ON SIMPLE K_4-GROUPS

Yann Bugeaud, Zhenfu Cao and Maurice Mignotte

§1. Introduction

Let $\mathbb{G}$ be a finite simple group and put $\pi(\mathbb{G}) = \{p \mid p \text{ is a prime and } p \mid |\mathbb{G}|\}$. We call $\mathbb{G}$ a simple K_n-group if $|\pi(\mathbb{G})| = n$. In [10], M. Herzog proved that if $\mathbb{G}$ is a simple K_3-group, then $\mathbb{G}$ is isomorphic to one of the following simple groups: $A_5, A_6, L_2(7), L_2(8), L_2(17), L_3(3), U_3(3)$ and $U_4(2)$ (see [9]). In [18], W. Shi discussed the case of the simple K_4-groups and posed the following problem: Is the number of simple K_4-groups finite or infinite? (also see [16], Problem 13.65). In [5], one of the authors gave a characterization of simple K_n-groups ($3 \leq n \leq 5$). For the simple K_4-groups, we have the following result. Here and in the sequel, we denote by $\mathbb{N}$ and $\mathbb{P}$ the sets of positive integers and the set of prime numbers, respectively.

Theorem 1. *If $\mathbb{G}$ is a simple K_4-group, then $\mathbb{G}$ is isomorphic to one of the following simple groups:*

$$\begin{aligned}
&A_7, A_8, A_9, A_{10}, M_{11}, M_{12}, J_2,\\
&L_3(2^2), L_3(2^3), L_3(5), L_3(7), L_3(17), L_4(3), O_5(2^2), O_5(3^2),\\
&O_5(5), O_5(7), O_7(2), O_8^+(2), G_2(3), U_3(2^2), U_3(2^3), U_3(3^2),\\
&U_3(5), U_3(7), U_4(3), U_5(2), S_z(2^3), S_z(2^5), {}^3D_4(2), {}^2F_4(2)', L_2(q),
\end{aligned}$$

where q is a prime power satisfying

$$q(q^2-1) = 2^{\alpha_1}3^{\alpha_2}p^{\alpha_3}r^{\alpha_4},\ \ \alpha_i \in \mathbb{N}\,(i = 1, \dots, 4), \tag{1}$$

with $p > 3$ and $r > 3$ distinct prime numbers.

From Theorem 1, we know that the simple K_4-group problem is equivalent to: Is the number of prime powers q satisfying (1) finite or infinite? In the present paper, we prove the following result.

Theorem 2. *All the solutions of (1) with $3 < p < r$ and p and r prime are listed below.*

(A) When $q = 2^{\alpha_1}$, all the solutions of equation (1) are
$\alpha_2 = \alpha_3 = \alpha_4 = 1, p = (2^{\alpha_1}+1)/3, r = 2^{\alpha_1} - 1, \alpha_1 > 3$;

1991 *Mathematics Subject Classification.* 11D61, 20D05, 20D06.

Key words and phrases. Exponential Diophantine equation, simple K_4-group, linear form in two p-adic logarithms.

The second author was supported by the Heilongjiang Provincial Natural Science Foundation.

$\alpha_1 = 4, \alpha_2 = \alpha_3 = \alpha_4 = 1, p = 5, r = 17.$

(B) When $q = 3^{\alpha_2}$, *all the solutions of equation (1) are*

$\alpha_1 = \alpha_2 = 4, \alpha_3 = \alpha_4 = 1, p = 5, r = 41;$

$\alpha_1 = 2, \alpha_2 = 5, \alpha_3 = 2, \alpha_4 = 1, p = 11, r = 61;$

$\alpha_1 = 2, \alpha_3 = \alpha_4 = 1, p = (3^{\alpha_2} + 1)/4, r = (3^{\alpha_2} - 1)/2, \alpha_2 > 2.$

(C) When $q = p^{\alpha_3}$, *the only solution of equation (1) is*

$\alpha_1 = 3, \alpha_2 = 1, \alpha_3 = 2, \alpha_4 = 1, p = 5, r = 13.$

(D) When $q = r^{\alpha_3}$, *all the solutions of equation (1) are*

$\alpha_1 = 5, \alpha_2 = \alpha_3 = \alpha_4 = 1, p = 5, r = 31;$

$\alpha_1 = 7, \alpha_2 = 2, \alpha_3 = \alpha_4 = 1, p = 7, r = 127;$

$\alpha_1 = 2^a, \alpha_2 = \alpha_3 = \alpha_4 = 1, p = (2^{2^a - 1} + 1)/3, r = 2^{2^a} + 1$, *where* $a > 2$ *such that* $2^a - 1$ *is prime;*

$\alpha_1 = 4, \alpha_2 = 1, \alpha_3 = \alpha_4 = 2, p = 5, r = 7;$

$\alpha_1 = 5, \alpha_2 = \alpha_3 = 2, \alpha_4 = 1, p = 7, r = 97;$

$\alpha_1 = 6, \alpha_2 = \alpha_3 = 2, \alpha_4 = 1, p = 17, r = 577;$

$\alpha_3 = \alpha_4 = 1, p = 2^{\alpha_1 - 1} 3^{\alpha_2} + \delta, r = 2^{\alpha_1} 3^{\alpha_2} + \delta, \delta \in \{-1, 1\}, \alpha_1 > 0, \alpha_2 > 0;$

$\alpha_1 = 2, \alpha_2 = 2^a, \alpha_3 = \alpha_4 = 1, p = (3^{2^a} + 1)/2, r = 2 \cdot 3^{2^a} + 1, a > 0;$

$\alpha_1 = 3, \alpha_3 = \alpha_4 = 1, p = (3^{\alpha_2} + 1)/4, r = 2 \cdot 3^{\alpha_2} + 1, \alpha_2 > 0;$

$\alpha_1 = 2, \alpha_3 = \alpha_4 = 1, p = (3^{\alpha_2} - 1)/2, r = 2 \cdot 3^{\alpha_2} - 1, \alpha_2 > 0.$

Corollary. *If the answer to one of the following seven problems is "yes", then the number of simple* K_4*-groups is infinite. Otherwise, the number of simple* K_4*-groups is finite.*

Problem 1. *Are there infinitely primes* $\alpha_1 > 3$ *with* $2^{\alpha_1} - 1,\ (2^{\alpha_1} + 1)/3 \in \mathbb{P}$*?*

Problem 2. *Are there infinitely odd primes* α_2 *with* $(3^{\alpha_2} - 1)/2,\ (3^{\alpha_2} + 1)/4 \in \mathbb{P}$*?*

Problem 3. *Are there infinitely odd primes* a *with* $2^a - 1,\ 2^{2^a} + 1,\ (2^{2^a - 1} + 1)/3 \in \mathbb{P}$*?*

Problem 4. *Are there infinitely positive integers* α_1, α_2 *with* $2^{\alpha_1 - 1} 3^{\alpha_2} + \delta,\ 2^{\alpha_1} 3^{\alpha_2} + \delta \in \mathbb{P}$, *where* $\delta = \pm 1$*?*

Problem 5. *Are there infinitely positive integers* a *with* $2 \cdot 3^{2^a} + 1,\ (3^{2^a} + 1)/2 \in \mathbb{P}$*?*

Problem 6. *Are there infinitely primes* $\alpha_2 \equiv 1 \pmod 4$ *with* $2 \cdot 3^{\alpha_2} + 1,\ (3^{\alpha_2} + 1)/4 \in \mathbb{P}$*?*

Problem 7. *Are there infinitely primes* $\alpha_2 \equiv 3 \pmod 4$ *with* $2 \cdot 3^{\alpha_2} - 1,\ (3^{\alpha_2} - 1)/2 \in \mathbb{P}$*?*

We see from our Corollary that, under usual hypotheses on the distribution of prime numbers in sequences, there exist only finitely many simple K_4-groups.

In [18], W. Shi claimed that the simple K_4-group problem is reduced to the following four Diophantine problems:

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

$$\begin{cases} 2^m - 1 = p, \\ 2^m + 1 = 3q^n, \end{cases} \ p, q \in \mathbb{P}, p > 3, q > 3, m, n \in \mathbb{N}, \tag{3}$$

$$(4)\qquad \begin{cases} 3^m - 1 = 2p^n, \\ 3^m + 1 = 4q, \end{cases} \quad p, q \in \mathbb{P}, p > 3, q > 3, m, n \in \mathbb{N},$$

$$(5)\qquad \begin{cases} 3^m - 1 = 2p, \\ 3^m + 1 = 4q^n, \end{cases} \quad p, q \in \mathbb{P}, p > 3, q > 3, m, n \in \mathbb{N}.$$

From the proof of Theorem 2, we see that Shi's result is correct. In [12], M. Le and G. Xu "give all solutions of (2)–(5) when $c > 1, n > 1$." But their proofs are incorrect. Indeed, they all depend on Lemma 3 of [11], which is false, see the comment of P. Yuan [19]. In fact, we can prove the following result by using an elementary method.

Theorem 3. *If $n > 1$ then (4) has only the solution $(p, q, m, n) = (11, 61, 5, 2)$ and (5) has no solution.*

Further, we show in Section 3 that (3) has no solution with $n > 1$.

§2. Proof of Theorem 3

In this section, we will use the following Lemmas to prove our theorem 3.

Lemma 1. *The Diophantine equation*

$$\frac{x^m - 1}{x - 1} = y^2, \ x, y, m \in \mathbb{N}, \ x > 1, m > 2$$

has only the solutions $(x, y, m) = (7, 20, 4)$ and $(3, 11, 5)$, whereas the equation

$$\frac{x^m + 1}{x + 1} = y^2, \ x, y, m \in \mathbb{N}, \ x > 1, m > 2$$

has no solution.

Proof. See [13]. For a generalization and an elementary proof of Lemma 1, see [6].

Lemma 2. *The Diophantine equation*

$$3x^2 + 1 = 4y^n, \ 2 \nmid n > 1, x, y, n \in \mathbb{N}$$

has only the solution $x = y = 1$.

Proof. This follows directly from a general result in [14]. A generalization and an elementary proof of Lemma 2 are given in [7].

Proof of Theorem 3. First, we assume that (p, q, m, n) is a solution of (4). If $2 \mid n$, then from $3^m - 1 = 2p^n$ and Lemma 1, we see that $m = 5, n = 2, p = 11$. Substituting $m = 5$ into $3^m + 1 = 4q$ in (4), we have that $q = 61$. If $2 \nmid n$, then (4) gives $p^n + 1 = 2q$ and so

$$(p + 1) \cdot (p^n + 1)/(p + 1) = 2q,$$

which is impossible since $2 \nmid n, n > 1$ and q is prime.

Next, assume that (p, q, m, n) is a solution of (5). By Lemma 1 and the equation $3^m + 1 = 4q^n$ in (5), we get that $2 \nmid mn$. So we have

$$3(3^{(m-1)/2})^2 + 1 = 4q^n, \ 2 \nmid n, n > 1,$$

which is impossible by Lemma 2. This proves Theorem 3.

§3. Preliminaries for Proof of Theorem 2 —The Diophantine equation $2^m + 1 = 3y^q$

The purpose of this section is to solve completely the Diophantine equation

$$2^m + 1 = 3y^q \quad \text{in integers } m \geq 2, q \geq 2, y \geq 2. \tag{6}$$

There is no loss of generality in assuming that q is prime. As a consequence, we solve (3) with $n > 1$.

Lemma 3. *The Diophantine equation (6) has no solution.*

Proof. We use the method which has already been applied successfully (see [3, 4]) to the Diophantine equation

$$\frac{x^m - 1}{x - 1} = y^q \quad \text{in integers } x \geq 2, y \geq 2, m \geq 3, q \geq 2,$$

after noticing that (6) corresponds to the above equation with $x = -2$.

For the reader's convenience, we will however explain the different steps of the proof. Assume in the sequel that there are integers $m \geq 2$, $y \geq 2$ and $q \geq 2$ with $2^m + 1 = 3y^q$.

- First step : upper bound for q.

Since (m, q, y) is a solution of (6), we have

$$2^m y^{-q} = \left(3 - \left(\frac{1}{y}\right)^q\right) =: \Lambda,$$

and we apply Théorème 4 of [2] to bound from above the 2-adic valuation of Λ, which we denote by $v_2(\Lambda)$. We check easily that y is odd and that y and 3 are multiplicatively independent, and we take

$$p = 2, g = 2,\ \alpha_1 = 3,\ \alpha_2 = \frac{1}{y},\ b_1 = 1,\ \text{and } b_2 = q$$

in Théorème 4 of [2], with

$$\log A_1 = \log 3,\ \log A_2 = \log y,\ \mu = 15 \text{ and } \nu = 10.$$

Thus, we get

$$m = v_2(\Lambda) \leq 36 \frac{\log 3}{(\log 2)^4} \log y \left(\max\left\{\log\left(\frac{q}{\log 3} + \frac{1}{\log y}\right) + 0.04, 10.4\right\}\right)^2. \tag{7}$$

However, we deduce from (6) that $m \log 2 \geq q \log y$, which together with (7) yields

$$q \leq 118.8 \left(\max\left\{\log\left(\frac{q}{\log 3} + \frac{1}{\log y}\right) + 0.04, 10.4\right\}\right)^2,$$

hence we get

$$q \leq 12850.$$

- Second step : some conditions on m and q.

Regarding (6) modulo 3, we immediately see that m must be odd. By results of Nagell and Ljunggren (see Ribenboim [17], pages 111 and 117), we know that q is odd and that 3 does not divide m.

Further, if $m \equiv 1 \pmod{q}$, then there exists an integer $\nu \geq 1$ with $m = \nu q + 1$, and (6) can be re-written as

$$3y^q - 2(2^\nu)^q = 1,$$

which has no solution with $y \geq 2$ by Theorem 1.1 of Bennett [1]. Consequently, (6) has no solution with $m \equiv 1 \pmod{q}$.

- Third step : local considerations.

From the two previous steps, we see that it remains us to solve (6) for every odd prime q_0 less than 12850. For such a q_0, we proceed as follows.

– We consider the first prime numbers p with $p \equiv 1 \,(\mathrm{mod}\ q_0)$ and we work modulo p,

– For each such p, it leads to some conditions on the exponent m of equation (6), more precisely it implies that m belongs to some set modulo $p - 1$,

– It appears that combining these conditions for several values of p and using that $m \not\equiv 0 (\mathrm{mod}\ 3)$ and $m \not\equiv 0 (\mathrm{mod}\ 2)$ (both results proved in the second step) yield $m \equiv 1 \,(\mathrm{mod}\ q_0)$, which is excluded by the above-mentioned result of Bennett. Hence, (6) has no solution (m, q_0, y).

As an illustration of the method, let us consider the equation $2^m + 1 = 3y^7$. Since y^7 is congruent to 0, 1, 12, 17 or 28 modulo 29, we get that m is congruent to 1, 6, 14, 16 or 17 modulo 28, hence, m being odd, m is congruent to 1 or 3 modulo 14. Then, we observe that for $m \equiv 3, 17$ or 31 mod 42 we have $2^m + 1 \equiv 9$ mod 43, hence we have $y^7 \equiv 3$ mod 43. This is a contradiction since $3^6 \not\equiv 1$ mod 43. Thus we have proved that m is congruent to 1 modulo 14, which is excluded by Bennett's result. Hence, (6) has no solution $(m, 7, y)$.

We perform these verifications on a computer, and it takes only half a day of CPU. We conclude that (6) has no solution, as claimed.

§4. Proof of Theorem 2

We will use also the following lemmas to prove our theorem.

Lemma 4. *The Diophantine equation*

$$3^m - 2y^q = 1, \;\; m > 2, y \geq 2, q \geq 2$$

has only the solution $(y, m, q) = (11, 5, 2)$.

Proof. See [3] or [4].

Lemma 5. *The Diophantine equation*

$$x^2 + 1 = 2y^n, \;\; n > 2, y > 1, x, y, n \in \mathbb{N}$$

has only the solution $(x, y, n) = (239, 13, 4)$.

Proof. See [14] and [15].

Lemma 6. *If x or y is prime, then the Diophantine equation*

$$x^m - y^n = 1, \; x > 1, y > 1, m > 1, n > 1, x, y, m, n \in \mathbb{N}$$

has only the solution $(x, y, m, n) = (3, 2, 2, 3)$.

Proof. See [8].

Proof of Theorem 2.

We solve equation (1) in which $p > 3$ and $r > 3$ are distinct prime numbers. Without loss of generality, in course of the proof, we do not consider the case of exchanging p^{α_3} and r^{α_4}. However, the solutions of (1) are listed in Theorem 2 with the convention $p < r$.

(A) When $q = 2^{\alpha_1}$, we get from (1) that

$$2^{2\alpha_1} - 1 = 3^{\alpha_2} p^{\alpha_3} r^{\alpha_4}.$$

Since $\gcd(2^{\alpha_1} + 1, 2^{\alpha_1} - 1) = 1$, we have

$$2^{\alpha_1} + 1 = 3^{\alpha_2}, \; 2^{\alpha_1} - 1 = p^{\alpha_3} r^{\alpha_4}, \tag{8}$$

or

$$2^{\alpha_1} - 1 = 3^{\alpha_2}, \; 2^{\alpha_1} + 1 = p^{\alpha_3} r^{\alpha_4}, \tag{9}$$

or

$$2^{\alpha_1} + 1 = 3^{\alpha_2} p^{\alpha_3}, \; 2^{\alpha_1} - 1 = r^{\alpha_4}, \tag{10}$$

or

$$2^{\alpha_1} - 1 = 3^{\alpha_2} p^{\alpha_3}, \; 2^{\alpha_1} + 1 = r^{\alpha_4}. \tag{11}$$

By Lemma 6, we see that both (8) and (9) are impossible. For (10), by the second equality of (10) and Lemma 6, we get that $\alpha_4 = 1$, and so $r = 2^{\alpha_1} - 1$ with $\alpha_1 > 2$. By the first equality of (10), we see that $\alpha_2 = 1$, i.e.

$$2^{\alpha_1} + 1 = 3p^{\alpha_3}.$$

It follows that $\alpha_3 = 1$ by Lemma 3.

For (11), by the second equality of (11) and Lemma 6, we get that $\alpha_4 = 1$, i.e. $r = 2^{\alpha_1} + 1$ and so $\alpha_1 = 2^a, a \in \mathbb{N}$. If $a = 1$, then the first equality of (11) is impossible. If $a > 1$, then $3 \mid 2^{2^{a-1}} - 1$. So from $\gcd(2^{2^{a-1}} + 1, 2^{2^{a-1}} - 1) = 1$ and the first equality of (11) we have

$$2^{2^{a-1}} - 1 = 3^{\alpha_2}, \; 2^{2^{a-1}} + 1 = p^{\alpha_3}.$$

It follows that $a = 2, \alpha_2 = \alpha_3 = 1, p = 5, r = 17$.

(B) When $q = 3^{\alpha_2}$, we get from (1) that

$$3^{2\alpha_2} - 1 = 2^{\alpha_1 + 1} p^{\alpha_3} r^{\alpha_4}.$$

Since $\gcd(3^{\alpha_2}+1, 3^{\alpha_2}-1)=2$ we have

$$3^{\alpha_2}+1=2^{\alpha_1},\ 3^{\alpha_2}-1=2p^{\alpha_3}r^{\alpha_4}, \tag{12}$$

or

$$3^{\alpha_2}-1=2^{\alpha_1},\ 3^{\alpha_2}+1=2p^{\alpha_3}r^{\alpha_4}, \tag{13}$$

or

$$3^{\alpha_2}+1=2^{\alpha_1}p^{\alpha_3},\ 3^{\alpha_2}-1=2r^{\alpha_4}, \tag{14}$$

or

$$3^{\alpha_2}-1=2^{\alpha_1}p^{\alpha_3},\ 3^{\alpha_2}+1=2r^{\alpha_4}. \tag{15}$$

By Lemma 6, we see that both (12) and (13) are impossible. For (14), if $\alpha_4>1$, then by Lemma 4 and the second equality of (14) we get that $\alpha_2=5, \alpha_4=2, r=11$, and so $\alpha_1=2, p=61, \alpha_3=1$. If $\alpha_4=1$, then the second equality of (14) gives $r=(3^{\alpha_2}-1)/2$ and $\alpha_2>2$. Hence, we get from the first equality of (14) that $\alpha_1=2$ and $2\nmid\alpha_3$ by Lemma 1. Therefore,

$$3(3^{(\alpha_2-1)/2})^2+1=4p^{\alpha_3},\ 2\nmid\alpha_3.$$

By Lemma 2, we get $\alpha_3=1$.

For (15), we see that $2\mid\alpha_2, \alpha_2>2$. Since $\gcd(3^{\alpha_2/2}+1, 3^{\alpha_2/2}-1)=2$ and

$$3^{\alpha_2/2}-1\equiv\begin{cases}0(\mathrm{mod}\ 8),\\ 2(\mathrm{mod}\ 8),\end{cases}\ 3^{\alpha_2/2}+1\equiv\begin{cases}2(\mathrm{mod}\ 8), & \text{if } 2\mid\alpha_2/2,\\ 4(\mathrm{mod}\ 8), & \text{if } 2\nmid\alpha_2/2.\end{cases}$$

Thus, by the first equality of (15), we get that

$$3^{\alpha_2/2}-1=2^{\alpha_1},\ 3^{\alpha_2/2}+1=2p^{\alpha_3}\ (\text{ if } 2\mid\alpha_2/2),$$

or

$$3^{\alpha_2/2}+1=2^{\alpha_1-1},\ 3^{\alpha_2/2}-1=2p^{\alpha_3}, \alpha_1-1=2\ (\text{ if } 2\nmid\alpha_2/2).$$

This gives $\alpha_1=4, \alpha_2=4, \alpha_3=\alpha_4=1, p=5, r=41$.

(C, D) When $q=p^{\alpha_3}$, we get from (1) that

$$p^{2\alpha_3}-1=2^{\alpha_1+1}3^{\alpha_2}r^{\alpha_4}.$$

Since $\gcd(p^{\alpha_3}+1, p^{\alpha_3}-1)=2$, we have

$$p^{\alpha_3}+1=2^{\alpha_1},\ p^{\alpha_3}-1=2\cdot 3^{\alpha_2}r^{\alpha_4}, \tag{16}$$

or

$$p^{\alpha_3}-1=2^{\alpha_1},\ p^{\alpha_3}+1=2\cdot 3^{\alpha_2}r^{\alpha_4}, \tag{17}$$

or

$$p^{\alpha_3}+1=2^{\alpha_1}3^{\alpha_2},\ p^{\alpha_3}-1=2r^{\alpha_4}, \tag{18}$$

or

$$p^{\alpha_3}-1=2^{\alpha_1}3^{\alpha_2},\ p^{\alpha_3}+1=2r^{\alpha_4}, \tag{19}$$

or

$$p^{\alpha_3}+1=2^{\alpha_1}r^{\alpha_4},\ p^{\alpha_3}-1=2\cdot 3^{\alpha_2}, \tag{20}$$

or

$$p^{\alpha_3}-1=2^{\alpha_1}r^{\alpha_4},\ p^{\alpha_3}+1=2\cdot 3^{\alpha_2}. \tag{21}$$

For (16), by Lemma 6, we know from the first equality of (16) that $\alpha_3=1$ and $\alpha_2>2$. Furthermore, (16) gives

$$2^{\alpha_1-1}-3^{\alpha_2}r^{\alpha_4}=1. \tag{22}$$

Considering the equality (22) mod 3 we obtain $2\mid\alpha_1-1$, and so

$$2^{(\alpha_1-1)/2}\pm 1=3^{\alpha_2},\ 2^{(\alpha_1-1)/2}\mp 1=r^{\alpha_4},$$

It follows that $((\alpha_1-1)/2,\alpha_2)=(1,1),(2,1),(3,2)$ and $r^{\alpha_4}=2\cdot 2^{(\alpha_1-1)/2}-3^{\alpha_2}$, thus

$$\alpha_1=5,\alpha_2=\alpha_3=\alpha_4=1,p=31,r=5$$

and

$$\alpha_1=7,\alpha_2=2,\alpha_3=\alpha_4=1,p=127,r=7.$$

For (17), similarly, we have that $\alpha_3=1,\alpha_1=2^a,a\in\mathbb{N}$ and

$$2^{2^a-1}-3^{\alpha_2}r^{\alpha_4}=-1. \tag{23}$$

If $\alpha_2>1$, then we get from (23) that $3\mid 2^a-1$. Hence, (23) gives

$$(2^{(2^a-1)/3}+1)(2^{2(2^a-1)/3}-2^{(2^a-1)/3}+1)=3^{\alpha_2}r^{\alpha_4},$$

and so

$$2^{(2^a-1)/3}+1=3^{\alpha_2-1},\ 2^{2(2^a-1)/3}-2^{(2^a-1)/3}+1=3r^{\alpha_4},$$

which is impossible. Therefore, $\alpha_2=1$ and so (23) gives

$$2^{2^a-1}+1=3r^{\alpha_4}.$$

By Lemma 3, this implies that $\alpha_4=1$. Further, 2^a-1 must be prime. Hence, $p=2^{2^a}+1$ and $a>2$ since $r\notin\{2,3\}$.

For (18), clearly, $2\nmid\alpha_3$. We get from the first equality of (18) that

$$2^{\alpha_1}3^{\alpha_2}=(p+1)\cdot(p^{\alpha_3}+1)/(p+1).$$

It follows that $\alpha_3 = 1$ since $2 \nmid (p^{\alpha_3} + 1)/(p + 1)$. By the first equality minus the second equality of (18), we have

$$2^{\alpha_1 - 1} 3^{\alpha_2} - r^{\alpha_4} = 1. \tag{24}$$

Similarly, (24) gives $\alpha_4 = 1$. Therefore, $r = 2^{\alpha_1 - 1} 3^{\alpha_2} - 1, p = 2^{\alpha_1} 3^{\alpha_2} - 1$.

For (19), by the same argument as in the proof for (18), we have $\alpha_3 = \alpha_4 = 1$ and so $r = 2^{\alpha_1 - 1} 3^{\alpha_2} + 1, p = 2^{\alpha_1} 3^{\alpha_2} + 1$.

For (20), we easily obtain that $\alpha_3 = 1$, and by the first equality minus the second equality of (20) we get that

$$2^{\alpha_1 - 1} r^{\alpha_4} - 3^{\alpha_2} = 1. \tag{25}$$

If $2 \mid \alpha_2$, then (25) gives $\alpha_1 = 2$ and so $\alpha_4 = 1$ by Lemma 5. Therefore, $\alpha_2 = 2^a, a \in \mathbb{N}$ since r is prime. This implies that $r = (3^{2^a} + 1)/2, p = 2 \cdot 3^{2^a} + 1$. If $2 \nmid \alpha_2$, then $\alpha_1 = 3, 2 \nmid \alpha_4$ by Lemma 1. Therefore, (25) gives

$$3(3^{(\alpha_2 - 1)/2})^2 + 1 = 4r^{\alpha_4}, \ 2 \nmid \alpha_4.$$

It follows from Lemma 2 that $\alpha_4 = 1$ and $\alpha_2 > 0$, whence $p = 2 \cdot 3^{\alpha_2} + 1$.

For (21), arguing as in the proof for (20), we have $\alpha_1 = 2, \alpha_3 = \alpha_4 = 1, p = 2 \cdot 3^{\alpha_2} - 1, r = (3^{\alpha_2} - 1)/2$, where $\alpha_2 > 0$.

This proves Theorem 2.

References

1. M. Bennett, *Rational approximation to algebraic number of small height : The diophantine equation* $|ax^n - by^n| = 1$, J. reine angew. Math., to appear.
2. Y. Bugeaud et M. Laurent, *Minoration effective de la distance p-adique entre puissances de nombres algébriques*, J. Number Theory **61** (1996), 311–342.
3. Y. Bugeaud and M. Mignotte, *On integers with identical digits*, Mathematika, to appear.
4. Y. Bugeaud, M. Mignotte and Y. Roy, *On the Diophantine equation* $\frac{x^n - 1}{x - 1} = y^q$, Pacific J. Math. **193** (2000), 257–268.
5. Z. Cao, *Some problems in Diophantine equations and its applications*, Ph.D thesis, Ch.5, 1999.
6. Z. Cao, *On the Diophantine equation* $\frac{ax^m - 1}{abx - 1} = by^2$, Chinese Sci. Bull. **36** (1991), no. 4, 275–278.
7. Z. Cao and X. Dong, *The Diophantine equation* $Ax^2 + B = y^n$, Chinese Sci. Bull. **43** (1998), no. 13, 1141–1142.
8. J. W. S. Cassels, *On the equation* $a^x - b^y = 1$, Amer. J. Math. **75** (1953), 159–162.
9. D. Gorenstein, Finite Simple Groups, An Introduction to Their Classification, Plenum Press, New York and London, 1982.
10. M. Herzog, *On finite simple groups of order divisible by three primes only*, J. Algebra **10** (1968), 383–388.
11. M. Le, *A note on perfect powers of the form* $x^{m-1} + ... + x + 1$, Acta Arith. **69** (1995), 91–98.
12. M. Le and G. Xu, *Some Diophantine problems of Simple* K_4- *groups(in Chinese)*, Sci. in China Ser. A **26** (1996), no. 9, 769– 773.
13. W. Ljunggren, *Noen setninger on ubestemte likninge av formen* $\frac{x^n - 1}{x - 1} = y^q$, Norsk Mat. Tidsskr **25** (1943), 17–20.
14. W. Ljunggren, *Über die Gleichungen* $1 + Dx^2 = 2y^n$ *und* $1 + Dx^2 = 4y^n$, Norsk Vid. Selsk. Forhandl **15** (1942), no. 30, 115–118.
15. W. Ljunggren, *Zur Theorie der Gleichung* $x^2 + 1 = Dy^4$, Avh. Norske. Vid. Akad. Oslo **1** (1942), no. 5, 1–27.

16. V. D. Mazurov and E. I. Khukhro, *Unsolved problems in Group theory*, 13th edition, Novsibirsk, The Kourovka Notebook, (1995), 130–148.
17. P. Ribenboim, *Catalan's Conjecture*, Academic Press, Boston (1994).
18. W. Shi, *On simple K_4-groups(in Chinese)*, Chinese Sci. Bull. **36** (1991), no. 17, 1281–1283.
19. P. Yuan, *Comment: "A note on perfect powers of the form $x^{m-1}+...+x+1$", Acta Arith. 69(1995), 91–98, by Maohua Le and "On the Diophantine equation $(x^m-1)/(x-1)=y^n$", Acta Arith. 83(1995), 363–366, by Li Yu and Maohua Le*, Acta Arith. **83** (1998), 199.

Université Louis Pasteur, U. F. R. de mathématiques, 67084 Strasbourg, France.
Department of Mathematics, Harbin Institute of Technology, Harbin 150001, P. R. China.

E-mail address: {bugeaud,mignotte}@math.u-strasbg.fr zfcao@hope.hit.edu.cn