

Characterizations of a finite groups of order pq and p^2q

Kuwali Das

Bodoland University, Kokrajhar Assam.

Abstract

In this paper, we study some interesting behavior of a finite group with order pq where p and q are different primes. We find structure of the group of order pq if the pair of primes (p, q) are twin primes, cousin primes and sexy primes respectively. We also study the behavior of a group where order of the group is p^2q .

AMS subject classification: 20K01, 11A41.

Keywords: Abelian group, Cyclic group, Twin primes, Cousin primes, Sexy primes.

1. Introduction

A number $n > 1$ is prime if it has only two divisors 1 and itself. Twin prime was coined by Paul Stäckel (1862 – 1919). Twin prime is a pair of prime numbers that has a prime gap of two, in other words, if p and $p + 2$ are both prime numbers then p and $p + 2$ are twin primes. Two is not considered as twin prime with the number three, since it violates the aforementioned rule. The first few twin primes are:

(3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), (59, 61), (71, 73), (101, 103), ...

Cousin primes are primes that differ by four. For example,

(3, 7), (7, 11) (13, 17), (19, 23), (37, 41), ...

Sexy primes are pair of primes of the form $(p, p + 6)$. That are named as Sex which is the Latin word for Six. The first few Sexy primes are:

(5, 11), (7, 13), (11, 17), (13, 19), (17, 23), (23, 29), (31, 37),

(37, 43), (41, 47), (47, 53), ...

A group is cyclic if it is generated by a single element. Also a group is Abelian if it satisfies the commutative law. It is well-known that every cyclic group is abelian.

In this paper, we study the structure of a group of order pq or p^2q , where p and q are different primes. We can easily characterize the group by observing the nature of primes. Before going to main section, we mention the followings:

Theorem 1.1. [2, Theorem 6.5] Let p and q be two distinct prime numbers. To be definite let $p < q$. If G is a group of order pq , then one of the following holds.

- (I) G is cyclic (Abelian).
- (II) It has two generators a and b such that

$$a^p = e, b^q = e, a^{-1}ba = b^r,$$

for some r such that $r \not\equiv 1 \pmod{q}$, $r^p \equiv 1 \pmod{q}$ and p divides $q - 1$ (Non-Abelian).

Remark 1.2. The above theorem gives that for any two primes $p < q$. Following cases happen.

- (1) If p does not divide $q - 1$, then any group G of order pq is cyclic.
- (2) If p divides $q - 1$ then there are only two non-isomorphic groups of order pq one of which is commutative (which is again cyclic as p and q are different primes) other is non-commutative.

In [2, p 176], we have the following for a finite group of order p^2q ; that is

A group of order p^2q , p and q being distinct prime numbers, is not simple. Further if $q < p$ and q does not divide $p^2 - 1$ then every group of order p^2q is Abelian.

In our next two sections, we find the following interesting results

Theorem 1.3. Let G be a group and $o(G) = pq$ where (p, q) is a pair of twin primes. Then G is an Abelian group.

Theorem 1.4. Let G be a group and $o(G) = pq$ where (p, q) is a pair of cousin primes with $(p, q) \neq (3, 7)$. Then G is an Abelian group.

Theorem 1.5. Let G be a group and $o(G) = pq$ where (p, q) is a pair of sexy primes with $(p, q) \neq (5, 11)$. Then G is an Abelian group.

Theorem 1.6. Let G be a group and $o(G) = pq$ where (p, q) is a pair of primes where $q = p + 2k$, for some positive integer k and $2k - 1$ is not a multiple of p . Then G is an Abelian group.

Theorem 1.7. Let G be a group and $o(G) = p^2q$ where (q, p) is a pair of twin primes not equal to $(3, 5)$. Then G is an Abelian group.

Theorem 1.8. Let G be a group and $o(G) = p^2q$ where (q, p) is a pair of cousin primes with $(q, p) \neq (3, 7)$. Then G is an Abelian group.

Theorem 1.9. Let G be a group and $o(G) = p^2q$ where (q, p) is a pair of sexy primes with $(q, p) \neq (5, 11)$ or $(7, 13)$. Then G is an Abelian group.

Theorem 1.10. Let G be a group and $o(G) = p^2q$ where (q, p) is a pair of primes where $q = p + 2k$, for some positive integer k and $4k^2 - 1$ is not a multiple of q . Then G is an Abelian group.

2. Characterization of a finite group of order pq , $p < q$

Theorem 2.1. Let G be a group and $o(G) = pq$ where (p, q) is a pair of twin primes. Then G is an Abelian group.

Proof. Since (p, q) is a pair of twin primes, therefore by definition of twin prime $q = p + 2$. Now,

$$\gcd(p, q - 1) = \gcd(p, p + 1) = 1,$$

since any two consecutive integers are always relatively prime. Therefore, $q - 1$ is not divisible by p .

By Remark of Theorem 6.5, [2][Theorem, 6.5, p 169], we can conclude that G is cyclic and so Abelian. ■

Theorem 2.2. Let G be a group and $o(G) = pq$ where (p, q) is a pair of cousin primes with $(p, q) \neq (3, 7)$. Then G is an Abelian group.

Proof. $(p, q) \neq (3, 7)$ is a pair of cousin primes, therefore $q = p + 4$. If $\gcd(p, q - 1) = \gcd(p, p + 3) = d$. then $d|p$ and $d|p + 3$ gives $d|3$ so $d = 1$ or 3 .

Again, $d|p$ gives $d = 1$ or p . Now, if $d = 3$ then $p = d = 3$, but $p \neq 3$ therefore d must be 1.

Hence, $d = \gcd(p, q - 1) = 1$. Therefore, $q - 1$ is not divisible by p . By Remark 1.2 of Theorem 6.5, [2][Theorem, 6.5, p 169], we can conclude that G is cyclic and hence Abelian. ■

Remark 2.3. If $(p, q) = (3, 7)$ then by [2][Theorem, 6.5, p 169], we can conclude that G is isomorphic to Z_{21} or G is isomorphic to the group $\{a, b|a^3 = b^7 = e, a^{-1}ba = b^2\}$.

Theorem 2.4. Let G be a group and $o(G) = pq$ where (p, q) is a pair of sexy primes with $(p, q) \neq (5, 11)$. Then G is an Abelian group.

Proof. $(p, q) \neq (5, 11)$ is a pair of sexy primes, therefore $q = p + 6$. If $\gcd(p, q - 1) = \gcd(p, p + 5) = d$. then $d|p$ and $d|p + 5$ gives $d|5$ so $d = 1$ or 5 . Again, $d|p$ gives

$d = 1$ or p .

Now, if $d = 5$ then $p = d = 5$. but we are not considering here the case $p = 5$ so $d = \gcd(p, q - 1) = 1$. Therefore, $q - 1$ is not divisible by p . By Remark 1.2 of Theorem 6.5, [2][Theorem, 6.5, p 169], we can conclude that G is cyclic and so Abelian. ■

Remark 2.5. If $(p, q) = (5, 11)$ then by Remark 2.3 of Theorem 6.5, [2][Theorem, 6.5, p 169], we can conclude that G is isomorphic to Z_{55} or $\{a, b | a^5 = b^{11} = e, a^{-1}ba = b^3\}$. We can generalized the above result as follows

Theorem 2.6. Let G be a group and $o(G) = pq$ where (p, q) is a pair of primes where $q = p + 2k$, for some positive integer k and $2k - 1$ is not a multiple of p . Then G is an Abelian group.

Proof. (p, q) is a pair of primes with $q = p + 2k$, for some positive integer k . Then if $\gcd(p, q - 1) = \gcd(p, p + 2k - 1) = d$. then $d | p$ and $d | p + 2k - 1$ gives $d | 2k - 1$ so $d = 1$ or $2k - 1$. Again, $d | p$ gives $d = 1$ or p .

Now, if $d = 2k - 1$ then $p = d = 2k - 1$. but $2k - 1$ is not a multiple of p . $d = \gcd(p, q - 1) = 1$. Therefore, $q - 1$ is not divisible by p . By Remark 1.2 of Theorem 6.5, [2][Theorem, 6.5, p 169], we can conclude that G is cyclic and hence Abelian. ■

3. Characterization of a group of order p^2q , where $q < p$

Theorem 3.1. Let G be a group and $o(G) = p^2q$ where (q, p) is a pair of twin primes not equal to $(3, 5)$. Then G is an Abelian group.

Proof. Since (q, p) is a pair of twin primes, therefore by definition of twin primes $p = q + 2$. Since we have from [2][Problem 7, p 176], G is abelian if q does not divide $p^2 - 1$. In case twin primes, $p = q + 2$, so, $p^2 - 1 = q^2 + 4q + 3$. Now, $q | p^2 - 1$ if $q | 3$. Hence, if $q = 3$ then $q | p^2 - 1$.

Therefore, q does not divide $p^2 - 1$ if $(q, p) \neq (3, 5)$. Hence G is Abelian if $(q, p) \neq (3, 5)$ is a pair of twin primes. ■

Theorem 3.2. Let G be a group and $o(G) = p^2q$ where (q, p) is a pair of cousin primes with $(q, p) \neq (3, 7)$. Then G is an Abelian group.

Proof. $(p, q) \neq (3, 7)$ is a pair of cousin primes, therefore $q = p + 4$. As $p^2 - 1 = q^2 + 8q + 15$, so $q | p^2 - 1$ if $q | 15$. There are only two possibilities for q , $q = 3$ or 5 . But if $q = 5$ then $p = 9$, is not a prime. So, we can conclude that $q | p^2 - 1$ if $(q, p) = (3, 7)$. Hence q does not divide $p^2 - 1$ if $(q, p) \neq (3, 7)$. Therefore in this case G is Abelian. ■

Theorem 3.3. Let G be a group and $o(G) = p^2q$ where (q, p) is a pair of sexy primes with $(q, p) \neq (5, 11)$ or $(7, 13)$. Then G is an Abelian group.

Proof. Since $(q, p) \neq (5, 11)$ or $(7, 13)$ is a pair of sexy primes, therefore $p = q + 6$. Here, $p^2 - 1 = q^2 + 12q + 35$ so $q|p^2 - 1$ if $q|35$. Hence there are only two possibilities for q , $q = 5$ or 7 . So, we can conclude that $q|p^2 - 1$ if $(q, p) = (5, 11)$. or $(7, 13)$. Hence q does not divide $p^2 - 1$ if $(q, p) \neq (5, 11)$. or $(7, 13)$. Therefore in this case G is Abelian. ■

Now, we mention a generalization of the above results.

Theorem 3.4. Let G be a group and $o(G) = p^2q$ where (q, p) is a pair of primes where $p = q + 2k$, for some positive integer k and $4k^2 - 1$ is not a multiple of q . Then G is an Abelian group.

Proof. Here, $p^2 - 1 = q^2 + 8qk + 4k^2 - 1$. So, $p^2 - 1$ is not a multiple of q if $4k^2 - 1$ is not multiple of q . So, in this case, we can conclude that G is Abelian. ■

Some Example of the above result. In the above theorem if we put $k = 4$ then $p = q + 8$. Now, some example of pair of primes of this form are $(3, 11)$, $(5, 13)$, $(11, 19)$, $(23, 31)$, $(53, 61)$... Since, here, $4k^2 - 1 = 63$. So, in this case, the last theorem can be written as

Theorem 3.5. Let G be a group and $o(G) = p^2q$ where (q, p) is a pair of primes where $q = p + 8$, and $(q, p) \neq (3, 11)$ or $(5, 13)$. Then G is an Abelian group.

Similarly if $k = 5$ then the pair of primes are $(3, 13)$, $(7, 17)$, $(13, 23)$, $(19, 29)$, $(31, 41)$, $(37, 47)$, ... we can write the (3.4) as

Theorem 3.6. Let G be a group and $o(G) = p^2q$ where (q, p) is a pair of primes where $q = p + 10$, and $(q, p) \neq (3, 13)$. Then G is an Abelian group.

Acknowledgement

The author like to thank Professor Khanindra Chowdhury for his valuable suggestions.

References

- [1] Andersen, J.K. Gigantic Sexy and Cousin Primes. Post to primeform user forum. Nov., 3, 2005.
- [2] Surjeet Singh and Qazi Zameeruddin, *Moden Algebra* Seventh Revised Edition, Vikas Publishing House.
- [3] Hardy, G.H. and Wright, E.M., *An introduction to the theory of numbers*, 5th ed. Oxford, England, Clarendon Press 1979.
- [4] Tomás Oliveira e Silva (7 April 2008). Tables of values of $\pi(x)$ and of $\pi^2(x)$. Aveiro University. Retrieved 7 January 2011.
- [5] Weisstein, Eric W. Twin Primes. From MathWorld—A Wolfram We Resource. <http://mathworld.wolfarm.com/Twinprimes.html>.

