The 6th Shing-Tung Yau High School Mathematics Award, 2013

Guangdong Guangya High School

Research on some particular simple groups by using elementary methods

Team members: Zhiyin Shao Ruiheng Xie Ziqi Zhao

The instructor: Min Xu

Research on some particular simple groups with elementary methods

S09

[ABSTRACT]

It is well known that group is a set with an algebra operation, which is often denoted by G. A simple group is the group which has only the 2 trivial normal subgroups. The importance of the simple groups may analogue to the prime numbers in the number theory. The classification of the finite simple groups was the central problem of 20th century's' algebra. In this research report, we

use Sylow theorem, Burnside theorem, group action and some other elementally group theory

methods to obtain some criteria of simple group. By using these criteria we determine the possible simple groups whose order less than 700. Generalizes the results in the reference [1], [2], [3], [4].We conclude that

Theorem A group G of order less or equal than 700 could not be simple except for

 $|G| \in \{60, 168, 360, 504, 660 \text{ and all primes}\}.$

KEYWORDS

finite group	subgroup	normal subgroup	simple group	Sylow theorem	group action
normalizer	centralizer	transitive permutation presentation		N/C theorem	

1

Group is one of the most important and fundamental concepts in the modern algebra. It was widely used in many fields in mathematics and scientific technology nowadays [5]. The study of the group theory dates back to the end of 18th century. Galois (1811~1832), the mathematician, created an algebraic system of "group" and "field" during his research on "whether the quintic equation can be solved by using radical or not". Finite groups are studied and used extensively. Among the theories of finite group, the Classification of finite simple groups' theorem is the key problem. It had been over 150 years for hundreds of mathematicians to work on the study to this theorem and it was not proved to be correct until 1981. There are 18 infinite families and 26 sporadic simple groups which are not in the infinite families. Many complex methods was used in proving the Classification of finite simple groups theorem such as methods in the abstract group theory, the representation theory, geometry, combinatory and the graph theory. In this paper, we used Sylow theorem, Burnside theorem and other elementary theorems like group action to discuss finite simple groups of order less than or equal to 700. All possible simple groups are found out and specific examples are given.

§ 1 Definitions and lemmas

Definition 2.1

Define \circ a binary operation in a nonempty set. If it satisfies the condition: (1) $(a \circ b) \circ c = a \circ (b \circ c) \forall a, b, c \in G$; (2) $\forall a \in G, \exists e \in G$, such that $a \circ e = e \circ a = a$; (3) $\forall a \in G, \exists b \in G$, such that $a \circ b = b \circ a = e$. Then we call (G, \circ) a group, or G for short. Hereinto, we define e the unit element or the identity. Element b, satisfies $a \circ b = b \circ a = e$, is called the inverse of a, denoted a^{-1} . We call the number of G 's elements order, denoted |G|. When G satisfies $|G| < \infty$, we call G finite group, otherwise we call G infinite group. In this paper, all groups are finite groups unless otherwise specified. Operational symbol " \circ " is left out when no confusion can arise.

Definition 2.2

If the multiplication of G satisfies communicative law that $ab = ba, \forall a, b \in G$

Then we define G by communicative group or Abelian group.

Definition 2.3

For $a \in G$, $n \in \mathbb{N}_+$, we define

$$a^n = \underbrace{a \circ a \circ \cdots \circ a}_n$$
, $a^0 = e$, $a^{-n} = (a^n)^{-1}$

Follow the definition, for $m, n \in \mathbb{Z}$, we have

$$a^m a^n = a^{m+n}$$

If *G* is a communicative group, we also have $(ab)^n = a^n b^n$.

Definition 2.4

Let H be a nonempty subset of G. If H is a group on the same operation of G, then we call H the subgroup of G, denoted $H \leq G$. It's obviously that any group G has two subgroups, $\{e\}$ and G, what we call trivial subgroup. If subgroup $H \neq G$, then we call H the proper subgroup of G, denoted by H < G.

Definition 2.5

Let G be a group, H, K be the subsets of G, define the product of H, K to

$$HK = \{hk \mid h \in H, k \in K\}$$

If $K = \{a\}$, then denoted $H\{a\} = Ha$ for short, so we also have $\{a\}H = aH$. We also define that

$$H^{-1} = \{h^{-1} \mid h \in H\}, \quad H^n = \{h_1 h_2 \cdots h_n \mid h_i \in H\}, n \in \mathbb{N}_+$$

Definition 2.6

Let G be a group, $S \subseteq G$, we define the intersection of all the subgroups of G that containing S to be the subgroup generated by S, denoted by $\langle S \rangle$, that is

$$\left\langle S \right\rangle = \bigcap_{\substack{H \le G \\ S \subseteq H}} H$$

It's not hard to prove that,

$$\langle S \rangle = \{e, a_1 a_2 \cdots a_n \mid a_i \in S \cup S^{-1}, n = 1, 2, \ldots\}.$$

Similarly, let $S_1, S_2, ..., S_r \subseteq G$, then we define the intersection of all the subgroups of G containing $S_1, S_2, ..., S_r$ to be the subgroup generated by $S_1, S_2, ..., S_r$, denoted by $\langle S_1, S_2, ..., S_r \rangle$, that is

$$\left\langle S_1, S_2, \dots, S_r \right\rangle = \bigcap_{\substack{H \le G \\ S_1, S_2, \dots, S_r \subseteq H}} H$$

It's not hard to prove that,

$$\langle S_1, S_2, \dots, S_r \rangle = \left\{ e, a_1 a_2 \cdots a_n \mid a_i \in \bigcup_{j=1}^r (S_j \cup S_j^{-1}), n = 1, 2, \dots \right\}.$$

Definition 2.7

Let G be a group, element $a \in G$, and then we define the subgroup $H = \langle a \rangle$, generated only by a to be a cyclic group. For element a in G, we define $\langle a \rangle$ to be the order of a, denoted by o(a), that is $o(a) = |\langle a \rangle|$. From this definition we know that o(a) is the minimum integer n that satisfies $a^n = e$. If integer n does not exist, then we call the order of a is infinite, denoted $o(a) = \infty$.

Definition 2.8

Let G be a group, subgroup $H \leq G$, element $a \in G$, we call those subsets shaped as aH (accordingly, Ha) to be one of the left cosets of H (accordingly, right cosets). Now, we can define a relation ~ in group G making any $a, b \in G$,

 $a \sim b \Leftrightarrow$ exists an $h \in H$, such that a = bh

So it's easily to know ~ is a equivalence equation on group G, the equivalence class where a is in is [a] = aH, so we have

$$G = \bigcup_{a \in G} aH$$

So group G can be divided into the union of several left cosets, we defined the number of all the different left cosets of H in G to be the index of H in G , denoted |G:H|. Consider that $|aH| = |H|, \forall a \in G$, we have

Lemma 2.9 (Lagrange theorem)[6]

Let G be a group, $H \leq G$ then |G| = |G:H||H|

Deduction 2.10

Let G be a group, then the order of any element is divisible by the order of G, that is $o(a) \mid |G|$, so we have $a^{|G|} = e$.

Deduction 2.11

Let G be a group, $H, K \leq G$, then we have

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

Definition 2.12

Let G be a group, $H \leq G$, if

$$gH = Hg, \forall g \in G$$
, or $gHg^{-1} = H, \forall g \in G$

then we call that H is a normal subgroup or invariant subgroup of G, denoted by $H \triangleleft G$. According to the definition of normal subgroup, any group G has two trivial normal subgroups: $\{e\}$ and G. We define the finite group which only has these two trivial normal subgroups to be a simple group.

Definition 2.13

Let G to be a group, $H \leq G$, we define

$$N_{G}(H) = \{g \in G \mid gHg^{-1} = H\} \text{ and } C_{G}(H) = \{g \in G \mid gh = hg, \forall h \in H\}$$

to be the normalizer and the centralizer of H in G respectively. By the definition, we have

 $H \triangleleft G \Leftrightarrow N_G(H) = G$, and $C_G(H) \triangleleft N_G(H)$

Lemma 2.14 [6]

Let G to be a group, $H \leq G$, and |G:H| = 2, then $H \triangleleft G$.

Definition 2.15

Let G to be a group, $H, K \leq G$, $a \in G$, we define the subset shaped as HaK of H, K to be a double cosets on G.

Lemma 2.16 [2]

Define all double cosets of H, K on G to be a partition, that is $G = \bigcup_{a \in G} HaK, HaK \cap HbK = \emptyset$

Lemma 2.17[2]

Let one of the double cosets of H, K on G to be HaK, so HaK can be expressed as the union of several right cosets of H (or the left cosets of K). The number of containing right cosets of H is

$$|K:K\cap aHa^{-1}|$$

The number of containing left cosets of K is

 $\left| aHa^{-1}:aHa^{-1}\cap K \right|$

Lemma 2.18 [6]

Let G be a group, $H \triangleleft G$, then all left cosets of H make up a group on the multiplication (aH)(bH) = (ab)H

We define it to be the quotient group of G on H, denoted by G/H, hereinto the unit element is H, the inverse of aH is $a^{-1}H$.

Definition 2.19

Let G, G' be groups. We define mapping $\varphi: G \to G'$ to be a homomorphism from G to G' where φ maintains operation. That is for any $a, b \in G$, we have

$$\varphi(ab) = \varphi(a)\varphi(b)$$

If φ is a injection (surjection), we call that φ is a monomorphism (epimorphism). Under the condition of the morphism is injective and subjective, group G is isomorphic to G', denoted by $G \cong G'$. Call that φ is an automorphism if G' = G. All automorphisms of G form a group, we define the group to be the group of automorphisms of G, denoted Aut(G).

Definition 2.20

Let G, G' be groups, mapping $\varphi: G \to G'$ be the homomorphism. Define

$$Ker\varphi = \{g \in G \mid \varphi(g) = e'\}$$

to be the kernel of the homomorphism. We also define

$$\operatorname{Im} \varphi = \{ \varphi(g) \mid g \in G \}$$

to be the image of the homomorphism. It is easy to see that $Ker \varphi \triangleleft G$, $\operatorname{Im} \varphi \leq G'$.

Lemma 2.21 (The fundamental homomorphism theorem)[6]

Let G, G' be groups, mapping $\varphi : G \to G'$ be the homomorphism, then we have $G / Ker \varphi \cong Im \varphi$

Lemma 2.22 (N/C theorem)[2] Let G be a group, $H \le G$, then $N_G(H) / C_G(H)$ is isomorphic to a subgroup of Aut(H)

Definition 2.23

Let G be a group, for any $a \in G$, define mapping

 $L(a): G \to G \quad , \quad g \mapsto ag$

Then we are easily to know that L(a) is a bijection on G, and $L(G) = \{L(a) | a \in G\}$ forms a group.

Lemma 2.24 [6]

Let M be a set, then all the bijections on M forms a group on the multiplication (compound) of the mapping. We define it to be the symmetric group of M, denoted by S(M). Any subgroup

of S(M) is defined to be the transformation group on M.

Lemma 2.25[6]

Let M be a finite set. We define the element in S(M) to be permutation, with the properties below:

 \mathbb{O} Any permutation in M can be expressed as the product of disjoint cycles. The decomposition is unique with loss of the order.

 $\ensuremath{\mathbb{O}}$ Any permutation in M can be expressed as the product of several transpositions. The odevity of

the different decomposition of a certain permutation is assured. We define the permutation which has odd transpositions to be odd permutation, which has even transpositions to be even permutation.

Lemma 2.26 (Cayley theorem)[6]

Any group G is isomorphic to a transformation group on a certain set, practically:

$$G \cong L(G) \leq S(G)$$

Lemma 2.27[6]

Infinite cyclic group must be isomorphic to integer additive group Z. Finite cyclic group must be isomorphic to a certain quotient group Z / nZ of integer additive group (denoted Z_n for short).

Lemma 2.28[6]

The subgroups of a cyclic group $G = \langle a \rangle$ are still cyclic group. All the subgroups of a certain infinite cyclic group Z are $\langle a^s \rangle$, $\forall s \in \mathbb{N}$. All the subgroups of a certain finite cyclic group Z_n of order n is $\langle a^s \rangle$, $\forall s \in \mathbb{N}, s | n$.

Lemma 2.29[2]

The automorphism group of cyclic group G is a transformation group. Infinite cyclic group Z only has two automorphism, $\operatorname{Aut}(Z) \cong Z_2$. Finite cyclic Z_n group of order n has $\varphi(n)$ automorphism (φ is Euler's function), $\operatorname{Aut}(Z_n) \cong \operatorname{U}(n)$.

Definition 2.30

Let G be a group, A be a non-empty set. If there exists a mapping:

$$\varphi: G \times A \to A$$
$$(g, a) \mapsto ga$$

Satisfies:

(1)
$$ea = a, \forall a \in A$$

(2) $g_1(g_2a) = (g_1g_2)a, \forall a \in A, g_1, g_2 \in G$

Then we call it group G actions on set A. The kernel of action $Ker\varphi = \{g \in G \mid ga = a, \forall a \in A\}$.

If $Ker \varphi = \{e\}$, then we call group G acts faithfully on set A.

Lemma 2.31[2]

Let group G actions on set A, then set A has a bijection between the set formed by all homomorphisms of group G on S(A).

Definition 2.32

Let group *G* actions on set *A* . For any $a \in A$, we define.

$$G_a = \left\{ g \in G \mid ga = a \right\} \text{ and } O_a = \left\{ ga \mid g \in G \right\}$$

to be the stabilizer and the orbit of a in G respectively. According to the definition, it's easily to know that $G_a \leq G$. If there is only one orbit when group G actions on set A, then for any $a, b \in A$, there exists $g \in G$, such that a = gb. We call this action transitive.

Lemma 2.33[7]

Let group G actions on set A. Define a relation ~ in set A, satisfying: for any $a, b \in A$, $a \sim b \Leftrightarrow$ there exists a $g \in G$, such that a = gb

6

So it's easily to know that \sim is an equivalence relation on set A. The equivalence classes where a is in is $[a] = O_a$, so

$$A = \bigcup_{a \in A} O_a$$

That means set A can be divided into the union of several orbits, and the action of G on O_a is transitive, $|O_a| = |G:G_a|$ so

$$|A| = \sum |O_a| = \sum |G:G_a|$$

Lemma 2.34[7]

Let G be a group, $H \le G$, $A = \{aH \mid a \in G\}$. Define a mapping:

$$\varphi: G \times A \to A$$
$$(g, aH) \mapsto (ga)H$$

Then we have

- (1) This is a group action.
- (2) This action is transitive.
- (3) The kernel of this action is $Ker\varphi = \bigcap_{g \in G} gHg^{-1}$;
- (4) $Ker \varphi = \bigcap_{g \in G} gHg^{-1}$ is the largest normal subgroup of G in H.

(Remark **)** According to this lemma and the simplicity of A_n ($n \ge 5$), we know that any simple group G must not contain subgroups of index ≤ 4 .

Lemma 2.35[7]

Let G be a group. Define a mapping:

$$\varphi: G \times G \to G$$
$$(g, a) \mapsto gag^{-1}$$

Then

(1) This is a group action.

(2) The kernel of this action is $Ker\varphi = \{g \in G \mid ga = ag, \forall a \in G\} = Z(G)$ (the center of group G)

group (G)

(3) For any
$$a \in G$$
, we have
 $G_a = \{g \in G \mid gag^{-1} = a\} = \{g \in G \mid ga = ag\} = C_G(a)$

 $O_a = \{ga \mid g \in G\}$ is defined to be the conjugate class where a is in.

Then we have the class equation:

$$|G| = \sum |O_a| = |Z(G)| + \sum_{a \notin Z(G)} |G: C_G(a)|$$

Lemma 2.36[7]

Let G be a group, $A = \{H \mid H \subseteq G\}$. Define a mapping:

$$\varphi: G \times A \to A$$
$$(g, H) \mapsto gHg^{-1}$$

Then

(1) This is a group action. (by conjugation)

(2)For any $H \in A$, we have

$$G_{H} = \{g \in G \mid gHg^{-1} = H\} = N_{G}(H), \text{ and } |O_{H}| = |G: N_{G}(H)|.$$

Lemma 2.37[7] (Cauchy theorem)

Suppose G a finite group, p is a prime satisfied p ||G|, then G must have subgroups of order p.

Lemma 2.38[2] (Sylow theorem the first)

Suppose *G* a finite group, *p* is a prime. If $|G| = p^n m$, (p,m) = 1, then group *G* must have a subgroup *P* of order p^n , called *Sylow* p – subgroup of *G*.

Lemma 2.39[7] (Sylow theorem the second)

Any two of the Sylow p - subgroup P_1, P_2 are conjugate in G, that is $\exists g \in G$, such that $P_1 = gP_2g^{-1}$.

Lemma 2.40[2] (Sylow theorem the third)

Suppose the number of Sylow p – subgroup of G is n_p , then $n_p \mid m$ and $n_p \equiv 1 \pmod{p}$.

Lemma 2.41[2]

If the number of Sylow p – subgroups of group G is $n_p \neq 1 \pmod{p^2}$, then there must exist two Sylow p – subgroups P_1, P_2 , such that $|P_i : P_1 \cap P_2| = p \ (i = 1, 2)$.

Lemma 2.42[2]

Let G be a finite group. P_1 is a p-subgroup but not a Sylow p-subgroup of G. P is the Sylow p-subgroup of G. Then there must exist $g \in G$, such that

$$P_1 < gPg^-$$

Lemma 2.43[2]

Let G be a finite group, P is a p-subgroup of G but not a Sylow p-subgroup. then $P < N_G(P)$.

Definition 2.44

Let G be a group. P is a Sylow p – subgroup of G. If there exists $N \triangleleft G$ satisfied

$$\begin{cases} N \cap P = \{e\} \\ NP = G \end{cases}$$

Then we define N to be the normal p – complement of G.

Lemma 2.45[2]

Let G be a finite group, P is the Sylow p – subgroup. If $C_G(P) = N_G(P)$, then G have a normal p – complement N.

Definition 2.46 Let *G* be a group, $\forall x, y \in G$, define $[x, y] = x^{-1}y^{-1}xy$ to be the commutator of x, y.

Definition 2.47 Let *G* be a group, define

$$G' = \left\langle \left[x, y \right] | x, y \in G \right\rangle$$

to be the commentator subgroup of G , then $G^{'} \lhd G$. So we can develop a definition: $G^{(1)} = G^{'}$,

 $G^{(n)} = (G^{(n-1)})'$, and we have

 $G \triangleright G' \triangleright G^{(2)} \triangleright \cdots \triangleright G^{(n)} \triangleright \cdots$

Definition 2.48

Let G be a group. If there exists $n \in N_+$, such that $G^{(n)} = \{e\}$, then we define G to be a solvable group.

Lemma 2.49 (Burnside theorem)[2]

Let G be a finite group, satisfied $|G| = p^a q^b$ and p, q are prime, $a, b \in N_+$, then G is a solvable group.

Lemma 2.50 [2]

Let G be a finite group, satisfied |G| = pm, (p,m) = 1 and p is a prime, P is the Sylow p - group of G. Then for any $x \in N_G(P) \setminus C_G(P)$, x can normalize up to $k = 1 + \frac{n_p - 1}{p}$ Sylow p - subgroups..

§ 2 the Induction of the non simple groups

In this part, some given conclusions are used to exclude the majority of non-simple groups. We used VB to find out the order less or equal than 700 of groups that satisfy those theorems.

Theorem 1 [2] If the order of G satisfies $|G| = p^a (a \in N_+ and a \ge 2)$, p is odd prime. Then G must not be a simple group.

The numbers satisfy theorems 1 within 700 are:

4, 8, 9, 16, 25, 27, 32, 49, 64, 81, 121, 125, 128, 169, 243, 256, 289, 343, 361, 512, 529, 625

Group of orders above can't be a simple group.

Theorem 2 [2] If the order of G can be expressed in |G| = pq, hereinto p, q are different prime numbers. Then G must not be a simple group.

The numbers satisfy theorem 2 within 700 are:

6, 10, 14, 15, 21, 22, 26, 33, 34, 35, 38, 39, 46, 51, 55, 57, 58, 62, 65, 69, 74, 77, 82, 85, 86, 87, 91, 93, 94, 95, 106, 111, 115, 118, 119, 122, 123, 129, 133, 134, 141, 142, 143, 145, 146, 155, 158, 159, 161, 166, 177, 178, 183, 185, 187, 194, 201, 202, 203, 205, 206, 209, 213, 214, 215, 217, 218, 219, 221, 226, 235, 237, 247, 249, 253, 259, 262, 265, 267, 274, 278, 287, 291, 295, 298, 299, 301, 302, 303, 305, 307, 309, 314, 319, 321, 323, 326, 327, 329, 334, 335, 339, 341, 346, 355, 358, 362, 365, 371, 377, 381, 382, 386, 391, 393, 394, 395, 398, 403, 407, 411, 413, 415, 417, 422, 427, 437, 445, 446, 447, 451, 453, 454, 458, 466, 469, 471, 473, 478, 481, 482, 485, 489, 493, 497, 501, 502, 505, 511, 512, 515, 517, 519, 526, 527, 533, 535, 537, 538, 542, 543, 545, 551, 553, 554, 559, 565, 566, 573, 579, 581, 583, 586, 589, 591, 597, 611, 614, 622, 623, 626, 629,

9

633, 634, 635, 649, 655, 662, 667, 671, 674, 679, 681, 685, 687, 689, 694, 695, 697, 698, 699.

Group of orders above can't be a simple group.

Theorem 3 Let the order of G be $|G| = p^a q$, p, q are different prime numbers, $a \in N_+, a \ge 2$, so G can't be a simple group.

The numbers satisfy theorem 3 within 700 are:

12, 18, 20, 24, 28, 40, 44, 45, 48, 50, 52, 54, 56, 63, 68, 75, 76, 80, 88, 92, 96, 98, 99, 104, 112, 116, 117, 124, 135, 136, 147, 148, 152, 153, 160, 162, 164, 171, 172, 175, 176, 184, 188, 189, 192, 207, 208, 212, 224, 232, 236, 242, 244, 245, 248, 250, 261, 268, 272, 275, 279, 284, 292, 296, 297, 304, 316, 320, 325, 328, 332, 333, 338, 344, 351, 352, 356, 363, 368, 369, 375, 376, 384, 387, 388, 404, 405, 412, 416, 423, 424, 425, 428, 436, 448, 452, 459, 464, 472, 475, 477, 486, 488, 496, 507, 508, 513, 524, 531, 536, 539, 544, 548, 549, 556, 567, 568, 575, 578, 584, 592, 596, 603, 604, 605, 608, 621, 628, 632, 637, 639, 640, 652, 656, 657, 664, 668, 686, 688, 692

Group of orders above can't be a simple group.

Theorem 4 Suppose that the order of G can be expressed as $|G| = p^2 q^2$, p, q are different prime numbers, then G can't be simple group.

The numbers satisfy theorem 4 within 700 are:

36, 100, 196, 225, 441, 484, 676

Group of orders above can't be a simple group.

Theorem 5 Suppose the order of G can be expressed as |G| = pqr, satisfying p > q > r to be different primes, then G must not be a simple group.

The numbers satisfy theorem 5 within 700 are:

30, 42, 66, 70, 78, 102, 105, 110, 114, 130, 138, 154, 165, 170, 174, 182, 186, 190, 195, 222, 230, 231, 238, 246, 255, 258, 266, 273, 282, 285, 286, 290, 310, 318, 322, 345, 354, 357, 370, 374, 385, 399, 402, 406, 410, 418, 426, 429, 430, 434, 435, 438, 442, 455, 465, 470, 474, 483, 494, 498, 506, 530, 534, 555, 561, 574, 582, 590, 595, 598, 602, 606, 609, 610, 615, 618, 627, 638, 642, 645, 646, 651, 654, 658, 663, 665, 670, 678, 682

Group of orders above can't be a simple group.

Theorem 6 Suppose the order of G can be expressed as |G| = 2n in the condition of n is odd, then G must not be a simple group.

The numbers satisfy theorem 6 within 700 are:

90, 126, 150, 210, 234, 270, 294, 306, 330, 342, 350, 378, 390, 414, 450, 462,

10

490, 510, 518, 522, 546, 550, 558, 562, 570, 594, 630, 650, 666, 690

Group of orders above can't be a simple group.

Theorem 7 By |G| denote the order of G, hereinto p is a prime, and p ||G|. If G has the only one *Sylow* p – subgroup, then G must not be simple group.

S09

The numbers satisfy theorem 7 within 700 are:

 $\begin{aligned} &84(n_7 = 1), 140(n_7 = 1), 156(n_{13} = 1), 200(n_5 = 1), 204(n_{17} = 1), 220(n_{11} = 1), 228(n_{19} = 1), \\ &252(n_7 = 1), 260(n_{13} = 1), 276(n_{23} = 1), 308(n_{11} = 1), 312(n_{13} = 1), 315(n_7 = 1), \\ &340(n_{17} = 1), 348(n_{29} = 1), 364(n_7 = 1), 372(n_{31} = 1), 408(n_{17} = 1), 440(n_{11} = 1), \\ &444(n_{37} = 1), 456(n_{19} = 1), 460(n_{23} = 1), 468(n_{13} = 1), 476(n_{17} = 1), 492(n_{41} = 1), \\ &516(n_{43} = 1), 525(n_7 = 1), 532(n_{19} = 1), 564(n_{47} = 1), 572(n_{13} = 1), 580(n_{29} = 1), \\ &585(n_{13} = 1), 588(n_7 = 1), 620(n_{31} = 1), 624(n_{13} = 1), 636(n_{53} = 1), 644(n_{23} = 1), \\ &680(n_{17} = 1), 684(n_{19} = 1), 693(n_{11} = 1), 696(n_{29} = 1), 700(n_5 = 1). \end{aligned}$

Group of orders above can't be a simple group.

Theorem 8 Suppose the order of G can be expressed as $|G| = p^a q^b$, hereinto p, q are different prime, $a, b \in N_+$. Then G must not be a simple group.

The numbers satisfy theorem 8 within 700 are:

72, 108, 144, 216, 288, 324, 392, 400, 432, 500, 576, 648, 675

Group of orders above can't be a simple group.

Theorem 9 If the order of G is a prime number, then G must be a simple group.

The numbers satisfy theorem 9 within 700 are:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691

Group of orders above can't be a simple group.

§ 3 Main Result

By using the theorems above, here we have 27 numbers below to discuss. (They cannot be solved by theorem $1\sim9$):

We can divided them into these part by recognizing their main method.

I. The situations solved by embedding.

(1) $|G| = 72 = 2^3 \times 3^2$, then

$$\begin{cases} n_2 \equiv 1 \pmod{2}, & \{n_3 \equiv 1 \pmod{3} \\ n_2 \mid 9, & \{n_3 \equiv 1 \pmod{3} \\ n_3 \mid 8 \\ n_2 = 1, 3, 9, & n_3 = 1, 4 \end{cases}$$

Suppose G is a simple group, then $n_a = 4$, we have $G \cong L(G) \lesssim S_4$. However $|G| = 72 \nmid 4! = 24$. This is a contradiction!

(2) $|G| = 108 = 2^2 \times 3^3$, then (n_2)

$$\begin{cases} n_2 \equiv 1 \pmod{2}, & \{n_3 \equiv 1 \pmod{3} \\ n_2 \mid 7, & \{n_3 \equiv 1 \pmod{3} \\ n_3 \mid 4 \\ n_3 = 1, 4 \end{cases}$$

According to the process above, we have $\,G\cong L_{(G)} \lesssim S_4$, $\,|G|=108 \nmid 4!=24$. This is a contradiction!

(3) $|G| = 120 = 2^3 \cdot 3 \cdot 5$, according to lemma 2.40,

$$\begin{cases} n_5 \equiv 1 \pmod{5} \\ n_5 \mid 24 \end{cases}$$

So $n_5 = 1$ or $n_5 = 6$. Suppose G is a simple group, then $n_5 = 6$. For any Sylow 5 – subgroup P of G, according to **lemma 2.36**, we have $|G: N_G(P)| = 6$. Consider the left multiplication of G on the left coset space of $N_G(P)$. This action induces the homomorphism φ on G to S_6 . According to **lemma 2.34**, we have

$$G / Ker \varphi \cong \varphi(G) \leq S_e$$

G is a simple group, therefore $Ker\varphi = 1$, so

$$G \cong \varphi(G) \leq S_6$$

According to the proof of the **theorem 6**, $\varphi(G)$ doesn't contain odd permutation, so

$$G \cong \varphi(G) \le A_6$$

So $|A_6: \varphi(G)| = 3$. According to the remark of **lemma 2.34**, this is impossible. So G is not a simple group.

(4) $|G| = 144 = 2^4 \times 3^2$, then

$$\begin{cases} n_2 \equiv 1 \pmod{2} &, & \begin{cases} n_3 \equiv 1 \pmod{3} \\ n_2 \mid 9 &, & \\ n_2 = 1, 3, 9, & & n_3 = 1, 4, 16 \end{cases}$$

Suppose G is a simple group, then $n_3 = 16$. For any two Sylow3-subgroups, if their intersection is $\{e\}$, then 16 Sylow3-subgroups have $16 \times (9-1) = 128$ non-unit element.

- \therefore There left144 128 = 16 element.
- \therefore n₂ = 1, G is not a simple group.
- \therefore There must have $\exists P_1, P_2 \in Syl_3(G)$, such that $|P_1 \cap P_2| = 3$
- $\therefore (P_1 \cap P_2) \lhd P_1 \text{ and } (P_1 \cap P_2) \lhd P_2. \text{ Let } N = N_G(P_1 \cap P_2), |N| \ge |(P_1 P_2)| = \frac{|P_1||P_2|}{|P_1 \cap P_2|} = \frac{9 \times 9}{3} = 27$
- |N| = 9e(e > 3, e | 16), e = 4,8,16
- $|: |G: \mathbb{N}| \le 4$. That means G subgroups with index less than 4. So G is not a simple group.
- (5) $|G| = 180 = 2^2 \times 3^2 \times 5$, then

$$\begin{cases} n_5 \equiv 1 \pmod{5}, & \{n_3 \equiv 1 \pmod{3} \\ n_5 \mid 36, & \{n_3 \equiv 1 \pmod{3} \\ n_3 \mid 20 \\ n_5 = 1, 6, 36, & n_3 = 1, 4, 10 \end{cases}$$

Suppose *G* is a simple group, then $n_5 = 6, G \lesssim A_6$. According to $|A_6:G|=2$, there is subgroups with index 2. So A_6 is not a simple group. This is a contradiction! So $n_5 = 36$, $n_3 = 10$. Suppose $\forall P_1, P_2 \in Syl_5(G)$, $P_1 \cap P_2 = \{e\}$, then there are $36 \times (5-1) = 144$ non-unit elements in Sylow5-subgroup, $10 \times (9-1) = 80$ non-unit elements in Sylow3-subgroup. $\therefore 144 + 80 > 180$ Therefore $\exists P_1 \cap P_2 \neq \{e\}$. $\therefore \exists |P_1 \cap P_2| = 3$, $P_1, P_2 \in Syl_3(G)$ $\therefore |P_1| = |P_2| = 3^2$

- : Sylow3-subgroups are all Abelian groups.
- $\therefore P_1 \cap P_2 \lhd P_i (i = 1, 2)$
- $\therefore N \triangleq N_{\mathsf{G}}(P_1 \cap P_2) \geq P_1, P_2, \ |N| \geq |P_1P_2| = \frac{|P_1||P_2|}{|P_1 \cap P_2|} = \frac{9 \times 9}{3} = 27$
- $\therefore |N| = 9k(k \ge 3, k \mid 20)$ $\therefore k = 4,5,10,20$

According to G is a simple group, we have |G: N| = 5 $\therefore |N| = 36$

∴ $^{G}/_{\text{Ker}\varphi} \lesssim A_{5}$. That means we can embed *G* in a permutation group of order 5. In simple group $G \oplus$, ker $\varphi = \{e\}$, so $G \lesssim A_{5}$. However |G| = 180, $|A_{5}| = 60$. That means we cannot embed G in a permutation group of order 5. This is a contradiction! So *G* is not a simple group.

(6) $|G| = 216 = 2^3 \times 3^3$, then

$$\begin{cases} n_3 \equiv 1 \pmod{3} \\ n_3 \mid 8 \\ 13 \end{cases}$$

$$n_3 = 1, 4$$

Suppose G is a simple group, then $n_3 = 4$, |G:N| = 4. This is a contradiction!

(7) When $|G| = 240 = 2^4 \cdot 3 \cdot 5$, according to **lemma 2.40**,

$$\begin{cases} n_5 \equiv 1 \pmod{5} \\ n_5 \mid 48 \end{cases}$$

Suppose G is a simple group, then there must be $n_5 = 6$. For any Sylow 5 – subgroup P of G, according to **lemma 2.36**, we have $|G: N_G(P)| = 6$. We can deduce that $G \cong \varphi(G) \le A_6$ as the proof in situation I (3). But |G| = 240 can't be divided by $|A_6| = 360$. This is a contradiction! So G is not a simple group.

(8) $|G| = 264 = 2^3 \times 3 \times 11$, then

$$n_{11} \equiv 1 \pmod{11}$$

 $n_{11} \mid 24$
 $n_{11} = 1,12$

Suppose G is a simple group, then $n_{11} = 12$, $N_G(P) = 22$. So $G \lesssim A_{12}$.

 \therefore $|A_{12}| = \frac{1}{2} \times 12!$. Hereinto the power of 11 is 1.

 $\therefore \text{We can regard the Sylow11-subgroups of } G \text{ as the Sylow11-subgroups of } \mathbb{A}_{12}.$ However there are $\frac{\mathbb{A}_{12}^{11}}{\mathbb{1}_{11\times 10}}$ Sylow11-subgroups in \mathbb{S}_{12}

$$\left|N_{A_{12}}(P)\right| = \frac{1}{2}\left|N_{S_{12}}(P)\right| = \frac{1}{2} \times \frac{12!}{\frac{A_{12}^{11}}{11 \times 10}} = 55$$

Since $N_{G}(P) \nmid N_{A_{12}}(P)$ is false, G is not a simple group.

(9) When $|G| = 300 = 2^2 \cdot 3 \cdot 5^2$, according to **lemma 2.40**,

$$\begin{cases} n_5 \equiv 1 \pmod{5} \\ n_5 \mid 12 \end{cases}$$

Suppose G is a simple group, there must have $n_5 = 6$. For any Sylow 5 – subgroup P of G, according to lemma 2.36 we know that $|G: N_G(P)| = 6$ We can deduce that $G \cong \varphi(G) \le A_6$ as the proof in situation(3). But |G| = 300 can't be divided by $|A_6| = 360$. This is a contradiction! So G is not a simple group.

(10) $|G| = 324 = 2^2 \times 3^4$, then

$$\begin{cases} n_3 \equiv 1 \pmod{3} \\ n_3 \mid 4 \end{cases}$$
$$n_3 = 1.4$$

Suppose G is a simple group, then $n_3 = 4$, |G: N| = 4. This is a contradiction!

(11) $|G| = 336 = 2^4 \times 3 \times 7$, then

$$\begin{cases} n_7 \equiv 1 \pmod{7} \\ n_7 \mid 48 \end{cases}$$

Suppose G is a simple group, then $n_7 = 8$, $|N_G(P)| = 42$, $G \leq A_g$. Since the power of 7 in $|A_g|$ is 1, we can regard the Sylow7-subgroup P as the Sylow7- subgroup

of A_g . The number of Sylow7-subgroup in S_g is $\frac{A_g^7}{7\times 6} = 960$.

 $\therefore |N_{S_8}(P)| = \frac{|S_8|}{960} = 42$

However $2|A_{g}| = |S_{g}| = |N_{S_{g}}(P)A_{g}| = \frac{|N_{S_{g}}(P)||A_{g}|}{|N_{S_{g}}(P) \cap A_{g}|}, |N_{S_{g}}(P)| = \frac{1}{2}|N_{S_{g}}(P)| = 21.$

And $42 = |N_{G}(P)| |N_{A_{g}}(P)| = 21$. This is a contradiction!

So *G* is not a simple group.

(12)
$$|G| = 392 = 2^3 \times 7^2$$
, then

$$\begin{cases} n_7 \equiv 1 \pmod{7} \\ n_7 \mid 8 \end{cases}$$
$$n_7 = 1.8$$

Suppose *G* is a simple group, then $n_7 = 8$. If $\forall P_i \cap P_j = \{e\}$, then 8 Sylow7-subgroup have8 × $(7^2 - 1) = 354$ non-unit elements in all. So there left392 - 384 = 8 elements. $\therefore n_2 = 1$. This is a contradiction. If $\exists |P_1 \cap P_2| = 7$, then $P_1 \cap P_2 \lhd P_i$ (i = 1,2). Let $N = N_G(P_1 \cap P_2)$ then $|N| \ge |P_1P_2| = \frac{|P_1||P_2|}{|P_1 \cap P_2|} = \frac{7^2 \times 7^2}{7} = 7^3$ $\therefore |N| = 7^2 k \quad (k \mid 8, k > 7)$ $\therefore |G: N| = 1$ $\therefore P_1 \cap P_2 \lhd G$. That means *G* has nontrivial normal subgroup, so *G* is a simple group.

(13)
$$|G| = 400 = 2^4 \times 5^2$$
, then

$$\begin{cases} n_5 \equiv 1 \pmod{5} \\ n_5 \mid 16 \\ n_5 = 1,16 \end{cases}$$

Suppose G is a simple group, then $n_5 = 16$. The order of Sylow5-subgroup P is 5².

 $\therefore \exists P_1 P_2 \in Syl_5(G), |P_1 \cap P_2| = 5$ $\therefore (P_1 \cap P_2) \lhd P_1 and (P_1 \cap P_2) \lhd P_2$

let N = N_G(P₁ ∩ P₂), |N| ≥ |(P₁P₂)| = $\frac{|P_1||P_2|}{|P_1 ∩ P_2|} = \frac{25 \times 25}{5} = 125$ \therefore |N| = 25k(k ≥ 5 \pounds k|16) k=8 or 16

 $|: |G: \mathbb{N}| \leq 2$. That means G has a subgroup with index equal to 2, so G is not a simple group.

(14) When $|G| = 560 = 2^4 \cdot 5 \cdot 7$, according to **lemma 2.40**,

$$\begin{cases} n_7 \equiv 1 \pmod{7} \\ n_7 \mid 80 \end{cases}$$

Suppose *G* is a simple group, then $n_5 = 6$. For any *Sylow* 7 – subgroup *P* of *G*, according to **lemma 2.36**, we have $|G: N_G(P)| = 8$. Considering the premultiplication effect of *G* on the left coset space of $N_G(P)$, this effect leads to the morphism φ from *G* to S_8 . According to **lemma 2.34**, we have

$$G / Ker \varphi \cong \varphi(G) \leq S_8$$

But G is a simple group, therefore $Ker \varphi = 1$, so

$$G \cong \varphi(G) \leq S_8$$

According to the proof of the **theorem 6**, $\varphi(G)$ doesn't contain odd permutation, so

$$G \cong \varphi(G) \le A_8$$

Because 7² can't divide $|A_8| = \frac{1}{2} \cdot 8!$, so we can regard the Sylow 7 – subgroup P of G as the Sylow 7 – subgroup of A_8 . The number of Sylow 7 – subgroups in S_8 is

$$\frac{P_8^7}{7\cdot 6} = 960$$

So $|N_{S_8}(P)| = |S_8|/960 = 42$. But $|N_G(P)| = 70$. This is a contradiction! So G is not a simple group.

(15) When $|G| = 600 = 2^3 \cdot 3 \cdot 5^2$, according to lemma 2.40, $\begin{cases} n_5 \equiv 1 \pmod{5} \\ n_5 \mid 24 \end{cases}$

Suppose G is a simple group, then $n_5 = 6$. For any Sylow 5 – subgroup P of G, according to lemma 2.36, we have $|G: N_G(P)| = 6$. We can deduce that $G \cong \varphi(G) \le A_6$ as the proof in situation(3). But |G| = 600 can't be divided by $|A_6| = 360$. This is a contradiction! So G is not a simple group.

 $(16)|G| = 648 = 2^3 \times 3^4$, then

 $\begin{cases} n_3 \equiv 1 \pmod{3} \\ n_3 \mid 8 \\ n_3 = 1, 4 \end{cases}$

Suppose G is a simple group, then $n_3 = 4$, $|G: \mathbb{N}| = 4$. This is a contradiction!

(17) When $|G| = 672 = 2^5 \cdot 3 \cdot 7$, according to **lemma 2.40**,

$$\begin{cases} n_7 \equiv 1 \pmod{7} \\ n_7 \mid 96 \end{cases}$$

Suppose G is a simple group, then $n_7 = 8$. For any Sylow 7 – subgroup P of G, according to lemma 2.36, we have $|G: N_G(P)| = 8$. Considering the premultiplication effect of G on the left

coset space of $N_G(P)$, this effect leads to the morphism φ from G to S_6 . According to lemma 2.34, we have

$$G / Ker \varphi \cong \varphi(G) \leq S_8$$

G is a simple group, therefore $Ker \varphi = 1$, so

$$G \cong \varphi(G) \le S_8$$

According to the proof of the **theorem 6**, $\varphi(G)$ doesn't contain odd permutation, so

$$G \cong \varphi(G) \le A_8$$

Because 7² can't divide $|A_8| = \frac{1}{2} \cdot 8!$, we can regard the *Sylow* 7 – subgroup *P* of *G* as the Sylow 7 – subgroup *A* of *G* as the

Sylow 7 – group of A_8 . The number of Sylow 7 – subgroup of is

$$\frac{P_8^{\prime}}{7\cdot 6} = 960$$

Therefore $|N_{S_8}(P)| = |S_8|/960 = 42$. But $|N_G(P)| = 96$. This is a contradiction! So *G* is not a simple group.

II. The situations solved by using cyclic group.

(1) When $|G| = 288 = 2^5 \times 3^2$,

$$\begin{cases} n_2 \equiv 1 \pmod{2}, & \{n_3 \equiv 1 \pmod{3} \\ n_2 \mid 9, & n_3 \mid 32 \end{cases}$$

Suppose G is a simple group, then $n_2 = 9$, $n_3 = 16 \neq 1 \pmod{3^2}$ \therefore There exist Sylow3-subgroup P_1 , P_2 , satisfying $|P_i: P_1 \cap P_2| = 3$, (i = 1, 2)

Let $N = N_G(P_1 \cap P_2)$, then $|N| \ge |P_1P_2| = \frac{|P_1||P_2|}{|P_1 \cap P_2|} = \frac{9 \times 9}{3} = 27$

$$\therefore |\mathbf{N}| = 9\mathbf{k}(\mathbf{k}|\mathbf{32}, \mathbf{k} \ge \mathbf{3})$$

: $|N| \ge 36$. According to N/C theorem. $N/C_G(P_1 \cap P_2) \lesssim Aut(P_1 \cap P_2)$

 $\therefore |C_{G}(P_{1} \cap P_{2})| \geq 18$

 \therefore There exists an element $x \in C_G(P_1 \cap P_2)$ of order 6

∴ G ≤ A₉. We can regard x as a permutation on A₉. For any $Q \in Syl_2(G)$, we have $|N_G(Q)| = |G|/n_2 = |Q| = 32$ ∴ x ∉ N_G(Q) (6 ∤ 32)

:. There is no fixed point of x in A_{p} . Suppose x can be expressed by the sum of m 2-cycle, n 3-cycle and y 6-cycle, then 9=2m+3n+6y.

$$\Rightarrow \begin{cases} m = 0\\ n = 1 \text{ or } \\ y = 1 \end{cases} \begin{cases} m = 0\\ n = 3 \text{ or } \\ y = 0 \end{cases} \begin{cases} m = 3\\ n = 1\\ y = 0 \end{cases}$$

According to 3 solutions above we can infer that x is an odd permutation. This is a contradiction! \therefore G is not a simple group.

(2) When $|G| = 420 \times 2^2 \times 3 \times 5 \times 7$

 $\begin{cases} n_7 \equiv 1 \pmod{7} \\ n_7 \mid 60 \end{cases}$

S09

Suppose G is a simple group, then $n_7 = 15$, $G \lesssim A_{15}$. $\forall P \in Syl_{17}(G)$, then $|N_G(P)| = 28$, Then $\frac{N_G(P)}{C_G(P)} \lesssim Aut(P)$ (6 order)

If $|C_G(P)| = |N_G(P)| = 28$, then G has normal 7-complement. So G is not a simple group. If $|C_G(P)| = 14$ (a cyclic group), fetch $x \in C_G(P)$, then $x^2 \in P$, $o(x^2) = 7$. So x can only normalize one Sylow7-subgroup P. $G \lesssim A_{15}$, so we can regard x as an element of order 14 with only one fixed point in A_{15} . Therefore x must be a 14-cycle, an odd permutation. This is a contradiction!

(3) When
$$|G| = 576 \times 2^6 \times 3^2$$
,

$$\begin{cases}
n_2 \equiv 1 \pmod{2}, & n_3 \equiv 1 \pmod{3} \\
n_2 \mid 9, & n_3 \mid 64 \\
n_2 = 1, 3, 9, & n_3 = 1, 4, 16, 64
\end{cases}$$

Suppose G is a simple group, then $n_2 = 9$. If $\exists P_1, P_2 \in Sly_3(G)$, then $|P_1 \cap P_2| = 3$.

Let
$$N = N_{G}(P_{1} \cap P_{2})$$
, then $|N| \ge \frac{|P_{1}P_{2}|}{|P_{1} \cap P_{2}|} = \frac{9 \times 9}{3} = 27$
 $\therefore |N| = 9k \ (k \ge 3, k \mid 26)$
 $\therefore |N| \ge 36, \ |C_{G}(P_{1} \cap P_{2})| = 9(\frac{k}{2}), \ \frac{N_{G}(P_{1} \cap P_{2})}{|C_{G}(P_{1} \cap P_{2})|} \lesssim |Aut(P_{1} \cap P_{2})| = 2$

 $\therefore C_{G}(P_{1} \cap P_{2}) \geq 18$

Then $C_G(P_1 \cap P_2)$ has a subgroup R of order 2, $R(P_1 \cap P_2)$ is a cyclic group of order 6. $\therefore \exists x \in C_G(P_1 \cap P_2)$ of order 6, then $x \notin N_G(P_1 \cap P_2)$. $G \sim A_9$, and L(x) has no fixed point. However there is no L(x) (even permutation) in A_9 . Suppose L(x) is expressed by *m* 2-cycle, and *n* 3-cycle. Then 2m + 3n = 9, m = 3, n = 1.

So L(x) is an odd permutation. This is a contradiction!

For any Sylow3-subgroup, there intersection is $\{e\}$. Suppose $n_3 = 16 \neq 1 \pmod{3^2}$, then must have two Sylow3-subgroups which intersection isn't $\{e\}$. This is a contradiction! So any two Sylow3-subgroup's intersection is $\{e\}$.

Suppose $n_a \neq 1 \pmod{3^2}$, then there must exists $P_i \cap P_j \neq \{e\}$. This contradicts with the

conclusion above.

∴ n₃ = 64

:.Sylow3-subgroups have $64 \times (3^2 - 1) = 512$ non-unit elements in all.

 \therefore There left 576 - 512 = 64 elements.

 \therefore n₂ = 1. So G is not a simple group.

(4) When $|G| = 612 = 2^2 \cdot 3^2 \cdot 17$, according to **lemma 2.40**,

$$\begin{cases} n_3 \equiv 1 \pmod{3}, & \{n_{17} \equiv 1 \pmod{17}\}\\ n_3 \mid 68, & n_{17} \mid 36 \end{cases}$$

Suppose *G* is a simple group, then $n_3 = 34$ and $n_{17} = 18$. For any Sylow 17subgroup *P* of *G*, according to **lemma 2.36**, we have $|G:N_G(P)| = 18$, $|N_G(P)| = 34$. According to **lemma 2.22**, $N_G(P)/C_G(P) \cong Aut(P)$'s one certain subgroup. |Aut(P)| = 17 - 1 = 16, so $|C_G(P)| = 17$ or $|C_G(P)| = 34$. If $|C_G(P)| = 34$, then according to **lemma 2.45**, group *G* has a normal 17 – complement,. So it's not a simple group. This is a contradiction! If $|C_G(P)| = 17$, because $n_3 = 34 \neq 1 \pmod{3^2}$, and according to **lemma 2.41**, there must exists two *Sylow* 3 – subgroups Q_1, Q_2 , such that $|Q_i: Q_1 \cap Q_2| = 3$ (i = 1, 2). So $Q_1 \cap Q_2 \triangleleft Q_1, Q_1 \cap Q_2 \triangleleft Q_2$

Therefore

$$Q_1, Q_2 \leq N_G(Q_1 \cap Q_2)$$

So

$$|N_G(Q_1 \cap Q_2)| \ge |Q_1 \cdot Q_2| = \frac{|Q_1||Q_2|}{|Q_1 \cap Q_2|} = 27$$

Suppose that $9||N_G(Q_1 \cap Q_2)|||G| = 2^2 \cdot 3^2 \cdot 17$, then $36||N_G(Q_1 \cap Q_2)|$. According to **lemma 2.22**,

 $N_G(Q_1 \cap Q_2)/C_G(Q_1 \cap Q_2) \cong Aut(Q_1 \cap Q_2)$'s one certain subgroup $|Aut(Q_1 \cap Q_2)| = 3 - 1 = 2$, so $|C_G(Q_1 \cap Q_2)|$ contains a factor 2. consider the Sylow 2 – subgroup R of $C_G(Q_1 \cap Q_2)$, then $R(Q_1 \cap Q_2) \leq G$ is a cyclic group of order 6. So G has an element x of order 6. According to **lemma 2.9**, $x \notin N_G(P)$, that means x can't normalize any Sylow 17 – subgroup P. Considering the premultiplication effect of G on the left coset space of $N_G(P)$, this effect leads to the morphism φ from G to S_8 . According to **lemma 2.34** and the proof of **theorem 6**, we can deduce that $\varphi(G)$ doesn't contain odd permutation, so

$$G \cong \varphi(G) \le A_{18}$$

Therefore we can regard x as an element of order 6 of A_{18} , and there is no fixed point. If x 's cyclic decomposition has a transformation, then x^2 is an elements of order 3 and there are at least two fixed points. So x^2 can normalize a certain Sylow 17 – subgroup P'. So $x^2 \in N_G(P')$, but $|N_G(P')| = 34$. Therefore, this is impossible! So x 's cyclic decomposition can only contains odd(≥ 2) 6 – cycles and several 3 – cycle. Suppose there are $2k (k \in N_+)$ 6 – cycle and l 3 – cycle in x 's cyclic decomposition. From

$$2k \times 6 + 3l = 18$$

we know that only k = 1, l = 2 is possible. That means the cyclic decomposition of x contains 2 6 – cycle and 2 3 – cycle. In this condition x^3 is an element of order 2 with exactly 6 fixed points. That is x^3 normalized 6 Sylow 17 – subgroups. $x^3 \in N_G(P) \setminus C_G(P)$, but according to **lemma 2.50**, we know that, x^3 can normalize up to

$$k = 1 + \frac{n_{17} - 1}{17} = 1 + \frac{18 - 1}{17} = 2$$
 Sylow 17 - subgroups.

This is a contradiction! Hence G is not a simple group

III. The situations solved by induction.

(1) When $|G| = 132 = 2^2 \cdot 3 \cdot 11$, according to **lemma 2.40**,

$$\begin{cases} n_{11} \equiv 1 \pmod{11}, & \{n_3 \equiv 1 \pmod{3} \\ n_{11} \mid 12, & n_3 \mid 44 \end{cases}$$

Suppose G is a simple group, then there must have $n_{11} = 12$ and $n_3 = 4$, 22. According to the remark of **lemma 2.34**, there must have $n_3 = 22$. So G contains

 $(11-1) \times 12 = 120$ elements of order 11

 $(3-1) \times 22 = 44$ elements of order 3

But 120 + 44 = 164 > 132. This is a contradiction. So G is not a simple group.

(2) When $|G| = 280 = 2^3 \cdot 5 \cdot 7$, according to **lemma 2.40**,

$$\begin{cases} n_5 \equiv 1 \pmod{5}, & \{n_7 \equiv 1 \pmod{7} \\ n_5 \mid 56, & n_7 \mid 40 \end{cases}$$

Suppose G is a simple group, then $n_5 = 56$ and $n_7 = 8$. So G has

 $(5-1) \times 56 = 224$ elements of order 5

 $(7-1) \times 8 = 48$ elements of order 7

Therefore left

$$280 - 224 - 48 = 8$$
 elements

But G has Sylow 2 – subgroups, so $n_2 = 1$. According to theorem 7, G is not a simple group.

(3) When $|G| = 380 = 2^2 \cdot 5 \cdot 19$, according to **lemma 2.40**,

$$\begin{cases} n_{19} \equiv 1 \pmod{19}, & n_5 \equiv 1 \pmod{5} \\ n_{19} \mid 20, & n_5 \mid 76 \end{cases}$$

Suppose G is a simple group, then $n_{19} = 20$ and $n_5 = 76$. So G has

 $(19-1) \times 20 = 360$ elements of order 19

 $(5-1) \times 76 = 304$ elements of order 5

But 360 + 304 = 664 > 380. This is a contradiction! So G is not a simple group.

(4) When $|G| = 495 = 3^2 \cdot 5 \cdot 11$, according to **lemma 2.40**,

$$\begin{cases} n_{11} \equiv 1 \pmod{11}, & \{n_3 \equiv 1 \pmod{3} \\ n_{11} \mid 45, & n_3 \mid 55 \end{cases}$$

Suppose G is a simple group, then $n_{11} = 45$ and $n_3 = 55$. So G has

 $(11-1) \times 45 = 450$ elements of order 11

 $(3-1) \times 55 = 110$ elements of order 3

But 450 + 110 = 560 > 495. This is a contradiction! So G is not a simple group.

(5) When $|G| = 520 = 2^3 \cdot 5 \cdot 13$, according to lemma 2.40,

$$\begin{cases} n_{13} \equiv 1 \pmod{13}, & \{n_5 \equiv 1 \pmod{5} \\ n_{13} \mid 40, & n_5 \mid 104 \end{cases}$$

Suppose G is a simple group, there must have $n_{13} = 40$ and $n_5 = 26$. So G has

 $(13-1) \times 40 = 480$ elements of order 13

 $(5-1) \times 26 = 104$ elements of order 5

But 480 + 104 = 584 > 520. This is a contradiction! So *G* is not a simple group.

(6) When $|G| = 616 = 2^3 \cdot 7 \cdot 11$, according to lemma 2.40,

$$\begin{cases} n_7 \equiv 1 \pmod{7} , & \{ n_{11} \equiv 1 \pmod{11} \\ n_7 \mid 88 , & \{ n_{11} \mid 56 \end{cases} \end{cases}$$

Suppose G is a simple group, there must have $n_7 = 8$ and $n_{11} = 56$. So G have

$$(7-1) \times 8 = 48$$
 elements of order 7

 $(11-1) \times 56 = 560$ elements of order 11

So there left

$$616 - 48 - 560 = 8$$
 elements

But group G has Sylow 2 – subgroup, so $n_2 = 1$. According to **theorem7**, we know that G is not a simple group.

IV. The situations solved by normal p-complement

(1) When $|G| = 396 = 2^2 \times 3^2 \times 11$ $\begin{cases} n_{11} \equiv 1 \pmod{11} \\ n_{11} \mid 36 \end{cases}$ $n_{11} = 1,12$ Suppose G is a simple group, then $n_{11} = 12$, $\forall P \in Syl_{11}(G)$, then $|N_G(P)| = 33$.

$$\frac{|N_{G}(P)|}{|C_{G}(P)|} \lesssim \operatorname{Aut}(p)$$

$$\left. \left. \left. \left| N_{\mathsf{G}}(\mathsf{P}) \right| \right/ _{\left| \mathsf{C}_{\mathsf{G}}(\mathsf{P}) \right|} \right| |\mathrm{Aut}(\mathsf{p})| = 10$$

 $\therefore |C_G(G)| = 33$

 $: N_G(P) = C_G(P)$. That means G has a normal 11-complement. So G is not a simple group. This is a contradiction!

(2) When $|G| = 528 = 2^4 \cdot 3 \cdot 11$, according to **lemma 2.40**,

$$\begin{cases} n_3 \equiv 1 \pmod{3} \\ n_3 \mid 176 \end{cases}$$

Suppose G is a simple group, then $n_3 = 16$. For any Sylow 3 – subgroup P of G, according to lemma 2.36, we have $|G:N_G(P)| = 16$, $|N_G(P)| = 33$. According to lemma 2.22,

21

 $N_G(P)/C_G(P)$ is isomorphic to a subgroup of Aut(P). According to lemma 2.9, $|N_G(P)/C_G(P)| | |\text{Aut}(P)| = 7-1 = 6$. So $N_G(P) = C_G(P)$. According to lemma 2.45, G has a normal 3 – complement and it is not a simple group.

(3) When $|G| = 540 = 2^2 \cdot 3^3 \cdot 5$, according to **lemma 2.40**,

 $\begin{cases} n_5 \equiv 1 \pmod{5} \\ n_5 \mid 108 \end{cases}$

Suppose G is a simple group, then $n_5 = 6$ or $n_5 = 26$. If $n_5 = 6$, then we have a contradiction. If $n_5 = 26$, for any Sylow 5 – subgroup P of G, according to lemma 2.36, we have $|G:N_G(P)| = 26$, $|N_G(P)| = 15$. According to lemma 2.22, $N_G(P)/C_G(P)$ is isomorphic to a subgroup of Aut(P). According to lemma 2.9, $|N_G(P)/C_G(P)| ||\text{Aut}(P)| = 5 - 1 = 4$. So $N_G(P) = C_G(P)$. According to lemma 2.45, G has a normal 5 – complement and it is not a simple group.

(4) When $|G| = 552 = 2^3 \cdot 3 \cdot 23$, according to **lemma 2.40**,

$$\begin{cases} n_{23} \equiv 1 \pmod{23} \\ n_{23} \mid 24 \end{cases}$$

Suppose *G* is a simple group, then $n_{23} = 24$. For any *Sylow* 23 – subgroup *P* of *G*, according to lemma 2.36, we have $|G: N_G(P)| = 24$, $|N_G(P)| = 23$. According to lemma 2.22, $N_G(P)/C_G(P)$ is isomorphic to a subgroup of Aut(*P*). According to lemma 2.9, $|N_G(P)/C_G(P)| || |\text{Aut}(P)| = 23 - 1 = 22$. So $N_G(P) = C_G(P)$. According to lemma 2.45, *G* has a normal 23 – complement and it is not a simple group.

V. The situations solved by using $n_p \neq 1 \pmod{p^2}$

(1) When $|G| = 432 = 2^4 \times 3^3$, $\begin{cases}
 n_3 \equiv 1 \pmod{3} \\
 n_3 \mid 16 \\
 n_3 = 1, 4, 16
 \end{cases}$

Suppose G is a simple group, then $n_3 = 16$.

∴ There must exists Sylow3-subgroup, $|P_1: P_1 \cap P_2| = 3, P_1 \cap P_2 = 9, N \triangleq N_G(P_1 \cap P_2) \ge P_1, P_2$ ∴ $|N| \ge |P_1P_2| = \frac{27 \times 27}{9} = \frac{|P_1||P_2|}{|P_1 \cap P_2|} = 81$

 \therefore |G: N| \leq 4, that means G must not be a simple group. This is a contradiction!

(2) When $|G| = 480 = 2^5 \times 3 \times 5$

 $\begin{cases} n_2 \equiv 1 \pmod{2} \\ n_2 \mid 15 \\ n_2 = 1, 3, 5, 15 \end{cases}$

Suppose G is a simple group, then $n_2 = 5,15$

Suppose $n_2 = 5$, then $G \lesssim A_5$. However $|G| = 480 \nmid |A_5| = 60$.

If $n_5 = 15 \not\equiv 1 \pmod{2^2}$, then there must be 2 Sylow2-subgroup P_1, P_2 satisfied $|P_i: P_1 \cap P_2| = 2$. That means $P_1 \cap P_2 \lhd P_i (i = 1, 2)$. Let $N = N_G(P_1 \cap P_2)$, then $|N| \ge |P_1, P_2| = \frac{|P_1||P_2|}{|P_1 \cap P_2|} = \frac{32 \times 32}{16} = 64$ $\therefore |G: N| \le 5$, so $G \lesssim A_5$. This is a contradiction!

VI. The situations which may be a simple group

(1) When |G| = 60, if $G \cong Z_{60}$, then G is not a simple group. If $G \cong A_5$, then G is a simple group.

(2) $|G| = 168 = 2^3 \times 3 \times 7$, The order of the simple group $PSL_2(F_7)[2]$ is

$$|PSL_2(F_7)| = \frac{(7^2 - 1)(7^7 - 1)}{(7 - 1)(2, 7 - 1)} = 168$$

However when $G \cong \mathbb{Z}_{162}$, it isn't a simple group. So group G of order 168 may be a simple group or may not.

(3) $|G| = 360 = 2^3 \times 3^2 \times 5$. Since $|A_6| = \frac{1}{2} |S_6| = 360$ and A_6 is a simple group.

However when $G \cong \mathbb{Z}_{260}$, it isn't a simple group. So group G of order 360 may be a simple group or may not.

(4) When $|G| = 504 = 2^3 \cdot 3^2 \cdot 7$. The order of the simple group $PSL_2(F_8)$ [2] is

$$|PSL_2(F_8)| = \frac{(8^2 - 1)(8^2 - 8)}{(8 - 1)(2, 8 - 1)} = 504$$

However when $G \cong Z_{504}$, it isn't a simple group. So group G of order 504 may be a simple group or may not.

(5) When $|G| = 660 = 2^2 \cdot 3 \cdot 5 \cdot 7$. The order of the simple group $PSL_2(F_{11})$ [2] is

$$\left| PSL_{2}(F_{11}) \right| = \frac{(11^{2} - 1)(11^{2} - 11)}{(11 - 1)(2, 11 - 1)} = 660$$

However when $G \cong Z_{660}$, it isn't a simple group. So group G of order 504 may be a simple group or may not.

Considering all the above, here we come to the conclusion.

Theorem 9 A group G of order less or equal than 700 could not be simple except for

 $|G| \in \{60, 168, 360, 504, 660\}$ and all prime numbers.

§ 4 Ending and the questions left

Basing on Sylow theorem, Burnside theorem and elementary group theories like group action, we got a series of conditions to judge whether the group is simple or not.

Theorem A group G of order less or equal than 700 could not be simple except for

 $|G| \in \{60, 168, 360, 504, 660 \text{ and all primes}\}$.

The distribution of simple group of low-order is discussed. But we can't make a discussion to simple groups of order more than 700. Above the whole paper, research on numbers of particular Sylow subgroups is the main work. Sometimes we can judge it directly by exact division, while sometimes some methods like group action or some properties of permutation group. All in all, analyzing should be directed against specific conditions and methods are not fixed.

Here G is a finite group and P is its subgroup, $|G| = p^r m, (p, m) = 1$. According to Lagrange theorem, we have

$$\left|G:P\right| = \left|G:N_{G}\left(P\right)\right| \cdot \left|N_{G}\left(P\right):P\right|$$

That is

$$|G| = |G: N_G(P)| \cdot |N_G(P): P| \cdot |P|$$

Thereinto

$$\left|G:N_{G}\left(P\right)\right|=n_{p}=1+kp\equiv1(\mod p), \quad \left|P\right|=p^{r}$$

With the notation $\left| N_{G}(P) : P \right| = v$, we have

$$|G| = (1+kp) \cdot v \cdot p^r$$

If an unified restrictive condition of the three parameter (k, v, r) above can be found, we are able to judge whether the group of high order is simple or not. This is an important question left to be studied.

Acknowledgment

During the research with the aim of classifying finite groups clearly, most papers on this topic were published from 1955 to 2004. In order to finish this task, about 100 authors written down more than ten thousand pages of words in over 500 weekly magazines.

It's know to all that mathematic research is an endless journey. This is the first time for us to take part in Shing-Tung Yau High School Mathematics Award. That's to say we are still at the beginning of the journey. Yet our paper is not mature and our analysis can't cover all aspects, we sincerely hope you teachers to point out every disadvantage for us. With your construction, we can go further in the future.

Here, we merely show our gratitude to all the professions, teachers, parents and students which have gave us help. No matter what the result is, we believe that this study would bring us great effective.

Reference

- Daoji Meng, Liangyun Chen, Yiqian Shi, Ruipu Bai. Abstract Algebra I Algebra based[M].Beijing: Science Press, 2010. 132.
- [2] Mingyao Xu. The finite group guidance [M].Beijing: Science Press, 2001. 80.
- [3] Huiqiang Tao. The Simplicity of Groups of Order within 100 [J]. Tianzhong Journal, 2010, 23(5): 9-11.
- [4] Nicolas, D, Meyer. Transfer Theory and its applications to the study of Simple groups[D].U.S.A: Southern Illinois University, 2010. 37-57.
- [5] Jiping Zhang. In the new century algebra (retrospect and prospect)[M]. Beijing: Peking University Press, 2002.
- [6] Shian Han, Lei Lin. Modern algebra [M]. Beijing: Science Press, 2009.
- [7] David, S. Dummit. Abstract Algebra [M]. U.S.A.: JOHN WILEY AND SONS INC, 2004.