A NOTE ON WEISENER THEOREM

Rulin Shen*

Department of Mathematics, Hubei University for Nationalities, Enshi, Hubei, P. R. China, 445000

*E-mail: rulinshen@gmail.com

(Received on: 25-01-11; Accepted on: 23-02-11)

ABSTRACT

Let \( \pi(n) \) be the prime divisor set of \( n \) and called that \( n \) is a \( \pi(n) \)-number. Denote by \( n_\pi \) the greatest divisor of \( n \) whose prime divisor set is \( \pi \). Let \( G \) be a finite group. Weisener Theorem states that the number \( w(n) \) of elements whose orders are multiples of \( n \) is either zero, or a multiple of \(|G|^{\pi(n)}\). In this paper we classify groups satisfied \( w(n) = 0 \) or a \( \pi(|G|)\pi(n) \)-number.

Keywords: Weisener theorem, number of elements, finite groups.


1. INTRODUCTION AND LEMMAS:

A fundamental result of Frobenius states that in a finite group the number of elements which satisfy the equation \( x^n = 1 \), where \( n \) divides the order of the group, is divisible by \( n \). This theorem and several generalizations were obtained by Frobenius at the turn of the 1900s. These results have stimulated a great amount of interest in counting solutions of equations in groups. Afterwards, Weisener gave a theorem about quantitative relations of numbers of elements (see Theorem 3, [6]). Let \( G \) be a finite group of order \(|G|\). Let \( o(g) \) denote the order of \( g \) (\( \in G \)). Let \( W(n) = \{ x \in G : n \mid o(x) \} \) where \( a \mid b \) means \( a \) divides \( b \) and let \( w(n) = |W(n)| \). Clearly, \( w(1) = |G| \). Let \( \pi(n) \) be the prime divisor set of \( n \) and called that \( n \) is a \( \pi(n) \)-number (we also assume that 1 is a \( \pi \)-number). Denote by \( n_\pi \) the greatest divisor of \( n \) whose prime divisor set is \( \pi \). Let \( G \) be a finite group. Weisener theorem states that the number \( w(n) \) of elements whose orders are multiples of \( n \) is either zero, or a multiple of \( |G|^{\pi(n)} \). In this paper we classify groups satisfied \( w(n) = 0 \) or a \( \pi(|G|)\pi(n) \)-number. We prove

**Theorem:** Suppose that \( w(n) = 0 \), or a \( \pi(|G|)\pi(n) \)-number for all \( n \). Then \( G \) is one of the following groups

(a) \( Z_2 \);

(b) Frobenius groups \( K: Z_2 \), where Sylow subgroup of \( K \) is of order a Fermat prime or isomorphic to \( Z_2^2 \);

(c) Frobenius groups \( Z_2^k: H \), where \( H \) is cyclic and Sylow subgroup of \( H \) is of order a Mersenne prime.

(d) Simple groups \( PSL_2(2^7), PSL_2(2^8), PSL_2(2^9) \) and \( PSL_2(2^{16}) \).

*Corresponding author: Rulin Shen*, *E-mail: rulinshen@gmail.com
Next we will cite some lemmas. On the set \( \pi(|G|) \) we define a graph \( G_{K}(G) \), called prime graph, whose vertices set is \( \pi(|G|) \) with the following adjacency relation: vertices \( r \) and \( s \) in \( \pi(|G|) \) are joined by edge if and only if \( rs \) is the order of some element of \( G \). Denote the connected components of the graph by \( \{ \pi_{i}, i=1,\ldots,s:=s(G) \} \), \( s(G) \) is said to the number of connected components of \( G \) and if \( 2 \in \pi(G) \), denote the component containing 2 by \( \pi_{1} \) always. The structure of the group which the number of connected components of prime graph is more than 1 is due to Gruenberg and Kegel as follows. Recall that a 2-Frobenius group \( G \) is \( ABC \), where \( A \) and \( AB \) are normal subgroups of \( G \), \( AB \) and \( BC \) are Frobenius group with kernel \( A \), \( B \) and complements \( B, C \) respectively.

**Lemma: 1** If a finite group \( G \) has the disconnected prime graph, then one of the following statements holds:

1. \( s(G) = 2 \) and \( G \) is a Frobenius group or 2-Frobenius.
2. There exists a non-abelian simple group \( S \) such that \( S \leq H = G/N \leq Aut(S) \), where \( N \) is the maximal normal soluble subgroup of \( G \). Furthermore, \( N \) and \( H/S \) are \( \pi_{i}(G) \)-subgroups, the prime graph \( G_{K}(S) \) is disconnected.

In [2] and [5] the prime graph components of non-abelian simple groups are given.

**Lemma: 2** If \( \pi(G)=\{p, q\} \) with \( p, q \) both odd primes, and \( G \) has no element of order \( pq \), then \( G \) is a Frobenius group or a 2-Frobenius group.

**Lemma: 3** Let \( G=ABC \) be a 2-Frobenius group as above. Suppose that \( AC \) is a \( p \)-group. Then \( \exp(AC) \geq p^{2} \).

**Proof:** Without loss of generality, we assume that \( A \) is elementary abelian \( p \)-group and \( C \) is of order \( p \). We regard \( BC \) acts on the vector space \( A \). Since \( p \) does not divide \( |B| \) and \( B \) acts nontrivially, \( A \) has a basis that is permuted semi-regularly by \( C \). This means that all orbits have size \( |C| \) (see Theorem 15.16, [1]). Let \( x_{1}, x_{2},\ldots, x_{p} \) be one \( C \)-orbit of basis vectors. Then the subgroup of \( A \) generated by \( \{x_{1}, x_{2},\ldots, x_{p}\} \) is elementary of order \( p^{r} \), and a basis is permuted transitively by \( C \). The \( p \)-group generated by \( \{x_{1}, x_{2},\ldots, x_{p}\} \) and \( C \), therefore, is isomorphic to the wreath product of a cyclic group \( Z_{p} \) by itself. That wreath product has exponent \( p^{2} \). More specifically, let \( c \) generate \( C \). Then the element \( x, c \) has order \( p^{2} \).

2. **Proof of Theorem:** Let \( \pi_{i}(G) \) be the set of order of elements of \( G \) and \( \pi(|G|)=\{p_{1}, p_{2}, \ldots, p_{m}\} \). Denote by \( s_{i} \) the number of elements of order \( i \). Suppose that \( |G|=p_{1}^{m_{1}}p_{2}^{m_{2}}\ldots p_{m}^{m_{m}} \) and \( n \) is a maximal order in \( \pi_{i}(G) \). And let \( |G|_{\text{max}}=p_{1}^{m_{1}}p_{2}^{m_{2}}\ldots p_{i}^{m_{i}} \). Since \( w(n) \) is a \( \{p_{1}, p_{2}, \ldots, p_{m}\} \)-number and \( \varphi(n) \mid w(n) \) with \( \varphi \) Euler function, we have \( n \) is a square-free number, that is a multiple of some primes. Thus every order of non-unit elements is a multiple of some primes. Now if there is odd prime order \( p \) which is not maximal in \( \pi_{i}(G) \). Without loss of generality, we assume that \( p \mid p_{1} \). Then we have the following identity formula

\[
p_{1}^{r_{1}}\ldots p_{m}^{r_{m}}w(p)=w(p_{1})+w(pr_{1})+\ldots+w(pr_{n}),
\]

where \( \{r_{1}, r_{2}, \ldots, r_{n}\} \subseteq \pi(|G|)/\{p_{1}\} \). So \( W(p_{r}) \) has no element of order \( 2p \) for \( i=1,2,\ldots, h \). In fact, otherwise \( w(2p) \) is odd, but \( w(p) \) and \( w(pr) \) is even for \( r\neq 2 \) since \( 2 \mid p-1 \mid \varphi(p) \mid w(p) \) and \( w(pr) \). This contradicts above equality. Therefore, odd prime \( p \) is disconnected to 2 in the prime graph of \( G \), that is 2 is a component of \( G_{K}(G) \). By Lemma 1 we divide into three cases to discuss.

**Case 1:** \( G \) is a Frobenius group. Suppose that \( K \) and \( H \) are kernel and complement of \( G \), respectively. Then \( H \) is one of square-free order since Sylow subgroup of \( H \) is a cyclic group of order prime.

If \( 2 \mid |H| \), then \( |H|=2 \) since \( s(G)=2 \). In addition, since \( K \) is nilpotent, suppose that \( \pi(K)=\{p_{1}, p_{2}, \ldots, p_{k}\} \).

© 2011, RJPA. All Rights Reserved
then \( w(p_1 p_2 \ldots p_k) = 2^i \), i.e.,

\[
(p_1^{i_1} - 1)(p_2^{i_2} - 1) \ldots (p_k^{i_k} - 1) = 2^i.
\]

(\(^*1\))

Denote by \( r_a \) the primitive prime divisor of \( q^i - 1 \) if \( r_a \mid q^i - 1 \), but \( r_a \) cannot divide \( q^i - 1 \) for every \( i < n \). By Zsigmondy theorem [7] there exists \( r_a \) always except the cases \( (n, q) = (6, 2) \) and \( (n, q) = (2, 2^i - 1) \) with nature number \( k \). If \( t \geq 3 \), then there primitive prime divisor of \( p^i - 1 \), and hence (\(^*1\)) has no solution. If \( t = 2 \), then \( p^2 - 1 \equiv 0 \), that is \( (p+1)(p-1) \equiv 0 \), and so \( p_0 = 3 \). If \( t = 1 \), then \( p_0 \) is a Fermat prime. Therefore Sylow subgroup of \( K \) is isomorphic to \( Z_{q^i} \) or \( Z_p \) with \( p \) a Fermat prime.

If \( 2 \mid |K| \), then \( K \) is elementary abelian 2-group and \( H \) is of square-free order. Hence \( H \) is cyclic or a metacyclic group with generated relations \( \langle a, b: a^n = b^m = 1, a^d = d \rangle \), where \( (r-1)n \equiv 1 \), \( r^n \equiv 1 \mod n \) and \( |H| = mn \) (see 10.1.10, [4]). If \( H \) is cyclic, then every prime divisor of \( |H| \) is a Mersenne prime. If \( H \) is meta-cyclic, obviously, \( (m, n) = 1 \) and \( \langle a \rangle \) is normal in \( H \). Since for every element \( x \) of \( \langle a \rangle \), \( \langle x \rangle \) is normal in \( H \), we have every element of order \( l \) of \( \langle a \rangle \) commutes with all elements of order \( l \) in \( \langle b \rangle \). In fact, otherwise there exists an element \( x_0 \in \langle a \rangle \) and \( y_0 \in \langle b \rangle \) such that \( \langle x_0 \rangle \not= \langle y_0 \rangle \) is a Frobenius group by Lemma 2, then \( K: \langle x_0 \rangle \not= \langle y_0 \rangle \) is a 2-Frobenius group. Now we regard as \( K \) a \( (x_0 \rangle \langle y_0 \rangle \)-module. By 8.3.5 of [3] we know that \( C_2(\langle y_0 \rangle) \not= 1 \), it implies that 2 is connected to an odd prime in the prime graph of \( G \), a contradiction. Since orders of \( a, b \) are both square-free, we have \( ab = ba \), hence \( H \) is abelian, a contradiction.

**Case 2:** \( G \) is a 2-Frobenius group. Suppose that \( G \) is \( ABC \), where \( A \) and \( AB \) are normal subgroups of \( G \), \( AB \) and \( BC \) are Frobenius group with kernel \( A \), \( B \) and complements \( B \), \( C \) respectively. Since \( B \) and \( C \) are both cyclic and \( B \) is of odd order, we have \( 2 \mid |AC| \). Hence \( AC \) is a 2-group since \( s(AC) = 2 \). By Lemma 3 we have \( exp(AC) \geq 4 \), a contradiction.

**Case 3:** There exists a non abelian simple group \( S \) such that \( S \leq H = G/N \leq Aut(S) \), where \( N \) is the maximal normal soluble subgroup of \( G \). Since \( N \) and \( H/S \) are \( \pi_4(G) \)-groups, \( N \) is a 2-group. In addition, since Sylow 2-subgroup of \( G \) is an elementary abelian group, we have \( G \cong N.S^* \), where \( S^* \leq Aut(S) \). Since the prime graph \( G/K(S) \) is disconnected and \( 2 \) is a component of \( G/K(S) \), by papers [2] and [5] it is easy to check that \( S \) is \( L_2(2^f) \), \( L_3(2^f) \) or \( Sz(2^{2m+1}) \). Since centralizers of field automorphisms of them have an element of order 2, we have \( S^* = S \). Furthermore, the exponents of Sylow 2-subgroups of \( L_3(2^f) \) and \( Sz(2^{2m+1}) \) are more than 2, so \( S^* = L_2(2^f) \).

Now suppose that \( T \) is a Frobenius subgroup of \( S \) of order \( 2(2^f+1) \). Then \( N \not= T \). By Lemma 3, the exponent of Sylow 2-subgroup of \( N \): \( T \) is more than 2, a contradiction. Therefore \( N = 1 \).

Since \( w(2^f) = \{2^f \mid 1\} = \phi(2^f - 1 \times 2^f) \times (2^f + 1) \), we have

\[
\pi(\phi(2^m - 1)) \subseteq \pi(2^m + 1) \cup \{2\},
\]

(\(^*2\))

and similarly we have

\[
\pi(\phi(2^m + 1)) \subseteq \pi(2^m - 1) \cup \{2\}.
\]

(\(^*3\))

Suppose that \( p \) is an odd prime divisor of \( f \). Let \( r_p \) and \( r_{2p} \) are primitive prime divisors of \( 2^p - 1 \) and \( 2^{2p} - 1 \), respectively. Then \( p \mid r_p - 1 \) and \( 2p \mid r_{2p} - 1 \). Also since \( r_p \mid \phi(2^i - 1) \) and \( r_{2p} \mid \phi(2^{2i} + 1) \), we have \( p \mid \phi(2^i - 1) \) and \( 2p \mid \phi(2^{2i} + 1) \). On the other hand, by (\(^*2\)), (\(^*3\)), \( \phi(2^f - 1) \), \( \phi(2^{2f} + 1) \) has only prime divisor 2 since \( 2^f - 1, 2^f + 1 \). Thus \( f \) is a power of 2, say, \( 2^n \). Denote by \( F_n \) the Fermat number \( 2^{2^n} + 1 \). If \( 1 \leq n \leq 4 \), it is easy to check that \( PSL_2(2^n) \) is satisfied the conditions of Theorem. If \( n = 5 \), then \( 17449 \mid \phi(2^6) \), but does not divide \( 2^{32} - 1 = 3 \times 5 \times 17 \times 257 \times 65537 \), a contradiction. If \( n \geq 6 \), then \( 2^{2^n-1} = F_1 F_2 \ldots F_{n-1} \). Thus \( F_3 \mid 2^{2^{256}} - 1 \). Since \( F_3 = 641 \times 6700417 \), we have \( 3 \mid \phi(F_3) \mid \phi(2^{17}) - 1 \), and hence \( 3 \mid 2^{256} + 1 \) by the (\(^*2\)), a contradiction.
REFERENCES:


1 Project supported by the NNSF of China (No.11026195) and the foundation of Educational Department of Hubei Province in China (No.Q20111901).

************