Wujie Shi (施武杰)
Chongqing University of Arts and Sciences
Suzhou University
shiwujie@outlook.com

Canadian Number Theory Association Conference

Laval University July 10, 2018

Introduction

Let G be a finite group and $Ch_i(G)$ be one of the following sets:

$Ch_1(G) = |G|$, that is, the order of G;

$Ch_2(G) = \pi_e(G) = \{ o(g) \mid g \in G \}$, that is, the set of element orders of G, (spectrum);

Our aim is to study the structure of G under certain arithmetical hypotheses of $Ch_i(G)$, $i = 1, 2$.

I am very interesting in $|G|$ and $Ch_2(G) = \pi_e(G)$ (spectrum).

They are all the sets of numbers

Some famous results for $|G|$

Sylow(1832-1918) theorem

Lagrange(1736-1813) theorem

$|G|$ is odd $\Rightarrow$ G solvable (1906, Burnside(1852-1927) posed, 1963, W. Feit(1930-2004) and J.G. Thompson(1932-) proved, Full paper 254 pages, filled an entire issue of the Pacific Journal of Mathematics, 1963, Thompson got Fields prize for it.)

$p^a q^b$ theorem: $|G| = p^a q^b \Rightarrow G$ solvable

Cauchy(1789-1857) theorem: $p \mid |G| \Leftrightarrow p \in \pi_e(G)$

Denote by $\boldsymbol{\pi_e(G)}$ (that is, $\mathbf{Ch_2}(\boldsymbol{G})$ in this talk) the set of all orders of elements in *G*.

For the set {|G|}, there are many famous and interesting results. But we do not know more information for the set $\boldsymbol{\pi_e(G)}$.

Obviously, $\boldsymbol{\pi_e(G)}$ is a subset of the set $\boldsymbol{Z^+}$ of positive integers, and a difficult problem is:

" Which subset of Z^+ can constitute a set of orders of element of a group? "

If $m \in \pi_e(G)$ and $n \mid m$, we have $n \in \pi_e(G)$, that is, it has a closure property for division. We only know it for this set.

Some interesting results for $\pi_e(G)$

Theorem 1.1(Brandl, Shi; 1991) Let G be a finite group whose element orders are consecutive integers. That is, $\pi_e(G) = \{1, 2, 3, \ldots, n\}$. Then $n \leq 8$. (J. of Algebra, 1991)

What about $\{1, \ldots, n-2, n-1, n\}$?

Means, the largest numbers are consecutive

If we divide the set $\pi_e(G)$ into {1}, the set $\pi_e'(G)$ consisting of primes and the set $\pi_e''(G)$ consisting of composite numbers, then we have

Theorem 1.2(Deng, Shi; 1997) Let G be any finite group. Then

$$|\pi_e'(G)| \leq |\pi_e''(G)| + 3,$$

and if the equality holds, then G is simple. Moreover, these simple groups are all determined only by the set $\pi_e(G)$.

(J. of Algebra, **1997**)

“ Which subset of Z^+ constitute a set of orders of element of a group? ”

This is an interesting and more difficulty problem.

In general, what kind of quantitative sets can be the set of conjugated invariants of a finite group (degree of characters, the size of conjugacy class, the number of same order elements, …)? These are all interesting and difficult problems.

Definition . For any $n \in Z^+$, set $\pi(n) := \{ p \mid p \text{ prime}, p \mid n \}$.
For a finite group G, set $\pi(G) := \pi(|G|)$.
From $p^a q^b$ theorem we have, if G is simple, then $|\pi(G)| \geq 3$.
Using the number $|\pi(G)|$, M. Herzog got the following result.

Theorem 3.2(M. Herzog; 1968). Let G be a finite simple group. If $|\pi(G)|=3$, then G is isomorphic to one of the following groups: A_5, $L_2(7)$, $L_2(8)$, A_6, $L_2(17)$, $L_3(3)$, $U_3(3)$ or $U_4(2)$.

D. Gorenstein called above eight simple groups as simple K_3-groups (i.e. $|\pi(G)|=3$).

We determined all simple K_4-groups (i.e. $|\pi(G)|=4$) using the classification theorem, but we do not know the number of simple K_4-groups is finite or infinite.

Theorem 3.3(Shi; 1991) Let G be a simple K_4-group. Then G is isomorphic to one of the following groups: A_n, $n = 7, 8, 9, 10$; M_{11}, M_{12}, J_2; $L_2(q)$, $q = 16, 25, 49, 81$; $L_3(q)$, $q = 4, 5, 7, 8, 17$; $L_4(3)$; $O_5(q)$, $q = 4, 5, 7, 9$; $O_7(2)$, $O_8^+(2)$, $G_2(3)$; $U_3(q)$, $q = 4, 5, 7, 8, 9$; $U_4(3)$; $U_5(2)$; ${}^3D_4(2)$; ${}^2F_4(2)'$; $Sz(8)$, $Sz(32)$; and $L_2(r)$, r being prime and satisfying the following equation:

$$r^2 - 1 = 2^a 3^b u^c, \tag{1}$$

where $a \geq 1$, $b \geq 1$, $c \geq 1$, u prime, $u > 3$;

$L_2(2^m)$ and satisfying the following equations:

$$\begin{cases} 2^m - 1 = u \\ 2^m + 1 = 3t^b \end{cases} \tag{2}$$

where $m \geq 1$, u, t primes, $t > 3$, $b \geq 1$;

$L_2(3^m)$ and satisfying the following equations:

$$\begin{cases} 3^m + 1 = 4t \\ 3^m - 1 = 2u^c \end{cases} \tag{3}$$

$$\begin{cases} 3^m + 1 = 4t^b \\ 3^m - 1 = 2u \end{cases} \tag{4}$$

where $m \geq 1$, u, t odd primes, $c \geq 1$, $b \geq 1$.

Remark 3.1. In 2001, some authors investigate these Diophantine systems and proved that equations (2), (3) and (4) have no other solution except $m = 5$, $u = 11$, $c = 2$ in (3) when the exponents are greater than 1.(Y. Bugeaud, Z. Cao and M. Mignotte, On simple K_4-groups, J. Algebra, 241(2001), 658~668.)

Question 3.1. The number of simple K_4-groups is determined by the number of solution of equations (1) ~ (4). But it is unknown whether the number of solution is finite or infinite. In other words, is the number of simple K_4-groups finite or infinite?

(UNSOLVED PROBLEMS IN GROUP THEORY 13.65. is the number of K4-groups finite or infinite? W. J. Shi)

It was verified that the number of simple K_4-groups is 101 if the largest prime divisor of the orders of groups is less than 10^{60}. We believe that the problem is more difficult that the number of simple K_4-groups is finite or infinite?

Recently, Zhang and Shi (2013) proved that

$$r^2 - 1 = 2^a 3^b u^c, \qquad (1)$$

if c > 1, (1) has only the solutions (r, u, a, b, c) = (97, 7, 6, 1, 2) and (r, u, a, b, c) = (577, 17, 7, 2, 2).

In the above paper we try to point out that it is very difficult to determine the infinitude of simple K_4-groups, and this problem goes far beyond what is known about Dickson's conjecture (L. E. Dickson, A new extension of Dirichlet's theorem on prime numbers, Messenger of mathematics 33(1904), 155-161.).

On the other hand, even if Dickson's conjecture holds, it is not obvious that the number of simple K_4-groups is infinite.

The number of K_2-simple groups = 0 ($p^a q^b$ theorem)

The number of K_3-simple groups = 8

(Herzog result)

The number of K_4-simple groups = finite or infinite?

Another Question is :

The number N of simple groups G whose order $|G| = m^k$ ($k > 1$).

R. Brauer, On groups whose order contains a prime to the first power, I, II , Amer. J. Math. 64(1940).

My teacher Prof. Chen proved:

If $k > 2$, then $N = 0$.

If $k = 2$, then G is a simple group of Lie type, $B_2(p)$

($|B_2(p)| = p^4(p^2-1)(p^4-1)/2$)

where p is a prime satisfying:

$$p = 1 + 2C_{2n+1}^{2} + 2^2 C_{2n+1}^{4} + \ldots.. + 2^n C_{2n+1}^{2n}$$

Taking n =1, we have p = 7 and $|B_2(7)| = 2^8 3^2 5^2 7^4$

Problem. How many p satisfying the above equality, finite or infinite？

In Creseenzo, P., Adv. Math. 17(1975),25-29.

The author consider the following Diophantine equation:

$$p^m - 2q^n = \pm 1,\ p,\ q \text{ primes and } m > 1,\ n > 1$$

Exception $239^2 - 2.13^2 = -1$, m = n = 2, if the above have solutions. We found (1982) that

$$3^5 - 2.11^2 = 1$$

Ques. 1. Whether or not $p^m - 2q^n = 1$(special Pell's equation) have other solution, except (p,q; m,n) = (3,11; 5,2)?

Related the above problem is the

$$p^2 - 2q^2 = -1,\ p, q \text{ are primes.}$$

Dr. Qu proved that if $p < 10^{15}$, then p = 7, 41, 63018038201, only three primes satisfy the above equality.

That is, for these p, $|B_2(p)| = m^2$. And, but the Problem is open.

Charactering all f.s.g using "two orders"

Characterizing all finite simple groups unitization using only the two sets: $|G|$ and $\pi_e(G)$.

Now we prove the following (posed in 1987):

Theorem 4.1 Let G be a group and M a finite simple group. Then **$G \cong M$ if and only if**
(a) $\pi_e(G)=\pi_e(M)$, and (b) $|G| = |M|$.

Proof. Using CFSG.

1. Sporadic simple groups, 1987, Shi.
2. PSL(n, q), 1990, Shi+Bi.
3. Suzuki–Ree groups, 1991, Shi+Bi.
4. A_n, 1992, Shi+Bi.
5. $G_2(q)$, $F_4(q)$, $E_6(q)$, $E_7(q)$, $E_8(q)$, ${}^3D_4(q)$, ${}^2E_6(q)$, 1994, Shi.
6. PSU(n,q), 2002, Cao+Shi.
7. ${}^2D_n(q)$, $D_l(q)$ (l odd), 2003, Xu+Shi
8. $C_n(q)$, $D_n(q)$, $D_l(q)$ (l even), 2009, Vasilev + Grechkoseeva + Mazurov

What meaning？

1. It say “number”, “the set of number” is very important in Mathematics. Of course!

   If we have no the factorization for the integers, no Sylow theorem!

2. The finite simple groups are very complex, but we may unify characterize them using the most simple concepts. i.e. all finite simple groups can determined by their “two orders”.

3. Our proof depend on the classification of CFSG.

Another related problem is the classification of simple C_{pp}-groups. **A group is called C_{pp}-group if the centralizers of p-elements are p-subgroups.**

For some special p, $p = 2^a 3^b + 1$ or $p = 2^a 5^b + 1$

Using CFSG and some lemmas of Diophantine equations, we determine thus C_{pp}-groups. (see Chen and Shi, Li)

Ques . How classify all finite C_{pp}-groups ?

Thank you for

Your attention !