A DIOPHANTINE EQUATION CONCERNING FINITE GROUPS

MAOHUA LE
A DIOPHANTINE EQUATION CONCERNING FINITE GROUPS

MAOHUA LE

In this paper we prove that all solutions \((y, m, n)\) of the equation \(3^m - 2y^n = \pm1\), \(y, m, n \in \mathbb{N}\), \(y > 1, m > 1, n > 1\), satisfy \(y < 10^6, m < 1.4 \cdot 10^{15}\) and \(n < 1.2 \cdot 10^5\).

1. Introduction. Let \(\mathbb{Z}, \mathbb{N}, \mathbb{P}, \mathbb{Q}\) be the sets of integers, positive integers, odd primes and rational numbers respectively. In [2], Cresenzo considered the solutions \((p, q, m, n, \delta)\) of the equation

\[(1) \ p^m - 2q^n = \delta, \ p, q \in \mathbb{P}, \ m, n \in \mathbb{N}, \ m > 1, n > 1, \delta \in \{-1, 1\},\]

which is concerned with finite groups. He claimed that if \((p, q, m, n, \delta) \neq (239, 13, 2, 4, -1)\), then \((m, n, \delta) = (2, 2, -1)\). However, we notice that \((1)\) has another solution \((p, q, m, n, \delta) = (3, 11, 5, 2, 1)\) with \((m, n, \delta) \neq (2, 2, -1)\). Thus it can be seen that the above result is not correct. If we follow the proof of Cresenzo, we can argue as follows. The above result is deduced from the following lemma:

**Lemma A ([2, Lemma 1]).** Suppose that \(q \in \mathbb{P}\) and \(x, m, n \in \mathbb{N}\). If

\[(2) \ x^m - 2q^n = \pm1, \ x > 1, m > 1, n > 1,\]

then \(m\) is a power of 2. Furthermore, the sign of the term \(\pm1\) must be negative.

Notice that if \(2 \nmid xm\), then from (2) we get

\[2q^k = x \mp 1\]

for some \(k \in \mathbb{N}\) with \(k < n\). Now there are two cases:

\[(3) \quad x = \begin{cases} 
3, & \text{if } k = 0, \\
2q^k \pm 1, & \text{if } k > 0.
\end{cases}\]
Hence, Lemma A is false since the first case of (3) was not considered in [2]. The lemma must be replaced by:

**Lemma A’**. Suppose that \( q \in \mathbb{P} \) and \( x, m, n, \in \mathbb{N} \). If (2) hold, then either \( x = 3 \) or \( x > 3 \) and \( m \) is a power of 2. Furthermore, in the last case, the sign of the term \( \pm 1 \) of (2) must be negative.

Thus, the correct main statement of [2] should be that the solutions \((p, q, m, n, \delta)\) of (1) satisfy either \( p = 3 \) or \( p > 3 \) and \((m, n, \delta) = (2, 2, -1)\) except when \((p, q, m, n, \delta) = (239, 13, 2, 4, -1)\). In this paper, we deal with the solutions of (1) with \( p = 3 \). We shall prove a general result as follows:

**Theorem.** The equation

\[
3^m - 2y^n = \delta, \quad y, m, n, \in \mathbb{N}, \quad y > 1, m > 1, n > 1, \delta \in \{-1, 1\},
\]

has only finitely many solutions \((y, m, n, \delta)\). Moreover, all solutions of (4) satisfy \( y < 10^6 \cdot 10^9, m < 1.4 \cdot 10^{15} \) and \( n < 1.2 \cdot 10^5 \).

2. Lemmas.

**Lemma 1.** Let \( k \in \mathbb{N} \) with \( \gcd(6, k) = 1 \). If \( k > 1 \) and \((X, Y, Z)\) is solution of the equation

\[
X^2 - 3Y^2 = k^Z, \quad X, Y, Z, \in \mathbb{Z}, \quad \gcd(X, Y) = 1, \quad Z > 0,
\]

then there exist \( X_1, Y_1 \in \mathbb{N} \) such that

\[
X_1^2 - 3Y_1^2 = k, \quad \gcd(X_1, Y_1) = 1,
\]

\[
1 < \frac{X_1 + Y_1\sqrt{3}}{X_1 - Y_1\sqrt{3}} < (2 + \sqrt{3})^2,
\]

\[
X + Y\sqrt{3} = (X_1 + \lambda Y_1\sqrt{3})^Z(u + v\sqrt{3}), \quad \lambda \in \{-1, 1\},
\]

where \((u, v)\) is a solution of the equation

\[
u^2 - 3v^2 = 1, \quad u, v \in \mathbb{Z}.
\]

**Proof.** Since the class number of the binary quadratic forms with discriminant 12 is equal to 1 and \( 2 + \sqrt{3} \) is a fundamental solution of (5), the lemma follows immediately from [6, Lemma 7]. \( \square \)
\textbf{Lemma 2 ([3])}. Let $a, b, k, n \in \mathbb{Z} \setminus \{0\}$ with $n \geq 3$. All solutions $(X, Y)$ of the equation
\[ aX^n - bY^n = k, \quad X, Y \in \mathbb{Z}, \]
\[ \text{satisfy } \max(|X|, |Y|) \leq 2n^{(n-1)/2-1/n}H^{n-3/n}|k|^{1/n}, \text{ where } H = \max(|a|, |b|). \]

\textbf{Lemma 3 ([7])}. The equation
\[ 1 + X^2 = 2Y^n, \quad X, Y, n \in \mathbb{N}, \quad X > 1, Y > 1, n > 2, \]
has no solution $(X, Y, n)$.

\textbf{Lemma 4 ([9])}. The equation
\[ \frac{X^m - 1}{X - 1} = Y^n, \quad X, Y, m, n \in \mathbb{N}, \quad X > 1, Y > 1, m > 2, n > 1, \]
\[ \text{has only solution } (X, Y, m, n) = (7, 20, 4, 2) \text{ with } 4|m. \]

\textbf{Lemma 5 ([10])}. The equation (6) has only solutions $(X, Y, m, n) = (3, 11, 5, 2), (7, 20, 4, 2)$ with $2|n$.

Let $\alpha$ be an algebraic number with the minimal polynomial
\[ a_0z^d + \cdots + a_{d-1}z + a_d = a_0 \prod_{i=1}^{d}(z - \sigma_i\alpha), \quad a_0 \in \mathbb{N}, \]
where $\sigma_1\alpha, \ldots, \sigma_d\alpha$ are all conjugates of $\alpha$. Then
\[ h(\alpha) = \frac{1}{d} \left( \log a_0 + \sum_{i=1}^{d} \log \max(1, |\sigma_i\alpha|) \right) \]
is called the logarithmic absolute height of $\alpha$.

\textbf{Lemma 6}. Let $\alpha_1, \alpha_2$ be real algebraic numbers with $\alpha_1 \geq 1, \alpha_2 \geq 1$, and let $D$ denote the degree of $\mathbb{Q}(\alpha_1, \alpha_2)$. Let $b_1, b_2 \in \mathbb{N}$, and let $b = b_1/Dh(\alpha_2) + b_2/Dh(\alpha_1)$. For any $T$ with $T > 1$, if $0.52 + \log b \geq T$ and $\Lambda = b_1 \log \alpha_1 - b_2 \log \alpha_2 \neq 0$, then
\[ \log |\Lambda| \geq -70 \left( 1 + \frac{0.1137}{T} \right)^2 D^4h(\alpha_1)h(\alpha_2)(0.52 + \log b)^2. \]
Proof. Let $B = \log(5c_4/c_1) + \log b$, $K = [c_1D^3Bh(\alpha_1)h(\alpha_2)]$, $L = [c_2DB]$, $R_1 = [c_3D^{3/2}B^{1/2}h(\alpha_2)]+1$, $S_1 = [c_3D^{3/2}B^{1/2}h(\alpha_1)]+1$, $R_2 = [c_4D^2Bh(\alpha_2)]$, $S_2 = [c_4D^2Bh(\alpha_1)]$, $R = R_1 + R_2 - 1$, $S = S_1 + S_2 - 1$, where $c_1, c_2, c_3, c_4$ are positive numbers. Notice that $(u - 1/T)v < [uv] \leq uv$ for any real numbers $u, v$ with $u \geq 0$ and $v \geq T$. By the proof of [4, Theorem 1 and 3], if $B \geq T$,

\[ (7) \quad \sqrt{c_1} = \frac{\rho + 1}{(\log \rho)^{3/2}} + \sqrt{\frac{(\rho + 1)^2}{(\log \rho)^3} + \frac{\rho + 1}{T \log \rho}}, \quad c_2 > \frac{2}{\log \rho}, \]

\[ c_3 = \max(\sqrt{c_1}, \sqrt{c_2}), \quad c_4 = \sqrt{2c_1c_2} + 1/T, \]

for any $\rho$ with $\rho > 1$, then

\[ (8) \quad \log |\Lambda| \geq -c_1c_2 \log \rho + 1)D^4h(\alpha_1)h(\alpha_2)B^2. \]

Setting $\rho = 5.803$. We may choose $c_1, c_2, c_3, c_4$ which make (7) hold and

\[ (9) \quad c_1c_2 \log \rho + 1 < 70 \left(1 + \frac{0.1137}{T}\right)^2, \quad B < 0.52 + \log b. \]

Substituting (9) into (8), the lemma is proved. \qed

3. Proof of Theorem. Let $(y, m, n, \delta)$ be a solution of (4).

Since

\[ (10) \quad \text{ord}_2(3^m + 1) = \begin{cases} 1, & \text{if } 2|m, \\ 2, & \text{if } 2 \nmid m, \end{cases} \]

for any $m \in \mathbb{N}$, if $\delta = -1$, then $m$ must be even. Further, by Lemma 3, it is impossible. By Lemma 4, (4) has no solution with $\delta = 1$ and $4|m$, and by Lemma 5, (4) has only solutions $(y, m, n, \delta) = (2, 2, 2, 1)$ and $(11, 5, 2, 1)$ with $\delta = 1$ and $2|n$. If $2|m$ and $2 \nmid n$, then from (4) we get

\[ (11) \quad 3^{m/2} + 1 = y_1^n, \quad 3^{m/2} - 1 = 2y_2^n, \quad y_1y_2 = y, \quad y_1, y_2 \in \mathbb{N}, 2|y_1. \]

Since $n > 2$, (11) is impossible by (10). Therefore, if $(y, m, n, \delta) \neq (2, 2, 2, 1)$ or $(11, 5, 3, 1)$, then $\delta = 1$ and $2 \nmid mn$. It is a well known
fact that \((3^m - 1)/(3 - 1)\) has a prime factor \(l\) with \(l \equiv 1 \pmod{m}\) (see [1]). So by (4) we have

\[(12)\quad y \geq 2m + 1 > 2n + 1.\]

If \(2 \nmid m\), then from (4) we get

\[(13)\quad A^2 - 3B^2 = y^n, \quad A, B \in \mathbb{N},\]

where

\[(14)\quad A = \frac{3^{(m+1)/2} - 1}{2}, \quad B = \frac{3^{(m-1)/2} - 1}{2}.\]

Since \(\gcd(6, y) = \gcd(A, B) = 1\) by Lemma 1, we see from (13) that

\[(15)\quad A + B\sqrt{3} = (X_1 + \lambda Y_1 \sqrt{3})^n(u + v\sqrt{3}), \quad \lambda \in \{-1, 1\},\]

where \((u, v)\) is a solution of (5), \(X_1, Y_1 \in \mathbb{N}\) such that

\[(16)\quad X_1^2 - 3Y_1^2 = y, \quad \gcd(X_1, Y_1) = 1,\]

\[(17)\quad 1 < \frac{X_1 + Y_1\sqrt{3}}{X_1 - Y_1\sqrt{3}} < (2 + \sqrt{3})^2.\]

Let

\[(18)\rho = 2 + \sqrt{3}, \quad \bar{\rho} = 2 - \sqrt{3}, \quad \varepsilon = X_1 + Y_1\sqrt{3}, \quad \bar{\varepsilon} = X_1 - Y_1\sqrt{3}.\]

Since \(A = 3B + 1\) by (14), we have

\[1 < \frac{A + B\sqrt{3}}{A - B\sqrt{3}} = \frac{(\sqrt{3} + 1)(\sqrt{3}^m - 1)}{(\sqrt{3} - 1)(\sqrt{3}^m + 1)} < 2.\]

Hence, by (15) and (17), we have

\[(19)\quad A + B\sqrt{3} = \begin{cases} \varepsilon^n \bar{\rho}^s, & \text{if } \lambda = 1, \\ \bar{\varepsilon}^n \rho^s, & \text{if } \lambda = -1, \end{cases}\]

where \(s \in \mathbb{Z}\) with \(0 \leq s \leq n\). From (19),

\[\varepsilon^n \bar{\rho}^s (\sqrt{3} - \lambda) = \bar{\varepsilon}^n \rho^s (\sqrt{3} + \lambda) - 2\lambda,\]
whence we obtain

\[(20) \quad \left| (2s + \lambda) \log \rho - n \log \frac{\varepsilon}{\bar{\varepsilon}} \right| = \frac{2}{\sqrt{3}^m} \sum_{j=0}^{\infty} \frac{\rho/h^{3-mi/2}}{2i+1} < \frac{4}{\sqrt{3}^m}. \]

Let \( \alpha_1 = \rho \) and \( \alpha_2 = \varepsilon/\bar{\varepsilon} \). Then \( Q(\alpha_1, \alpha_2) = Q(\sqrt{3}) \). We see from (5), (16) and (18) that

\[(21) \quad h(\alpha_1) = \frac{1}{2} \log \rho, \quad h(\alpha_2) = \log \varepsilon. \]

Furthermore, since \( 3^m > 2y^n \), by (17) and (21),

\[(22) \quad h(\alpha_2) < \log \rho \sqrt{y}. \]

Let \( b = (2n + 1)/2h(\alpha_2) + n/2h(\alpha_1) \). Recall that \( 0 \leq s \leq n \). By Lemma 6, if \( n > 10^5 \), then

\[(23) \quad \log \left| (2s + \lambda) \log \rho - n \log \frac{\varepsilon}{\bar{\varepsilon}} \right| > -1145h(\alpha_1)h(\alpha_2)(0.52 + \log b)^2. \]

Since

\[ b < \frac{2n + 1}{2 \log \rho \sqrt{y}} + \frac{n}{\log \rho} < \frac{2n + 1}{2 \log 3.732 \sqrt{2n + 1}} + \frac{n}{1.317} < 0.8n, \]

by (12) and (22), the combination of (20) and (23) yields

\[ 1 + 760(\log \sqrt{y})(0.3 + \log n)^2 > n \log \sqrt{y}, \]

whence we deduce that

\[(24) \quad n < 1.2 \cdot 10^5. \]

Let \( m = rn + t \), where \( r, t \in \mathbb{Z} \) with \( r \geq 0 \) and \( 0 \leq t < n \). Then (4) can be written as

\[(25) \quad 3^t(3^r)^n - 2y^n = 1. \]

It implies that \((X, Y) = (3^r, y)\) is a solution of the equation

\[ 3^tX^n - 2Y^n = 1, \quad X, Y \in \mathbb{Z}. \]

Thus, by Lemma 2, we get from (24) and (25) that \( y < 10^{6 \cdot 10^9} \) and \( m < 1.4 \cdot 10^{15} \). The theorem is proved.

**Remark.** By a better estimates for the lower bound of linear forms in two logarithms by Laurent, Mignotte and Nesterenko [5], the upper bound of solutions of (4) in Theorem can be improved.
A DIOPHANTINE EQUATION

Acknowledgment. The author thanks the referee for his valuable suggestions.

REFERENCES


Received December 7, 1992. Supported by National Natural Science Foundation of China.

ZHANJIANG TEACHERS COLLEGE
P. O. Box 524048
ZHANJIANG, GUANGDONG
P. R. CHINA
On Banach spaces $Y$ for which $B(C(\Omega), Y) = K(C(\Omega), Y)$

SHAMIM ISMAIL ANSARI

Convergence of infinite exponentials

GENNADY BACHMAN

Cohomologie d’intersection modérée. Un théorème de de Rham

BOHUMIL CENKL, GILBERT HECTOR and MARTINTXO SARALEGI-ARANGUREN

Kleinian groups with an invariant Jordan curve: $J$-groups

RUBEN A. HIDALGO

Multiplicative functions on free groups and irreducible representations

M. GABRIELLA KUHN and TIM STEGER

A Diophantine equation concerning finite groups

MAOHUA LE

Nilpotent characters

GABRIEL NAVARRO

Smooth extensions and quantized Fréchet algebras

XIAOLU WANG