On Finite Simple Groups of Cube Order

Dedicated to Professor Toru Ishihara on his 65th birthday

By
Shin-ichi KATAYAMA

Department of Mathematical and Natural Sciences,
Faculty of Integrated Arts and Sciences,
The University of Tokushima,
1-1, Minamijosanjima-cho, Tokushima 770-8502, JAPAN
e-mail address : katayama@ias.tokushima-u.ac.jp

(Received September 28, 2007)

Abstract

In [17], M. Newman, D. Shanks and H. C. Williams have shown that the order of a symplectic group $S_p(2n, \mathbf{F}_q)$ is square if and only if $n = 2$ and $q = p$. Here p is a prime called a NSW prime. In this paper, we shall show that there is no symplectic group of cube order.

2000 Mathematics Subject Classification. Primary 11D41; Secondary 11E57

Introduction and Preliminaries

In their paper [17], M. Newman, D. Shanks and H. C. Williams have shown that a symplectic group $S_p(2n, \mathbf{F}_q)$ has a square order if and only if $n = 2$ and $q = p$, where p is a NSW prime. The main result given in [17] is the following.

Proposition 1. *The order of a symplectic group $S_p(2n, q)$ is square if and only if $(n, q) = (2, S_{2m+1})$, where S_{2m+1} is a NSW prime .*

Now we shall recall the definition of NSW numbers in P. Ribenboim's book [18]. We define a sequence $\{S_{2m+1}\}$ by putting

$$S_{2m+1} = \frac{(1+\sqrt{2})^{2m+1} + (1-\sqrt{2})^{2m+1}}{2}.$$

We call a prime NSW number S_{2m+1} to be a NSW prime. For example, $S_3 = 7, S_5 = 41$ and $S_7 = 239$ are the first three NSW primes. In [9], we have verified the conjecture announced in [17] is true. Namely, we have shown that the order of any finite simple group G is not square when $G \neq S_p(4, q)$. Thus it is a natural problem to ask the existence of finite simple groups of higher powers. In this paper, we shall consider the existence of finite simple group of cube order. For the sake of simplicity, we restrict ourselves to the special case $G = S_p(2n, q)$. We shall show the following main theorem.

Theorem. *There is no symplectic group $G = S_p(2n, q)$ of cube order.*

Firstly we shall prepare the preliminary lemmas which we will use in later.

Lemma 1 (Bertrand's postulate). *If n is an integer > 2, there exists an odd prime p such that*

$$n/2 < p \leq n.$$

Lemma 2 (Breusch [3]). *For $n \geq 7$, there exists a prime p of the form $6k + 1$ such that*

$$n/2 < p \leq n.$$

Lemma 3 (Shorey, Bugeaud and et al [1], [19]). *For any $n \geq 3$, the diophantine equation*

$$\frac{x^{2n} - 1}{x^2 - 1} = y^3$$

has no integer solution in integers $x > 1, y > 1$.

Lemma 4 (Ljunggren [11]). *If $n \equiv 1, 2, 4$ mod 6 and ≥ 4, then the diophantine equation*

$$\frac{x^n - 1}{x - 1} = y^3$$

has no integer solution in integers $|x| > 1, y > 1$.

We note that $\left\{\dfrac{x^n - 1}{x - 1}\right\}$ is the Lucas sequence associated to the pair $(x + 1, x)$ and satisfies the following elementary relation on the greatest common divisor.

Lemma 5 (Ribeiboim [18]).

$$\left(\frac{x^m - 1}{x - 1}, \frac{x^n - 1}{x - 1}\right) = \frac{x^{(m,n)} - 1}{x - 1}.$$

Lemma 6 (Delaunay [4], [5]). *The diophantine equation*

$$x^3 + dy^3 = 1 \quad (d > 1)$$

has at most one integer solution with $xy \neq 0$. Moreover the solution (x, y) corresponds to the binomial fundamental unit $x + y\sqrt[3]{d}$ in the ring $\mathbf{Z}[\sqrt[3]{d}]$.

1. Proof of the main result

We know the order of the symplectic group is

$$|S_p(2n,q)| = \frac{q^{n^2}}{d}\prod_{i=1}^{n}(q^{2i}-1),$$

where $d = (2, q-1)$. Hence we can write

$$|S_p(2n,q)| = \frac{q^{n^2}}{d}(q^2-1)^n\prod_{i=1}^{n}\left(\frac{q^{2i}-1}{q^2-1}\right).$$

We shall treat the case $3|n$ and $3 \not| \, n$ separately. In the following, we shall consider the easier case $3|n$.

Case 1) $3|n$.
We can write $n = 3m$. Then we have

$$|S_p(2n,q)| = |S_p(6m,q)| = (q^{3m}(q^2-1))^{3m}\frac{1}{d}\prod_{i=1}^{3m}\left(\frac{q^{2i}-1}{q^2-1}\right).$$

Then we see $|S_p(6m,q)|$ is cube if and only if $\frac{1}{d}\prod_{i=1}^{3m}\left(\frac{q^{2i}-1}{q^2-1}\right)$ is cube. From Lemma 1, we can take an odd prime p which satisfies $3m/2 < p \leq 3m$ for any positive integer m. Take the factor $\frac{q^{2p}-1}{q^2-1}$ of $|S_p(6m,q)|$. Then we see

$$\frac{1}{d}\prod_{i=1}^{3m}\left(\frac{q^{2i}-1}{q^2-1}\right) = \left(\frac{q^{2p}-1}{q^2-1}\right)\cdot\frac{1}{d}\prod_{i=1(\neq p)}^{3m}\left(\frac{q^{2i}-1}{q^2-1}\right).$$

Here we note that $\frac{q^{2p}-1}{q^2-1} = q^{2(p-1)} + \cdots + q^2 + 1$ is always odd. Hence we see $\left(\frac{q^{2p}-1}{q^2-1}, d\right) = 1.$

Moreover, from Lemma 5, we have

$$\left(\frac{q^{2p}-1}{q^2-1}, \frac{q^{2i}-1}{q^2-1}\right) = 1,$$

for any $1 \leq i\ (\neq p) \leq 3m$. Thus we see if $|S_p(6m,q)|$ is cube then $\frac{q^{2p}-1}{q^2-1}$ must be cube. From Lemma 3, we know there is no integer solution with $q, y > 1$ for $\frac{q^{2p}-1}{q^2-1} = y^3$. Hence we have shown that $|S_p(6m,q)|$ is never a cube for any positive integer m.

Case 2) $3 \not| n$.

In the next, we shall treat the case $3 \not| n$. In the case $n \geq 7$, we can take a prime p of the form $6k+1$ which satisfies $n/2 < p \leq n$ from Lemma 2. Take the factor $\frac{q^{2p}-1}{q^2-1}$ of $|S_p(2n,q)|$. Then we have

$$\begin{aligned}
\left(\frac{q^{2p}-1}{q^2-1}, \frac{q^{2i}-1}{q^2-1}\right) &= 1 \text{ for any } 1 \leq i\ (\neq p) \leq n,\\
\left(\frac{q^{2p}-1}{q^2-1}, d\right) &= 1,\\
\left(\frac{q^{2p}-1}{q^2-1}, q^2-1\right) &= 1 \text{ or } p.
\end{aligned}$$

Thus if $|S_p(2n,q)|$ is cube, then the factor $\frac{q^{2p}-1}{q^2-1}$ must satisfy $\frac{q^{2p}-1}{q^2-1} = y^3$ or py^3 or p^2y^3 for some positive integer y. We note here that

$$\frac{q^{2p}-1}{q^2-1} = \left(\frac{q^p-1}{q-1}\right)\left(\frac{q^p+1}{q+1}\right)$$

with $\left(\frac{q^p-1}{q-1}, \frac{q^p+1}{q+1}\right) = 1$. Thus we can conclude that the assumption $|S_p(2n,q)|$ is cube implies

$$\frac{q^p-1}{q-1} = y^3 \text{ or } \frac{q^p+1}{q+1} = \frac{(-q)^p-1}{(-q)-1} = y^3 \text{ for some positive integer } y,$$

which contradicts Lemma 4. Thus we have shown $|S_p(2n,q)|$ is never a cube for $n \geq 7$.

Finally, we shall verify $|S_p(2n,q)|$ is not cube for remaining cases $n = 1, 2, 4$ and 5.

In the case $n = 1$, we have

$$|S_p(2,q)| = q(q+1)\left(\frac{q-1}{d}\right) \quad \text{with } d = (2, q-1).$$

Here we see $(q, q+1) = 1$, $\left(q, \frac{q-1}{d}\right) = 1$, and $\left(\frac{q-1}{d}, q+1\right) = 1$ or 2. Therefore, if $|S_p(2,q)|$ is cube, then we must have $q = x^3$ for some integer $x > 1$. Also we must have $q + 1 = y^3$ or $2y^3$ or $4y^3$ for some integer $y > 1$.
If $q + 1 = y^3$, then it contradicts the classical fact $x^3 + y^3 \neq z^3$ for $xyz \neq 0$. If $q + 1 = 2y^3$, then from Lemma 6 the solution (x, y) corresponds to the fundamental unit $x + y\sqrt[3]{2}$ of $\mathbf{Z}[\sqrt[3]{2}]$. Since the fundamental unit ε of $\mathbf{Z}[\sqrt[3]{2}]$ with $0 < \varepsilon < 1$ is $\varepsilon = -1 + \sqrt[3]{2}$, we must have $x = y = 1$, which contradicts the condition $q = x^3 > 1$.
If $q + 1 = 4y^3$, then in the same way as above the solution (x, y) corresponds to the fundamental unit $x + y\sqrt[3]{4}$ of $\mathbf{Z}[\sqrt[3]{4}]$. Since the fundamental unit η of $\mathbf{Z}[\sqrt[3]{4}]$ with $0 < \eta < 1$ is $\eta = \varepsilon^2 = 1 + \sqrt[3]{4} - \sqrt[3]{16}$, we know there is no solution which satisfies $x^3 + 1 = 4y^3$. Thus we can conclude $|S_p(2,q)|$ is never a cube for any q.

In the case $n = 2$, we have

$$|S_p(4,q)| = q^4\left(\frac{q^2-1}{d}\right)^2 \cdot d \cdot (q^2+1) \quad \text{with } d = (2, q-1).$$

Here we see $\left(q, \frac{q^2-1}{d}\right) = 1$, $(q, q^2+1) = 1$, $(q, d) = 1$, $(q^2+1, d) = 1$ or 2, and $\left(q^2+1, \frac{q^2-1}{d}\right) = 1$ or 2. Therefore, if $|S_p(4,q)|$ is cube, then we must have $q = x^3$ for some integer $x > 1$. Also we must have $q^2 + 1 = y^3$ or $2y^3$ or $4y^3$ for some integer $y > 1$.
If $q^2 + 1 = (x^2)^3 + 1 = y^3$, then it contradicts the classical fact $x^3 + y^3 \neq z^3$ for $xyz \neq 0$. If $q^2 + 1 = (x^2)^3 + 1 = y^3$ or $q^2 + 1 = (x^2)^3 + 1 = 4y^3$, then in the same way as in the case $n = 1$, we can see there are no solutions when $x, y > 1$ from Lemma 6. Thus we can conclude $|S_p(4,q)|$ is never a cube for any q.

In the case $n = 4$, we have

$$|S_p(8,q)| = \frac{1}{d}q^{16}(q^2-1)^2(q^4-1)^2(q^4+q^2+1)(q^4+1) \quad \text{with } d = (2, q-1).$$

It is easy to see if $|S_p(8,q)|$ is cube, then $q = x^3$ with some integer $x > 1$. Moreover we see $(q^4+1, d) = 1$ or 2, $(q^4+1, q) = 1$, $(q^4+1, q^2-1) = 1$ or 2, $(q^4+1, q^4-1) = 1$ or 2, and $(q^4+1, q^4+q^2+1) = 1$. Therefore, if $|S_p(8,q)|$ is cube, then we must have $q^4 + 1 = (x^4)^3 + 1 = y^3$ or $2y^3$ or $4y^3$ for some integer

$y > 1$. In the same way as in the case $n = 1$, we can see there are no solutions for $x, y > 1$ from Lemma 6. Thus we can conclude $|S_p(8,q)|$ is never a cube for any q.

Finally we shall consider the case $n = 5$. Then we have

$$|S_p(10,q)| = \frac{1}{d}q^{25}(q^2-1)^3(q^4-1)^2(q^4+q^2+1)(q^4+1)\left(\frac{q^{10}-1}{q^2-1}\right),$$

with $d = (2, q-1)$. It is easy to see if $|S_p(10,q)|$ is cube, then $q = x^3$ with some integer $x > 1$. Moreover we see $(q^4+1, d) = 1$ or 2, $(q^4+1, q) = 1$, $(q^4+1, q^4-1) = 1$ or 2, $(q^4+1, q^4+q^2+1) = 1$ or 2, and $\left(q^4+1, \frac{q^{10}-1}{q^2-1}\right) = 1$. Therefore, if $|S_p(10,q)|$ is cube, then we must have $q^4+1 = (x^4)^3+1 = y^3$ or $2y^3$ or $4y^3$ for some integer $y > 1$. In the same way as in the above cases, we can see there are no solutions for $x, y > 1$ from Lemma 6. Thus we can conclude $|S_p(10,q)|$ is never a cube for any q, which completes the proof of our main theorem.

References

[1] Y. Bugeaud, M. Mignotte, Y. Roy and T. N. Shorey, *The equation* $\frac{x^n-1}{x-1} = y^q$ *has no solution with* x *square*, Math. Proc. Cambridge Philos. Soc., **127** (1999), 353–372.

[2] Y. Bugeaud and M. Mignotte, *l'équation de Nagell-Ljunggren* $\frac{x^n-1}{x-1} = y^q$, Enseign. Math., **48** (2002), 147–168.

[3] R. Breusch, *Zur Verallgemeinerung der Bertrandschen Postulates dass zwischen* x *und* $2x$ *stets Primzahlen liegen.* Math. Z., **34** (1932), 505–526.

[4] B. Delaunay, *Vollständige Lösung der unbestimmten Gleichung* $X^3q + Y^3 = 1$ *in ganèn Zahlen*, Math. Z., **28** (1928), 1–9.

[5] B. Delaunay, *Über die Darstellung der Zahlen durch die binäre kubische Formen mit negativer Discriminante*, Math. Z., **31** (1930), 1–26.

[6] P. Erdős, *Über die Primzahlen gewisser arithmetischen Reihen*, Math. Z., **39** (1935), 473–491.

[7] D. Gorenstein, Finite Groups, 2nd ed., Chelsea, New York, 1980.

[8] D. Gorenstein, Finite Simple Groups; An Introduction to Their Introduction, Plenum Press, New York, 1982.

[9] S. Katayama, *On finite simple groups of square order*, preprint.

[10] W. Ljunggren, *Zur Theorie der Gleichung* $x^2 + 1 = Dy^4$, Avh. Norske Vid Akad. Oslo, No. 5, **1** (1942).

[11] W. Ljunggren, *Noen setninger om ubestemte likninger av formen* $\frac{x^n - 1}{x - 1} = y^q$, Norsk Mat. Tidsskrift, **25** (1943), 17–20 (in Norwegian).

[12] W. Ljunggren, *On an improvement of a theorem of T. Nagell concerning the diophantine equation* $AX^3 + BY^3 = C$, Math. Scan., **1** (1953), 297–309.

[13] D. S. Mitrinović, J. Sándor and B. Crstici, Handbook of Number Theory, Kluwer Acad. Publishers, Dordrecht, 1996.

[14] L. J. Mordell, Diophantine Equations, Academic Press, London, 1969

[15] T. Nagell, *Note sur l'équation indéterminée* $\frac{x^n - 1}{x - 1} = y^q$, Norsk Mat.Tidsskr, **2** (1920), 75–78.

[16] T. Nagell, *Sur L'impossibilité de l'equation indetérminée* $x^p + 1 = y^2$, Norsk Mat. Forenings Skrifter, **1** (1921), Nr. 3.

[17] M. Newman, D. Shanks and H. C. Williams, *Simple groups of square order and an interesting sequence of primes*, Acta Arithmetica, **38** (1980), 210–217.

[18] P. Ribenboim, The Book of Prime Number Records, 3rd ed., Springer-Verlag, New York, 1996.

[19] N. Saradha and T. N. Shorey, *The equation* $\frac{x^n - 1}{x - 1} = y^q$ *with* x *square*, Math. Proc. Cambridge Philos. Soc., **125** (1999), 1-19.

[20] M. Suzuki, Finite Simple Groups, Kinokuniya-shoten, Tokyo, 1987 (in Japanese).