$ is a subgroup of both H and K .

$$\therefore o(H \cap K) \mid p \text{ and } o(H \cap K) \mid q \Rightarrow o(H \cap K) \mid (p, q) \Rightarrow o(H \cap K) \mid 1 \Rightarrow o(H \cap K) = 1$$

$$\Rightarrow H \cap K = \{e\}$$

We know if H and K are normal subgroups of G such that $H \cap K = \{e\}$,

Then $hk = kh \forall h \in H$ and $k \in K$.

Now H and K , being groups of prime orders, are cyclic.

\therefore let $H = \langle a \rangle$, $K = \langle b \rangle$ so that $o(a) = o(H) = p$, $o(b) = o(K) = q$

Now $ab = ba$ [because $hk = kh \forall h \in H$ and $k \in K$]. And $(o(a), o(b)) = (p, q) = 1$

Therefore $o(ab) = o(a) \cdot o(b) = pq = o(G)$ Thus G has an element ab of order pq thus G is cyclic.

After proving the result 2.7 the group satisfying the condition of 2.7 will always be cyclic group and as cyclic group is always abelian and by using 2.1 abelian group of composite order is not simple.

Theorem 2.8 Thus to conclude If G is a group such that $o(G) = pq$ where $p < q$ and $p \nmid q-1$. Then G can not be simple. This result can be applied to number of groups keeping mind all the conditions required by using this result we can easily see that the groups having orders 15, 33, 51, 65, 69, 77, 85, 87, 91, 95, 115, 119, 123, 133, 141, 143, 145, 159, 161, 177, 185, 187 are not simple.

Theorem 2.9 Let G be a group of order pqr where $p < q < r$ are primes then G is not simple

Proof: If possible G be simple thus no Sylow subgroup is normal By Sylow's Second Theorem, the number of Sylow p -subgroup is $1+kp$ where $1+kp|qr$ Thus $1+kp = q$ or r or qr ($\geq q$)

Again by Sylow's Second Theorem, the number of Sylow q -subgroup is $1+k'q$ where $1+k'q|p$

Thus $1+k'q = p$ or r or pr

Thus number of Sylow p -subgroup of $G \geq q$

If $1+k'q = p$ then $k'q = p-1$ which means that $q|p-1$ which is not true as $p < q$

Thus number of Sylow q -subgroup of $G = r$ or pr ($\geq r$)

Again by Sylow's Second Theorem, the number of Sylow r -subgroup is $1+k''r$ where

$1+k''r|pq$

Thus $1+k''r = p$ or q or pq

If $1+k''r = p$ then $k''r = p-1$ which means that $r|p-1$ which is not true as $p < r$

If $1+k''r = q$ then $k''r = q-1$ which means that $r|q-1$ which is not true as $q < r$

Thus number of Sylow r -subgroup of $G = pq$

Now sylow p -subgroups have atleast $q(p-1)$ elements of order p , sylow q -subgroups have atleast $r(q-1)$ elements of order q and sylow r subgroups have $p(r-1)$ elements of order r .

Therefore $pqr = o(G) \geq q(p-1) + r(q-1) + pq(r-1) + 1 = qp - q + rq - r + pqr - pq + 1$

$\Rightarrow 0 \geq -q + rq - r + 1$

$\Rightarrow 0 \geq (q-1)(p-1)$ which is absurd thus our supposition is wrong hence G is not simple.

This result can also be used to check that groups of order 30, 42, 66, 70, 78, 102, 105, 110, 114, 130, 138, 154, 165, 170, 182, 186, 190, 195 are not simple.

Theorem 2.10 A group of order p^2q is not simple, where p and q are distinct primes.

Proof: Let $o(G) = p^2q$ where $(p, q) = 1$

We have two cases

Case I $p > q$

By Sylow's Second Theorem, the number of Sylow p -subgroup is $1+kp$ where $1+kp|q$

Thus $1+kp = 1$ or q

If $1+kp = q$ then $kp = q-1 \Rightarrow p|q-1$ which is not possible as $p > q$

Thus $1+kp = 1$ then sylow p -subgroup is unique hence normal in G hence G has a proper Normal subgroup thus G is not simple then we are through

Case II $p < q$

Again by Sylow's Second Theorem, the number of Sylow p -subgroup is $1+kp$ where $1+kp|q$

If $1+kp = 1$ then sylow p -subgroup is unique hence normal in G hence G has a proper Normal subgroup thus G is not simple then we are through

if $1+kp = q$ then number of sylow p -subgroups is q

Again by Sylow's Second Theorem, the number of Sylow q -subgroup is $1+k'q$ where $1+k'q|p^2$ Thus $1+k'q = 1, p$ or p^2

If $1+k'q = 1$ then sylow q -subgroup is unique hence normal in G hence G has a proper Normal subgroup thus G is not simple then we are through

$1+k'q = p$ then $q|p-1$ which is not possible as $q > p \therefore 1+k'q = p^2$

Thus there are p^2 sylow q subgroups having atleast $p^2(q-1)$ elements of order q . also there are q sylow p -subgroups having atleast $q(p^2-1)$ elements of order p or p^2

$\therefore p^2q = o(G) \geq p^2(q-1) + q(p^2-1) + 1 \Rightarrow p^2q \geq p^2q - p^2 + qp^2 - q + 1$

$\Rightarrow 0 \geq (p^2-1)(q-1)$ which is not possible as p, q are primes thus in all the cases G has a proper normal subgroup. Hence G is not simple

This result can be used to check that groups of order 12, 20, 28, 44, 45, 52, 63, 68, 75, 76, 92, 98, 99, 116, 117, 124, 147, 148, 153, 164, 171, 174, 175, 188

Theorem 2.11 A group of order p^2q^2 is not simple ($p \neq 2, q \neq 3$)

(For $p = 2, q = 3$ the result is proved separately)

Proof: W.l.o.g $p < q$

No. of Sylow q subgroups = $1+kq$ Where $1+kq \mid p^2 \therefore 1+kq = 1, p, p^2$
 If $1+kq = 1$ then G has unique Sylow q - subgroup which is normal in G hence G is not simple.
 If $1+kq = p \Rightarrow kq = p - 1 \Rightarrow q \mid p - 1$ not possible as $p < q$
 If $1 + kq = p^2 \Rightarrow kq = p^2 - 1 \Rightarrow q \mid p^2 - 1 \Rightarrow q \mid (p - 1)(p + 1)$
 $\Rightarrow q \mid p - 1$ or $q \mid p + 1$ {as q is a prime No.}
 If $q \mid p - 1$ we get contradiction as $p < q$
 If $q \mid p + 1$ we again get a contradiction as $p < q$ and $p \neq 2, q \neq 3$
 Thus G has unique Sylow q subgroup which is normal in G . Hence G is not simple.
 This result can be applied to the groups of order 100, 196

Theorem 2.12 If G is a group such that $o(G) = p^n$ where p is a prime number then $Z(G) \neq \{e\}$

Theorem 2.13 If G is a group such that $o(G) = p^2$ then G is abelian

Proof: Since $o(G) = p^2$ therefore by applying 2.13 $Z(G) \neq \{e\}$ thus $o(Z(G)) \neq 1$

We know that $Z(G)$ is a normal subgroup of G therefore by using Lagrange's theorem

$$o(Z(G)) \mid o(G) \Rightarrow o(Z(G)) \mid p^2$$

$$\Rightarrow o(Z(G)) = 1 \text{ or } p \text{ or } p^2$$

But $o(Z(G)) \neq 1$ thus $o(Z(G)) = p$ or p^2

Let $o(Z(G)) = p$ thus there exist an element $a \in G$ but $a \notin Z(G)$

Also $x \in Z(G) \Rightarrow ax = xa \Rightarrow x \in N(a) \Rightarrow Z(G) \subseteq N(a)$ as $Z(G)$ is itself a group therefore it is a subgroup of $N(a)$ thus by using Lagrange's theorem $o(Z(G)) \mid o(N(a))$

$p \mid o(N(a)) \Rightarrow o(N(a)) = p$ or p^2 but if $o(N(a)) = p = o(Z(G))$ then $N(a) = Z(G)$ which is not the case as $a \in N(a)$ but $a \notin Z(G)$ thus $o(N(a)) = p^2 = o(G) \Rightarrow a \in Z(G)$ which is a contradiction as $a \notin Z(G)$. Hence $o(Z(G)) \neq p$ Thus $o(Z(G)) = p^2 = o(G) \Rightarrow Z(G) = G$ thus G is abelian

Thus the result 2.13 proves that all the groups having order p^2 will be abelian and as already proved in 1.2 abelian group of composite order is not simple so we conclude that a group of order p^2 is not simple. This result can be applied to show that groups of order 4, 9, 125, 49, 121, 169

Theorem 2.14

ODD TEST: A group of order $2n$ where $n > 1$ is odd is not simple.

Proof: Since $o(G)$ is even therefore G contains an element of order 2

Let a be an element of G such that $o(a) = 2$

Define $f_a: G \rightarrow G$ by $f_a(x) = ax$

f_a is 1-1

Let $x, y \in G$ such that $f_a(x) = f_a(y) \Rightarrow ax = ay \Rightarrow x = y$ {Cancellation laws hold in a group}

$\Rightarrow f_a$ is 1-1

f_a is onto

Also $\forall x \in G$ there exist $a^{-1}x \in G$ such that $f_a(a^{-1}x) = a(a^{-1}x) = (aa^{-1})x = ex = x$ thus f_a is onto

Thus f_a is a permutation thus $f_a \in A(G)$

$$\forall x \in G f_a^2(x) = f_a(f_a(x)) = f_a(ax) = a(ax) = (aa)x = a^2x = ex = x$$

Therefore every f_a - orbit contains two elements and number of distinct orbits of $f_a = \frac{2n}{2} = n$

Since every orbit corresponds to a cycle, therefore every f_a is decomposed into n cycles say

$\sigma_1, \sigma_2, \sigma_3, \dots, \sigma_n$ each of length 2

i.e. $f_a = \sigma_1 \sigma_2 \sigma_3 \dots \sigma_n$ where each σ_i is a transposition $\Rightarrow f_a$ is an odd permutation (n is odd)

Let $K = \{f_g: g \in G\}$

Claim: K is a subgroup of $A(G)$

Clearly $I(x) = x = ex = f_e(x) \forall x \in G$

Therefore $I = f_e \in K$ so that $K \neq \emptyset$

Let $f_{g_1}, f_{g_2} \in K$.

Then $(f_{g_1} \circ f_{g_2})(x) = f_{g_1}(f_{g_2}(x)) = f_{g_1}(g_2x) = g_1(g_2x) = (g_1g_2)x = f_{g_1g_2}(x) \forall x \in G$

Therefore, $f_{g_1} \circ f_{g_2} = f_{g_1g_2} \in K$.

Hence K is a subgroup of $A(G)$ [as K is finite subset of finite group $A(G)$]

Define $\Psi: G \rightarrow K$ by $\Psi(g) = f_g \forall g \in G$.

Ψ is homomorphism:

For $g_1, g_2 \in G$, we have

$$\Psi(g_1g_2) = f_{g_1g_2} = f_{g_1} \circ f_{g_2} = \Psi(g_1) \circ \Psi(g_2).$$

Therefore, Ψ is homomorphism.

Ψ is 1-1:

Let $\Psi(g_1) = \Psi(g_2); g_1, g_2 \in G$

$$\Rightarrow f_{g_1} = f_{g_2} \Rightarrow f_{g_1}(x) = f_{g_2}(x) \forall x \in G \Rightarrow g_1x = g_2x \Rightarrow g_1 = g_2$$

Therefore Ψ is 1 – 1

Ψ is onto:

$\forall f_g \in K$, there exists $g \in G$ such that $\Psi(g) = f_g$

Therefore Ψ is onto. Thus $G \simeq K$.

Therefore k contains a normal subgroup say N of index 2 hence g contains a normal subgroup $H = \Psi^{-1}(N)$ of index 2 and we know that if a group has subgroup of index 2 then it is a normal subgroup. Thus g has a proper normal subgroup thus G is not simple.

This test is very useful for testing group of various orders. Since we have confined ourselves to groups of order upto 200 so by using this important test we easily arrive at the conclusion that groups with orders 6, 10, 14, 18, 22, 26, 30, 34, 38, 42, 46, 50, 54, 58, 62, 66, 70, 74, 78, 82, 86, 90, 94, 98, 102, 106, 110, 114, 118, 122, 126, 130, 134, 138, 142, 146, 150, 154, 158, 162, 166, 170, 174, 178, 182, 186, 190, 194, 198. This result is applicable for large number of groups for testing the simplicity.

Theorem 2.15 If $o(G) = p^n$ where p is a prime number then any subgroup of order p^{n-1} (here the existence of subgroup of order p^{n-1} is ensured by Sylow's first theorem) is normal subgroup of G thus G has a proper normal subgroup hence G can not be simple. This result applies to the groups of order 4, 8, 16, 32, 64, 128, 25, 125, 27, 81, 49, 121, 169

Theorem 2.16 Index theorem: let H be a proper subgroup of a finite group G such that $O(G) \nmid [G:H]!$. Then there exist a proper normal subgroup of G contained in H hence G is not simple.

Proof. Let $S = \{xH; x \in G\}$ be the set of all left cosets of H in G and

$\Phi: G \rightarrow A(S)$ defined by $\Phi(g) = \Phi_g$ where

$\Phi_g: S \rightarrow S$ is such that $\Phi_g(xH) = gxH \forall g \in G$

Then by above theorem $\Phi: G \rightarrow A(S)$ is a homomorphism

Therefore by fundamental theorem $G/\text{Ker } \Phi \simeq \Phi(G)$

Therefore $o(G/\text{Ker } \Phi) = o(\Phi(G))$

Now $o(S) = [G:H] \Rightarrow o(A(S)) = [G:H]!$

Also $o(\Phi(G)) \mid o(A(S)) \Rightarrow o(\Phi(G)) \mid [G:H]! \Rightarrow o(G/\text{Ker } \Phi) \mid [G:H]!$

$\frac{o(G)}{o(\text{Ker } \Phi)} \mid [G:H]! \Rightarrow o(\text{Ker } \Phi) > 1 \Rightarrow \text{Ker } \Phi$ is a normal subgroup of G

Hence G is not simple Also $\text{Ker } \Phi \subseteq H$. Hence the proof.

This result applies to the groups of order 12, 24, 36, 48, 96, 108, 160, 192 to check that these groups are not simple. So the groups which could be simple are of order 56, 60, 72, 112, 120, 132, 144, 168, and 180. Out of these groups of order 56, 72, 112, 120, 132, 144, 180 can be eliminated by solving each of the problem independently.

Thus after applying all the results we see that there are only few possible groups upto order 200 which can be simple. So conclude that only groups from order 1 to 200 (of course of composite order) that can be simple are of order 60, 168.

References

1. Gallian JA. Contemporary Abstract Algebra, Narosa Publishing House, New Delhi.
2. Singh Surjeet, Qazi Zameeruddin, Modern Algebra. Vikas Publishing House, New Delhi (8th Edition), 2006.
3. Herstein IN, Topics in Algebra (Second Edition), Wiley Eastern Limited, New Delhi.
4. Artin Algebra M. Prentice Hall of India, New Delhi, 1994.
5. Bhattacharya PB, Jain SK, Nagpal SR. Basic Abstract Algebra. Cambridge University Press, New Delhi.
6. Fraleigh JB. A First Course in Abstract Algebra, Narosa Publishing House, New Delhi.