Then F is unimodular and

$$S = \begin{pmatrix} 1 & 0 \\ 0 & S^* \end{pmatrix} [F]. \tag{4.49}$$

Consider $m^* = m-1$, $u_l^* = u_l - 1$ and $v_l^* = v_l$ for $l = 1, \ldots, r$, $s_0^* = s_0$, $\mathfrak{s}_0^* = \mathfrak{s}_0$, and $\mathfrak{q}^* = \mathfrak{q}$. Then $u_l^* + v_l^* = m^*$, $s_0^* \mathfrak{s}_0^{*-1} = \mathfrak{C}\mathfrak{C}^\tau$ and $(\mathfrak{C}, \mathfrak{q}^*) = \mathfrak{D}$, $4ds_0^*\mathfrak{P} \mid \mathfrak{q}^*$ since $\mathfrak{P}^* = \mathfrak{P}$, and $\operatorname{sgn}(s_0^*) = \{(-1)^{v_l^*}\}$ since $v_l^* = v_l$. (4.1) is satisfied by the '$*$system' in view of the fact that $|S| = |S^*|$ (see (4.49)).

Now let $\tau = 1$. By property (i) of the Gauss sums and (4.49), we have

$$G(\varrho^*, S) \cdot \big(G(\varrho^*, 1)\big)^{-1} = G(\varrho^*, S^*) \tag{4.50}$$

where $\varrho^* = \varrho$ satisfies (4.3). Substituting, for $G(\varrho^*, S)$ from (4.2) and for $G(\varrho^*, 1)$ from Lemma 5, in (4.50), we see that the '$*$system' satisfies the Gauss sum condition.

Thus the '$*$system' satisfies all the conditions of the theorem and $m^* = m-1$. Therefore by the induction assumption there exists an integral h-matrix $S_0^* \sim S^* \bmod \mathfrak{q}^*$ such that $r(S_0^*) = m-1$, $\operatorname{sig}(S_0^*) = \{(u_l - 1, v_l)\}$, $\delta(S_0^*) = \mathfrak{s}_0$, $K(S_0^*) = \langle s_0 \rangle$. Then

$$S_0 = \begin{pmatrix} 1 & 0 \\ 0 & S_0^* \end{pmatrix}$$

can easily be seen to have all the required properties.

This completes the proof of the theorem.

References

[1] H. Braun, *Geschlechter quadratischer Formen*, J. Reine. Angew. Math. 182 (1940), pp. 32-49.

[2] — *Zur Theorie der hermitischen Formen*, Abh. Math. Sem. Hans. Univ. 14 (1941), pp. 61-150.

[3] E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, New York 1948.

[4] — *Über die L-Funktionen und den Dirichletschen Primzahlsatz für einen beliebigen Zahlkörper*, Math. Werke, Göttingen (1959), pp. 178-197.

[5] E. Landau, *Über Ideale und Primideale in Idealklassen*, Math. Zeit. 2 (1918), pp. 52-154.

[6] H. Minkowski, *Gesammelte Werke*, Bd. I.

[7] C. L. Siegel, *Über die analytische Theorie der quadratischer Formen I*, Ann. Math. 36 (1935), pp. 527-606.

[8] — *Über die analytische Theorie der quadratischer Formen III*, Ann. Math. 38 (1937), pp. 212-291.

TATA INSTITUTE OF FUNDAMENTAL RESEARCH, BOMBAY

Reçu par la Rédaction le 27. 2. 1963

ACTA ARITHMETICA
VIII (1963)

On the diophantine equation $y^2 - k = x^3$

by

W. LJUNGGREN (Oslo)

1. Let k denote any rational integer. The problem of solving the equation

$$y^2 - k = x^3, \quad k \neq 0 \tag{1}$$

in rational integers x, y has been the subject of many papers and has attracted great interest for more than three centuries. However, no general method is known for determining all solutions of a given equation of the form (1). A summary of earlier results is given in a paper by T. Nagell [8] and in two papers by O. Hemer [3], [4]. Cf. L. J. Mordell [6] for the history of this and allied problems.

It is well-known that the solution of (1) can be brought back to the solution in rational integers u, v of a finite number of equations of the type $f(u, v) = 1$, where $f(u, v)$ is a binary cubic form with integral coefficients. By virtue of a famous theorem due to A. Thue [15] the equation (1) has only a finite number of solutions for a given k.

These cubic forms have negative or positive discriminants according as $k > 0$ or $k < 0$. In case $k > 0$ one has solved all equations with $k \leqslant 100$. An essential tool in obtaining this result is the use of the theorems due to T. Nagell and B. Delaunay [8] concerning cubic forms with negative discriminant. In case $k < 0$ is the problem much more difficult since there are not yet general theorems as to the representations of 1 by binary cubic forms with positive discriminant. Cf. Ljunggren [5].

It was shown by Mordell [7] that the diophantine equation

$$v^2 = 4u^3 - g_2 u - g_3, \tag{2}$$

where g_2 and g_3 are given rational integers, has at most a finite number of rational integral solutions (u, v), when its right-hand side has no squared factor in u. He proved that to every integral solution (u, v) of (2) there corresponded a binary *quartic* with invariants g_2 and g_3 which represented unity, and conversely.

In (1) we have $g_2 = 0$, $g_3 = -4k$, and the problem is now to find all representations of 1 by certain binary, biquadratic forms having these invariants. Since such a form $f_4(x, y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$ has negative discriminant $D = 2^8(g_2^3 - 27g_3^2) = -2^{12}\cdot 3^3\cdot k^2$, the corresponding equation $f_4(x, -1) = 0$ will have two real roots η and η' and two complex roots η'' and η'''. In consequence of the well-known theorem due to Dirichlet concerning the units in algebraic number fields, the field $Q(\eta)$, Q denoting the field of rational numbers, has two independent units ε_1 and ε_2 of infinite order. It is easily shown that the only roots of unity are ± 1 (cf. T. Nagell [9], p. 356). Since it is sufficient to treat forms with $a = 1$, the equation $f_4(x, y) = 1$ implies

$$x + \eta y = \pm \varepsilon_1^{n_1}\cdot \varepsilon_2^{n_2}. \tag{3}$$

The equation (3) gives two exponential equations for determining n_1 and n_2. Therefore we can make use of the p-adic method developed by Th. Skolem in a series of papers [12], [13], [14].

In case $k < 0$ there are 22 unsolved equations with $|k| \leqslant 100$, namely $-k = 7, 15, 18, 23, 25, 26, 28, 39, 45, 47, 53, 55, 60, 61, 63, 71, 72, 79, 87, 89, 95, 100$. In this paper I confine myself to give the complete solution for $k = -7$ and $k = -15$, since I have not yet really checked the basic character of the occuring pair of independent units for all the remaining values of k.

Papers of J. W. S. Cassels [2] and E. S. Selmer [11] concerning the *rational* solutions of (1) contain much of interest also for our problem.

2. The equation

$$x^3 - 7 = y^2 \tag{4}$$

may be written

$$(x-\theta)(x^2 + x\theta + \theta^2) = y^2,$$

where $\theta^3 = 7$, θ real. The common ideal factors of $[x-\theta]$ and $[x^2 + x\theta + \theta^2]$ divide 21, since $(x^2 + x\theta + \theta^2) - (x-\theta)(x+2\theta) = 3\theta^2$. From (4) we therefore conclude, using the fact that $(y, 21) = 1$:

$$[x-\theta] = \mathfrak{a}^2, \tag{5}$$

where $\mathfrak{a}$ is an ideal in $Q(\theta)$. Since the classnumber of $Q(\theta)$ is 3, [2], it follows that $\mathfrak{a}$ must be a principal ideal. The equation (5) is then equivalent to

$$x - \theta = \varepsilon\lambda^2,$$

where ε is a unit and λ is an integer, both in $Q(\theta)$. We have to distinguish between two cases

1° $x - \theta = (a + b\theta + c\theta^2)^2$,

2° $x - \theta = (4 + 2\theta + \theta^2)(a + b\theta + c\theta^2)^2$,

a, b and c denoting rational integers. Here is $(2-\theta)(4+2\theta+\theta^2) = 1$, and $4 + 2\theta + \theta^2 > 1$ is a fundamental unit in $Q(\theta)$. Cf. [2]. We find

$$(a + b\theta + c\theta)^2 = (a^2 + 14bc) + \theta(2ab + 7c^2) + \theta^2(b^2 + 2ac).$$

1° then implies

$$2ab + 7c^2 = -1, \qquad b^2 + 2ac = 0.$$

Since $(b, c) = 1$, the second equation gives $c = \pm 1$. It may be supposed without loss of generality that $c = 1$. Hence

$$ab = -4, \qquad b^2 = -2a,$$

from which it follows that $b = 2$ and $a = -2$, corresponding to

$$32 - \theta = (-2 + 2\theta + \theta^2)^2. \tag{6}$$

In this case we have the only solutions $(x, y) = (32, \pm 181)$.

We now turn to the second possibility, giving

$$(a^2 + 14bc) + 2(2ab + 7c^2) + 4(b^2 + 2ac) = 0, \tag{7}$$

$$2(a^2 + 14bc) + 4(2ab + 7c^2) + 7(b^2 + 2ac) = -1. \tag{8}$$

Combining these equations we get

$$b^2 + 2ac = 1 \tag{9}$$

whence $(b, c) = 1$ and $(b + c, c) = 1$.

Equation (7) may be written

$$(a + 2b + 4c)^2 = 2c(b + c). \tag{10}$$

We must distinguish between two cases:

(i) c even. Since b is odd, (10) implies

$$c = 2e\alpha^2, \qquad b + c = e\beta^2 \qquad \text{and} \qquad a + 2b + 4c = 2e_1\alpha\beta,$$

where $\alpha \geqslant 0$, $\beta \geqslant 0$, $e = \pm 1$, $e_1 = \pm 1$ and α, β integers in Q. Hence

$$a = 2e(-2\alpha^2 - \beta^2 + ee_1\alpha\beta), \qquad b = e(\beta^2 - 2\alpha^2), \qquad c = 2e\alpha^2.$$

Inserting these values for a, b and c in (9) we obtain

$$(\beta ee_1)^4 - 12(\beta ee_1)^2\alpha^2 + 8(\beta ee_1)\alpha^3 - 12\alpha^4 = 1. \tag{11}$$

Putting

$$\eta^4 - 12\eta^2 + 8\eta - 12 = 0, \tag{12}$$

we conclude that $\beta ee_1 + \alpha\eta$ must be a unit with norm $+1$ in the field $Q(\eta)$. The numbers

$$\omega_1 = \tfrac{1}{2}\eta^2 \qquad \text{and} \qquad \omega_2 = \tfrac{1}{4}(\eta^3 - 2\eta) \tag{13}$$

are integers in $Q(\eta)$, because

$$\omega_1^2 = 3\eta^2 - 2\eta + 3 \qquad \text{and} \qquad \omega_2^2 = 6 - 4\eta + 7\eta^2 - \eta\omega_1.$$

Now it can be proved (see section 4) that

$$\varepsilon_1 = \tfrac{1}{2}[\eta^3 - 4\eta^2 + 3\eta - 2]^2, \qquad \varepsilon_2 = \tfrac{1}{4}(\eta^3 + 4\eta^2 - 2\eta + 4) \tag{14}$$

is a pair of fundamental units in the ring $Z[1, \eta, \omega_1, \omega_2]$, Z denoting the ring of rational integers. This yields

$$\beta e e_1 + a\eta = \pm \varepsilon_1^{n_1} \varepsilon_2^{n_2}, \tag{15}$$

(ii) c odd. (10) now implies

$$a = 2e(-\alpha^2 - 2\beta^2 + ee_1\alpha\beta), \qquad b = e(2\beta^2 - \alpha^2), \qquad c = e\alpha^2 .$$

Inserting these values in (9) we find

$$4\beta^4 - 12\beta^2\alpha^2 + 4ee_1\beta\alpha^3 - 3\alpha^4 = 1 , \tag{16}$$

or

$$(2\beta ee_1)^4 - 12(2\beta ee_1)^2\alpha^2 + 8(2\beta ee_1)\alpha^3 - 12\alpha^4 = 4 , \tag{17}$$

i.e.

$$N(2\beta ee_1 + \alpha\eta) = 4 .$$

Noticing

$$(\eta^3 - 4\eta^2 + 3\eta - 2)(-3\eta^3 - 10\eta^2 + 4\eta - 8) = 4 , \tag{18}$$

we get, after some calculations,

$$\frac{2\beta ee_1 + \alpha\eta}{\eta^3 - 4\eta^2 + 3\eta - 2} = a_0 + b_0\eta + c_0\eta^2 + d_0\eta^3 + \tfrac{1}{2}\eta^3(\alpha + \beta ee_1) , \tag{19}$$

where a_0, b_0, c_0 and d_0 are integers in Q. This proves that the left-hand side of (19) is a unit in $Z[\eta]$, because α and βee_1 are both odd rational integers, the last fact resulting from (16). Hence

$$2\beta ee_1 + \alpha\eta = \pm(\eta^3 - 4\eta^2 + 3\eta - 2)\varepsilon_1^{n_1}\varepsilon_2^{n_2} . \tag{20}$$

Combining (15) and (20), we get in both cases

$$u_1 + v_1\eta = (\eta^3 - 4\eta^2 + 3\eta - 2)^p(\eta^3 + 4\eta^2 - 2\eta + 4)^q , \tag{21}$$

where u_1, v_1, p and q are rational integers.

3. In this section we study the equation (21). We put $p = 3x + r$ and $q = 3y + s$, where $r = 0$ or ± 1 and $s = 0$ or ± 1. Further we calculate

$$\begin{aligned} &(\eta^3 - 4\eta^2 + 3\eta - 2)^3 = 1 - 3\eta^3 + 9A = 1 + 3\xi_1, \qquad \xi_1 = -\eta^3 + 3A , \\ &(\eta^3 + 4\eta^2 - 2\eta + 4)^3 = 1 + 3\eta + 3\eta^2 + 3\eta^3 + 9B = 1 + 3\xi_2, \\ &\qquad\qquad \xi_2 = \eta + \eta^2 + \eta^3 + 3B, \end{aligned} \tag{22}$$

denoting by A and B algebraic numbers belonging to $Z[\eta]$.

Treating the equation (21) as a congruence mod 3 we obtain the necessary condition

$$V(r, s) = (\eta^3 - \eta^2 + 1)^r(\eta^3 + \eta^2 + \eta + 1)^s \equiv 1 \pmod 3 . \tag{23}$$

An easy calculation shows that

$$\begin{aligned} &V(1, 0) \equiv 1 - \eta^2 + \eta^3, && V(-1, 0) \equiv 1 + \eta - \eta^2, \\ &V(0, 1) \equiv 1 + \eta + \eta^2 + \eta^3, && V(0, -1) \equiv 1 - \eta - \eta^2 - \eta^3, \\ &V(1, -1) \equiv 1 - \eta + \eta^2 - \eta^3, && V(1, 1) \equiv 1 + \eta - \eta^3, \\ &V(-1, 1) \equiv 1 - \eta + \eta^3, && V(-1, -1) \equiv 1 + \eta^2 \pmod 3, \end{aligned} \tag{24}$$

such that the condition (23) is only fulfilled for $r = s = 0$.

Here use is made of (18) and the equality

$$(\eta^3 + 4\eta^2 - 2\eta + 4)(\eta^3 - 2\eta^2 - 14\eta + 32) = -16 . \tag{25}$$

The equation (21) may now be written

$$u_1 + v_1\eta = (1 + 3\xi_1)^x(1 + 3\xi_2)^y ,$$

or

$$u_1 + v_1\eta = 1 + 3(x\xi_1 + y\xi_2) + 3^2(\ ) + 3^3(\ ) + \dots$$

Inserting the values of ξ_1 and ξ_2 from (22), we obtain

$$u_1 + v_1\eta = 1 + 3\big(-x\eta^3 + y(\eta + \eta^2 + \eta^3)\big) + 3^2(\ ) + 3^3(\ ) + \dots ,$$

yielding the following 3-adic developments:

$$\begin{aligned} 0 &= 3y + 3^2(\ ) + 3^3(\ ) + \dots , \\ 0 &= -3x + 3y + 3^2(\ ) + 3^3(\ ) + \dots , \end{aligned}$$

or

$$\begin{aligned} 0 &= y + 3(\ ) + 3^2(\ ) + \dots , \\ 0 &= -x + y + 3(\ ) + 3^2(\ ) + \dots \end{aligned} \tag{26}$$

According to a theorem of Th. Skolem ([13], p. 180), the equations (26) have at most one solution x, y, because

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

Obviously this solution is $x = y = 0$, corresponding to c even, with $n_1 = n_2 = 0$ and $a = 0$, $\beta ee_1 = \pm 1$. Hence $a = -2e$, $b = e$, $c = 0$ and

$$2 - \theta = (4 + 2\theta + \theta^2)(2 - \theta)^2 .$$

The only solutions of 2° is then $x = 2$, $y = \pm 1$.

Then it is proved:

Theorem 1. *The diophantine equation $x^3 - 7 = y^2$ has exactly two solutions in positive, rational integers x, y, namely $x = 2$, $y = 1$ and $x = 32$, $y = 181$.*

4. We are now going to prove that the units ε_1 and ε_2 in (14) constitute a pair of fundamental units in the ring $Z[1, \eta, \omega_1, \omega_2]$. The equations (18) and (25) show that ε_1 and ε_2 are really units. That these units are independent can be shown by computation of the regulator, but this fact is easier proved in the following way: A relation of the form $\varepsilon_1^{n_1} \cdot \varepsilon_2^{n_2} = 1$ implies an equation of the type (21) with $v_1 = 0$. However, in section 3 we proved this to be impossible unless $n_1 = n_2 = 0$. By the usual method of solving the quartic equation (12) we find $\eta > 0$ and $\eta' < 0$ as the real roots of

$$\eta^2 + 2\eta\sqrt{2-\theta} = 2 + 2\theta + \frac{2}{\sqrt{2-\theta}},$$

and η'', η''' as the complex roots in the equation

$$\eta^2 - 2\eta\sqrt{2-\theta} = 2 + 2\theta - \frac{2}{\sqrt{2-\theta}}.$$

Let $(-1)^i D_i$ denote the determinant of the matrix formed from the matrix below by removing its ith column, $i = 1, 2, 3, 4$:

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ \eta & \eta' & \eta'' & \eta''' \\ \eta^2 & \eta'^2 & \eta''^2 & \eta'''^2 \end{bmatrix}.$$

Some computations give the following inequalities:

$$\begin{gathered} 3.2673 < \eta < 3.2674, \quad -3.86 < \eta' < -3.85, \quad |\eta''| = |\eta'''| < 0.98, \\ |D_1| < 35.6, \quad |D_2| < 19.11, \quad |D_3| = |D_4| < 96.974. \end{gathered} \tag{27}$$

At first we want to prove that ε_2 is no power of another unit in $Z[1, \eta, \omega_1, \omega_2]$. Assuming

$$\varepsilon = \left(\tfrac{1}{4}(a + b\eta + c\eta^2 + d\eta^3)\right)^n, \quad n > 1, \tag{28}$$

ε denoting any unit in the ring mentioned above, we obtain from (28) and the corresponding expressions for the conjugates of ε:

$$d = \frac{4}{\sqrt{D}}\left(D_1 \varepsilon^{1/n} + D_2 \varepsilon'^{1/n} + D_3 \varepsilon''^{1/n} + D_4 \varepsilon'''^{1/n}\right), \tag{29}$$

$$c = \frac{-4}{\sqrt{D}}\left(D_1 \eta \varepsilon^{1/n} + D_2 \eta' \varepsilon'^{1/n} + D_3 \eta'' \varepsilon''^{1/n} + D_4 \eta''' \varepsilon'''^{1/n}\right), \tag{29'}$$

$$b = \frac{4}{\sqrt{D}} \times \tag{29''}$$
$$\times\left(D_1(\eta^2 - 12)\varepsilon^{1/n} + D_2(\eta'^2 - 12)\varepsilon'^{1/n} + D_3(\eta''^2 - 12)\varepsilon_2''^{1/n} + D_4(\eta'''^2 - 12)\varepsilon_3'''^{1/n}\right).$$

From the inequalities

$$18.66 < \varepsilon_2 < 18.80, \quad 3.45 < \varepsilon_2' < 3.49, \quad |\varepsilon_2''| = |\varepsilon_2'''| < \tfrac{1}{8} \tag{30}$$

we then derive, putting $\varepsilon = \varepsilon_2$

$$|d| < \frac{4}{3\cdot 7\cdot 64\sqrt{3}}\left(35.6\sqrt{18.80} + 19.11\sqrt{3.49} + 96.974\cdot 2\right),$$

$$|d| < \frac{4}{2327}(157 + 36 + 194) = \frac{1548}{2327} < 1, \quad \text{i.e.} \quad d = 0,$$

$$|c| < \frac{4(157\cdot 3.27 + 36\cdot 3.86 + 194\cdot 0.98)}{2327} < 2, \quad \text{i.e.} \quad c = 0,$$

because c is even in $Z[1, \eta, \omega_1, \omega_2]$. From the values $c = 0$, $d = 0$ it follows that $a \equiv b \equiv 0 \pmod 4$. However, an equation $(a_1 + b_1\eta)^n = \varepsilon_2$ would give a contradiction because $\varepsilon_2 \notin Z[\eta]$.

Consequently ε_2 is no power of another unit in $Z[1, \eta, \omega_1, \omega_2]$.

In the following reasonings we need three lemmas:

LEMMA 1. *The units ε_1, $\varepsilon_1\varepsilon_2$ and $\varepsilon_1\varepsilon_2^{-1}$ are neither squares, nor cubes in $Z[1, \eta, \omega_1, \omega_2]$.*

Proof. It is easily shown that

$$\left(\tfrac{1}{4}(a + b\eta + c\eta^2 + d\eta^3)\right)^2 \equiv a^2 + b_1\eta + c_1\eta^2 + d_1\eta^3 \pmod 3,$$

b_1, c_1 and d_1 denoting rational integers. Since

$$\begin{gathered} \varepsilon_1 \equiv -1 - \eta + \eta^2 \pmod 3, \quad \varepsilon_1\varepsilon_2 \equiv -1 + \eta - \eta^3 \pmod 3, \\ \varepsilon_1\varepsilon_2^{-1} \equiv -1 - \eta^2 + \eta^3 \pmod 3 \end{gathered} \tag{31}$$

it follows that $a^2 = -1 \pmod 3$, which is impossible.

Further we find

$$\left(\tfrac{1}{4}(a + b\eta + c\eta^2 + d\eta^3)\right)^3 \equiv a + (b + c + d)\eta^3 \pmod 3,$$

which contradicts the values of ε_1, $\varepsilon_1\varepsilon_2$ and $\varepsilon_1\varepsilon_2^{-1}$ in (31). Thus our lemma is proved.

LEMMA 2. *There are no units in $Z[1, \eta, \omega_1, \omega_2]$ of the form $p + q\eta + \omega_1$, $q = 0$ or ± 1.*

Proof. Some calculations give the following values of the norm of $p + q\eta + \omega_1$:

$$\begin{aligned} N(p + \eta + \omega_1) &= p^4 + 12p^3 + 30p^2 + 12p + 45, \\ N(p - \eta + \omega_1) &= p^4 + 12p^3 + 6p^2 - 20p + 21, \\ N(p + \omega_1) &= p^4 + 12p^3 + 30p^2 - 28p + 9. \end{aligned}$$

$N(p + q\eta + \omega_1) = \pm 1$ implies p even, and hence it is obvious that all cases can be excluded mod 16.

LEMMA 3. *There are no units in* $Z[1, \eta, \omega_1, \omega_2]$ *of the form* $p+q\eta+\omega_2$, $q = 0, \pm 1, \pm 2$ *or* 3.

Proof. Some further calculations give

$$N(p+q\eta+\omega_2) = p^4-6p^3+A(q)p^2+B(q)p+C(q)\,,$$

where the values of the coefficients $A(q)$, $B(q)$ and $C(q)$ are given by the following table:

q	0	-1	1	-2	2	3
$A(q)$	-84	-24	-168	12	-276	-408
$B(q)$	56	28	12	-24	-152	-488
$C(q)$	-42	-90	-18	-18	-450	-2058

$N(p+q\eta+\omega_2) = \pm 1$ implies p odd, and mod 8 we conclude that the norm -1 must be excluded. Since $C(q) \equiv 0 \pmod 3$, we deduce $p \not\equiv 0 \pmod 3$. Mod 3 we then obtain $1+B(q)p \equiv 1 \pmod 3$, a contradiction unless $q=1$ or $q=-2$. However, in these cases we get the equations $p^4-6p^3-168p^2+12p-19 = 0$ and $p^4-6p^3+12p^2-24p-19 = 0$ respectively. Both imply $p = \pm 1$ or $p = \pm 19$, which is easily seen to be impossible. Hence our lemma is proved.

A finite procedure of finding a pair of fundamental units when there are only two units, has been developed by W. E. H. Berwick [1]. However, in order to prove our statement concerning the units ε_1 and ε_2, we prefer to make use of a method previously employed by the author [5].

Let τ_1 and τ_2 denote a pair of fundamental units in the ring $Z[1, \eta, \omega_1, \omega_1]$. Then we have

$$\varepsilon_2 = \tau_1^u\tau_2^v\,, \qquad (u, v) = 1\,. \tag{32}$$

Now it is possible to determine two rational integers m, n, such that $um-vn = 1$. Inserting this in (32) we obtain

$$(\varepsilon_2^m\tau_1^{-1})^u = (\varepsilon_2^n\tau_2)^v\,,$$

or

$$\varepsilon_2^m\tau_1^{-1} = \varkappa_1^v \quad \text{and} \quad \varepsilon_2^n\tau_2 = \varkappa_1^u\,,$$

i.e.

$$\tau_1 = \varepsilon_2^m\varkappa_1^{-v} \quad \text{and} \quad \tau_2 = \varepsilon_2^{-n}\varkappa_1^u\,.$$

Consequently the *units* ε_2 *and* $\varkappa_1$ *form a pair of fundamental units.*

This implies

$$\varepsilon_1\varepsilon_2^x = \varkappa_1^y\,, \tag{33}$$

and there is no loss of generality in assuming $y > 0$. We want to show that (33) is impossible unless $y = 1$.

Putting

$$x = ky+r\,, \qquad |r| \leqslant \tfrac{1}{2}y$$

(33) can be written

$$\varepsilon_1\varepsilon_2^r = \varkappa^y\,, \tag{34}$$

where $y \geqslant 5$ on account of Lemma 1.

We must distinguish between two cases:

1° $r \geqslant 0$. In (29), (29′) and (29″) we put

$$\varepsilon = \varkappa = \varepsilon_1^{1/y}\varepsilon_2^{r/y}\,, \qquad \tfrac{1}{2} > r/y \geqslant 0\,, \qquad y \geqslant 5\,.$$

By means of (27), (30) and the inequalities

$$0.00016 < \varepsilon_1 < 0.0002\,, \qquad 8438.3 < \varepsilon_1' < 8540.1\,, \qquad |\varepsilon_1''| = |\varepsilon_1'''| < 0.75\,,$$
$$|\eta^2-12| < 1.325\,, \qquad |\eta'^2-12| < 2.9\,, \qquad |\eta''^2-12| = |\eta'''^2-12| < 12.97$$

we get the following upper bounds for the coefficients d, c and b

$$|d| < \frac{4}{2\,3^2\,7}\big(35.6\sqrt{18.80}+19.11\sqrt[5]{8540.1}\cdot\sqrt{3.49}+96.974\cdot 2\big) < 1\,,$$
$$|c| < 3 \quad \text{and} \quad |b| < 6\,.$$

Hence $d = 0$, $c = 0$ or ± 2 and $b = 0$ or ± 4, because $a \equiv 0 \pmod 4$, $c \equiv 0 \pmod 2$ and $b+2d \equiv 0 \pmod 4$. We then conclude

$$\pm\varkappa = p+q\eta+\omega_1\,, \qquad q = \pm 1\,, \qquad q = 0$$

but this contradicts Lemma 2.

2° $r = -r_1$, $r_1 > 0$. Replacing ε_2 by ε_2^{-1} we get

$$|d| < \frac{4}{2\,3^2\,7}\big(35.6+19.11\sqrt[5]{8540.1}+96.974\sqrt[4]{18.80\cdot 3.49}\cdot 2\big) < 2\,,$$
$$|c| < \frac{4}{2\,3^2\,7}\big(35.6\cdot 3.27+19.11\sqrt[5]{8540.1}\cdot 3.86+96.974\sqrt[4]{18.80\cdot 3.29}\cdot 2\big) < 2\,,$$
$$|b| < \frac{4}{2\,3^2\,7}(35.6\cdot 1.33+118.5\cdot 2.9+552.7\cdot 12.97) < 13\,,$$

i.e., either $d = 0$, $c = 0$ or $d = \pm 1$, $c = 0$, $b = \pm 2$, ± 6 or ± 10, remembering that $b+2d \equiv 0 \pmod 4$. The first possibility is already exclused and the second one contradicts Lemma 3.

Then our statement concerning the units ε_1 and ε_2 is proved.

5. In this and the following section we are going to consider the diophantine equation $y^2+15 = x^3$. As in case $k = 7$ we find

$$[x-\theta] = \mathfrak{a}^3\,, \qquad \theta^3 = 15\,, \tag{35}$$

where $\mathfrak{a}$ is an ideal in $Q(\theta)$. The classnumber of $Q(\theta)$ is 2, and as representatives of the classes of ideals in $Q(\theta)$ may be chosen [1] and $\mathfrak{p}_2$, where

$$\mathfrak{p}_2\cdot\mathfrak{p}_2' = 2 \quad \text{and} \quad \mathfrak{p}_2^2 = [-11+2\theta+\theta^2]\,.$$

See E. S. Selmer [10]. If $\mathfrak{a}$ is a principal ideal, the equation (35) is equivalent either to $x-\theta = \lambda^3$ or to $x-\theta = \varepsilon\lambda^3$, where ε is a basic unit and

λ an integer, both in $Q(\theta)$. As in section 2, case 1°, it is easily shown that the first possibility must be excluded. Taking into consideration the formula

$$1+\theta = (-11+2\theta+\theta^2)^2\varepsilon^{-1}, \qquad \varepsilon = 1-30\theta+12\theta^2,$$

corresponding to the solutions $(x, y) = (1, \pm 4)$ of $y^2-15 = x^3$, the second possibility gives us

$$(x-\theta)(1+\theta) = x+(x-1)\theta-\theta^2 = (a+b\theta+c\theta^2)^2,$$

from which we conclude

$$b^2+2ac = -1 \quad \text{and} \quad (a^2+30bc)-(2ab+15c^2) = 1.$$

Since the first equation implies that a, b, c are all odd rational integers, the second equation is impossible mod 4.

If $\boldsymbol{a} \sim \boldsymbol{p}_2$, the equation (35) is equivalent either to

$$4(x-\theta) = (-11+2\theta+\theta^2)\lambda^2, \tag{36}$$

or to

$$4(x-\theta) = (-11+2\theta+\theta^2)\varepsilon\lambda^2.$$

Utilizing the knowledge of the solutions $(x, y) = (109, \pm 1138)$ of the equation $y^2-15 = x^3$, we find

$$109+\theta = (-11+2\theta+\theta^2)\varepsilon^{-1}(14+2\theta-3\theta^2)^2.$$

In the second case this implies

$$4(x-\theta)(109+\theta) = (a+b\theta+c\theta^2)^2,$$

i.e.

$$b^2+2ac = -4 \quad \text{and} \quad (a^2+30bc)-109(2ab+15c^2) = 4\cdot 109^2,$$

from which we deduce that a, b, c are all even rational integers. Putting $a = 2a_1$, $b = 2b_1$ and $c = 2c_1$, the equations may be written

$$b_1^2+2a_1c_1 = -1 \quad \text{and} \quad (a_1^2+30b_1c_1)-109(2a_1b_1+15c_1^2) = 109^2.$$

However, this last equation is impossible mod 4 for odd integers a_1, b_1, c_1.

We now turn to the remaining case (36). From (36) it follows, putting $\lambda = a+b\theta+c\theta^2$ and $a_2 = a^2+30bc$, $b_2 = 2ab+15c^2$, $c_2 = b^2+2ac$

$$a_2+2b_2-11c_2 = 0, \tag{37'}$$

$$2a_2-11b_2+15c_2 = -4. \tag{37''}$$

The equation (37′) may be written

$$(5b-13c)(3b-7c) = (a+2b-11c)^2.$$

Hence

$$5b-13c = de\alpha^2, \quad 3b-7c = de\beta^2 \quad \text{and} \quad a+2b-11c = de_1\alpha\beta,$$

where $\alpha \geqslant 0$, $\beta \geqslant 0$, $d \geqslant 1$, $e = \pm 1$, $e_1 = \pm 1$ and α, β integers in Q. These equations yield the following values of a, b and c

$$4a = de(29\beta^2-19\alpha^2+4\alpha\beta ee_1), \quad 4b = de(13\beta^2-7\alpha^2), \quad 4c = de(5\beta^2-3\alpha^2). \tag{38}$$

Eliminating a_2 between (37′) and (37″) we get

$$15b_2-37c_2 = 4.$$

Making use of (38) the last equation may be written

$$-\alpha^4+3\alpha^3\beta ee_1-3\alpha^2\beta^2+5\alpha\beta^3 ee_1-3\beta^4 = \frac{4}{d^2},$$

or, putting $\alpha-\beta ee_1 = h$, $\beta ee_1 = k$:

$$h^4+h^3k-4hk^3-k^4 = \frac{-4}{d^2}.$$

The possibility $d = 1$ is easily excluded mod 2. For $d = 2$ we obtain

$$h^4+h^3k-4hk^3-k^4 = -1. \tag{39}$$

Setting

$$\eta^4-\eta^3+4\eta-1 = 0,$$

we conclude that $h+k\eta$ must be a unit with norm -1 in the field $Q(\eta)$. Now it can be proved that η and $2-\eta^2$ is a pair of fundamental units in $Z[\eta]$. It is obvious that η is a unit, and $2-\eta^2$ is a unit in virtue of the relation

$$(2-\eta^2)(2-7\eta+5\eta^2-2\eta^3) = 1.$$

This yields

$$h+k\eta = \pm\eta^{n_1}(2-\eta^2)^{n_2}, \qquad n_1 \text{ odd}. \tag{40}$$

6. Here we want to show that the only solution of (40) in rational integers n_1, n_2 is $n_1 = 1$, $n_2 = 0$.

We find

$$\eta^6 = 1+3\xi_1 \quad \text{and} \quad (2-\eta^2)^3 = 1+3\xi_2,$$

where

$$\xi_1 = -\eta-\eta^2-\eta^3 \quad \text{and} \quad \xi_2 = 4-7\eta-3\eta^2-3\eta^3.$$

Putting $n_1 = 6u+r$ and $n_2 = 3v+s$, we have to study the equation

$$\pm(h+k\eta) = \eta^r(2-\eta^2)^s(1+3\xi_1)^u(1+3\xi_2)^v, \tag{41}$$

for $r = \pm 1$ or 3 and $s = 0$ or ± 1.

Regarding (41) as a congruence mod 3, it is easily found that the only possibility which may occur is $r = 1$, $s = 0$. Now (41) gives

$$\pm(h+k\eta) = \eta+3(u\xi_1\eta+v\xi_2\eta)+3^2(\ )+3^3(\ )+\dots$$

or

$$\pm h+(-1\pm k)\eta = 3\big(u(-1+\eta-\eta^2+\eta^3)+v(\eta-\eta^2)\big)+3^2(\ )+3^3(\ )+\ldots$$

This yields the following 3-adic developments

$$(42)\qquad \begin{aligned} 0 &= -u-v+3(\ )+3^2(\ )+\ldots,\\ 0 &= u+3(\ )+3^2(\ )+\ldots \end{aligned}$$

According to a theorem of Th. Skolem ([13], p. 180), the equations (42) have at most one solution u, v, because

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

Obviously this solution is $u = v = 0$, corresponding to $n_1 = 1$, $n_2 = 0$, which was to be proved. This implies $h = 0$, $k = \pm 1$ and further on $a = \beta e e_1 = \pm 1$ and $a = 7e$, $b = 3e$, $c = e$. The final result is then

$$4(4-\theta) = (-11+2\theta+\theta^2)(7+3\theta+\theta^2)^2,$$

i.e. $x = 4$. Then it is proved:

THEOREM 2. *The diophantine equation $x^3-15 = y^2$ has exactly one solution in positive rational integers x, y, namely $x = 4$, $y = 7$.*

7. At last we give some interesting remarks in connection with the solution of our problem for $k = -7$ and $k = -15$. The corresponding equations are easily shown to be impossible if y is even. In case y is odd, we deduce

$$2^{(-k-7)/4}\cdot\frac{y+\sqrt{k}}{2} = \frac{1+\sqrt{k}}{2}\left(\frac{a+b\sqrt{k}}{2}\right)^3,$$

from which it follows

$$a^3+3a^2b+3kab^2+kb^3 = 2^{(5-k)/4}.$$

This equation may be written

$$(a+b)^3-3(1-k)(a+b)b^2+2(1-k)b^3 = 2^{(5-k)/4},$$

i.e.

$$(a+b)^3-24(a+b)b^2+16b^3 = 8, \qquad k = -7,$$
$$(a+b)^3-48(a+b)b^2+32b^3 = 32, \qquad k = -15.$$

Putting in the first case $a+b = 2u$, $b = v$ and in the second one $a+b = 4u$, $b = v$, we obtain

$$(43)\qquad u^3-6uv^2+2v^3 = 1$$

and

$$(44)\qquad v^3-6v^2u+2u^3 = 1,$$

respectively.

Hence, by the way we have got the complete solution of (43) and of (44), where the cubic forms on the left-hand side have positive discriminants. The equation (43) has the two solutions $(u, v) = (1, 0)$ and $(u, v) = (1, 3)$, while the equation (44) has the only solution $(u, v) = (0, 1)$.

In the introduction we mentioned that in case $k > 0$ the equation (1) could be investigated by working in a cubic field with one fundamental unit only. This implies that the problem of finding all representations of 1 by certain quartics could be dealt with in an easier way, obviating the difficulties arising from the fact that the corresponding biquadratic fields have two fundamental units. Since $y^2-15 = x^3$ has exactly the solutions mentioned in section 5 we conclude (cf. [8], p. 37):

The equation

$$x^4-6x^2y^2+32xy^3-3y^4 = 1$$

has no solution in integers x, y with $y \neq 0$.

References

[1] W. E. H. Berwick, *Algebraic number-fields with two independent units*, Proc. London Math. Soc. 34 (1932), pp. 360-378.

[2] J. W. S. Cassels, *The rational solutions of the diophantine equation $Y^2 = X^3-D$*, Acta Math. 82 (1950), pp. 243-273.

[3] O. Hemer, *On the diophantine equation $y^2-k = x^3$* (diss.), Uppsala 1952.

[4] — *Notes on the diophantine equation $y^2-k = x^3$*, Arkiv för Mat. 3 (1954), pp. 67-77.

[5] W. Ljunggren, *Einige Bemerkungen über die Darstellung ganzer Zahlen durch binäre kubische Formen mit positiver Diskriminante*, Acta Math. 75 (1942), pp. 1-21.

[6] L. J. Mordell, *A chapter in the theory of numbers*, Cambridge 1947.

[7] — *Note on the integer solutions of the equation $Ey^2 = Ax^3+Bx^2+Cx+D$*, Mess. of Math. 51 (1922), pp. 169-171.

[8] T. Nagell, *L'analyse indéterminée du degré superieur*, Mem. des Sci. Math. 39 (1929).

[9] — *Sur quelques questions dans la théorie des corps biquadratiques*, Arkiv för Mat. 26 (1961), pp. 347-376.

[10] E. S. Selmer, *Tables for the purely cubic field $K(\sqrt[3]{m})$*, Avh. Norske Vid. Akad. Oslo, I. 1955, No. 5, pp. 1-32.

[11] — *The rational solutions of the diophantine equation $\eta^2 = \xi^3-D$ for $|D| \leqslant 100$*, Math. Scand. 4 (1956), pp. 281-286.

[12] Th. Skolem, *Einige Sätze über gewisse Reihenentwicklungen und exponentiale Beziehungen mit Anwendung auf diophantische Gleichungen*, Skr. Norske Vid. Akad. Oslo, I. 1933, No. 6, pp. 1-61.

[13] — *Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen*, 8de Skand. Mat. Kongress, Stockholm 1934, pp. 163-188.

[14] — *Einige Sätze über p-adische Potenzreihen mit Anwendung auf gewisse exponentielle Gleichungen*, Math. Ann. 11 (1935), pp. 399-424.

[15] A. Thue, *Über Annäherungswerte algebraischer Zahlen*, Journ. f. Math. 135 (1909), pp. 284-305.

Reçu par la Rédaction le 19. 2. 1963