Bulletin of the Iranian Mathematical Society (2020) 46:1669–1674
https://doi.org/10.1007/s41980-019-00350-z

ORIGINAL PAPER

On the Number of Simple K_4 Groups

Shaohua Zhang[1] · Wujie Shi[2,3]

Received: 30 July 2019 / Accepted: 30 December 2019 / Published online: 25 January 2020

Abstract
In this paper, by solving Diophantine equations involving simple K_4-groups, we will try to point out that it is not easy to prove the infinitude of simple K_4-groups. This problem goes far beyond what is known about Dickson's conjecture at present.

Keywords Exponential Diophantine equation · Simple K_4-group · Dickson's conjecture · Zsigmondy's theorem

Mathematics Subject Classification 11D61 · 11D45 · 20D05

1 Introduction

A finite simple group is called a K_n-group if its order is divisible by exactly n different primes. By a classical $p^a q^b$ theorem of Burnside, every group of order $p^a q^b$ is solvable, where p and q are primes, and a and b are positive integers; hence, there is no simple K_2-group. On the other hand, there are only eight different simple K_3-groups [1]. In this paper, we concentrate on describing simple K_4-groups.

Communicated by Mohammad Reza Darafsheh.

This work was supported partially by the NSFC (No. 11671063) and Scientific Research Innovation Team Project Affiliated to Yangtze Normal University (No. 2016XJTD01).

✉ Wujie Shi
shiwujie@outlook.com

Shaohua Zhang
zhangshaohua@yznu.edu.cn

[1] School of mathematics and statistics, Yangtze Normal University, Chongqing 408102, People's Republic of China

[2] Department of Mathematics, Chongqing University of Arts and Sciences, Chongqing 402160, People's Republic of China

[3] School of Mathematics, Suzhou University, Suzhou 215006, People's Republic of China

In the famous book *Unsolved Problems in Group Theory*, the following problem is asked: is the number of simple K_4-groups finite or infinite? See [2]: Problem 13.65. This problem is the first to be posed by the second author Shi [3]. Denote by $\mathbb{N}$ and $\mathbb{P}$ the set of positive integers and the set of prime numbers, respectively. In [3], the second author claimed that the simple K_4-group problem can be reduced to the four Diophantine problems:

$$p^2 - 1 = 2^a 3^b q^c,\ p, q \in \mathbb{P},\ p > 3,\ q > 3,\ a, b, c \in \mathbb{N}, \tag{1.1}$$
$$2^m - 1 = p,\ 2^m + 1 = 3q^n,\ p, q \in \mathbb{P},\ p > 3,\ q > 3,\ m, n \in \mathbb{N}, \tag{1.2}$$
$$3^m - 1 = 2p^n,\ 3^m + 1 = 4q,\ p, q \in \mathbb{P},\ p > 3,\ q > 3,\ m, n \in \mathbb{N}, \tag{1.3}$$
$$3^m - 1 = 2p,\ 3^m + 1 = 4q^n,\ p, q \in \mathbb{P},\ p > 3,\ q > 3,\ m, n \in \mathbb{N}. \tag{1.4}$$

In 2001, Bugeaud et al. [4] showed that if $n > 1$, (1.2) and (1.4) have no solution and (1.3) has only the solution $(p, q, m, n) = (11, 61, 5, 2)$.

In Sect. 2, we will prove that if $c > 1$, (1.1) has only the solutions $(p, q, a, b, c) = (97, 7, 6, 1, 2)$ and $(p, q, a, b, c) = (577, 17, 7, 2, 2)$. Our methods are slightly different from those in [4].

Thus, the infinitude of simple K_4-groups can be decided by the following three Diophantine problems:

$$p^2 - 1 = 2^a 3^b q,\ p, q \in \mathbb{P},\ p > 3,\ q > 3,\ a, b \in \mathbb{N}, \tag{1.5}$$
$$2^m - 1 = p,\ 2^m + 1 = 3q,\ p, q \in \mathbb{P},\ p > 3,\ q > 3,\ m \in \mathbb{N}, \tag{1.6}$$
$$3^m - 1 = 2p,\ 3^m + 1 = 4q,\ p, q \in \mathbb{P},\ p > 3,\ q > 3,\ m \in \mathbb{N}. \tag{1.7}$$

By considering Diophantine equations (1.5), (1.6) and (1.7), one will see that it is very difficult to determine the infinitude of simple K_4-groups, and this problem goes far beyond what is known about the following Dickson's conjecture [5] at present. In fact, if the Diophantine equation (1.6) has infinitely many solutions for $p, q \in \mathbb{P}$, $p > 3, q > 3$, $m \in \mathbb{N}$, then $f_1(x) = x$ and $f_2(x) = 3x - 2$ represent simultaneously primes for infinitely many integers x. This is the special case of Dickson's conjecture. Unfortunately, this case is open. The Diophantine equations (1.5) and (1.7) can be similarly discussed. For the details, see Sect. 3.

Dickson Conjecture: Let $1 \leq s \in \mathbb{N}$, $f_i(x) = a_i + b_i x$ with a_i and b_i integers, $b_i \geq 1$ (for $i = 1, \ldots, s$). If there does not exist any integer $n > 1$ dividing all the products $\prod_{i=1}^{i=s} f_i(k)$, for every integer k, then there exist infinitely many natural numbers m such that all numbers $f_1(m), \ldots, f_s(m)$ are primes.

The case $s = 1$ is Dirichlet's theorem. Two special cases are well-known conjectures: there are infinitely many twin primes ($f_1(x) = x$ and $f_2(x) = x + 2$ represent simultaneously primes for infinitely many integers x), and there are infinitely many Sophie Germain primes ($f_1(x) = x$ and $f_2(x) = 2x + 1$ represent simultaneously primes for infinitely many integers x). As we know, even these two simple cases, nobody has proved up until now, let alone other special cases.

2 Main Theorem and Its Proof

Theorem 2.1 *If $1 < c \in \mathbb{N}$, $p, q \in \mathbb{P}$, $p > 3$, $q > 3$, and $a, b \in \mathbb{N}$, then the Diophantine equation $p^2 - 1 = 2^a 3^b q^c$ has only the solutions $(p, q, a, b, c) = (97, 7, 6, 1, 2)$ and $(p, q, a, b, c) = (577, 17, 7, 2, 2)$.*

Lemma 2.2 (Zsigmondy's theorem [6]) *If $a > b > 0$, $\gcd(a, b) = 1$ and $n > 1$ are positive integers, then $a^n + b^n$ has a prime factor that does not divide $a^k + b^k$ for all positive integers $k < n$, with the exception $2^3 + 1^3$; $a^n - b^n$ has a prime factor that does not divide $a^k - b^k$ for all positive integers $k < n$ unless $a = 2$, $b = 1$ and $n = 6$; or $a + b$ is a power of 2 and $n = 2$.*

Lemma 2.3 [7] *The Diophantine equation $3^m - 2y^q = 1$ has only the solution $(y, m, q) = (11, 5, 2)$ satisfying $2 < m \in \mathbb{N}$, $2 \le y, q \in \mathbb{N}$.*

Lemma 2.4 [8] *The Diophantine equation $x^m - y^n = 1$ has only the solution $(x, y, m, n) = (3, 2, 2, 3)$ satisfying $1 < m, n \in \mathbb{N}$, $x, y \in \mathbb{P}$.*

Lemma 2.5 [9] *The Diophantine equation $x^2 + 1 = 2y^n$ has only the solution $(x, y, n) = (239, 13, 4)$ satisfying $x, y, n \in \mathbb{N}$, $y > 1, n > 2$.*

Lemma 2.6 [10] *The Diophantine equation $3x^2 + 1 = 4y^n$ with $1 < n \equiv 1(\mod 2)$ and $x, y, n \in \mathbb{N}$ has only the solution $x = y = 1$.*

Lemma 2.7 [4] *The Diophantine equation $2^m + 1 = 3y^q$ with $1 < m, 1 < y, 1 < q \in \mathbb{N}$ has no solution.*

Proof of theorem 2.1 If $1 < c \in \mathbb{N}$, Diophantine equation $p^2 - 1 = 2^a 3^b q^c$ has solutions (p, q, a, b, c) such that $p, q \in \mathbb{P}$, $p > 3$, $q > 3$, $a, b \in \mathbb{N}$, then $a \ge 3$ and $p^2 \equiv 1 (\mathrm{mod}\ 2^a)$. Notice that if $a \ge 3$, $x^2 \equiv 1 (\mathrm{mod}\ 2^a)$ has only four solutions, say $x \equiv \pm 1, \pm 1 + 2^{a-1} (\mathrm{mod}\ 2^a)$. Therefore, we must have $p = \pm 1 + 2^{a-1} + k2^a$ with $k \in \mathbb{N} \cup \{0\}$. If $p = 1 + 2^{a-1} + k2^a$, then we have $(2k+1)(1+2^{a-2}+k2^{a-1}) = 3^b q^c$ by $p^2 - 1 = 2^a 3^b q^c$. But $\gcd(2k+1, 1+2^{a-2}+k2^{a-1}) = 1 = \gcd(3^b, q^c)$. Therefore, $2k+1 = 3^b$ or $2k+1 = q^c$. When $p = -1 + 2^{a-1} + k2^a$, we still have $2k + 1 = 3^b$ or $2k + 1 = q^c$. Thus, when $k \in \mathbb{N}$, $p^2 - 1 = 2^a 3^b q^c$ can be reduced to the following Diophantine problems with $3 \le a$, $1 \le b$, $1 < c \in \mathbb{N}$, $p, q \in \mathbb{P}$, $p > 3, q > 3$:

$$2k + 1 = 3^b, q^c = 1 + 2^{a-2} + k2^{a-1}, p = 1 + 2^{a-1} + k2^a, \tag{2.1}$$

$$2k + 1 = q^c, 3^b = 1 + 2^{a-2} + k2^{a-1}, p = 1 + 2^{a-1} + k2^a, \tag{2.2}$$

$$2k + 1 = 3^b, q^c = -1 + 2^{a-2} + k2^{a-1}, p = -1 + 2^{a-1} + k2^a, \tag{2.3}$$

$$2k + 1 = q^c, 3^b = -1 + 2^{a-2} + k2^{a-1}, p = -1 + 2^{a-1} + k2^a. \tag{2.4}$$

□

Rewriting these equations, we get (with $3 \le a$, $1 \le b$, $1 < c \in \mathbb{N}$, $p, q \in \mathbb{P}$, $p > 3$, $q > 3$):

$$q^c - 1 = 2^{a-2} 3^b, p = -1 + 2q^c, \tag{2.5}$$

$$3^b - 1 = 2^{a-2}q^c,\ p = -1 + 2 \times 3^b, \tag{2.6}$$
$$q^c + 1 = 2^{a-2}3^b,\ p = 1 + 2q^c, \tag{2.7}$$
$$3^b + 1 = 2^{a-2}q^c,\ p = 1 + 2 \times 3^b. \tag{2.8}$$

Next, we will prove that if $1 < c$, then (2.6), (2.7), (2.8) have no solution and (2.5) has only two solutions satisfying the conditions.

Clearly, if (2.7) has solutions, then $c \neq 2$. By Lemma 2.2, $q^c + 1$ has at least one prime factor m that does not divide $q^r + 1$ for all positive integers $r < c$. However, $m \neq 2, 3$. This leads to a contradiction since $q^c + 1 = 2^{a-2}3^b$.

Now, let us consider (2.8). Assume that $3^b + 1 = 2^{a-2}q^c$ has solutions. If b is even, then $a = 3$. By Lemma 2.5, it is impossible. Hence, b is odd. We deduce that $a = 4$ and get that $3^b + 1 = 4q^c$. If c is even, then $3^b + 1 = 4q^c$ has no solution with $c > 1$ [11]. If c is odd, then $3^b + 1 = 4q^c$ has no solution by Lemma 2.6 (since $c > 1$). So, (2.8) has no solution.

Suppose that (2.6) $3^b - 1 = 2^{a-2}q^c$ has solutions. If b is odd, then $a = 3$ and $3^b - 1 = 2q^c$ has no solution such that $p = -1 + 2 \times 3^b$ by Lemma 2.3. Let b be even. Write $b = 2r$. We obtain that $a \geq 5$ and $\frac{3^r-1}{2}\frac{3^r+1}{2} = 2^{a-4}q^c$. By Lemma 2.4, one can prove that $\frac{3^r-1}{2}\frac{3^r+1}{2} = 2^{a-4}q^c$ has no solution. Thus, (2.6) has no solution.

If $q^c - 1 = 2^{a-2}3^b$ has solutions with $c > 1$, then $c = 2$ by Lemma 2.2. By Lemma 2.4, one can obtain that (2.5) has only solutions $(q, a, b) = (7, 6, 1)$ and $(q, a, b) = (17, 7, 1)$. It leads that Diophantine equation $p^2 - 1 = 2^a 3^b q^c$ has only solutions $(p, q, a, b, c) = (97, 7, 6, 1, 2)$ and $(p, q, a, b, c) = (577, 17, 7, 2, 2)$ satisfying $p, q \in \mathbb{P}$, $p > 3$, $q > 3$, $a, b, c \in \mathbb{N}$ and $c > 1$.

Finally, we consider the case $k = 0$. Obviously, $p^2 - 1 = 2^a 3^b q^c$ can be reduced to the following Diophantine problems with $3 \leq a$, $1 \leq b$, $1 < c \in \mathbb{N}$, $p, q \in \mathbb{P}$, $p > 3$, $q > 3$:

$$3^b q^c = 1 + 2^{a-2},\ p = 1 + 2^{a-1}, \tag{2.9}$$
$$3^b q^c = -1 + 2^{a-2},\ p = -1 + 2^{a-1}. \tag{2.10}$$

By Lemma 2.4, if (2.9) or (2.10) has solutions, then b must be 1. Furthermore, using Lemma 2.7, one can show that (2.9) and (2.10) have no solution satisfying the conditions. This proves Theorem 2.1.

3 Our Conclusion

In this section, we will try to point out that it is not easy to prove the infinitude of simple K_4-groups. By (1.5), (1.6), (1.7), one will see that the infinitude of simple K_4-groups can be equivalently decided by the following Diophantine problems:

$$2^m - 1 = p,\ 2^m + 1 = 3q,\ p, q \in \mathbb{P},\ p > 3, q > 3, m \in \mathbb{N}, \tag{3.1}$$
$$3^m - 1 = 2p,\ 3^m + 1 = 4q,\ p, q \in \mathbb{P},\ p > 3, q > 3, m \in \mathbb{N}, \tag{3.2}$$
$$q - 1 = 2^{a-2}3^b,\ p = -1 + 2q,\ p, q \in \mathbb{P}, a \geq 3, a, b \in \mathbb{N}, \tag{3.3}$$

$$3^b - 1 = 2^{a-2}q,\ p = -1 + 2 \times 3^b,\ p, q \in \mathbb{P}, a \geq 3, a, b \in \mathbb{N}, \tag{3.4}$$

$$q + 1 = 2^{a-2}3^b,\ p = 1 + 2q,\ p, q \in \mathbb{P}, a \geq 3, a, b \in \mathbb{N}, \tag{3.5}$$

$$3^b + 1 = 2^{a-2}q,\ p = 1 + 2 \times 3^b,\ p, q \in \mathbb{P}, a \geq 3, a, b \in \mathbb{N}, \tag{3.6}$$

$$3q = 1 + 2^{a-2},\ p = 1 + 2^{a-1},\ p, q \in \mathbb{P}, a \geq 3, a \in \mathbb{N}, \tag{3.7}$$

$$3q = -1 + 2^{a-2},\ p = -1 + 2^{a-1}.p, q \in \mathbb{P}, a \geq 3, a \in \mathbb{N}. \tag{3.8}$$

Hence, if the number of simple K_4-groups is infinite, then one of the following holds:

$$\begin{aligned} f_1(x) &= x \text{ and} \\ f_2(x) &= 3x - 2 \text{ represent simultaneously primes for infinitely} \\ &\quad \text{many integers x by (3.1)}, \end{aligned} \tag{3.9}$$

$$\begin{aligned} f_1(x) &= x \text{ and} \\ f_2(x) &= 2x - 1 \text{ represent simultaneously primes for infinitely} \\ &\quad \text{many integers x by (3.2) or (20)}, \end{aligned} \tag{3.10}$$

$$\begin{aligned} f_1(x) &= x \text{ and} \\ f_2(x) &= 2x + 1 \text{ represent simultaneously primes for infinitely} \\ &\quad \text{many integers x by (3.5)}, \end{aligned} \tag{3.11}$$

$$\begin{aligned} f_1(x) &= x \text{ and} \\ f_2(x) &= 4x + 1 \text{ represent simultaneously primes for infinitely many integers x} \\ &\quad \text{by (3.4)(Note that by (3.4) one can deduce that a must be 3.)}, \end{aligned} \tag{3.12}$$

$$\begin{aligned} f_1(x) &= x \text{ and} \\ f_2(x) &= 2^{a-1}x - 1 \text{ represent simultaneously primes for infinitely many integers x} \\ &\quad \text{by (3.6), where } a = 3 \text{ or } a = 4, \end{aligned} \tag{3.13}$$

$$\begin{aligned} f_1(x) &= x \text{ and} \\ f_2(x) &= 6x - 1 \text{ represent simultaneously primes for infinitely} \\ &\quad \text{many integers x by (3.7)}, \end{aligned} \tag{3.14}$$

$$\begin{aligned} f_1(x) &= x \text{ and} \\ f_2(x) &= 6x + 1 \text{ represent simultaneously primes for infinitely} \\ &\quad \text{many integers x by (3.8)}. \end{aligned} \tag{3.15}$$

Clearly, (3.9), (3.10), (3.11), (3.12), (3.13), (3.14) and (3.15) are all special cases of Dickson's conjecture. This goes far beyond what is known about Dickson's conjecture at present. Anyway, due to that fact it is closely tied with many topics in number theory such as Fermat's primes, Mersenne primes, Dickson's conjecture and so on, we think that determining the number of simple K_4-groups is significative. It should be given much attention.

Acknowledgements We are very thankful to the referees for their valuable comments improving the presentation of the paper.

References

1. Herzog, M.: On finite simple groups of order divisible by three primes only. J. Algebra **10**, 383–388 (1968)
2. Mazurov, V.D., Khukhro, E.I.: Unsolved Problems in Group Theory, 13th edn, pp. 130–148. The Kourovka Notebook, Novosibirsk (1995)
3. Shi, W.: On simple K_4-groups. Chin. Sci. Bull. **36**(17), 1281–1283 (1991)
4. Bugeaud, Y., Cao, Z., Mignotte, M.: On simple K4-groups. J. Algebra **241**(2), 658–668 (2001)
5. Dickson, L.E.: A new extension of Dirichlet's theorem on prime numbers. Messenger Math. **33**, 155–161 (1904)
6. Zsigmondy, K.: Zur Theorie der Potenzreste. J. Monatshefte fur Mathematik **3**(1), 265–284 (1892)
7. Bugeaud, Y., Mignotte, M., Roy, Y.: On the Diophantine equation $\frac{x^n-1}{x-1} = y^q$. Pac. J. Math. **193**, 257–268 (2000)
8. Cassels, J.W.S.: On the equation $a^x - b^y = 1$. Am. J. Math. **75**, 159–162 (1953)
9. Ljunggren, W.: Zur Theorie der Gleichung $x^2 + 1 = Dy^4$. Avh. Norske. Vid. Akad. Oslo **1**(5), 1–27 (1942)
10. Cao, Z., Dong, X.: The Diophantine equation $Ax^2 + B = y^n$. Chin. Sci. Bull. **43**(13), 1141–1142 (1998)
11. Cao, Z.: On the Diophantine equation $\frac{ax^m-1}{abx-1} = by^2$. Chin. Sci. Bull. **36**(4), 275–278 (1991)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.