JOURNAL OF THE
CHUNGCHEONG MATHEMATICAL SOCIETY
Volume **27**, No. 3, August 2014
http://dx.doi.org/10.14403/jcms.2014.27.3.427

SIMPLICITY OF GROUPS OF EVEN ORDER

Minjung Choi* and Seungkook Park**

Abstract. In this paper, we show that groups of order $2^n pq$, where p, q are primes of the from $p = 2^n - 1$, $q = 2^{n-1} + p$ with $n \geq 3$, are not simple and groups of order $2^n pq^t$ for $t \geq 2$, where p, q are odd primes of the form $p = 2^m - 1$, $q = 2^n - 1$ with $m < n$, are not simple.

1. Introduction

A nontrivial group is called a simple group if it has no nontrivial proper normal subgroup. Simple groups have been studied for quite a long time. Every finite simple abelian group is isomorphic to a cyclic group of prime order. Feit and Thompson [2] showed that groups of odd order are solvable and hence nonabelian simple groups must be of even order, that is, nonabelian groups of odd order are not simple. In 1904, Burnside [1] proved that groups of order $p^a q^b$, where p, q are primes and a, b are nonnegative integers, are solvable. Thus nonabelian groups of order $p^a q^b$, where p, q are primes and a, b are nonnegative integers, are not simple. In 2009, Salunke and Gotmare [3] showed that if a group G has order $2m$, where m is an odd number, then G has a subgroup of index 2 and hence G is not simple. The simplicity of groups of order $2^n p^m q^l$, where p, q are primes and $n \geq 2$, $m \geq 1$, $l \geq 1$, are not known. In this paper, we show that groups of order $2^n pq$, where p, q are primes of the from $p = 2^n - 1$, $q = 2^{n-1} + p$ with $n \geq 3$, are not simple and groups of order $2^n pq^t$ for $t \geq 2$, where p, q are odd primes of the form $p = 2^m - 1$, $q = 2^n - 1$ with $m < n$, are not simple.

Received April 22, 2014; Accepted July 10, 2014.
2010 Mathematics Subject Classification: Primary 20D05; Secondary 20D20.
Key words and phrases: simple group, Mersenne prime.
Correspondence should be addressed to Seungkook Park, skpark@sookmyung.ac.kr.
This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (NRF-2012R1A1A1015699).

2. Main results

We give the definition of Mersenne prime and some examples.

Definition 2.1. A Mersenne prime is a prime number of the form $2^n - 1$.

Example 2.2. *The first four Mersenne primes are 3, 7, 31 and 127 when* $n = 2, 3, 5$ *and* 7.

Lemma 2.3. *Let n be an integer greater than or equal to 3. Let $p = 2^n - 1$ and $q = 2^{n-1} + p$. Then*

$$2^i p \not\equiv 1 \pmod{q} \text{ for } i = 1,\ 2,\ \ldots,\ n-1.$$

Proof. Let $x = 2^i p$ for some $1 \le i \le n-1$. We divide the ranges of i into two cases, odd and even.

Case 1. i is odd.
Let $X = x - 2^i q + 2^{i-1} q - 2^{i-2} q + \cdots - 2q + q$. Then

$$\begin{aligned} X &= 2^i(2^n - 1) - 2^i(2^n + 2^{n-1} - 1) \\ &\quad + 2^{i-1}(2^n + 2^{n-1} - 1) - \cdots - 2(2^n + 2^{n-1} - 1) + (2^n + 2^{n-1} - 1) \\ &= (2^{n+i} - 2^i) - (2^{n+i} + 2^{n+i-1} - 2^i) \\ &\quad + (2^{n+i-1} + 2^{n+i-2} - 2^{i-1}) - \cdots - (2^{n+1} + 2^n - 2) + (2^n + 2^{n-1} - 1) \\ &= 2^{n-1} - 2^{i-1} + \cdots + 2 - 1. \end{aligned}$$

Let $y = -2^{i-1} + \cdots + 2 - 1$. Then $X = 2^{n-1} + y$. Since i is odd, we have $y = (-2^{i-1} + 2^{i-2}) + \cdots + (-2^2 + 2) - 1 < 0$. Thus

$$X = 2^{n-1} + y \ < \ 2^{n-1} \ < \ 2^{n-1} + 2^n - 1 = q.$$

On the other hand,

$$X = 2^{n-1} + y > 2^i + y = 2^i - 2^{i-1} + 2^{i-2} - \cdots + 2 - 1 = 2^{i-1} + 2^{i-3} + \cdots + 1 \ge 1.$$

Thus $1 < X < q$. Since $x \equiv X \pmod{q}$, $x \equiv X \not\equiv 1 \pmod{q}$.

Case 2. i is even.
Let $Z = x - 2^i q + 2^{i-1} q - 2^{i-2} q + \cdots - 2^2 q + 2q$. Then

$$\begin{aligned} Z &= 2^i(2^n - 1) - 2^i(2^n + 2^{n-1} - 1) + 2^{i-1}(2^n + 2^{n-1} - 1) \\ &\quad - \cdots - 2^2(2^n + 2^{n-1} - 1) + 2(2^n + 2^{n-1} - 1) \\ &= (2^{n+i} - 2^i) - (2^{n+i} + 2^{n+i-1} - 2^i) + (2^{n+i-1} + 2^{n+i-2} - 2^{i-1}) \\ &\quad - \cdots - (2^{n+2} + 2^{n+1} - 2^2) + (2^{n+1} + 2^n - 2) \\ &= 2^n - 2^{i-1} + \cdots + 2^2 - 2 \end{aligned}$$

Let $w = -2^{i-1} + \cdots + 2^2 - 2$. Then $Z = 2^n + w$. Since i is even, $w = (-2^{i-1} + 2^{i-2}) + \cdots + (-2^3 + 2^2) - 2 < 0$. Thus

$$Z = 2^n + w < 2^n < 2^n + p = q.$$

On the other hand,

$$Z = 2^n + w > 2^i + w = 2^i - 2^{i-1} + \cdots + 2^2 - 2 = 2^{i-1} + 2^{i-3} + \cdots + 2 > 1.$$

Thus $1 < Z < q$. Since $x \equiv Z \pmod{q}$, $x \equiv Z \not\equiv 1 \pmod{q}$. □

Proposition 2.4. *Let n be an integer greater than or equal to 3. Let G be a group of order $2^n pq$ where p, q are primes of the form $p = 2^n - 1$ and $q = 2^{n-1} + p$. Then G is not simple.*

Proof. We will assume that G is simple and deduce a contradiction. Let n_q be the number of Sylow q-subgroups in G. Then by the Sylow's theorem, $n_q \mid 2^n p$ and $n_q \equiv 1 \pmod{q}$. Since $n_q \mid 2^n p$, the number n_q must be one of $1, 2, \ldots, 2^n, p, 2p, \ldots, 2^n p$. Since $n_q \equiv 1 \pmod{q}$ and $1 < p < q$, $n_q \neq p$. Also $n_q \neq 2^i$ for $i = 1, 2, \ldots, n$ because of the fact that $1 < 2^i < 2^n + 2^{n-1} - 1 = q$ for $i = 1, 2, \ldots, n$. By Lemma 2.3, $n_q \neq 2^i p$ for $i = 1, 2, \ldots, n-1$. Thus $n_q = 1$ or $2^n p$. If $n_q = 1$, that is, if there is only one Slyow q-subgroup, then it must be a normal subgroup of G which is a contradiction. Now we consider the case when $n_q = 2^n p$. There are $2^n p$ Sylow q-subgroups of order q. Note that distinct Sylow q-subgroups intersect in 1. Therefore the number of elements of order q is $2^n p(q-1)$. The number of elements of order not equal to q is $|G| - 2^n p(q-1) = 2^n p$. Next we consider the number of Sylow p-subgroups. Since $n_p \equiv 1 \pmod{p}$ and $n_p \neq 1$, $n_p \geq p + 1 = 2^n$. Thus the number of elements of order p is greater than or equal to $2^n(p-1)$. Hence the number of elements of order not equal to q and p is less than or equal to $|G| - 2^n p(q-1) - 2^n(p-1) = 2^n$ which implies that G has one Sylow 2-subgroup. Thus G contains a normal Sylow 2-subgroup of order 2^n which is a contradiction. Therefore G is not simple. □

Remark 2.5. A_5 is the smallest non-abelian simple group of order 60. Note that $60 = 2^2(2^2 - 1)(2 + 2^2 - 1)$ is of the form $2^n pq$ where p, q are primes of the form $p = 2^n - 1$ and $q = 2^{n-1} + p$ with $n = 2$.

We give some examples of Proposition 2.4.

Example 2.6. *Groups of order* $616 = 2^3(2^3 - 1)(2^2 + 2^3 - 1)$, $46624 = 2^5(2^5 - 1)(2^4 + 2^5 - 1)$ *or* $3104896 = 2^7(2^7 - 1)(2^6 + 2^7 - 1)$ *are not simple by Proposition 2.4.*

Proposition 2.7. *Let G be group of order $2^n pq^t$ where $t \geq 2$ and p, q are odd primes of the form $p = 2^m - 1$, $q = 2^n - 1$ with $2 \leq m < n$. Then G is not simple.*

Proof. Suppose that G is simple. Let n_q be the number of Sylow q-subgroups. Then $n_q | 2^n p$. Thus the number n_q must be one of $1, 2, 2^2, \ldots, 2^{n-1}, 2^n, p, 2p, \ldots, 2^n p$. Since G is simple, $n_q \neq 1$. Let $a = 2^i$ for some $1 \leq i \leq n-1$. Since $1 < a < q$ and $1 < p < q$, $a \not\equiv 1 \pmod q$ and $p \not\equiv 1 \pmod q$. Thus $n_q \neq a$ and $n_q \neq p$. Let $n_q = 2^i p$ for some $1 \leq i \leq n$. We divide the ranges of i into two parts, $1 \leq i \leq n-m$ and $n - m < i \leq n$.

Case 1. $1 \leq i \leq n - m$.
Since $n_q = 2^i p = 2^i(2^m - 1) \leq 2^{n-m}(2^m - 1) = 2^n - 2^{n-m} < 2^n - 1 = q$ and $n_q = 2^i(2^m - 1) \geq 2(2^m - 1) = 2p > 1$, $n_q = 2^i p \not\equiv 1 (\mathrm{mod}\, q)$.

Case 2. $n - m < i \leq n$.

$$\begin{aligned} n_q = 2^i p = 2^i(2^m - 1) &= 2^{m+i} - 2^i \\ &> 2^{m+i} - 2^{i+(m-1)} = 2^{m+i-1} \geq 2^n > 2^n - 1 = q. \end{aligned}$$

Let $k = i - (n - m)$ and let $A = n_q - 2^{k-1}q + 2^{k-2}q - \cdots - q$. Then

$$\begin{aligned} A &= n_q - 2^{k-1}q + 2^{k-2}q - \cdots - q \\ &= 2^i(2^m - 1) - 2^{k-1}(2^n - 1) + 2^{k-2}(2^n - 1) - \cdots - (2^n - 1) \\ &= (2^{i+m} - 2^i) - (2^{n+k-1} - 2^{k-1}) - (2^{n+k-2} - 2^{k-2}) - \cdots - (2^n - 1) \\ &= 2^{m+i} - 2^i - 2^n(2^{k-1} + 2^{k-2} + \cdots + 1) + (2^{k-1} + 2^{k-2} + \cdots + 1) \\ &= 2^{n+k} - 2^i - 2^n(2^k - 1) + (2^k - 1) \\ &= 2^n - 1 + 2^k - 2^i. \end{aligned}$$

If $k = 1$, then

$$A = 2^n - 1 + 2^k - 2^i = 2^n - 1 + 2 - 2^{n-m+1} = 2^{n-m}(2^m - 2) + 1 > 1.$$

If $1 < k \leq m$, that is, $n - m + 1 < i \leq n$, then

$$A = 2^n - 1 + 2^k - 2^i > 2^n - 1 + 2 - 2^i \geq 1.$$

On the other hand, since $2^k - 2^i < 0$, we have

$$A = 2^n - 1 + 2^k - 2^i < 2^n - 1 = q.$$

Thus $1 < A < q$. Since $n_q \equiv A \pmod q$, $n_q \equiv A \not\equiv 1 \pmod q$. Hence $n_q \neq 2^i p$. Therefore $n_q = 2^n$. Let N is a normalizer of Sylow q-subgroup. Then $|G : N| = 2^n$. Let G act on the 2^n left cosets of N by $g \cdot xN =$

$(gx)N$, where $g \in G$ and xN is a left coset of N. Then we get a permutation representation

$$\rho : G \to S_{2^n}.$$

Since $\ker \rho$ is a normal subgroup of G and G is simple, $\ker \rho = 1$. Thus G is isomorphic with a subgroup of S_{2^n}. Hence $|G| \mid |S_{2^n}|$, that is, $2^n(2^m-1)(2^n-1)^t \mid (2^n)!$. Then $(2^m-1)q^t \mid q!$ which is a contradiction. Therefore G is not simple. □

We give some examples of Proposition 2.7.

EXAMPLE 2.8. *Groups of order* $1176 = 2^3(2^2-1)(2^3-1)^2$, $6673184 = 2^5(2^3-1)(2^5-1)^3$ *or* $266027988992 = 2^{11}(2^5-1)(2^{11}-1)^2$ *are not simple by the Proposition 2.7.*

References

[1] W. Burnside, *On Groups of Order $p^\alpha q^\beta$*, Proc. London Math. Soc. **S2-1** (1904), no. 1, 388-392.

[2] W. Feit and J. G. Thompson, *Solvability of groups of odd order*, Pacific J. Math. **13** (1963), no. 3, 775-1029.

[3] J. N. Salunke and A. R. Gotmare, *Converse of Lagrange's theorem and solvable groups*, Bull. Marathwada Math. Soc. **10** (2009), no. 1, 36-42.

*

Department of Mathematics
Sookmyung Women's University
Seoul 140-742, Republic of Korea
E-mail: mjchoi@sookmyung.ac.kr

**

Department of Mathematics
Sookmyung Women's University
Seoul 140-742, Republic of Korea
E-mail: skpark@sookmyung.ac.kr