MATH. SCAND. 21 (1967), 149–158

ON THE DIOPHANTINE EQUATION $Ax^4 - By^2 = C$ $(C = 1, 4)$

W. LJUNGGREN

Introduction,

In a previous paper [7] I have given a method for obtaining an upper bound for the number of solutions in rational integers x, y of any equation of the form $x^2 + 1 = Dy^4$. In case $D = 2$ the complete solution was found. The same method also works for the more general equation $Ax^4 - By^2 = 1$, B not a square. Unfortunately, the procedure involves large computational work, so it has been desirable to search for simpler methods. For the special equation $3x^4 - 2y^2 = 1$ such a method was found by R. T. Bumby [2]. However, his paper contains also a good deal of calculation, and the method used seems not to be suitable for generalization to all equations $Ax^4 - By^2 = 1$.

In a recent paper J. H. E. Cohn [3] has given an elementary treatment of diophantine equations of the types $y^2 - Dx^4 = \pm C$ and $x^4 - Dy^2 = \pm C$ where $C = 1$ or $C = 4$. He considers only values of D for which the equation $x^2 - Dy^2 = -4$ has a solution (x, y), when both x and y are odd rational integers. For this case he obtained the complete solution, and the method of determining possible non-trivial solutions is very simple. However, apart from the equation $x^2 + 1 = Dy^4$ all these equations were already solved by the author in papers [4]–[6], [8]–[10], and *without any restriction on D*. In [6] and [9] the author also solved in an elementary way the equation $x^2 + 1 = Dy^4$, imposing on D the condition mentioned above. However, his method for finding the only possible solution x, y was quite complicated.

Cohn's method has certain similarities with that used by the author in [9]. Operating with Jacobi's symbol instead of that of Legendre, he obtains his simple procedure for determining possible solutions.

In the following we assume that the odd positive integers A and B have the property that the diophantine equation

$$Az_1^2 - Bz_2^2 = 4 \tag{1}$$

has solutions in *odd*, positive integers z_1 and z_2. The solvability of (1) can always be decided in a simple way. For this well-known fact consult

Received February 10, 1967.

for instance Arndt [1] or Nagell [11]. By the way we note that $AB \equiv 5 \pmod 8$ is a necessary but not sufficient condition.

Let (a,b) be the least solution of (1) in odd, positive integers. Then all solutions of (1) in positive integers z_1, z_2 are given by the formula

$$\tfrac{1}{2}(z_1 A^{\frac{1}{2}} + z_2 B^{\frac{1}{2}}) = (\tfrac{1}{2}(aA^{\frac{1}{2}} + bB^{\frac{1}{2}}))^n , \tag{2}$$

where n is a positive integer in the case $A = 1$ and an odd positive integer otherwise.

Combining my method in [10] with an idea from that of Cohn (see [3]), we obtain the following two theorems:

THEOREM 1. *The diophantine equation*

$$Ax^4 - By^2 = 4 \tag{3}$$

has at most two solutions in positive integers x,y. If $a = h^2$ and $Aa^2 - 3 = k^2$, there are two solutions, namely $x = h$ and $x = hk$. If $a = h^2$ and $Aa^2 - 3 \neq k^2$, there is one solution $x = h$. If $a = 5h^2$ and $A^2a^4 - 5Aa^2 + 5 = 5k^2$, there is one solution $x = 5hk$.

THEOREM 2. *Under the given condition on A and B, the diophantine equation*

$$Ax^4 - By^2 = 1 \tag{4}$$

has at most one solution in positive integers x,y. If $x = x_1$, $y = y_1$ is a solution, then

$$x_1 A^{\frac{1}{2}} + y_1 B^{\frac{1}{2}} = (\tfrac{1}{2}(aA^{\frac{1}{2}} + bB^{\frac{1}{2}}))^3 .$$

1. Notations.

Let $\varepsilon > 1$ be any unit with norm $+1$ in the algebraic number field $Q(D^{\frac{1}{2}})$, $D > 0$, and let further ε' denote the conjugate unit, such that $\varepsilon\varepsilon' = 1$. We introduce the following notations, where n, m, p and t denote natural numbers, n odd:

$$H_m(\varepsilon) = \frac{\varepsilon^m - \varepsilon'^m}{\varepsilon - \varepsilon'} = H_m ,$$

$$P_n(\varepsilon) = \varepsilon'^{\frac{1}{2}(n-1)} \frac{\varepsilon^n - 1}{\varepsilon - 1} = H_{\frac{1}{2}(n+1)}(\varepsilon) + H_{\frac{1}{2}(n-1)}(\varepsilon) ,$$

$$Q_n(\varepsilon) = \varepsilon'^{\frac{1}{2}(n-1)} \frac{\varepsilon^n + 1}{\varepsilon + 1} = H_{\frac{1}{2}(n+1)}(\varepsilon) - H_{\frac{1}{2}(n-1)}(\varepsilon) ,$$

$$R_p = \varepsilon^{2^p} + \varepsilon'^{2^p} .$$

Here we have

$$H_n(\varepsilon) = P_n(\varepsilon)\, Q_n(\varepsilon)\,.$$

From the well-known formula [12, p. 154]

$$x^n+y^n = \sum_{i=0}^{\frac{1}{2}(n-1)} (-1)^i \frac{n}{n-i}\binom{n-i}{i}(x+y)^{n-2i}(xy)^i\,,$$

we obtain for t odd, putting $x=\varepsilon^{\frac{1}{2}t}$, $y=\varepsilon'^{\frac{1}{2}t}$,

$$(5)\qquad Q_n(\varepsilon^t) = \sum_{i=0}^{\frac{1}{2}(n-1)} (-1)^i \frac{n}{n-i}\binom{n-i}{i}(\varepsilon+\varepsilon'+2)^{\frac{1}{2}(n-1)-i}\left(Q_t^2(\varepsilon)\right)^{\frac{1}{2}(n-1)-i}\,.$$

Especially for $t=1$, since $Q_1(\varepsilon)=1$,

$$(6)\qquad Q_n(\varepsilon) = \sum_{i=0}^{\frac{1}{2}(n-1)} (-1)^i \frac{n}{n-i}\binom{n-i}{i}(\varepsilon+\varepsilon'+2)^{\frac{1}{2}(n-1)-i}\,.$$

2. Proof of some lemmas.

LEMMA 1. $H_m \equiv H_{m-6} \pmod 8$ *if* $\varepsilon+\varepsilon'$ *is odd.*

PROOF. $H_m - H_{m-6} = (\varepsilon^{m-3}+\varepsilon'^{m-3})H_3 \equiv 0 \pmod 8$, since

$$H_3 = \varepsilon^2+\varepsilon'^2+1 = (\varepsilon+\varepsilon')^2-1 \equiv 0 \pmod 8\,.$$

LEMMA 2. $Q_n(\varepsilon)\equiv 1 \pmod 8$ *if* $n\equiv \pm 1 \pmod{12}$ *and* $\varepsilon+\varepsilon'$ *odd.* $Q_n(\varepsilon)\equiv -(\varepsilon+\varepsilon') \pmod 8$ *if* $n\equiv \pm 5 \pmod{12}$ *and* $\varepsilon+\varepsilon'$ *odd.*

PROOF. If $n=12k+1$, we get $Q_n(\varepsilon)=H_{6k+1}-H_{6k}\equiv H_1\equiv 1 \pmod 8$, on account of lemma 1. If $n=12k+5$, we find $Q_n(\varepsilon)=H_{6k+3}-H_{6k+2}\equiv H_3-H_2\equiv -(\varepsilon+\varepsilon') \pmod 8$. The remaining two congruences can be proved in the same way.

LEMMA 3. $H_m \not\equiv 0 \pmod 3$ *if* $(m,6)=1$.

PROOF. This follows immediately from the congruences $H_m\equiv H_{m-6} \pmod 3$ if $(\varepsilon+\varepsilon',3)=1$ and $H_m\equiv -H_{m-2} \pmod 3$ if $(\varepsilon+\varepsilon',3)=3$.

LEMMA 4. $R_p\equiv 2 \pmod n$ *if* $\varepsilon+\varepsilon'+2\equiv 0 \pmod n$, $p\geqq 1$.

PROOF. We proceed by induction. We have

$$\varepsilon^2+\varepsilon'^2-2 = (\varepsilon+\varepsilon')^2-4 = (\varepsilon+\varepsilon'+2)(\varepsilon+\varepsilon'-2) \equiv 0 \pmod n\,.$$

Assuming $R_p\equiv 2 \pmod n$, we obtain by squaring

$$R_p{}^2 \equiv R_{p+1}+2 \equiv 4 \pmod n, \text{ or } R_{p+1} \equiv 2 \pmod n\,.$$

LEMMA 5.

$$R_p \equiv \varepsilon+\varepsilon'-1 \pmod{Q_5(\varepsilon)} \quad \textit{if } p \textit{ is odd},$$
$$R_p = -(\varepsilon+\varepsilon') \pmod{Q_5(\varepsilon)} \quad \textit{if } p \textit{ is even}.$$

PROOF. $Q_5(\varepsilon)=(\varepsilon+\varepsilon')^2-(\varepsilon+\varepsilon')-1$, which gives

$$\varepsilon^2+\varepsilon'^2 = (\varepsilon+\varepsilon')^2-2 \equiv (\varepsilon+\varepsilon')-1 \pmod{Q_5(\varepsilon)}.$$

Hence

$$\varepsilon^4+\varepsilon'^4 = (\varepsilon^2+\varepsilon'^2)^2-2 \equiv (\varepsilon+\varepsilon')^2-2(\varepsilon+\varepsilon')-1 \equiv -(\varepsilon+\varepsilon') \pmod{Q_5(\varepsilon)}.$$

If $R_p\equiv(\varepsilon+\varepsilon')-1 \pmod{Q_5(\varepsilon)}$ we get $R_{p+1}\equiv-(\varepsilon+\varepsilon') \pmod{Q_5(\varepsilon)}$ and $R_{p+2}\equiv(\varepsilon+\varepsilon')-1 \pmod{Q_5(\varepsilon)}$.

LEMMA 6. *None of the equations* $Q_9(\varepsilon)=z^2$, $Q_9(\varepsilon)=3z^2$ and $Q_9(\varepsilon)=2z^2$ *have solutions in positive integers* $\varepsilon+\varepsilon'$ *and* z.

PROOF. We have $Q_9(\varepsilon)=Q_3(\varepsilon)Q_3(\varepsilon^3)=u(u^3+3u^2-3)$, where $u=\varepsilon+\varepsilon'-1$. The equation $Q_9(\varepsilon)=z^2$ implies, either

$$u = 3h^2, \quad u^3+3u^2-3 = 3k^2 \tag{7}$$

or

$$u = h^2, \quad u^3+3u^2-3 = k^2 \tag{8}$$

The last equation in (7) is impossible mod 9, and the last equation in (8) gives

$$h^6+3h^4-3 = k^2, \tag{9}$$

which is impossible for $h\geqq 3$, since it is easy to check that

$$2h^3+3h > 2k > 2h^3+3h-1.$$

Equation (9) is impossible also for $h=2$, but is satisfied for $h=1$, which gives $\varepsilon+\varepsilon'=2$, but this value must be excluded.

The equation $Q_9(\varepsilon)=3z^2$ implies

$$u = 9h^2, \quad u^3+3u^2-3 = 3k^2,$$

from which we conclude that $3^5h^6+3^4h^4-1=k^2$, impossible mod 3.

The equation

$$u(u^3+3u^2-3) = 2z^2$$

implies, since $u\equiv 0 \pmod 3$ is impossible,

$$u = 2h^2, \quad u^3+3u^2-3 = k^2.$$

From $8h^6+12h^4-3=k^2$, we deduce

$$2(2h^2+1)(2h^4+2h^2-1) = k^2+1,$$

which is impossible since $2h^4+2h^2-1\equiv -1 \pmod 4$.

LEMMA 7. *The equation* $Q_n(\varepsilon)=nz^2$ *with* $\varepsilon+\varepsilon'+2\equiv 0 \pmod{n^2}$ *has no solution in integers* $\varepsilon+\varepsilon'$ *and* z *provided. that the odd squarefree integer* n *contains a primefactor* $q\equiv 3 \pmod 4$.

PROOF. Putting $n=mq$, $(m,q)=1$, we find

$$Q_n(\varepsilon) = Q_m(\varepsilon)\, Q_q(\varepsilon^m) = mqz^2 .$$

From (5) we derive that the greatest common divisor of $Q_m(\varepsilon)$ and $Q_q(\varepsilon^m)$ divides q. Further it follows from (6) that $Q_m(\varepsilon)\not\equiv 0 \pmod q$ while $Q_q(\varepsilon^m)\equiv -q \pmod{q^2}$. Hence

$$Q_m(\varepsilon) = mh_1^2, \qquad Q_q(\varepsilon^m) = qh_2^2 ,$$

the last equation giving $h_2^2+1\equiv 0 \pmod q$, which is impossible.

LEMMA 8. *The equation* $Q_n(\varepsilon)=nz^2$ *with* $\varepsilon+\varepsilon'+2\equiv 0 \pmod{n^2}$ *has no solution in integers* $\varepsilon+\varepsilon'$ *and* z, *provided that the odd squarefree integer* $n\not\equiv 5 \pmod{24}$ *and* $\varepsilon+\varepsilon'$ *is odd.*

PROOF. According to lemma 7 we assume $n\equiv 1 \pmod 4$. At first we prove that $n=8t+1$, t an integer, is impossible. We find

$$Q_n(\varepsilon)+1 = (\varepsilon^{2t}+\varepsilon'^{2t})(H_{2t+1}-H_{2t}) .$$

Putting $2t=2^p t_1$, $(t_1,2)=1$, $p\geqq 1$, we get that R_p is a divisor of nz^2+1, and consequently $(-n/R_p)=1$. Now it is easily found that $R_p\equiv -1 \pmod 8$, and from lemma 4 we have $R_p\equiv 2 \pmod n$. Using these facts, we get

$$1 = \left(\frac{-n}{R_p}\right) = -\left(\frac{n}{R_p}\right) = -\left(\frac{R_p}{n}\right) = -\left(\frac{2}{n}\right) = -1 ,$$

a contradiction. Putting $n=8r+5$, we distinguish between the two cases $r\equiv 2 \pmod 3$ and $r\equiv 1 \pmod 3$. If $r\equiv 2 \pmod 3$, we get $n\equiv 0 \pmod 3$, which must be excluded according to lemma 6. If $r\equiv 1 \pmod 3$, we get $n\equiv 1 \pmod{12}$ and therefore $nz^2\equiv 1 \pmod 8$, on account of lemma 2 if $\varepsilon+\varepsilon'$ is odd, i.e. $n\equiv 1 \pmod 8$, a contradiction.

3. Proof of two propositions.

PROPOSITION 1. $Q_n(\varepsilon)$ *is not a square for* $n>3$ if $\varepsilon+\varepsilon'$ *is an odd natural number.*

PROOF. A proof by elementary means is given in my paper [10]. However, for the sake of completeness, I add a proof. It is sufficient to assume $n=4t+3$ since the case $n=4t+1$ can be handled in exactly the same manner. From

(10) $$Q_n(\varepsilon) = z^2$$

we conclude

$$z^2+1 = (\varepsilon^{t+1}+\varepsilon'^{t+1})(H_{t+1}(\varepsilon)-H_t(\varepsilon)) .$$

If t is odd, we put $t+1=2^p t_1$, $(t_1 2)=1$, $p\geqq 1$, which gives $z^2+1\equiv 0 \pmod{R_p}$. This is impossible since $R_p\equiv -1 \pmod 8$. If t is even and $t\equiv 2 \pmod 3$, then

$$\frac{\varepsilon^3+\varepsilon^3}{\varepsilon+\varepsilon'} = (\varepsilon+\varepsilon')^2-3 \equiv -2 \pmod 8$$

is a divisor of z^2+1, which is also impossible. If t is even and $t\equiv 1 \pmod 3$ then both $\varepsilon+\varepsilon'$ and $\varepsilon+\varepsilon'-1$ are divisors of z^2+1, again impossible, since $\varepsilon+\varepsilon'\equiv 1 \pmod 4$ would imply $\varepsilon+\varepsilon'-1\equiv 0 \pmod 4$. Consequently $t\equiv 0 \pmod 3$ i.e. $n\equiv 0 \pmod 3$. In the same way we find if $n>1$ and $n\equiv 1 \pmod 4$ that $n\equiv 0 \pmod 3$.

REMARK. By substituting $\varepsilon=-\varrho$, $\varepsilon'=-\varrho^2$, where $\varrho^2+\varrho+1=0$, it is easily shown that $\varepsilon+\varepsilon'-1$ divides $H_{t+1}(\varepsilon)-H_t(\varepsilon)$.

According to lemma 6 it now only remains to discuss the case $n=3m$, where $(m,3)=1$. Equation (10) can be written

$$Q_m(\varepsilon)\, Q_3(\varepsilon^m) = z^2 .$$

The greatest common divisor of $Q_m(\varepsilon)$ and $Q_3(\varepsilon^m)$ divides 3 (formula (5)), $Q_m(\varepsilon)$ however is not divisible by 3, the last fact following from lemma 3, since $Q_m(\varepsilon)$ is a divisor of $H_m(\varepsilon)$. Hence

$$Q_m(\varepsilon) = z_1^2, \qquad Q_3(\varepsilon^m) = z_2^2 .$$

The first part of the proof shows that $m=1$, i.e. $n=3$ is a possible solution.

PROPOSITION 2. *The equation $Q_n(\varepsilon)=nz^2$ with $\varepsilon+\varepsilon'+2\equiv 0 \pmod{n^2}$ has no solution in integers $\varepsilon+\varepsilon'$ and z if $\varepsilon+\varepsilon'$ is odd and $n>5$ and squarefree.*

PROOF. Lemmas 7 and 8 show that it is sufficient to treat the case $n=24k+5$. We find

$$Q_n(\varepsilon)+Q_5(\varepsilon) = (\varepsilon^{6k}+\varepsilon'^{6k})(H_{6k+3}-H_{6k+2}) . \tag{11}$$

Putting $k=2^{p-1}k_1$, $(k_1,2)=1$, $p\geqq 1$, we have that R_p is a divisor of the right-hand side of (11). From (11) now follows

$$1 = \left(\frac{-nQ_5}{R_p}\right) = -\left(\frac{nQ_5}{R_p}\right) = -\left(\frac{n}{R_p}\right)\left(\frac{Q_5}{R_p}\right) = -\left(\frac{R_p}{n}\right)\left(\frac{Q_5}{R_p}\right)$$

$$= -\left(\frac{2}{n}\right)\left(\frac{Q_5}{R_p}\right) = \left(\frac{Q_5}{R_p}\right).$$

By lemma 2 it follows that $Q_n(\varepsilon)\equiv-(\varepsilon+\varepsilon')\pmod 8$, and therefore $\varepsilon+\varepsilon'\equiv 3\pmod 8$ and $Q_5\equiv 5\pmod 8$. Then we derive

$$1=\left(\frac{Q_5}{R_p}\right)=\left(\frac{R_p}{Q_5}\right)=\left(\frac{\varepsilon+\varepsilon'-1}{Q_5}\right)\quad\text{for } p \text{ odd}$$

and

$$1=\left(\frac{-(\varepsilon+\varepsilon')}{Q_5}\right)=\left(\frac{\varepsilon+\varepsilon'}{Q_5}\right)=\left(\frac{Q_5}{\varepsilon+\varepsilon'}\right)=\left(\frac{-1}{\varepsilon+\varepsilon'}\right)=-1\quad\text{for } p \text{ even},$$

a contradiction. Putting in the first case $\varepsilon+\varepsilon'-1=2T$, $T\equiv 1\pmod 4$, we find further

$$1=\left(\frac{2}{Q_5}\right)\left(\frac{T}{Q_5}\right)=-\left(\frac{T}{Q_5}\right)=-\left(\frac{Q_5}{T}\right)=-\left(\frac{-1}{T}\right)=-1,$$

and our proposition is proved.

4. Proof of theorems 1 and 2.

All solutions of $Ax^4-By^2=C$, $C=1,4$, in positive integers x,y are given by

$$(x^2A^{\frac12}+yB^{\frac12})C^{-\frac12}=(\tfrac12(aA^{\frac12}+bB^{\frac12}))^n, \tag{12}$$

where n is an *odd*, positive number.

This follows immediately from (2) if we can prove that (2) is true also if $A=1$. It is well known that $C=1$ implies $n\equiv 0\pmod 3$. But an equation

$$x^2+yB^{\frac12}=(\tfrac12(a+bB^{\frac12}))^{6m}=\lambda^6$$

results in

$$2x^2=\lambda^6+\lambda'^6,\qquad \lambda\lambda'=1,$$

or, putting $\lambda+\lambda'=t$,

$$2x^2=(t^2-2)((t^2-2)^2-3). \tag{13}$$

From (13) we easily derive

$$t^2-2=2h^2,\qquad 4h^4-3=k^2$$

with the only solution $t=2$, which is clearly impossible.

If $C=4$, an equation

$$\tfrac12(x^2+yB^{\frac12})=\lambda_1^2$$

gives $x^2=\lambda_1^2+\lambda_1'^2=(\lambda_1+\lambda_1')^2-2=t_1^2-2$, which is also impossible. With the notation

$$\varepsilon=(\tfrac12(aA^{\frac12}+bB^{\frac12}))^2=\tfrac12(Aa^2-2+ab(AB)^{\frac12})$$

we get from (12)

$$2C^{-\frac{1}{2}}x^2 = aQ_n(\varepsilon), \qquad \varepsilon+\varepsilon'+2 = Aa^2 . \tag{14}$$

At first we shall prove theorem 1. The equation (14) can then be written

$$x^2 = aQ_n(\varepsilon) . \tag{15}$$

Putting $a=rh^2$, r without any squared factor >1, we deduce from (15)

$$Q_n(\varepsilon) = rk^2 . \tag{16}$$

On account of (6) it is easily seen that r is a divisor of n, say $n=rn_1$. If $r=1$, we get $n=1$ or $n=3$ (proposition 1). If $r>1$, we rewrite (16) in the form

$$Q_{n_1}(\varepsilon)\,Q_r(\varepsilon^{n_1}) = rk^2$$

yielding

$$Q_{n_1}(\varepsilon) = k_1^2, \qquad Q_r(\varepsilon^{n_1}) = rk_2^2 .$$

The first of these equations implies $n_1=1$ or $n_1=3$ (proposition 1), and the second one gives as the only possibility $r=5$ (proposition 2). But $Q_5(\varepsilon^3)=5k_3^2$ can be written

$$5\left(\tfrac{1}{5}(2(\varepsilon^3+\varepsilon'^3)-1)\right)^2 = 1+4k_3^2 ,$$

impossible, since $2(\varepsilon^3+\varepsilon'^3)\equiv 0 \pmod 4$. Theorem 1 now follows as an immediate consequence.

Then we proceed to prove theorem 2. From (12) we get

$$x^2A^{\frac{1}{2}}+yB^{\frac{1}{2}} = \left(\tfrac{1}{2}(aA^{\frac{1}{2}}+bB^{\frac{1}{2}})\right)^{3m} . \tag{17}$$

We distinguish between two cases:

1° $m\equiv 0 \pmod 3$. Equation 17 implies, putting $m=3r$,

$$x^2A^{\frac{1}{2}}+yB^{\frac{1}{2}} = \varepsilon_1^{\frac{9}{2}} , \tag{18}$$

where

$$\varepsilon_1^{\frac{1}{2}} = \left(\tfrac{1}{2}(aA^{\frac{1}{2}}+bB^{\frac{1}{2}})\right)^r = \tfrac{1}{2}(uA^{\frac{1}{2}}+vB^{\frac{1}{2}}) .$$

Hence

$$2x^2 = uQ_9(\varepsilon_1) . \tag{19}$$

The greatest common divisor of u and $Q_9(\varepsilon_1)$ divides 9, and if $u\equiv 0 \pmod 3$, then $Q_9(\varepsilon_1)\equiv 9 \pmod{27}$. From (19) we then conclude either

$$u = k_1^2, \qquad Q_9(\varepsilon_1) = 2k_2^2 ,$$

or

$$u = 2k_1^2, \qquad Q_9(\varepsilon_1) = k_2^2 ,$$

both systems being impossible on account of lemma 6.

2° $m\not\equiv 0 \pmod 3$. Putting

$$\varepsilon_2^{\frac{1}{2}} = \left(\tfrac{1}{2}(aA^{\frac{1}{2}}+bB^{\frac{1}{2}})\right)^m = \tfrac{1}{2}(u_1A^{\frac{1}{2}}+v_1B^{\frac{1}{2}}), \quad (u_1,2)=1,$$

we get from (17)

$$2x^2 = u_1Q_3(\varepsilon_2),$$

yielding either

$$u_1 = h^2, \quad Q_3(\varepsilon_2) = 2k^2, \tag{20}$$

or

$$u_1 = 3h^2, \quad Q_3(\varepsilon_2) = 6k^2. \tag{21}$$

The first case gives the equation $Ah^4-Bv_1^2=4$, $(h,2)=1$. From theorem 1 we then conclude

$$\tfrac{1}{2}(h^2A^{\frac{1}{2}}+v_1B^{\frac{1}{2}}) = \left(\tfrac{1}{2}(aA^{\frac{1}{2}}+bB^{\frac{1}{2}})\right)^t, \quad t=1 \text{ or } t=5,$$

since $t=3$ must be excluded, h being odd. Hence

$$x^2A^{\frac{1}{2}}+yB^{\frac{1}{2}} = \left(\tfrac{1}{2}(aA^{\frac{1}{2}}+bB^{\frac{1}{2}})\right)^{3t}. \tag{22}$$

We shall show that $t=5$ never occurs. For $t=5$ we write (22) in the form

$$x^2A^{\frac{1}{2}}+yB^{\frac{1}{2}} = (a_1A^{\frac{1}{2}}+b_1B^{\frac{1}{2}})^5, \tag{23}$$

putting

$$\left(\tfrac{1}{2}(aA^{\frac{1}{2}}+bB^{\frac{1}{2}})\right)^3 = (a_1A^{\frac{1}{2}}+b_1B^{\frac{1}{2}}).$$

From (23) it follows

$$x^2 = a_1(16A^2a_1^4-20A^2a_1^2+5),$$

giving either

$$a_1 = h_1^2, \quad 16A^2a_1^4-20Aa_1^2+5 = k_1^2, \tag{24}$$

or

$$a_1 = 5h_1^2, \quad 16A^2a_1^4-20Aa_1^2+5 = 5k_1^2. \tag{25}$$

The last equations in (24) and (25) can be written,

$$(8Aa_1^2-5)^2-5 = 4k_1^2 \quad \text{and} \quad 5(40Ah_1^4-1)^2 = 1+4k_1^2,$$

respectively. Obviously, these equations have no solutions in integers h_1, k_1, with $Aa_1^2>4$. Consequently, the only possibility for (20) is given by (22) with $t=1$.

At last we have to discuss the system (21). Here we find $9Ah^4-Bv_1^2=4$, $(h,2)=1$. We put

$$\left(\tfrac{1}{2}(aA^{\frac{1}{2}}+bB^{\frac{1}{2}})\right)^s = \tfrac{1}{2}(a_sA^{\frac{1}{2}}+b_sB^{\frac{1}{2}}), \quad (s,6)=1,$$

where s denotes the least exponent such that $a_s\equiv 0 \pmod 3$, and shall show that $s=1$ is a necessary condition. Clearly $(Bb,3)=1$. Assuming $(a,3)=1$, we derive from $Aa^2-Bb^2=4$ that $A-B\equiv 1 \pmod 3$, giving

either $A \equiv 2$ or $A \equiv 0 \pmod 3$. In the first case the least value of s is 3, in the second case $s = 2$, contrary to the assumption. On account of theorem 1 we obtain

$$x^2 A^{\frac{1}{3}} + yB^{\frac{1}{3}} = \left(\tfrac{1}{2}(aA^{\frac{1}{3}} + bB^{\frac{1}{3}})\right)^{3t}, \quad t = 1 \text{ or } t = 5,$$

where $t = 5$ is excluded as in the foregoing case.

This completes the proof of theorem 2.

REFERENCES

1. F. Arndt, *Untersuchungen über einige unbestimmte Gleichungen zweiten Grades, und über die Verwandlung der Quadratwurzel aus einem Bruche in einen Kettenbruch*, Arch. d. Math. und Physik 12 (1849), 211–276.
2. R. T. Bumby, *The diophantine equation* $3x^4 - 2y^2 = 1$, Math. Scand. 21 (1967), 144–148.
3. J. H. E. Cohn, *Eight diophantine equations*, Proc. London Math. Soc. (3) 16 (1966), 153–166.
4. W. Ljunggren, *Einige Eigenschaften der Einheiten reeller quadratischer und reinbiquadratischer Zahlkörper. Mit Anwendungen auf die Lösung einer Klasse unbestimmter Gleichungen 4. Grades*, Skr. Norske Vid. Akad. Oslo, Mat.-Naturv. Klasse, 1936, No. 12, 73 pp.
5. W. Ljunggren, *Über die unbestimmte Gleichung* $Ax^2 - By^4 = C$, Arch. for Math. og Naturv. (Oslo) 41, Nr. 10 (1938), 18 pp.
6. W. Ljunggren, *Über die Gleichung* $x^4 - Dy^2 = 1$, Arch. for Math. og Naturv. (Oslo) 45, 1942, 61–70.
7. W. Ljunggren, *Zur Theorie der Gleichung* $x^2 + 1 = Dy^4$, Avh. Norske Vid. Akad. Oslo I, 1942, No. 5, 1942, 27 pp.
8. W. Ljunggren, *Einige Sätze über unbestimmte Gleichungen von der Form* $Ax^4 + Bx^2 + C = Dy^2$, Skr. Norske Vid. Akad. Oslo, Mat.-Naturv. Klasse, 1942, No. 9, 53 pp (1943).
9. W. Ljunggren, *On the diophantine equation* $x^2 + 4 = Ay^4$, Norske Vid. Selsk. Forh. (Trondheim) 24 (No. 18) (1951), 82–84.
10. W. Ljunggren, *Ein Satz über die Gleichung* $Ax^2 - By^4 = C$ $(C = 1, 2, 4)$, Comptes Rendus du Douzième Congrès des Mathématiciens Scandinaves, Lund (1953), 188–194.
11. T. Nagell, *On a special class of diophantine equations of the second degree*, Ark. för Mat. 3 (1954), 51–65.
12. O. Perron, *Algebra* I, Berlin, 1932.

UNIVERSITY OF OSLO, NORWAY