Simplifying the Solution of Ljunggren's Equation

\[ X^2 + 1 = 2Y^4 \]

RAY STEINER

Department of Mathematics and Statistics, Bowling Green State University, Bowling Green, Ohio 43403-0221

AND

NIKOS TZANAKIS

Department of Mathematics, University of Crete, Iraklion, Crete, Greece

Communicated by Hans Zassenhaus

Received July 17, 1989; revised January 23, 1990

In 1942 Ljunggren gave a very complicated proof of the fact that the only positive integer solutions of the equation

\[ X^2 + 1 = 2Y^4 \] (1.1)

are \( (X, Y) = (1, 1) \) and \( (239, 13) \). In the present paper we give a simpler solution of Ljunggren’s problem. This is accomplished by reducing the problem to a Thue equation and then solving it by using a deep result of Mignotte and Waldschmidt on linear forms in logarithms and continued fractions. © 1991 Academic Press, Inc.

I. INTRODUCTION

In 1942 Ljunggren [4] gave a very complicated proof of the following

**THEOREM 1.** The only positive integer solutions of the diophantine equation

\[ X^2 + 1 = 2Y^4 \] (1.1)

are \( (X, Y) = (1, 1) \) and \( (239, 13) \).

Ljunggren’s proof depends upon the study of units of relative norm \(-1\) in a quadratic extension of a quartic field and Skolem’s \(p\)-adic method and is very difficult to follow. Indeed, the late Professor L. J. Mordell used to say: “One cannot imagine a more involved solution (of Eq. (1)). One could only wish for a simpler proof.”

The purpose of this paper is to fulfill Mordell’s desire by giving a simpler
solution of (1.1). This is accomplished by reducing it to a Thue equation and then solving the latter by using some elementary results of Tzanakis and de Weger [6], a deep but easily applicable result of Mignotte and Waldschmidt [5] on lower bounds for linear forms in logarithms of algebraic numbers and the theory of continued fractions. In fact, our solution is conceptually quite simple; anyway, far simpler than Ljunggren's solution. As in any case in which the theory of linear forms in logarithms of algebraic numbers is applied to the solution of a specific Diophantine equation, high precision calculations are required. A remarkable fact in our solution is that, thanks to Mignotte and Waldschmidt's theorem, the decimal digits required in our computations are "very few" compared to analogous situations: 30 decimal digits suffice!

II. DERIVATION OF THE THUE EQUATION

Factorization of Eq. (1.1) over the Gaussian field yields

\[(X + i)(X - i) = 2Y^4,\]

and we have \(2 = -i(1 - i)^2\). Clearly, both \(X + i\) and \(X - i\) must be divisible by \(1 + i\) and none of them by \((1 + i)^2\). Therefore, we have the ideal equation

\[\left(\frac{X + i}{1 + i}\right)\left(\frac{X - i}{1 + i}\right) = (Y)^4,\]

in which the two ideals in the left-hand side are relatively prime. It follows then that

\[(X + i) = i^s(1 + i)(a + bi)^4, \quad s \in \{0, 1, 2, 3\}, \quad (2.1)\]

where \(a, b \in \mathbb{Z}\) and \(Y = \text{Norm}(a + bi) = a^2 + b^2\). Consider now (2.1). If \(s = 0\) or \(2\) then \(\text{Im}\{(1 + i)(a + bi)^4\} = 1\) or \(-1\), respectively. If \(s = 1\) then \((X + i) = -(1 - i)(a + bi)^4\). Replacing \(b\) by \(-b\) (this does not affect \(Y\)) and taking conjugates gives \(\text{Im}\{(1 + i)(a + bi)^4\} = 1\). Finally, if \(s = 3\) then in a completely analogous way we obtain a similar equation with \(-1\) in the right-hand side. We conclude therefore that, in any case, (2.1) implies

\[\pm 1 = \text{Im}\{(1 + i)(a + bi)^4\} = a^4 + 4a^3b - 6a^2b^2 - 4ab^3 + b^4.\]

To simplify the last equation a bit we make the substitution \(a = x - y, b = y\) and we obtain the Thue equation

\[x^4 - 12x^2y^2 + 16xy^3 - 4y^4 = \pm 1.\]
Note that $Y$ is related to $x, y$ by

$$Y = (x - y)^2 + y^2. \quad (2.2)$$

**III. Solution of the Thue Equation**

$$x^4 - 12x^2y^2 + 16xy^3 - 4y^4 = \pm 1. \quad (3.1)$$

In this section we will prove the following:

**Theorem 2.** The only solutions of (3.1) are given by $(x, y) = (1, 3), (1, 0), (1, 1), (5, 2)$.

In view of (2.2), Theorem 2 immediately implies Theorem 1.

**3.1. Preliminaries**

Let $\theta$ be defined by

$$\theta^4 - 12\theta^2 + 16\theta - 4 = 0.$$ 

It is easy to check that $\mathbb{Q}(\theta) = \mathbb{Q}(\rho)$, where

$$\rho = \sqrt{4 + 2\sqrt{2}},$$

and this is a totally real normal (Galois) field, since the four conjugates of $\rho$ are: $\pm \rho$ and $\pm (-3\rho + \frac{1}{2}\rho^3) = \pm \sqrt{4 - 2\sqrt{2}}$. Put

$$\mathbb{K} = \mathbb{Q}(\rho) \quad \text{and} \quad R = \mathbb{Z}[1, \rho, \frac{1}{2}\rho^2, \frac{1}{2}\rho^3].$$

The four conjugates of $\theta$ are

$$\theta^{(1)} = 2 + \rho - \frac{1}{2}\rho^2, \quad \theta^{(2)} = 2 - \rho - \frac{1}{2}\rho^2$$

$$\theta^{(3)} = -2 - 3\rho + \frac{1}{2}\rho^2 + \frac{1}{2}\rho^3, \quad \theta^{(4)} = -2 + 3\rho + \frac{1}{2}\rho^2 - \frac{1}{2}\rho.$$

In view of (3.1), $x - y\theta$ is a unit of the order $R$. Applying Billevic’s method [1] (see [6, Appendix I]) we computed the following triad of fundamental units of $R$:

$$e_1 = -1 - \rho + \rho^2 + \frac{1}{2}\rho^3 = -6 + 21\theta - \frac{5}{2}\theta^2 - 2\theta^3$$

$$e_2 = -5 - 2\rho + 4\rho^2 + \frac{3}{2}\rho^3 = -25 + 79\theta - 9\theta^2 - \frac{15}{2}\theta^3$$

$$e_3 = -7 - 2\rho + \frac{11}{2}\rho^2 + 2\rho^3 = -36 + 111\theta - \frac{25}{2}\theta^2 - \frac{21}{2}\theta^3$$
Thus we obtain
\[ x - y \theta = \pm \epsilon_1 \epsilon_2 \epsilon_3, \quad (a_1, a_2, a_3) \in \mathbb{Z}^3 \] (3.2)

and we put
\[ A = \max\{|a_1|, |a_2|, |a_3|\}. \]

### 3.2. Searching for Solution with Small \(|y|\)

A direct search shows that the only solutions \((x, y)\) of (3.1) with \(|y| \leq 5\) are those listed in the following table, in which the corresponding values of the \(a_i\)'s in (3.2) are also shown.

<table>
<thead>
<tr>
<th>(a_1)</th>
<th>(a_2)</th>
<th>(a_3)</th>
<th>(\pm (x, y))</th>
</tr>
</thead>
<tbody>
<tr>
<td>-1</td>
<td>2</td>
<td>1</td>
<td>(1, 3)</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>(1, 0)</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>-1</td>
<td>(1, 1)</td>
</tr>
<tr>
<td>10</td>
<td>-2</td>
<td>-4</td>
<td>(5, 2)</td>
</tr>
</tbody>
</table>

Now let \((x, y)\) be a solution of (3.1). In view of the above table we may assume that \(|y| \geq 6\). We put
\[ \beta = x - y \theta. \]

According to a simple lemma (see [6, Chap. II, Lemma 1.1]), if \(|y| > Y_1\), then there exists an index \(i_0 \in \{1, 2, 3, 4\}\) such that
\[ |\beta^{(i_0)}| \leq C_1 |y|^{-3}. \] (3.3)

The formulas of \(Y_1\) and \(C_1\) give in our case
\[ Y_1 = 3, \quad C_1 = 1.3604. \]

Let \(d_0, d_1, d_2, \ldots\) be the partial quotients and \(p_1/q_1, p_2/q_2, \ldots\) the convergents in the continued fraction expansion of \(\theta^{(i_0)}\) (for the actual computation of the continued fraction of a real algebraic number see [3] or [7, Chap. 4]). Put in view of the above mentioned lemma, \(x/y = p_n/q_n\) for some \(n = 1, 2, \ldots\). By a well-known result on continued fractions, we have
\[ \frac{1}{(d_{n+1} + 2)q_n^2} < \left| \theta^{(i_0)} - \frac{p_n}{q_n} \right|. \]

Combine this with the first relation (3.3) and the fact that \(|q_n| = |y|\) to obtain
\[ d_{n+1} > \frac{|q_n|^2}{C_1} - 2 \] (3.4)
(note that \(|q_n| = |y| \geq 6\); on the other hand, since \(|q_n|\) grows very fast with \(n\), we expect that (3.4) can be true for only a very few values of \(n\).

We now want to search for solutions of (3.1) in the range \(6 \leq |y| \leq 10^{30}\). For every \(i_0 \in \{1, 2, 3, 4\}\) we check which convergents satisfy (3.4). If some \(p_n/q_n\) is such a convergent, then we check whether \((x, y) = (p_n, q_n)\) is a solution of (3.1).

In this way we checked that no solution exists in the range \(6 \leq |y| \leq 10^{30}\). Therefore, from now on we suppose that

\[
|y| > 10^{30}
\]

and we will prove that (3.1) has no solutions in this range. This will imply that the only solutions of (3.1) are \(+ (x, y) = (1, 3), (1, 0), (1, 1), (5, 2)\).

We note now that from (3.6) we can easily find a useful lower bound for \(A\) as follows (this idea is due to A. Pethö): For every \((i, j) \in \{1, 2, 3\} \times \{1, 3, 4\}\) put

\[
v_j = \begin{cases} 1 & \text{if } |e_i^{(j)}| > 1 \\ -1 & \text{if } |e_i^{(j)}| < 1 \end{cases}
\]

and hence, from any pair \(j_1, j_2 (j_1 \neq j_2)\) we have

\[
| \beta^{(j_1)} - \beta^{(j_2)} | \leq \frac{E_{j_1}^A + E_{j_2}^A}{|\theta^{(j_1)} - \theta^{(j_2)}|}.
\]

Therefore, if we know a lower bound for \(|y|\) (such as in (3.5), for example), then we can find a lower bound for \(A\). Note that \(j_1\) and \(j_2\) can be chosen in such a way that the resulting lower bound for \(A\) can be the best possible. For example, in our case an easy computation shows that

\[
E_1 < 32476.1, \quad E_2 < 28.1422, \quad E_3 < 33.9, \quad E_4 < 34.1
\]

and if we choose \(j_1 = 2, j_2 = 4 (|\theta^{(2)} - \theta^{(4)}| > 2.16478)\) and take into account (3.5), then we easily see from (3.6) that

\[
A \geq 20.
\]

3.3. From (3.2) to an Inequality Involving a Linear Form in Logarithms

Let \(i_0 \in \{1, 2, 3, 4\}\) be as before (we have to check four possibilities). Take any pair \((j, k)\) of indices from the set \{1, 2, 3, 4\} such that the three
indices $i_0, j, k$ be distinct. Consider the $i_0, j, k$-conjugates of the relation 
$\beta = x - y\theta$ and eliminate $x$ and $y$ to obtain

$$\frac{\theta^{(i_0)} - \theta^{(j)}}{\theta^{(i_0)} - \theta^{(k)}} \cdot \frac{\beta^{(k)}}{\beta^{(j)}} - 1 = - \frac{\theta^{(k)} - \theta^{(j)}}{\theta^{(k)} - \theta^{(i_0)}} \cdot \frac{\beta^{(i_0)}}{\beta^{(j)}}.$$  \hfill (3.8)

For simplicity in our notation we put

$$\delta_0 = \frac{\theta^{(i_0)} - \theta^{(j)}}{\theta^{(i_0)} - \theta^{(k)}}, \quad \delta_i = \frac{\varepsilon^{(k)}}{\varepsilon^{(j)}} \quad (i = 1, 2, 3).$$

In view of (3.2), (3.8) becomes

$$\delta_0 \delta_1 \delta_2 \delta_3 - 1 = - \frac{\theta^{(k)} - \theta^{(j)}}{\theta^{(k)} - \theta^{(i_0)}} \cdot \frac{\beta^{(i_0)}}{\beta^{(j)}}.$$  \hfill (3.9)

If we put

$$A = \log |\delta_0 \delta_1 \delta_2 \delta_3|$$

and estimate the right-hand side of (3.9) with the aid of (3.3) we can prove easily (see [6, Chap. II, Lemma 1.2]) that, if $|y| > Y_2^*$ then $0 < |A| < 1.39 C_1 C_3/C_2 |y|^{-4}$. The formulas of $Y_2^*$ and $C_3$ in our case give

$$Y_2^* = 3 \quad \text{and} \quad C_3 = 6.02734$$

and therefore

$$0 < |A| < 13.146 |y|^{-4}. \hfill (3.10)$$

We would like now, to replace the right-hand side of (3.10) by an expression containing $A$ but not $|y|$. We first need some notations. Consider the $4 \times 3$ matrix

$$\delta = (\log |\varepsilon^{(i)}|)_{1 \leq h \leq 3, 1 \leq i \leq 4}.$$ 

For every $j \in \{1, 2, 3, 4\}$ let $\delta_j$ be the matrix which results from $\delta$ if we omit the $j$th row. Then $|\det(\delta_j)|$ is equal to the regulator of the order $R$ (in our case this is equal to 4.8835898...). Let

$$N_0 = \min\{3 \cdot \min_{1 \leq j \leq 4} N[\delta_j^{-1}], \max_{1 \leq j \leq 4} N[\delta_j^{-1}]\},$$

where, in general, for an $m \times n$ matrix $(a_{ij})$, $N[(a_{ij})]$ is the row-norm of the matrix defined by

$$N[(a_{ij})] = \max_{1 \leq i \leq m} \left( \sum_{j=1}^{n} |a_{ij}| \right).$$
Define also

\[ |\bar{\theta}| = \max_{1 \leq i \leq 4} |\theta^{(i)}|. \]

Then, for a solution satisfying \(|y| > 10^5\) we can easily show (see [2, relation (3)]) that

\[ A \leq C_5 \log |y|, \quad C_5 = N_0 \left( 1 + \frac{1}{S} \log_{10} |\bar{\theta}| \right). \] (3.11)

Combine now (3.10) and (3.11) to obtain

\[ 0 < |A| \leq 13.146 \cdot e^{-4A/\varepsilon_5}. \] (3.12)

In our case \(S = 30\) and we computed that \(N_0 \leq 5.475513\), so that

\[ C_5 < 5.58594. \]

Then, in view also of (3.7), (3.12) implies

\[ 0 < |A| < e^{-0.5872777A}, \] (3.13)

and this is the required inequality. Note that (3.13) combined with (3.7) implies, in particular

\[ |A| < 7.93 \cdot 10^{-6}. \] (3.14)

3.4. Explicit Computation of \(A\)

As already noted, once \(i_0\) is chosen we can choose \(j\) and \(k\) arbitrarily \((i_0 \neq j \neq k \neq i_0)\). So, we make the following choices:

If \(i_0 = 3\) or \(4\) we take \(k = 1\) and \(j = 2\). In both cases it is a routine matter to compute that

\[ |\delta_1| = \varepsilon_1^{-2} \varepsilon_3^2, \quad |\delta_2| = \varepsilon_1^{-8} \varepsilon_2^2 \varepsilon_3^4, \quad |\delta_3| = \varepsilon_1^{-4} \varepsilon_3^4. \]

Also, if \(i_0 = 3\) then

\[ \delta_0 = \frac{\theta^{(3)} - \theta^{(2)}}{\theta^{(3)} - \theta^{(1)}} = \frac{-4 - 2\rho + \rho^2 + \frac{1}{2} \rho^3}{-4 - 4\rho + \rho^2 + \frac{1}{2} \rho^3} = -1 + \rho + \frac{1}{2} \rho^2 = \varepsilon_1^{-1} \varepsilon_3 \]

and, analogously, if \(i_0 = 4\) then \(\delta_0 = -\varepsilon_1^{-1} \varepsilon_3\). Thus, if \(i_0 = 3\) or \(4\) then

\[ A = \log(\varepsilon_1^{-1} \varepsilon_3) + a_1 \log(\varepsilon_1^{-2} \varepsilon_3^2) + a_2 \log(\varepsilon_1^{-8} \varepsilon_2^2 \varepsilon_3^4) + a_3 \log(\varepsilon_1^{-4} \varepsilon_3^4) \]

\[ = (1 + 2a_1 + 4a_3) \log(\varepsilon_1^{-1} \varepsilon_3) + 2a_2 \log(\varepsilon_1^{-4} \varepsilon_2^2 \varepsilon_3^4) \]

\[ = (1 + 2a_1 + 2a_2 + 4a_3) \log(\varepsilon_1^{-1} \varepsilon_3) - 2a_2 \log(\varepsilon_1^3 \varepsilon_2^{-1} \varepsilon_3^{-1}). \]
In an analogous way we find that if $i_0 = 1$ or $2$ then
\[
A = (1 + 2a_1 + 4a_3) \log(e_1^{-1}e_2^{-1}e_3^{-1}) + 2a_2 \log(e_1^2e_2^{-1})
= 2a^2 \log(e_1^{-1}e_3) + (1 + 2a_1 + 2a_2 + 4a_3) \log(e_1^3e_2^{-1}e_3^{-1}).
\]
Thus
\[
A = b_1 \log \gamma_1 + b_2 \log \gamma_2,
\]
where
\[
\gamma_1 = e_1^{-1}e_3 = -1 + \rho + \frac{1}{2} \rho^2,
\gamma_2 = e_1^3e_2^{-1}e_3^{-1} = 3 - 3\rho - \frac{1}{2} \rho^2 + \frac{1}{2} \rho^3
\]
and
\[
(b_1, b_2) = (1 + 2a_1 + 2a_2 + 4a_3, -2a_2) \text{ or } (2a_2, 1 + 2a_1 + 2a_2 + 4a_3). 
\tag{3.15}
\]

We now put
\[
B = \max \{|b_1|, |b_2|\},
\]
so that $B \leq 8.05A$ and then, by (3.13),
\[
0 < |A| < e^{-C_6 B}, \quad C_6 = 0.072954. \tag{3.16}
\]

3.5. An Upper Bound for $B$

Up to now, the results and arguments were elementary. At this point we use a really deep theorem of Mignotte and Waldschmidt.

**Theorem [5, Corollary 1.1]**. Let $\alpha_1, \alpha_2$ be two multiplicatively independent algebraic numbers and $b_1, b_2$ two positive rational integers such that $b_1 \log \alpha_1 \neq b_2 \log \alpha_2$ (where $\log \alpha_i$ $(i = 1, 2)$ is an arbitrary but fixed determination of the logarithm). Define $D = D[\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}]$, $B = \max\{|b_1|, |b_2|\}$ and choose two positive real numbers $a_1, a_2$ satisfying
\[
a_j = \max\left\{1, h(\alpha_j) + \log 2, \frac{2e |\log \alpha_j|}{D}\right\} \quad (j = 1, 2)
\]
(where, as usual, $h(\cdot)$ denotes the absolute logarithmic height). Then,
\[
|b_1 \log \alpha_1 - b_2 \log \alpha_2| \geq \exp\{-500D^4a_1a_2(7.5 + \log B)^2\}.
\]

It is easy to check that in our case the above theorem implies
\[
|A| > \exp\{-500 \cdot 4^4 \cdot 2.63 \cdot (7.5 + \log B)^2\}
\]
and this inequality combined with (3.16) gives
\[
B < 4.05 \cdot 10^9.
\]
3.6. Reducing the Upper Bound of $B$

Equation (3.16) is equivalent to

$$\left| \delta - \frac{b_1}{b_2} \right| < \frac{1}{|b_2|} \cdot \frac{1}{|\log \gamma_1|} \cdot e^{-C \delta B},$$

(3.17)

where $\delta = -\log \gamma_2 / \log \gamma_1$ and $B < C = 4.05 \cdot 10^9$. We have

$$\frac{1}{|b_2|} \cdot \frac{e^{-C \delta B}}{|\log \gamma_1|} < \frac{1}{1.61489 |b_2|} \cdot 1.075681^{-B} < \frac{1}{2.1 |b_2|^2},$$

provided that $B \geq 60$. Now let $\tilde{\delta}$ be a rational approximation of $\delta$ such that

$$|\tilde{\delta} - \delta| < \frac{1}{1000C^2}.$$  \hspace{1cm} (3.18)

Then,

$$\left| \tilde{\delta} - \frac{b_1}{b_2} \right| \leq \left| \tilde{\delta} - \delta \right| + \left| \delta - \frac{b_1}{b_2} \right| < \frac{1}{1000C^2} + \frac{1}{2.1 |b_2|^2}$$

$$< \frac{1}{1000 |b_2|^2} + \frac{1}{2.1 |b_2|^2} \leq \frac{1}{2 |b_2|^2},$$

which implies that $b_1/b_2$ is a convergent of the continued fraction expansion of $\tilde{\delta}$. Denote by $d_0, d_1, d_2, \ldots$ the partial quotients and by $p_1/q_1, p_2/q_2, \ldots$ the convergents in the continued fraction expansion of $\delta$. Suppose that $b_1/b_2 = p_n/q_n$. Then,

$$\frac{1}{(d_{n+1}+2) |b_2|^2} \leq \frac{1}{(d_{n+1}+2) |q_n|^2} < \left| \tilde{\delta} - \frac{p_n}{q_n} \right| = \left| \tilde{\delta} - \frac{b_1}{b_2} \right|$$

$$\leq \left| \tilde{\delta} - \delta \right| + \left| \delta - \frac{b_1}{b_2} \right|$$

$$< \frac{1}{1000C^2} + \frac{1}{1.61489 |b_2|} \cdot 1.075681^{-B},$$

from which

$$d_{n+1} + 2 > \left( 10^{-3} + \frac{B}{1.61489} \cdot 1.075681^{-B} \right)^{-1} > 29$$

provided that $B \geq 104$. We computed a rational approximation $\tilde{\delta}$ of $\delta$ up to 30 decimal digits (so that (3.18) is satisfied) and we looked for all
convergents $p_n/q_n$ of $\delta$ with $\max\{p_n, q_n\} \geq 104$ and such that $d_{n+1} \geq 28$. It turned out that no such convergent exists and consequently there are no solutions of (3.17) with $B \geq 104$. If $60 \leq B < 104$ then, by our previous arguments, $b_1/b_2$ is a convergent in the continued fraction expansion of $\delta$, but it is straightforward to check that no convergent $p_i/q_i$ satisfies $60 \leq \max\{|p_i|, |q_i|\} < 104$.

Therefore we are left with the case $B \leq 59$. From (3.17) we see that $b_2/b_1 > 1$; i.e., $B = |b_2|$, and by (3.15) $b_1$, $b_2$ have opposite parities. Since they must satisfy (3.17), we have $B \geq 4$ and then (3.17) implies in particular that

$$0.140343 < |b_2| < 0.359009 |b_2|.$$ (3.19)

We have determined all pairs $(|b_1|, |b_2|)$, satisfying $4 \leq |b_2| \leq 59$ and (3.19), and for each such pair we calculated the corresponding value of $A$. In all cases it turned out that $|A| > 0.00209$, which contradicts (3.14). This contradiction completes the proof of Theorem 2.

REFERENCES


5. M. Mignotte and M. Waldschmidt, Linear forms in two logarithms and Schneider's method, II in "Publication de l'Institut de recherche mathématique avancée, 373/P-206, Strasbourg, 1988."
