MATH. SCAND. 76 (1995), 50–60

ON THE SYSTEM OF DIOPHANTINE EQUATIONS $x^2 - 6y^2 = -5$ and $x = 2z^2 - 1$

MAURICE MIGNOTTE AND ATTILA PETHŐ*

1. Introduction.

The aim of this paper is to prove the following

THEOREM 1. *The system of diophantine equations*

$$x^2 - 6y^2 = -5 \quad \text{and} \quad x = 2z^2 - 1 \tag{1}$$

has only the solutions $(x, y, z) = (16561, \pm 6761, \pm 91); (71, \pm 29, \pm 6); (17, \pm 7, \pm 3); (7, \pm 3, \pm 2); (1, \pm 1, \pm 1)$ *and* $(-1, \pm 1, 0)$.

Our system of equations is a quartic model of an elleptic curve. It has only finitely many integer solutions by a well known result of Siegel [11], moreover they are effectively computable by Baker [1]. It is still interesting to solve it, because the elementary method of J. H. E. Cohn [3], which was further developed by McDaniel and Ribenboim [4] failed. The Siegel-Baker method, which is the combination of algebraic and transcendental number theoretical tools is complicated. It requires detailed knowledge of certain quartic number fields and the solution of several quartic Thue equations.

There are two crucial points in our proof:

1. We prove in Section 2 that under general conditions a diophantine equation $x^2 - dy^2 = m$ with the side condition $x = az^2 - b$ can be "homogenized", i.e. can be transformed to finitely many equations $x^2 - dy^2 = m_i$ with $x = a_i z^2$. In this step we use an idea of Mordell [8].

2. After the "homogenization" we get mixed exponential-polynomial equations in $n, z \in \mathbf{Z}$ of type

$$a\alpha^n - b\beta^n = cz^2. \tag{2}$$

* Research partially supported by Hungarian National Foundation for Scientific Research Grant No 1641/90.

Received September 27, 1993.

This can be solved theoretically by using results of transcendental number theory, see Pethö [9] and Shorey and Stewart [10]. Unfortunately none of these methods is applicable in practice. Generalizing the argument of Mignotte [5] and Mignotte and Pethö [6], [7] we are able to reformulate (2) directly enough into linear forms in logarithms of suitable algebraic numbers to use efficiently the known reduction techniques.

2. Homogenization of the problem.

In the first step toward the proof of our main theorem we use an idea of Mordell [8] to translate (1) into finitely many "homogeneous" equations.

THEOREM 2. *Let* $a, b, d, m \in \mathbb{Z}$, *d square-free. Assume that* $x_0 = -b$, y_0, z_0 *are rational integers which satisfy*

$$x^2 - dy^2 = m \quad \text{and} \quad x = az^2 + b. \tag{3}$$

Then, for all solutions $(x, y, z) \in \mathbb{Z}^3$ *of* (3), *there exist integers* e, f, Δ *with* $(e, f) = 1$, $f^2 - de^2 = \Delta$, *where* Δ *divides* $2dm$, *if d is odd, and* dm, *if d is even,*

$$x = 2ed\frac{fy_0 - ex_0}{\Delta} - x_0,$$

$$y = 2e\frac{dey_0 - fx_0}{\Delta} + y_0;$$

$$az^2 = 2ed\frac{fy_0 - ex_0}{\Delta}.$$

PROOF. Let $(x, y, z) \in \mathbb{Z}^3$ be a solution of (3). If $x = x_0$ then the choice $\Delta = -d$, $f = 0$, $e = 1$ satisfies the assertion. In the sequel we may assume $x \neq x_0$. Let e and f be coprime integers with

$$y - y_0 = \frac{e}{f}(x - x_0).$$

Inserting this formula for y into (3) and using $x_0^2 - dy_0^2 = m$ we get

$$x + x_0 - d\frac{e^2}{f^2}(x - x_0) = 2\frac{e}{f}dy_0,$$

which proves the stated parametrized form of x and y.

As $(e, f) = 1$ and x and y are integers, the numbers $2d\frac{fy_0 - ex_0}{\Delta}$ and $2\frac{dey_0 - fx_0}{\Delta}$ are integers too and Δ is coprime with e. We have further

$$2dx_0\frac{fy_0 - ex_0}{\Delta} + 2dy_0\frac{dey_0 - fx_0}{\Delta} = -\frac{2dem}{\Delta}.$$

Thus Δ divides $2dm$. If d is even then 4 does not divide $f^2 - de^2$ because d is square-free and $(e, f) = 1$. Thus $\Delta \mid dm$ in this case.

Inserting the paremetrized formula for x into the second equation of (3) we get the equation for z and the proof of the theorem is completed.

COROLLARY 1. *All rational integer solutions x, y, z of* (1) *have the form* $x = 12e\frac{f-e}{\Delta} - 1$, $y = 2e\frac{6e-f}{\Delta} + 1$, $z^2 = 6e\frac{f-e}{\Delta}$, *where* $\Delta = 1, -2, 3, -6$ *and*

$$f^2 - 6e^2 = \Delta. \tag{4}$$

PROOF. We apply Theorem 1 with $d = 6$, $m = -5$, $a = 2$, $b = -1$, $(x_0, y_0, z_0) = (1, 1, 1)$. Then there exist $e, f \in \mathbb{Z}$, which satisfy (4) with $\Delta \mid 30$. The only values of Δ with these conditions are $1, -2, 3, -6, -5, 10, -15$ and 30.

Assume that $5 \mid \Delta$ and there exist $e, f \in \mathbb{Z}$ with (4) and

$$6e(f - e) = \Delta z^2. \tag{5}$$

As by (4), 5 does not divide e, we have $5 \mid (f - e)$ by (5). We can rewrite (4) and (5) as follows

$$-\frac{\Delta}{5} = \left(\frac{6e - f}{5}\right)^2 - 6\left(\frac{e - f}{5}\right)^2 \quad \text{and} \quad -6e\frac{f - e}{5} = -\frac{\Delta}{5}z^2.$$

Now put $E_1 = \frac{e - f}{5}$ and $F_1 = \frac{6e - f}{5}$, then $E_1, F_1 \in \mathbb{Z}$ and they satisfy $F_1^2 - 6E_1^2 = -\frac{\Delta}{5}$ and $6E_1(F_1 - E_1) = -\frac{\Delta}{5}z^2$. Thus it is enough to solve (4) and (5) for those values of Δ which are not divisible by 5.

LEMMA 1. *Let $\Delta = 1, -2, 3$ or 6 and $e, f \in \mathbb{Z}$, $e \neq 0$ be a solution of* (4) *and* (5). *Put $\alpha = 5 + 2\sqrt{6}$ and $\beta = 5 - 2\sqrt{6}$. Then there exist $n, w \in \mathbb{Z}$ such that*

$$\frac{e}{2} = \frac{\alpha^{2n+1} - \beta^{2n+1} 4\sqrt{6}}{4\sqrt{6}} = w^2, \qquad \textit{if} \quad \Delta = 1,$$

$$e = \frac{(2 + \sqrt{6})\alpha^{2n} - (2 - \sqrt{6})\beta^{2n}}{2\sqrt{6}} = w^2, \qquad \textit{if} \quad \Delta = -2,$$

$$e = \frac{(3 + \sqrt{6})\alpha^{2n} - (3 - \sqrt{6})\beta^{2n}}{2\sqrt{6}} = w^2 \qquad \textit{if} \quad \Delta = 3, \textit{ and}$$

$$e = \frac{\alpha^{2n} + \beta^{2n}}{2} = w^2, \qquad \text{if} \quad \Delta = -6.$$

PROOF. We way assume $e \geqq 0$ without loss of generality. In the sequel $\square$ denotes an unspecified square.

(i) **Let** $\Delta = 1$. We have e even and f odd, hence $f - e$ odd by (4). Hence $e = 2 \square$ or $e = 6 \square$. By the theory of Pellian equations there exist $m \in \mathbf{Z}$ and $\varepsilon \in \{-1, 1\}$ such that

$$e = \varepsilon \frac{\alpha^m - \beta^m}{2\sqrt{6}}.$$

Let $a_m = \dfrac{\alpha^m - \beta^m}{4\sqrt{6}}$ for $m \in \mathbf{Z}$. As $a_{-m} = -a_m$ we may assume $\varepsilon = 1$ and $m \geqq 0$. Thus we get the equations

$$(6) \qquad a_m = \frac{\alpha^m - \beta^m}{4\sqrt{6}} = \delta_1 \square$$

with $\delta_1 = 1$ or 3. It is easy to see that $3 \mid a_m$ holds iff $3 \mid m$. Let $m = 3k$ and $a'_k = \dfrac{a_{3k}}{3}$. We have $a'_0 = 0$, $a'_1 = 33$ and $a'_{k+2} = 970a'_{k+1} - a'_k$ for $k \geqq 0$.

The sequence $\{a'_k \bmod 5\}_{k=0}^{\infty}$ is periodic, and its period is (0, 3, 0, 2). As $(\frac{2}{5}) = (\frac{3}{5}) = -1$ we see that if (6) holds with $\delta_1 = 3$, then $6 \mid m$. Let $m = 6k$, and for $n \in \mathbf{Z}$ put $b_n = \alpha^n + \beta^n$. Then

$$(7) \qquad a'_{2k} = \frac{a_{6k}}{3} = \frac{a_{3k}}{3} b_{3k}.$$

We have also

$$\left(\frac{b_k}{2}\right)^2 - \left(\frac{\alpha - \beta}{2}\right)^2 a_k^2 = 1,$$

hence $(a_k, b_k) = \begin{cases} 2 & \text{for } k \text{ even} \\ 1 & \text{for } k \text{ odd} \end{cases}$.

Assume that $m > 0$ is the smallest even integer with $a'_m = x^2$. Then, by (7) we have $a'_m b_{3m} = x^2$, hence m must be even, say $m = 2m_1$ and $a'_{2m_1} = x_1^2$, and $b_{6m_1} = 2x_2^2$. Continuing this proces, assume that $2m_k$ is the smallest even divisor of m such that $a'_{2m_k} = 2x_k^2$ with an integer x_k. Then $a'_{2m_k} b_{3m_k} = 2x_k^2$. Let m_k odd. Then a'_{m_k} is odd, and a square, which is a contradiction. Hence m_k is even and either a square or $2\square$ in contradiction with the choice of m and m_k.

This means, that in (6) the case $\delta_1 = 3$ is not possible.

Now we claim, that if a positive even integer m satisfies (6), *then there exists an odd divisor of m, which satisfies* (6) *too.*

Let $m = 2m_1 > 0$ be the smallest even solution of (6). Then as $a_{2m_1} = a_{m_1}b_{m_1} = \square$ and $(a_{m_1}, b_{m_1}) = \begin{cases} 1, & \text{if } m_1 \text{ odd} \\ 2, & \text{if } m_1 \text{ even} \end{cases}$, either m_1 is odd and $a_{m_1} = \square$ or m_1 is even and $a_{m_1} = 2\square$. Continuing this argument we get the proof of the claim and the lemma in the present case.

(ii) **Let** $\Delta = -2$. We have $e = \square$ or $3\square$ by (5) and

$$e = \varepsilon\frac{(2+\sqrt{6})\alpha^m - (2-\sqrt{6})\beta^m}{2\sqrt{6}} = a_m$$

with a suitable $\varepsilon \in \{-1, 1\}$ and $m \in \mathbf{Z}$ by (4). It is easy to see that $a_{-m} = a_{m-1}$, hence we may assume again $\varepsilon = 1$ and $m \geqq 0$. We have $3 \mid a_m$ if and only if $m \equiv 1 \pmod 3$.

Let $b_m = \dfrac{a_{3m+1}}{3}$ for $m \geqq 0$. Then we have $b_0 = 3$, $b_1 = 2907$ and the relation $b_{m+2} = 970b_{m+1} - b_m$ for $m \geqq 0$. The period of the sequence $\{b_m \bmod 5\}_{m=0}^{\infty}$ is $(3, 2, 2, 3)$ which means that $e = 3\square$ is not possible.

If $e = \square$, *then* $f - e = -3\square$ this implies that m has to be even.

(iii) **Let** $\Delta = 3$. In this case e is odd, hence a square by (5). Let

$$a_m = \frac{(3+\sqrt{6})\alpha^m - (3-\sqrt{6})\beta^m}{2\sqrt{6}}$$

for $m \in \mathbf{Z}$. Then $e = a_m$ for a suitable m. Considering a_m modulo 4 we see that $a_m = \square$ is only possible if m is even.

(iv) **Let** $\Delta = -6$. Now $e = \square$ by (5) and

$$e = \sqrt{6}\frac{\alpha^m + \beta^m}{2\sqrt{6}} = \frac{\alpha^m + \beta^m}{2} = a_m$$

for a suitable $m \in \mathbf{Z}$. Considering a_m modulo 3 we see that $a_m = \square$ is only possible if m is even.

3. Application of linear forms.

Let the algebraic number β be a zero of the irreducible polynomial $p(x) = a_n x^n + \ldots + a_0 \in \mathbf{Z}[x]$, where $(a_n, \ldots, a_0) = 1$. Denote $\beta_1 = \beta, \ldots, \beta_n$ the zeros of $p(x)$. The absolute logarithmic height of β is defined by

$$h(\beta) = \frac{1}{n}\log\left(\prod_{i=1}^{n} \max\{1, |\beta_i|\}\right).$$

In this section we will use the following theorem of Waldschmidt [12].

THEOREM 3. *Let* $\alpha_1, \ldots, \alpha_n$ *be non-zero algebraic numbers; for* $i = 1, \ldots, n$, *let* $\log \alpha_i$ *be a determination of the logarithm of* α_i. *Suppose that the numbers* $\log \alpha_1, \ldots, \log \alpha_n$ *are* Q*-linearly independent. Put*

$$D = [\mathbb{Q}(\alpha_1, \ldots, \alpha_n) \colon \mathbb{Q}] \quad \text{and} \quad g = [\mathbb{R}(\log \alpha_1, \ldots, \log \alpha_n) \colon \mathbb{R}].$$

Let $A_1, \ldots, A_n$, A, E *and* f *be positive real numbers such that*

$$\log A_i \geqq h(\alpha_i), \quad (1 \leqq i \leqq n), \quad A = \max\{A_1, \ldots, A_n\}$$

and

$$e \leqq E \leqq \min\left\{A_1^D, \ldots, A_n^D, \frac{nD}{f}\left(\sum_{i=1}^{n} \frac{|\log \alpha_i|}{\log A_i}\right)^{-1}\right\}.$$

Let $b_1, \ldots, b_n$ *be rational integers with* $b_n \neq 0$. *Put*

$$M = \max_{1 \leqq j \leqq n} \left\{\frac{|b_n|}{\log A_j} + \frac{|b_j|}{\log A_n}\right\},$$

$$Z_0 = \max\left\{7 + 3\log n, \frac{g}{D}\log E, \log\left(\frac{D}{\log E}\right)\right\}, \quad G_0 = \max\{4nZ_0; \log M\}$$

and

$$U_0 = \max\{D^2 \log A, D^{n+2} G_0 Z_0 \log A_1 \ldots \log A_n (\log E)^{-n-1}\}.$$

Then the linear form

$$\Lambda = b_1 \log \alpha_1 + \ldots + b_n \log \alpha_n$$

satisfies

$$|\Lambda| \geqq \exp\left\{-1500 g^{-n-2} 2^{2n} n^{3n+5} \left(1 + \frac{g}{f}\right)^n U_0\right\}.$$

Let α be a real quadratic unit and $\mathsf{K} = \mathbb{Q}(\alpha)$. Let γ' denotes the conjugate of $\gamma \in \mathsf{K}$. Take $\beta = \alpha'$ and assume that $\alpha > |\beta|$. Let a, b and $c \in \mathsf{Z}_\mathsf{K}$. Assume that the integers $m, x \geqq 0$ satisfy the equation

$$a\alpha^{2m} - b^2\beta^{2m} = cx^2.$$

Our aim in this section is to prove an upper bound for m.

Let $\mathsf{L} = \mathsf{K}(\sqrt{-c})$ and assume that L is a quadratic extension of K, i.e. $[\mathsf{L} \colon \mathbb{Q}] = 4$. Then our equation implies

$$N_{\mathsf{L}/\mathbb{Q}}(b\beta^m + \sqrt{-c}\,x) = N_{\mathsf{L}/\mathbb{Q}}(a) = A, \tag{8}$$

with some rational integer A.

Choose in $\mathbf{Z}_{\mathsf{L}}$ units $\eta_2, \ldots, \eta_r$; $r = 1, 2$ or 3 such that the group $\mathscr{U}$ generated by $\eta_1 = \alpha, \eta_2, \ldots, \eta_r$ has finite index in the group of units of $\mathbf{Z}_{\mathsf{L}}$. There exists in $\mathbf{Z}_{\mathsf{L}}$ a maximal finite set of, with respect to $\mathscr{U}$, non-associated elements of norm A. This set will be denoted by $\mathscr{A}$. Then there exist for all $m, x \in \mathbf{Z}$ with (8) a $\gamma \in \mathscr{A}$ and $\varepsilon \in \mathscr{U}$ such that

$$b\beta^m + \sqrt{-c}x = \gamma\varepsilon. \tag{9}$$

Let order the conjugates $\mathsf{L}^{(i)}, i = 1, 2, 3, 4$ of L according the following ordering of the conjugates of $\sqrt{-c}$: $\sqrt{-c}, -\sqrt{-c}, \sqrt{-c'}, -\sqrt{-c'}$.

It is easy to see that if $m > m_0$ then

$$\frac{1}{2}\frac{\sqrt{|a|}}{|\gamma^{(i)}|}\alpha^m < |\varepsilon^{(i)}| < \frac{2\sqrt{|a|}}{|\gamma^{(i)}|}\alpha^m \tag{10}$$

for $i = 1, 2$; and if $b' > 0$, which we may assume without loss of generality, then

$$\frac{b'}{2|\gamma^{(3)}|}\alpha^m < |\varepsilon^{(3)}| < 2\frac{b'}{|\gamma^{(3)}|}\alpha^m \tag{11}$$

and

$$\frac{|a'|}{2b'|\gamma^{(4)}|}\alpha^{-3m} < |\varepsilon^{(4)}| < \frac{2|a'|}{b'|\gamma^{(4)}|}\alpha^{-3m} \tag{12}$$

hold. We remark that if $b' < 0$ than only the role of $\varepsilon^{(3)}$ and $\varepsilon^{(4)}$ changes.

The last inequalities imply that if $c' > 0$ then (8) has only finitely many solutions and they are very easy to compute. In fact $\varepsilon^{(3)}$ and $\varepsilon^{(4)}$ are in this case conjugate complex members, hence

$$\frac{b'}{2|\gamma^{(3)}|}\alpha^m < |\varepsilon^{(3)}| = |\varepsilon^{(4)}| < \frac{2|a'|}{b'|\gamma^{(4)}|}\alpha^{-3m},$$

i.e. $m < \frac{1}{4}\log\left|\frac{4a'\gamma^{(3)}}{b'^2\gamma^{(4)}}\right|$.

The situation is more interesting when $c' < 0$. Then $\varepsilon^{(3)}$ and $\varepsilon^{(4)}$ are real numbers and we will use estimations on linear forms in logarithms of algebraic numbers to establish an upper bound for m.

Let first $c > 0$ (and $c' < 0$). Then L has two nonreal and two real conjugates and there exist $u_1, u_2 \in \mathbf{Z}$ with $\varepsilon = \eta_1^{u_1}\eta_2^{u_2}$. The estimations (10) with $i = 2$ and (11) yield

$$|u_1| < \frac{2m\log\alpha\,|\log|\eta_2^{(3)}| - \log|\eta_2^{(2)}||}{R} + c_1$$

and

$$|u_2| < \frac{4m\log^2\alpha}{R} + c_1,$$

where R denotes the regulator of $\mathcal{U}$ and

$$c_1 = 2\log\left(3\overline{|a|\,|b^2|}\overline{\left|\frac{1}{\gamma}\right|}\right)\max\{\log\alpha, \log\overline{|\eta_2|}\}/R.$$

We have

$$\gamma^{(1)}\varepsilon^{(1)} + \gamma^{(2)}\varepsilon^{(2)} = 2b\beta^m,$$

hence

$$\left|1 + \frac{\gamma^{(2)}}{\gamma^{(1)}}\left(\frac{\eta_2^{(2)}}{\eta_2^{(1)}}\right)^{u_2}\right| < \frac{4b}{\sqrt{|a|}}\alpha^{-2m}.$$

If $m > m_0$, then $\frac{4b}{\sqrt{|a|}}\alpha^{-2m} < \frac{1}{2}$ and so

$$|\Lambda_1| = \left|\arg\left(-\frac{\gamma^{(2)}}{\gamma^{(1)}}\right) + u_2\arg\left(\frac{\eta_2^{(2)}}{\eta_2^{(1)}}\right) + u_0\pi\right| < \frac{4.1\,|b|}{\sqrt{|a|}}\alpha^{-2m},$$

with $u_0 \in \mathbf{Z}$ and $-\pi \leqq \arg(z) \leqq \pi$ for every $z \in \mathbf{C}$. The last inequality yields $|u_0| < |u_2| + 2$. We can set in Theorem 3
$n = 3$, $D = 4$, $g = 1$
$log\, A_1 = h\left(\frac{\gamma^{(2)}}{\gamma^{(1)}}\right)$, $\log A_2 = h\left(\frac{\eta_2^{(2)}}{\eta_2^{(1)}}\right)$, $\log A_3 = \frac{1}{2}$
$E = e$, $M = 4(|u_2| + 1)$
$Z_0 = 7 + 3\log 3$, $G_0 = \log M$
$U_0 = 4^5(7 + 3\log 3)\frac{1}{2}h\left(\frac{\gamma^{(2)}}{\gamma^{(1)}}\right)h\left(\frac{\eta_2^{(2)}}{\eta_2^{(1)}}\right)\log M,$
and get

$$|\Lambda_1| > \exp\left\{-2\cdot 10^6 h\left(\frac{\gamma^{(2)}}{\gamma^{(1)}}\right)h\left(\frac{\eta_2^{(2)}}{\eta_2^{(1)}}\right)\log M\right\}.$$

Comparing the lower and upper bounds for $|\Lambda_1|$ we conclude

$$2m\log\alpha - \log\frac{4.1\,|b|}{\sqrt{|a|}} < 2\cdot 10^{16}h\left(\frac{\gamma^{(2)}}{\gamma^{(1)}}\right)h\left(\frac{\eta_2^{(2)}}{\eta_2^{(1)}}\right) \log\left(\frac{16m\log^2\alpha}{R} + 4c_1 + 4\right). \tag{13}$$

This inequality yields an upper bound for m, which we shall only compute knowing the actual values of the accouring parameters.

Let now $c < 0$ (and $c' < 0$). Then all conjugates of L are real and there exist $u_1, u_2, u_3 \in \mathbf{Z}$ with $\varepsilon = \eta_1^{u_1}\eta_2^{u_2}\eta_3^{u_3}$. We recall that $\eta_1 = \alpha$. The estimations (10) with $i = 1,2$ and (11) yield

$$|u_i| < \frac{4m\log^2\alpha\log h}{R} + c_2, \quad i = 2,3$$

with $c_2 = 3\sqrt{3}\log(3\,\overline{|a|}\,\overline{|b^2|}\,\overline{|\tfrac{1}{\gamma}|})\log\alpha\log\overline{|\eta_2|}\log\overline{|\eta_3|}/R$ and $h = \max\{\overline{|\eta_2|}, \overline{|\eta_3|}\}$.

Similarly to the above case, but working with real instead of complex logarithms we get

$$|\Lambda_2| = \left|\log\left|\frac{\gamma^{(2)}}{\gamma^{(1)}}\right| + u_2\log\left|\frac{\eta_2^{(2)}}{\eta_2^{(1)}}\right| + u_3\log\left|\frac{\eta_3^{(2)}}{\eta_3^{(1)}}\right|\right| < \frac{5.6\,|b|}{\sqrt{|a|}}\alpha^{-2m}.$$

The parameters in the application of Waldschmidt's theorem are the same as earlier except that $\log A_3 = h\left(\frac{\eta_3^{(2)}}{\eta_3^{(1)}}\right)$, $M = 2\,|u_2|$ and $U_0 = 4^5(7 + 3\log 3)$ $h\left(\frac{\gamma^{(2)}}{\gamma^{(1)}}\right)h\left(\frac{\eta_2^{(2)}}{\eta_2^{(1)}}\right)h\left(\frac{\eta_3^{(2)}}{\eta_3^{(1)}}\right)\log M$. Hence Theorem 3 implies

$$(14) \qquad 2m\log\alpha - \log\frac{5.6\,|b|}{\sqrt{|a|}} < 4.10^{16}h\left(\frac{\gamma^{(2)}}{\gamma^{(1)}}\right)h\left(\frac{\eta_2^{(2)}}{\eta_2^{(1)}}\right)h\left(\frac{\eta_3^{(2)}}{\eta_3^{(1)}}\right) \log\left(\frac{8m\log^2\alpha\log h}{R} + 2c_2\right).$$

REMARK 1. The argument of this section can be easily generalized to the case when α is not a unit. Then we have to apply lower bounds for linear forms in p-adic logarithms.

4. Proof of Theorem 1.

In table 1, we are listing the data necessary for the application of the method of section 3 to the equations given in Lemma 1. We are using the notations $\alpha = 5 + 2\sqrt{6}$, $\beta = 5 - 2\sqrt{6}$ and $\vartheta = \sqrt{-c}$.

Δ	a	b	c	r	η_2	η_3	γ
1	1	β^2	$-12 + 5\sqrt{6}$	2	$5 - 2\vartheta - 2\sqrt{6}$		1
-2	$-\alpha$	1	$-(6 + 2\sqrt{6})$	3	$1 + \vartheta$	$2 + \vartheta - \frac{\vartheta}{2}$	1
3	α	1	$4 + 2\sqrt{6}$	2	$1 + \vartheta$		1
-6	-1	1	-2	3	$\sqrt{2 + \sqrt{3}}$	$\frac{(1 + \sqrt{3})(2 + \sqrt{2})}{2}$	$\sqrt{2} + \sqrt{3}$

Table 1.

We are giving the details of the proof only for the case $\Delta = 1$, when our equation has by Lemma 1 the form

$$\alpha^{2m} - \beta^2\beta^{2m} = 4\beta\sqrt{6}w^2 = 4(5\sqrt{6} - 12)w^2.$$

It is easy to see that it has only one solution $(m, w) = (0, 1)$ in the range $0 \leqq m \leqq 10$. If $m > 10$ then (10) is obviously true. Thus we may assume in the sequel $m > 10$. The algebraic number field. $\mathsf{L} = \mathbb{Q}(\sqrt{6}, \sqrt{12 - 5\sqrt{6}})$, has two real and two non-real conjugates. Its regulator is $R = 6.83836\ldots$ and we get

$$|u_2| < 3.07398m + 8.95847.$$

As $\gamma = 1$ there are only two summands in Λ_1, actually it has the form

$$\Lambda_1 = \left| u_2 \arg\left(\frac{5 - 2\sqrt{6} + 2\sqrt{12 - 5\sqrt{6}}}{5 - 2\sqrt{6} - 2\sqrt{12 - 5\sqrt{6}}} \right) + u_0\pi \right| < 0.042\alpha^{-2m}.$$

As we proved, there are generaly three logarithms in Λ_1, but in the actual example we have only two, therefore in the, to (14) analogous inequality we get a much better constant. More precisely we have

$$4.58486m + 3.17387 < 6.81595 \cdot 10^{11} \log(12.4m + 40),$$

which implies $m < 5 \cdot 10^{12}$ and $|u_2| < 1.55 \cdot 10^{13}$. Dividing the inequality for Λ_1 by $u_2\pi$ we see that, as $m > 10$, u_0/u_2 is a convergent of

$$\arg\left(\frac{\eta_2^{(2)}}{\eta_2^{(1)}} \right) \Big/ \pi = \delta$$

$$= 0.935578452737003090881416003671806172524452553121 55\ldots$$

The denominator of the 20th convergent of δ, $\dfrac{51706546491839}{55266927472061}$, is larger then 10^{14}, hence

$$|u_0 - u_2\vartheta| \geqq |51706546491839 - 55266927472061\vartheta| > 1.6132 \cdot 10^{-13},$$

which implies $m \leqq 5$. Thus our equation has only the trivial solution.

The proof Theorem 1 is similar in the other cases. We may always set $m_0 = 10$ and the upper bound for m computed from (13) or (14) depending on the value of r is in all cases less then 10^{20}. To fill the gap between 10 and 10^{20} we can use the above reduction procedure, originally due to Baker and Davenport [2].

The solution $(-1, \pm 1, 0)$ of (1) comes from the equation $\dfrac{\alpha^m - \beta^m}{4\sqrt{6}} = w^2$ for even exponents, and is $n = w = e = 0$. The other solutions given in Theorem

1 follow from the solutions of the equations in Lemma 1, which are $(\Delta, n, e) = (1,0,2); (-2,0,1); (3,0,1); (-6,0,1)$ and $(-6, 1, 49)$.

REFERENCES

1. A. Baker, *Bounds for the solutions of the hyperelliptic equation*, Math. Proc. Cambridge Philos. Soc. 65 (1969), 439–444.
2. A. Baker and H. Davenport, *The equations* $3x^2 - 2 = y^2$ *and* $8x^2 - 7 = z^2$, Quart. J. Math. Oxford 20 (1969), 129–137.
3. J. H. E. Cohn, *Squares in some recurrent sequences*, Pacific J. Math. 41 (1972), 631–646.
4. W. L. McDaniel and P. Ribenboim, *Squares and double-squares in Lucas sequences*, C.R. Math. Rep. Acad. Sci. Canada 14 (1992), 104–108.
5. M. Mignotte, *Su una classe di equazioni del tipo* $a^n + b^n = z^2$, Rend. Sem. Fac. Sci. Univ. Cagliari 62 (1992), fasc. 1.
6. M. Mignotte et A. Pethö, *Sur les carrés dans certaines suites de Lucas*, J. Théorie des Nombres de Bordeaux 5 (1993), 333–341.
7. M. Mignotte és A. Pethö, *Az* $a^n + b^n = z^3$ *diofantoszi egyenletről*, Mat. Lapok, to appear.
8. L. J. Mordell, *Diophantine Equations*, Academic Press, 1969.
9. A. Pethö, *Perfect powers in second orer linear recurrences*, J. Number Theory 15 (1983), 117–127.
10. T. N. Shorey and C. L. Stewart, *On the Diophantine equation* $ax^{2t} + bx^ty + cy^2 = d$ *and pure powers in recurrences*, Math. Scand. 52 (1983), 24–36.
11. C. L. Siegel, *The integral solution of the equation* $y^2 = ax^n + bx^{n-1} + \ldots + k$, J. London Math. Soc. 1 (1926), 66–68.
12. M. Waldschmidt, *Minorations de combinaisons linéaires de logarithmes de nombres algébriques*, Canad. J. Math. 45 (1993), 176–224.

DÉPARTMENT DE MATHEMATIQUE ET INFORMATIQUE
UNIVERSITÉ LOUIS PASTEUR
RUE RENÉ DESCARTES 7
STRASBOURG
FRANCE

LABORATORY OF COMPUTER SCIENCE
UNIVERSITY MEDICAL SCHOOL DEBRECEN
NAGYERDEI KRT. 98
H-4028 DEBRECEN
HUNGARY