MATH. SCAND. 1 (1953)

ON AN IMPROVEMENT OF A THEOREM OF T. NAGELL CONCERNING THE DIOPHANTINE EQUATION $Ax^3+By^3 = C$

WILHELM LJUNGGREN

1. The Diophantine equation

$$(1) \qquad x^3+Dy^3 = 1 ,$$

where D denotes a positive rational integer, which is not a cube, was solved completely by B. Delaunay [1] who showed that it has at most one solution in rational integers x and y when $y \neq 0$. If $x = x_1, y = y_1$ is an integral solution, then

$$\zeta = x_1+y_1 D^{\frac{1}{3}}$$

is the fundamental unit of the ring $R(1, D^{\frac{1}{3}}, D^{\frac{2}{3}})$.

T. Nagell [5; 6; 7; 8] proved the same theorem independently of Delaunay and, moreover, a stronger form of the latter part of the theorem. Nagell [7; 8] proved that ζ is the fundamental unit of the field $K(D^{\frac{1}{3}})$, except when $D = 19$, 20 and 28, in which cases ζ is the square of the fundamental unit. These values of D correspond to the solutions $x = -8, y = 3$; $x = -19, y = 7$; and $x = -3, y = 1$.

Nagell [7] generalized these results, showing that the Diophantine equation

$$(2) \qquad Ax^3+By^3 = C \qquad (C = 1 \text{ or } C = 3) ,$$

where A and B are > 1 when $C = 1$ and where AB is not divisible by 3 when $C = 3$, has at most one solution in rational integers x and y.

He also obtained the following result: Put $A = ac^2$ and $B = bd^2$, where a, b, c and d are positive rational integers, relatively prime in pairs, and possessing no squared factors. If $x = x_1, y = y_1$ is a solution, then

$$\zeta = C^{-1}\big(x_1 A^{\frac{1}{3}} + y_1 B^{\frac{1}{3}}\big)^3 = \xi^{2^r},$$

where ξ is the fundamental unit of the field $K\big((ac^2b^2d)^{\frac{1}{3}}\big)$, $0 < \xi < 1$, and where r is a rational integer $\geqq 0$.

Received October 18, 1953.

There is one exception to this theorem, viz. the equation $2x^3+y^3 = 3$, which has the two solutions $x = y = 1$ and $x = 4, y = -5$. *This exception is not taken into consideration in the following.*

Without knowing an upper limit for the integer r, Nagell succeeded in constructing an algorithm to decide if (2) is solvable or not. In the former case, this algorithm gives a method to determine the solution of the equation (cf. [7, pp. 257 and 263]). This method, a sort of *descente finie*, is, however, too cumbersome to be practical.

Nagell [7; 9; 10] has treated the question of determining an upper limit of r. His investigations have been continued by P. Hæggmark [2]. Several interesting results are obtained, but no complete solution of this problem has hitherto been found. In this paper we prove that $r \leqq 1$. This is the best possible result, since Nagell [7, pp. 258 and 264] has proved that $r = 1$ for an infinity of fields $K\big((ac^2b^2d)^{\frac{1}{3}}\big)$. This yields the following result:

THEOREM: *The Diophantine equation*

$$Ax^3+By^3 = C\,,$$

where $C = 1$ *or* $C = 3$, *where* A *and* B *are* > 1 *when* $C = 1$, *and where* AB *is not divisible by* 3 *when* $C = 3$, *has at most one solution in rational integers* x *and* y. *If* $x = x_1, y = y_1$ *is an integral solution, then* $C^{-1}(x_1A^{\frac{1}{3}} + y_1B^{\frac{1}{3}})^3$ *is either the fundamental unit in the field* $K\big((AB^2)^{\frac{1}{3}}\big)$ *or the square of this unit.*

2. Let η, $0 < \eta < 1$, be a unit in $K\big((AB^2)^{\frac{1}{3}}\big)$. Then we must have, if $r > 1$,

$$C^{-1}(xA^{\frac{1}{3}}+yB^{\frac{1}{3}})^3 = \eta^4\,, \tag{3}$$

where

$$\eta^3-p\eta^2+q\eta-1 = 0\,, \tag{4}$$

p and q denoting rational integers. This gives us

$$\begin{aligned}\eta^4 &= 1 + 3C^{-1}x^2y(A^2B)^{\frac{1}{3}} + 3C^{-1}xy^2(AB^2)^{\frac{1}{3}}\,,\\ \eta'^4 &= 1 + 3C^{-1}x^2y\varrho(A^2B)^{\frac{1}{3}} + 3C^{-1}xy^2\varrho^2(AB^2)^{\frac{1}{3}}\,,\\ \eta''^4 &= 1 + 3C^{-1}x^2y\varrho^2(A^2B)^{\frac{1}{3}} + 3C^{-1}xy^2\varrho(AB^2)^{\frac{1}{3}}\,, \qquad \varrho^3 = 1,\ \varrho \neq 1\,,\end{aligned} \tag{5}$$

where η' and η'' are the conjugates of η. The equations (5) imply

$$\eta^4+\eta'^4+\eta''^4 = 3\,, \tag{6}$$

or

$$\begin{aligned}(p^2-2q)^2 - 2(q^2-2p) &= 3\,,\\ q = p^2 \pm (p-1)\big(\tfrac{1}{2}(p^2+2p+3)\big)^{\frac{1}{2}}\,,\end{aligned} \tag{7}$$

that is

$$q = p^2 + (p-1)M, \tag{8}$$

$$M^2 - 2\left(\tfrac{1}{2}(p+1)\right)^2 = 1. \tag{9}$$

From (5) we further obtain

$$\eta^4+\varrho\eta'^4+\varrho^2\eta''^4 = 9C^{-1}xy^2(AB^2)^{\frac{1}{3}},$$
$$\eta^4+\varrho^2\eta'^4+\varrho\eta''^4 = 9C^{-1}x^2y(A^2B)^{\frac{1}{3}}.$$

By multiplication of these two equations we get

$$\eta^8+\eta'^8+\eta''^8-(\eta\eta'')^4-(\eta\eta')^4-(\eta'\eta'')^4 = 81C^{-2}ABx^3y^3,$$
$$(\eta^4+\eta'^4+\eta''^4)^2 - 3\left((\eta\eta'')^4+(\eta\eta')^4+(\eta'\eta'')^4\right) = 81C^{-2}ABx^3y^3,$$

$$9 - 3\left((q^2-2p)^2-2(p^2-2q)\right) = 81C^{-2}ABx^3y^3. \tag{10}$$

From (7) we find $q^2-2p = \frac{1}{2}\left((p^2-2q)^2 - 3\right)$; inserting this expression in (10) we get the result

$$3 - (p^2-2q)^4 + 6(p^2-2q)^2 + 8(p^2-2q) = 108C^{-2}ABx^3y^3.$$

Putting for brevity $p^2-2q = t$, this equation can be written

$$(t+1)^3(t-3) = -108C^{-2}Ax^3(C-Ax^3); \tag{11}$$

hence

$$6C^{-1}Ax^3 = 3 + (t-2)\left(\tfrac{1}{3}(t^2+4t+6)\right)^{\frac{1}{2}},$$

that is,

$$t^2+4t+6 = 3N^2$$

or

$$(p^2-2q+2)^2 + 2 = 3N^2, \tag{12}$$

$$6C^{-1}Ax^3 = 3 + (p^2-2q-2)N. \tag{13}$$

Consequently, we have to solve the system (9) and (12). This can also be written in the following form

$$M^2 - 2\left(\tfrac{1}{2}(p+1)\right)^2 = 1, \tag{14}$$

$$\left(p^2+2(p-1)M-2\right)^2 + 2 = 3N^2, \tag{15}$$

making use of (8). The corresponding values of q, A, B and C are determined by (8) and (13).

In the following sections it will be shown that the only solutions of the system (14) and (15) in rational integers p, M and N are

$$p = -1, M = 1, N = \pm 3; \qquad p = 3, M = -3, N = \pm 3;$$
$$p = 3, M = 3, N = \pm 11,$$

with q equal to -1, 3 and 15, respectively. In the first two cases we find either $Ax^3 = C$ or $By^3 = C$, which is impossible. In the last case we get the equation $2x^3+y^3 = 3$ with $\eta = (1-2^{\frac{1}{3}})^2$ and

$$\tfrac{1}{3}(4\cdot 2^{\frac{1}{3}}-5)^3 = (1-2^{\frac{1}{3}})^8 .$$

Then our theorem is proved.

3. We have

$$(16)\quad \big(p^2+2(p-1)M-2\big)^2 + 2 = (p+2M+2)^2\big((M-2)^2 + 2(\tfrac{1}{2}(p-1))^2\big),$$

because the value of each side of (16) is found to be equal to

$$4(p^3-p^2-2p+2)M + 3p^4-4p^2-8p+12 ,$$

using that $2M^2 = p^2+2p+3$. Instead of solving (14) and (15) we can solve the system

$$(17)\qquad M^2 - 2\big(\tfrac{1}{2}(p+1)\big)^2 = 1 ,$$

$$(18)\qquad (M-2)^2 + 2\big(\tfrac{1}{2}(p-1)\big)^2 = 3N_1^2, \qquad N = N_1(p+2M+2) .$$

From (18) we deduce

$$(19)\qquad M-2 + \tfrac{1}{2}(p-1)(-2)^{\frac{1}{2}} = e\big(1+e_1(-2)^{\frac{1}{2}}\big)\big(u+v(-2)^{\frac{1}{2}}\big)^2 , \quad e = \pm 1, e_1 = \pm 1 .$$

Hence

$$M = 2 + e(u^2-2v^2) - 4ee_1uv , \qquad \tfrac{1}{2}(p+1) = 1 + ee_1(u^2-2v^2) + 2euv.$$

Inserting these values in (17) we obtain

$$\big(2+e(u^2-2v^2)-4ee_1uv\big)^2 - 2\big(1+ee_1(u^2-2v^2)+2euv\big)^2 = 1 ,$$

or

$$(20)\quad (u^2-2v^2+8e_1uv)^2 - 2(6uv-e)^2 - 4e(1-e_1)(u^2-2v^2) + 16e(e_1-1)uv = -1 .$$

In this equation we have $e_1 = 1$, because if we had $e_1 = -1$ we would get

$$(u^2+uv+v^2)^2 + e(u^2+uv+v^2) \equiv 1 \pmod 3 ,$$

that is, $e \equiv 0 \pmod 3$, which is impossible. Then (20) reduces to

$$(u^2-2v^2+8uv)^2 - 2(6uv-e)^2 = -1 ,$$

or

$$f(u, v) \equiv u^4+16u^3v-12u^2v^2-32uv^3+4v^4+24euv-1 = 0 .$$

According to a theorem of C. L. Siegel [11] the equation $f(u, v) = 0$ has only a finite number of solutions in integers u and v, because the algebraic curve $f(u, v) = 0$ is of genus 3, but the proof gives no method for determining the possible solutions u and v. In the following sections we will show that there are only the trivial solutions

$$u = \pm 1, v = 0; \qquad u = 1, v = 1, e = 1; \qquad u = -1, v = -1, e = 1\,.$$

These values of u and v give precisely the solutions of p and M mentioned in the first section.

4. From (17) we deduce

$$M = \tfrac{1}{2}e_2(E^{2n}+E'^{2n}), \qquad \tfrac{1}{2}(p+1) = \tfrac{1}{2}e_2 2^{\frac{1}{2}}(E^{2n}-E'^{2n})\,,$$

where $E = 1+2^{\frac{1}{2}}$, $E' = 1-2^{\frac{1}{2}}$, $e_2 = \pm 1$ and $n = 0, \pm 1, \pm 2, \pm 3, \ldots$. Inserting these expressions in (19) we get

$$\left(\tfrac{1}{2}(1+i)E^{2n} + \tfrac{1}{2}(1+i)E'^{2n}\right)e_2 - 2 - i\,2^{\frac{1}{2}} = e(1+i\,2^{\frac{1}{2}})(u+i\,2^{\frac{1}{2}}v)^2\,.$$

Now we find

(21) $$\tfrac{1}{2}(1+i)E^{2n} + \tfrac{1}{2}(1+i)E'^{2n} = (-1)^{n-1}2^{\frac{1}{2}}+E\vartheta^2\,,$$

where

(22) $$\vartheta = \tfrac{1}{2}(E^n+E'^n) - \tfrac{1}{2}iE'(E^n-E'^n)\,.$$

This yields

(23) $$E\vartheta^2 - ee_2(1+i\,2^{\frac{1}{2}})(u+iv\,2^{\frac{1}{2}})^2 = 2^{\frac{1}{2}}\left((-1)^n+e_2(i+2^{\frac{1}{2}})\right).$$

Putting

$$\theta = \left(E(1+i\,2^{\frac{1}{2}})\right)^{\frac{1}{2}} = \left(\tfrac{1}{2}E(3^{\frac{1}{2}}+1)\right)^{\frac{1}{2}} + i\left(\tfrac{1}{2}E(3^{\frac{1}{2}}-1)\right)^{\frac{1}{2}}$$

and

$$\theta_1 = \left(E'(1+i\,2^{\frac{1}{2}})\right)^{\frac{1}{2}} = -\left(\tfrac{1}{2}E^{-1}(3^{\frac{1}{2}}-1)\right)^{\frac{1}{2}} + i\left(\tfrac{1}{2}E^{-1}(3^{\frac{1}{2}}+1)\right)^{\frac{1}{2}}$$

we find

$$\theta\theta_1 = i(1+i2^{\frac{1}{2}}) \quad \text{and} \quad \theta_1 = -iE'\theta,\ \theta = -iE\theta_1\,.$$

The algebraic number field $K(\theta)$ is of the eighth degree, and $K(\theta) = K(\theta_1)$. If ξ is any number in $K(\theta)$, we denote by ξ', ξ'', ξ''' the conjugates obtained by changing in ξ the sign of θ, the signs of i and of $2^{\frac{1}{2}}$, the signs of i and of $2^{\frac{1}{2}}$ and of θ, respectively. The conjugates of θ, obtained in this way, are $-\theta$, θ_1 and $-\theta_1$ and those of θ_1 are $-\theta_1$, $-\theta$ and θ.

The algebraic number

(24) $$\alpha = \frac{\left(\vartheta E^{\frac{1}{2}} + (ee_2)^{\frac{1}{2}}(1+i\,2^{\frac{1}{2}})^{\frac{1}{2}}(u+iv\,2^{\frac{1}{2}})\right)^2}{2^{\frac{1}{2}}\left((-1)^n + e_2(i+2^{\frac{1}{2}})\right)}$$

is a unit in $K(\theta)$ with relative norm 1 in the subfield $k(i,\, 2^{\frac{1}{2}})$. In fact, we find

(25) $$\alpha+\alpha' = -2 + \vartheta^2E\left(e_2+i((-1)^n-e_2 2^{\frac{1}{2}})\right) \quad \text{and} \quad \alpha\alpha' = 1\,.$$

Further we find

$$(\alpha+\alpha'+2)\big((-1)^n+e_2(i+2^{\frac12})\big) = 2^{3/2}\vartheta^2 E\,,$$
$$(\alpha''+\alpha'''+2)\big((-1)^n-e_2(i+2^{\frac12})\big) = -2^{3/2}\vartheta''^2 E'\,.$$

By addition of these two equations we get

$$(\alpha+\alpha'+\alpha''+\alpha'''+4)(-1)^n + e_2(i+2^{\frac12})(\alpha+\alpha'-\alpha''-\alpha''') = 8(-1)^n\,,$$

using the fact that $\vartheta^2 E-\vartheta''^2 E' = 2^{3/2}(-1)^n$, which follows easily from (23). Consequently:

$$(26)\qquad (\alpha+\alpha'+\alpha''+\alpha''') + e_2(-1)^n(i+2^{\frac12})(\alpha+\alpha'-\alpha''-\alpha''') = 4\,.$$

In the number field $K(\theta)$ there are 3 independent units, and it is easily shown that the group of units with relative norm 1 in the subfield $k(i,\, 2^{\frac12})$ is generated by two independent units, say ε_1 and ε_2 (cf. Ljunggren [3, p. 8]). Then we must have

$$(27)\qquad \alpha = \pm\varepsilon_1{}^x\varepsilon_2{}^y\,,$$

because ± 1 are the only roots of unity whose squares equal 1. Inserting this in (26) we get two exponential equations to determine the exponents x and y, and therefore we can make use of the p-adic method developed by Th. Skolem in a series of papers [12; 13; 14; 15].

5. In the same way as in my paper [4, pp. 13–17] it can be shown that

$$\varepsilon_1 = \frac{(E^{\frac12}+i(1+i\,2^{\frac12})^{\frac12})^2}{2^{\frac12}(E+i)} = \tfrac12\big(-i-E'+\theta(i-E')\big)$$

and

$$\varepsilon_2 = \frac{(E'^{\frac12} - i(1+i\,2^{\frac12})^{\frac12})^2}{-2^{\frac12}(E'-i)} = \varepsilon_1{}'' = \tfrac12\big(i-E-\theta(i+E')\big)$$

is a pair of fundamental units. Further we note the units

$$\varepsilon_1\varepsilon_2{}^{-2} = \frac{(E^{\frac12}(-iE'+2^{\frac12}) + (1+i\,2^{\frac12})^{\frac12})^2}{2^{\frac12}(E+i)}\,,$$

$$\varepsilon_1{}^3 = \frac{(E^{\frac12}(1+iE'\,2^{\frac12}) + i(1+i\,2^{\frac12})(1+i\,2^{\frac12})^{\frac12})^2}{-2^{\frac12}(E+i)}\,.$$

For the sake of brevity we write

$$s(\varepsilon_1{}^x\varepsilon_2{}^y) = \varepsilon_1{}^x\varepsilon_2{}^y + \varepsilon_1{}'^x\varepsilon_2{}'^y + \varepsilon_1{}''^x\varepsilon_2{}''^y + \varepsilon_1{}'''^x\varepsilon_2{}'''^y\,,$$
$$d(\varepsilon_1{}^x\varepsilon_2{}^y) = \varepsilon_1{}^x\varepsilon_2{}^y + \varepsilon_1{}'^x\varepsilon_2{}'^y - \varepsilon_1{}''^x\varepsilon_2{}''^y - \varepsilon_1{}'''^x\varepsilon_2{}'''^y$$

and $e_2(-1)^n = t$. Hence, from (26) and (27)

$$s(\varepsilon_1{}^x\varepsilon_2{}^y) + t(i+2^{\frac{1}{2}})d(\varepsilon_1{}^x\varepsilon_2{}^y) = \pm 4\,. \tag{28}$$

We first prove some lemmas:

Lemma 1: *If* (x, y) *is a solution of* (28), *then* $(-x, -y)$ *is also a solution.*

This follows immediately from the equations $\varepsilon_1\varepsilon_1{}' = 1$, $\varepsilon_1{}''\varepsilon_1{}''' = 1$, $\varepsilon_2\varepsilon_2{}' = 1$, $\varepsilon_2{}''\varepsilon_2{}''' = 1$.

Lemma 2: *If* (x, y) *is a solution of* (28), *then* $(-y, x)$ *is a solution of*

$$s(\varepsilon_1{}^x\varepsilon_2{}^y) - t(i+2^{\frac{1}{2}})d(\varepsilon_1{}^x\varepsilon_2{}^y) = \pm 4\,. \tag{29}$$

Since $\varepsilon_2 = \varepsilon_1{}''$, $\varepsilon_2{}' = \varepsilon_1{}'''$, $\varepsilon_2{}'' = \varepsilon_1{}'$, $\varepsilon_2{}''' = \varepsilon_1$, we have $s(\varepsilon_1{}^x\varepsilon_2{}^y) = s(\varepsilon_1{}^{-y}\varepsilon_2{}^x)$ and $d(\varepsilon_1{}^x\varepsilon_2{}^y) = -d(\varepsilon_1{}^{-y}\varepsilon_2{}^x)$, and the lemma is proved.

Lemma 3: *Equation* (27) *is not satisfied by* (x, y) *if* $x \equiv y \equiv 0 \pmod 2$.

Proof: We find $\alpha\alpha'' = \mu^2/(4i\,2^{\frac{1}{2}})$, where μ is an integer in $K(\theta)$. Putting $\alpha = \lambda^2$, λ being a unit in $K(\theta)$, we obtain $(\lambda\lambda'')^2 = \mu^2/(4i\,2^{\frac{1}{2}})$, whence $4i\,2^{\frac{1}{2}} = \mu^2(\lambda'\lambda''')^2$. Since $4i\,2^{\frac{1}{2}} = \big((2+2i)/2^{\frac{1}{4}}\big)^2$ we conclude that $2^{\frac{1}{4}}$ belongs to $K(\theta)$. It is easily seen that this is impossible.

Lemma 4: *Equation* (27) *is not satisfied by* (x, y) *if* $x \equiv y \equiv 1 \pmod 2$.

Proof: Putting $\alpha\varepsilon_1\varepsilon_2 = \lambda^2$ we get $(\alpha\varepsilon_1\varepsilon_2)(\alpha''\varepsilon_1{}''\varepsilon_2{}'') = \alpha\alpha''\varepsilon_2{}^2 = (\lambda\lambda'')^2$. From the preceding proof it follows that this is impossible.

Lemma 5: *The system of equations* (26) *and* (27) *is not satisfied by* (x, y), *either if* $x \equiv 0 \pmod 2$, $y \equiv 1 \pmod 2$, $t = 1$ *or if* $x \equiv 1 \pmod 2$, $y \equiv 0 \pmod 2$, $t = -1$.

Proof: In the first case we find $\alpha\varepsilon_2 = \mu^2/(4ie_2 2^{\frac{1}{2}})$ and in the second one $\alpha\varepsilon_1 = \mu_1{}^2/(4ie_2 2^{\frac{1}{2}})$. As before we see that these numbers are not squares of any unit in $K(\theta)$.

From these lemmas we conclude that it is sufficient to study the equation

$$s(\varepsilon_1{}^x\varepsilon_2{}^y) + (i+2^{\frac{1}{2}})d(\varepsilon_1{}^x\varepsilon_2{}^y) = \pm 4, \qquad x \textit{ odd}, y \textit{ even}. \tag{30}$$

6. Now we find

$$\varepsilon_1{}^8 = 1+4B, \quad B = 4P+\theta Q, \quad P = -7+5\cdot 2^{\frac{1}{2}}+i(11\cdot 2^{\frac{1}{2}}-14),$$
$$Q = 54\cdot 2^{\frac{1}{2}}-78+i(2^{\frac{1}{2}}-4)\,,$$

$$\varepsilon_2^8 = 1+4B_1, \quad B_1 = 4P_1+\theta_1 Q_1, \quad P_1 = -7-5\cdot 2^{\frac{1}{2}}+i(11\cdot 2^{\frac{1}{2}}+14)\,,$$
$$Q_1 = -54\cdot 2^{\frac{1}{2}}-78+i(2^{\frac{1}{2}}+4)\,.$$

Putting $x = 8m_1+r$, $y = 8n_1+s$, where $r = \pm 1$ or ± 3 and $s = 0$, ± 2 or 4, and applying the first lemma of Section 5, we see that it is sufficient to treat the following eight cases:

$$\begin{array}{ll} 1^\circ\ r = 1, s = 0, & 2^\circ\ r = 1, s = -2\,, \\ 3^\circ\ r = 1, s = 2, & 4^\circ\ r = 1, s = 4\,, \\ 5^\circ\ r = 3, s = 0, & 6^\circ\ r = 3, s = -2\,, \\ 7^\circ\ r = 3, s = 2, & 8^\circ\ r = 3, s = 4\,. \end{array}$$

Let β denote any integer in $K(\theta)$. For the sake of brevity we introduce the notation

$$s(\beta\varepsilon_1^r\varepsilon_2^s) + (i+2^{\frac{1}{2}})\,d(\beta\varepsilon_1^r\varepsilon_2^s) = p(\beta\varepsilon_1^r\varepsilon_2^s)\,.$$

Then $p(\beta\varepsilon_1^r\varepsilon_2^s)$ is an integer in $k(i2^{\frac{1}{2}})$. The equation (30) implies

$$(31)\qquad p(\varepsilon_1^r\varepsilon_2^s) + 4\binom{m_1}{1}p(B\varepsilon_1^r\varepsilon_2^s) + 4\binom{n_1}{1}p(B_1\varepsilon_1^r\varepsilon_2^s) + \ldots$$
$$+\, 4^q\sum_{k=0}^{q}\binom{m_1}{q-k}\binom{n_1}{k}p(B^{q-k}B_1^k\varepsilon_1^r\varepsilon_2^s) + \ldots = \pm 4\,.$$

Now we have that ε_1^2, $\varepsilon_1\varepsilon_2$ and ε_2^2 all belong to the ring

$$R(1,\, 2^{\frac{1}{2}},\, i,\, i2^{\frac{1}{2}},\, \theta,\, \theta 2^{\frac{1}{2}},\, \theta i,\, \theta i 2^{\frac{1}{2}}).$$

Hence it is obvious that $p(B^{q-k}B_1^k\varepsilon_1^r\varepsilon_2^s) \equiv 0 \pmod 2$.

The cases 3°, 4°, 6°, 7° and 8° can be excluded at once. In fact, we find $p(\varepsilon_1^r\varepsilon_2^s) = -12-16i2^{\frac{1}{2}}$, -140, -44, $4+48i2^{\frac{1}{2}}$ and $340+96i2^{\frac{1}{2}}$, respectively, and further $p(B\varepsilon_1^r\varepsilon_2^s) \equiv p(B_1\varepsilon_1^r\varepsilon_2^s) \equiv 0 \pmod 8$ in all these cases, which contradicts the validity of (31) mod 32. The remaining three cases must be studied separately.

2°: We get $p(\varepsilon_1\varepsilon_2^{-2}) = 4$, $p(B\varepsilon_1\varepsilon_2^{-2}) = 8\cdot 223 - 8\cdot 17i2^{\frac{1}{2}}$, $p(B_1\varepsilon_1\varepsilon_2^{-2}) = -32\cdot 3+15\cdot 8i2^{\frac{1}{2}}$ and $p(B^2\varepsilon_1\varepsilon_2^{-2}) \equiv p(B_1^2\varepsilon_1\varepsilon_2^{-2}) \equiv p(BB_1\varepsilon_1\varepsilon_2^{-2}) \equiv 0$ (mod 8).

Using that $B = \theta 2^{\frac{1}{2}}(i+2^{\frac{1}{2}}+2N)$, $B_1 = \theta_1 2^{\frac{1}{2}}(i+2^{\frac{1}{2}}-2N'')$, where N belongs to R, we find

$$(32)\qquad p(B^{q-k}B_1^k\varepsilon_1^r\varepsilon_2^s) = 2^{[q/2]+1}(a_{qk}+b_{qk}i2^{\frac{1}{2}})\,,$$

a_{qk} and b_{qk} denoting integers in $k(1)$.

On the right-hand side of (31) we must have $+4$. Otherwise (31) could not be valid mod 16. Dividing by 32 we then obtain

$$(33)\quad m_1(223-17i2^{\frac{1}{2}}) + n_1(-12+15i2^{\frac{1}{2}}) + 2\big(f(m_1, n_1)+g(m_1, n_1)i2^{\frac{1}{2}}\big)$$
$$+ 2^3\sum_{k=0}^{3}\binom{m_1}{3-k}\binom{n_1}{k}(a_{3k}+b_{3k}i2^{\frac{1}{2}})+\ldots$$
$$+ 2^{2q+[q/2]-4}\sum_{k=0}^{q}\binom{m_1}{q-k}\binom{n_1}{k}(a_{qk}+b_{qk}i2^{\frac{1}{2}})+\ldots = 0,$$

where $f(m_1, n_1)$ and $g(m_1, n_1)$ are polynomials in m_1 and n_1 with coefficients which are integers in $k(1)$.

The exponent of the highest power of 2 which divides $(q-k)!\,k!$ is $\leq q-1$. The general term in (33) can thus be written in the form

$$2^{q+[q/2]-3}\big(f_q(m_1, n_1) + g_q(m_1, n_1)i2^{\frac{1}{2}}\big),$$

where $f_q(m_1, n_1)$ and $g_q(m_1, n_1)$ are polynomials in m_1 and n_1 with coefficients which are integers in relation to 2 in $k(1)$.

Now (33) yields the following 2-adic developments:

$$(34)\qquad \begin{aligned} 0 &= m_1 \qquad +2(\quad)+2^2(\quad)+2^3(\quad)+\ldots, \\ 0 &= m_1+n_1+2(\quad)+2^2(\quad)+2^3(\quad)+\ldots. \end{aligned}$$

According to a theorem of Th. Skolem [13, p. 180], the equations (34) have at most one solution m_1, n_1, because

$$\begin{vmatrix} 1 & 0 \\ 1 & 1 \end{vmatrix} = 1.$$

Obviously this solution is $m_1 = n_1 = 0$, corresponding to $\alpha = \varepsilon_1\varepsilon_2^{-2}$. On account of Lemmas 1 and 2 the three other possibilities are $\varepsilon_1^{-1}\varepsilon_2^{2}$, $\varepsilon_1^{-2}\varepsilon_2^{-1}$ and

$$\varepsilon_1^{2}\varepsilon_2 = \frac{\big((1-iE'2^{\frac{1}{2}})E^{\frac{1}{2}}+(1+i2^{\frac{1}{2}})^{\frac{1}{2}}\big)^2}{-2^{\frac{1}{2}}(E'-i)},$$

the two last units giving $u = \pm 1$, $v = 0$, $e = e_2 = 1$ and $n = 1$. See (22) and (24).

5°: Here we find $p(\varepsilon_1^3) = 4$, $p(B\varepsilon_1^3) = -2^3\cdot 21+2^4\cdot 165i2^{\frac{1}{2}}$,

$$p(B_1\varepsilon_1^3) = -2^4\cdot 33 - 2^4\cdot 129i2^{\frac{1}{2}}$$

and $p(B^2\varepsilon_1^3) \equiv p(BB_1\varepsilon_1^3) \equiv p(B_1^2\varepsilon_1^3) \equiv 0 \pmod 8$. As in the previous case we get the 2-adic developments:

$$\begin{aligned} 0 &= m_1 \qquad +2(\quad)+2^2(\quad)+2^3(\quad)+\ldots, \\ 0 &= m_1+n_1+2(\quad)+2^2(\quad)+2^3(\quad)+\ldots. \end{aligned}$$

The only solution $m_1 = n_1 = 0$ gives $\alpha = \varepsilon_1^3$, ε_1^{-3}, ε_2^3 or ε_2^{-3}; and the first two units yield $u = v = 1$, $e = 1$, $e_2 = -1$, $n = -1$ and $u = v = -1$ with the same values of e, e_2 and n.

1°: If we proceed as in the two previous cases we find that there are *at most two solutions* m_1, n_1. Since only one solution is known, namely $m_1 = n_1 = 0$, we have to use other p-adic developments in order to prove that no other solutions exist. *At first we prove that* $m_1 \equiv n_1 \equiv 0 \pmod 8$. We get

$$p(\varepsilon_1) = 4, \quad p(B\varepsilon_1) = -2^3\cdot 69 + 2^4\cdot 15 i 2^{\frac{1}{2}},$$
$$p(B_1\varepsilon_1) = 2^6\cdot 9 + 2^5\cdot 21 i 2^{\frac{1}{2}}, \quad p(B^2\varepsilon_1) = -2^3\cdot 909 - 2^4\cdot 7785 i 2^{\frac{1}{2}},$$
$$p(BB_1\varepsilon_1) = -2^3\cdot 1355 + 2^3\cdot 679 i 2^{\frac{1}{2}},$$
$$p(B_1{}^2\varepsilon_1) = -2^3\cdot 36297 + 2^6\cdot 339 i 2^{\frac{1}{2}}.$$

Further we find that $p(B^{q-k}B_1{}^k\varepsilon_1) \equiv 0 \pmod{16}$ for $q = 3$ and $k = 1, 2, 3$ and for $q = 4$ and $k = 1, 2, 3, 4$.

As in case 2° we obtain the equation

$$\begin{aligned} (35) \qquad & m_1(-69 + 30 i 2^{\frac{1}{2}}) + n_1(72 + 84 i 2^{\frac{1}{2}}) \\ & + 2^2\left\{\binom{m_1}{2}(-909 - 2\cdot 7785 i 2^{\frac{1}{2}}) + m_1 n_1(-1355 + 679 i 2^{\frac{1}{2}}) \right. \\ & \left. \qquad + \binom{n_1}{2}(-36297 + 2^3\cdot 339 i 2^{\frac{1}{2}})\right\} \\ & + 2^5\sum_{k=0}^{3}\binom{m_1}{3-k}\binom{n_1}{k}(a_k + b_k i 2^{\frac{1}{2}}) + 2^7\sum_{k=0}^{4}\binom{m_1}{4-k}\binom{n_1}{k}(c_k + d_k i 2^{\frac{1}{2}}) + \dots \\ & + 2^{2q+[q/2]-4}\sum_{k=0}^{q}\binom{m_1}{q-k}\binom{n_1}{k}(a_{qk} + b_{qk} i 2^{\frac{1}{2}}) + \dots = 0, \end{aligned}$$

a_k, b_k, c_k, and d_k being integers in $k(1)$. From (35) it is easily seen that $m_1 \equiv n_1 \equiv 0 \pmod 2$. Neglecting the trivial solution $m_1 = n_1 = 0$, we can put $m_1 = 2^w m_2$ and $n_1 = 2^w n_2$, $w \geqq 1$ and $(m_2, n_2) = 1$. For $q \geqq 5$ the general term in (35) is divisible by $2^{q+[q/2]+w-2}$, that is at least by 2^{w+5}. Then it is obvious that m_2 is even and n_2 is odd. Now we get the congruence

$$\begin{aligned} & m_2(-69 + 30 i 2^{\frac{1}{2}}) + n_2(72 + 84 i 2^{\frac{1}{2}}) + 2m_2(2^w m_2 - 1)(-909 - 2\cdot 7785 i 2^{\frac{1}{2}}) \\ & + 2^{w+2}m_2 n_2(-1355 + 679 i 2^{\frac{1}{2}}) + 2n_2(2^w n_2 - 1)(-36297 + 2^3\cdot 339 i 2^{\frac{1}{2}}) \\ & \equiv 0 \pmod{32}. \end{aligned}$$

This gives the following two congruences mod 16:

$$-69m_2 + 72n_2 + 1818m_2 - 2^{w+1} + 2n_2 \equiv 0 \pmod{16},$$
$$15m_2 + 42n_2 + 2m_2 - 2^{w+1}m_2 n_2 - 8 \equiv 0 \pmod{16}.$$

Simplifying we obtain

$$5m_2+10n_2 \equiv 2^{w+1} \pmod{16},$$
$$m_2+10n_2 \equiv 2^{w+1}m_2n_2+8 \pmod{16}.$$

Hence $40n_2 \equiv 2^{w+1}(5m_2n_2-1)+8 \pmod{16}$, and thus $w \geqq 3$. Now we find $\varepsilon_1^{64} \equiv 1 \pmod{(11-6i2^{\frac{1}{2}})}$ and $\varepsilon_1^{192} \equiv 1 \pmod{193}$. In the next section we will use 193-adic developments in order to prove that $m_1 = n_1 = 0$ is the only solution of (31) in case 1°.

7. Cumbersome calculations give us

$$\varepsilon_1^{16} = -174015+122176\cdot 2^{\frac{1}{2}}+i(212096-149824\cdot 2^{\frac{1}{2}})$$
$$+\theta\{(128400-90448\cdot 2^{\frac{1}{2}})+i(296672-210040\cdot 2^{\frac{1}{2}})\},$$
$$\varepsilon_1^{32} \equiv -16019+7437\cdot 2^{\frac{1}{2}}+i(5320-11580\cdot 2^{\frac{1}{2}})$$
$$+\theta\{(2319+11264\cdot 2^{\frac{1}{2}})+i(14153+17228\cdot 2^{\frac{1}{2}})\} \pmod{193^2},$$
$$\varepsilon_1^{96} \equiv -17537\cdot 2^{\frac{1}{2}}+193\,\theta\{(-11+44\cdot 2^{\frac{1}{2}})+i(-86-86\cdot 2^{\frac{1}{2}})\} \pmod{193^2},$$
$$\varepsilon_1^{192} \equiv 1+193\,\theta\{(7-56\cdot 2^{\frac{1}{2}})+i(-66-33\cdot 2^{\frac{1}{2}})\} \pmod{193^2}.$$

We have $\varepsilon_1^{192} = 1+193C$ and $\varepsilon_2^{193} = 1+193C_1$, where

$$C \equiv (7-56\cdot 2^{\frac{1}{2}})+i(-66-33\cdot 2^{\frac{1}{2}}) \pmod{193},$$
$$C_1 \equiv (7+56\cdot 2^{\frac{1}{2}})-i(-66+33\cdot 2^{\frac{1}{2}}) \pmod{193}.$$

If in (30) we insert $x = 192m_3+64r_1+1$ and $y = 192n_3+64s_1$ we get the 193-adic development

(36) $$p(\varepsilon_1^{64r_1+1}\varepsilon_2^{64s_1})+193(\quad)+193^2(\quad)+193^3(\quad)+\ldots = 4.$$

Here is $r_1 = -1$, 0 or 1 and $s_1 = -1$, 0 or 1. The first condition to be fulfilled is

(37) $$p(\varepsilon_1^{64r_1+1}\varepsilon_2^{64s_1}) \equiv 4 \pmod{193}.$$

This implies $r_1 = s_1 = 0$. In the remaining eight cases we find, in fact, denoting for brevity the left-hand side of the congruence (37) by (r_1, s_1):

$$(0,-1) \equiv 60-13i2^{\frac{1}{2}};\quad (0,1) \equiv -58-89i2^{\frac{1}{2}},\quad (1,0) \equiv 49-7i2^{\frac{1}{2}},$$
$$(1,1) \equiv 33-86i2^{\frac{1}{2}},\quad (1,-1) \equiv 65+72i2^{\frac{1}{2}};\quad (-1,0) \equiv -47-95i2^{\frac{1}{2}},$$
$$(-1,1) \equiv 83-8i2^{\frac{1}{2}},\quad (-1,-1) \equiv 22-80i2^{\frac{1}{2}},$$

the congruences being mod 193. In the calculations we make use of the fact that

$$\varepsilon_1^{64} \equiv -48-61i2^{\frac{1}{2}}+\theta\{(27-78\cdot 2^{\frac{1}{2}})+i(50+73\cdot 2^{\frac{1}{2}})\} \pmod{193}.$$

The equation (36) can now be written

$$m_3 p(C\varepsilon_1) + n_3 p(C_1\varepsilon_1) + 193(\quad) + 193^2(\quad) + \ldots = 0 .$$

Further we find $p(C\varepsilon_1) \equiv 88 - 14i\,2^{\frac{1}{2}}$ (mod 193) and $p(C_1\varepsilon_1) \equiv 80 + 60i\,2^{\frac{1}{2}}$ (mod 193), and hence

$$0 = 88m_3 + 80n_3 + 193(\quad) + 193^2(\quad) + \ldots,$$
$$0 = -14m_3 + 60n_3 + 193(\quad) + 193^2(\quad) + \ldots.$$

Since

$$\begin{vmatrix} 88 & 80 \\ -14 & 60 \end{vmatrix} \not\equiv 0 \pmod{193}$$

the only solution is $m_3 = n_3 = 0$, according to the theorem of Th. Skolem mentioned in Section 6. Hence $x = 1, y = 0$, that is, $\alpha = \varepsilon_1, \varepsilon_1^{-1}, \varepsilon_2$ or ε_2^{-1}. To ε_1 corresponds the solution $u = 1, v = 0, e = -1, e_2 = 1$ and $n = 0$; to ε_1^{-1} corresponds the solution $u = -1, v = 0$ with the same values of e, e_2 and n.

Then it is shown that the only solutions of u and v are $u = \pm 1, v = 0$; $u = 1, v = 1$; $u = -1, v = -1$. Hence our theorem in Section 1 is proved.

REFERENCES

1. B. Delaunay, *On the complete solution of the equation* $X^3\varrho + Y^3 = 1$, Publ. Soc. Math. Charkow (1916). (Russian.) See also his paper: *Vollständige Lösung der unbestimmten Gleichung* $X^3q + Y^3 = 1$ *in ganzen Zahlen*, Math. Z. 28 (1928), 1–9.
2. P. Häggmark, *On an unsolved question concerning the diophantine equation* $Ax^3 + By^3 = C$, Ark. Mat. 1 (1950), 279–294.
3. W. Ljunggren, *Einige Eigenschaften der Einheiten reeller quadratischer und rein-biquadratischer Zahlkörper usw.*, Skr. Norske Vid. Akad. Oslo, Mat.-Naturv. Klasse, 1936 No. 12, 1–73.
4. W. Ljunggren, *Zur Theorie der Gleichung* $x^2 + 1 = Dy^4$, Avh. Norske Vid. Akad. Oslo, Mat.-Naturv. Klasse, 1942 No. 5, 1–27.
5. T. Nagell, *Vollständige Lösung einiger unbestimmten Gleichungen dritten Grades*, Skr. Norske Vid. Akad. Oslo, Mat.-Naturv. Klasse, 1922 No. 14, 1–13.
6. T. Nagell, *Über die Einheiten in reinen kubischen Zahlkörpern*, Skr. Norske Vid. Akad. Oslo, Mat.-Naturv. Klasse, 1923 No. 11, 1–34.
7. T. Nagell, *Solution complète de quelques équations cubiques à deux indéterminées*, J. Math. pur. appl., (9) 4 (1925), 209–270.
8. T. Nagell, *Einige Gleichungen von der Form* $ay^2 + by + c = dx^3$, Avh. Norske Vid. Akad. Oslo, Mat.-Naturv. Klasse, 1930 No. 7, 1–15.
9. T. Nagell, *Zahlentheoretische Notizen VII–IX*, Norsk mat. forenings skrifter, Serie 1 No. 17 (1927), 1–23.
10. T. Nagell, *Zahlentheoretische Sätze*, Avh. Norske Vid. Akad. Oslo, Mat.-Naturv. Klasse, 1930 No. 5, 1–12.
11. C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abh. preuss. Akad. Wiss., Phys.-math. Kl., 1929 Nr. 1, 1–70.

12. Th. Skolem, *Einige Sätze über gewisse Reihenentwicklungen und exponentiale Beziehungen mit Anwendung auf diophantische Gleichungen,* Skr. Norske Vid. Akad. Oslo, Mat.-Naturv. Klasse, 1933 No. 6, 1–61.

13. Th. Skolem, *Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen,* 8de Skandinaviska Matematikerkongressen i Stockholm 1934, 163–188.

14. Th. Skolem, *Einige Sätze über p-adische Potenzreihen mit Anwendung auf gewisse exponentielle Gleichungen,* Math. Ann. 111 (1935), 399–424.

15. Th. Skolem, *Anwendung exponentieller Kongruenzen zum Beweis der Unlösbarkeit gewisser diophantischer Gleichungen,* Avh. Norske Vid. Akad. Oslo, Mat.-Naturv. Klasse, 1937 No. 12, 1–16.

UNIVERSITY OF BERGEN, NORWAY.