ECONOMETRIC INSTITUTE

A CLASS OF DIOPHANTINE EQUATIONS CONNECTED WITH CERTAIN ELLIPTIC CURVES CURVES OVER $Q(\sqrt{-13})$.

R.J. STROEKER

REPORT 7621/M

ERASMUS UNIVERSITY ROTTERDAM, P.O. BOX 1738, ROTTERDAM, THE NETHERLANDS

ECONOMETRIC INSTITUTE

A CLASS OF DIOPHANTINE EQUATIONS CONNECTED WITH CERTAIN ELLIPTIC CURVES OVER $Q(\sqrt{-13})$.

by

R.J. Stroeker

Report no. 7621/M

ERASMUS UNIVERSITY ROTTERDAM, P.O. BOX 1738, ROTTERDAM, THE NETHERLANDS

A CLASS OF DIOPHANTINE EQUATIONS CONNECTED WITH CERTAIN ELLIPTIC CURVES OVER $\mathbb{Q}(\sqrt{-13})$.

by R.J. Stroeker

0. INTRODUCTION

In the course of trying to construct an elliptic curve with good reduction everywhere over an imaginary quadratic number field K of small discriminant (if such a curve exists then the classnumber of K has to be unequal to 1, see [5], p. 16), we came across the following Diophantine equation

$$(0.1) \qquad x^3-13y^2 = \pm\, 2^n 3^3$$

in rational integers x,y and n ($n \geq 0$). Some of the solutions of (0.1) correspond to elliptic curves over $K := \mathbb{Q}(\sqrt{-13})$ with good reduction at every place, with the possible exception of the prime $\wp$ above 2 (cf. [5], p. 37). Although, unfortunately, we did not achieve our goal (i.e. find a curve with good reduction at $\wp$ as well), we feel that equation (0.1) is interesting enough in itself to justify a detailed discussion.

Clearly, equation (0.1) has infinitely many solutions (x,y,n) or no solution at all. Indeed, if (x,y,n) is a solution, so is $(2^{2t}x, 2^{3t}y, n+6t)$ for every $t \in \mathbb{Z}$, $t \geq 0$. This leads to

<u>DEFINITION</u>. A solution $(x,y,n) \in \mathbb{Z}^3$, $n \geq 0$ of (0.1) is called basic iff

$$\left.\begin{array}{c} x = x't^2,\ y=y't^3,\ n\geq 6t \\ x',y',t \in \mathbb{Z} \end{array}\right\} \Rightarrow \quad t = \pm 1.$$

It is obvious that a solution is either basic or results from a basic solution in the above indicated way.

Firstly, we note that any solution (x,y,n) satisfies $n\equiv 0 \pmod 3$. Indeed, this is an immediate consequence of $x^3\equiv 0,\pm 1$ or $\pm 8 \pmod{13}$.

In the following sections we shall therefore study the Diophantine equation

$$(0.2) \qquad x^3-13y^2 = \tau 2^{3m}3^3, \tau = \pm 1$$

with $x,y,m \in \mathbb{Z}$ and $y,m\geq 0$.

The object of this paper is to prove

<u>THEOREM</u>. The Diophantine equation (0.2) has precisely nine basic solutions, namely

$(x,y,m)=(3,0,0)$ and $(6,0,1)$ in case $\tau=1$ and $(x,y,m)=(-3,0,0),(-6,0,1),$ $(-2,4,1),(21,27,1),$ $(1438,15124,1),$ $(-11,31,3)$ and $(1189,11561,7)$ in case $\tau = -1$.

1. TWO LEMMA'S

In this section we shall state and prove two lemmas, which play an essential part in the proof of the theorem.

LEMMA 1. The Diophantine equation

$$(1.1)\qquad 13x^2=(2^n+9)^2-108 \quad x,n \in \mathbb{N}$$

has the solutions $(x,n) = (1,1),(11,5)$ and no others.

PROOF. Let (x,n) be a solution of (1.1). Put $K:=\mathbb{Q}(\sqrt{3})$. Then (1.1) may be written as

$$\mathrm{Norm}_{K/\mathbb{Q}}(2^n+9+6\sqrt{3}) = 13x^2.$$

Thus

$$(1.2)\qquad 2^n+9\pm6\sqrt{3} = \varepsilon 2^r(4+\sqrt{3})^s(a+b\sqrt{3})^2,$$

where $r,s \in \{0,1\}$, a and b are rational integers and ε is unit of O_K, the ring of integers of K. Taking norms, we obtain $r=0$, $s=1$ and $\mathrm{Norm}_{K/\mathbb{Q}}\varepsilon=1$.

Now $\eta:=2-\sqrt{3}$ is a fundamental unit of K. Hence we may take $\varepsilon=\pm\eta^t$ with $t \in \{0,1\}$. In case $t=0$, we have, by comparing the coefficients of $\sqrt{3}$ on either side of (1.2),

$$a^2+3b^2 \equiv \pm 2 \pmod 8$$

and this is impossible. Hence $t=1$. Now (1.2) becomes

$$(1.3)\qquad \pm(2^n+9)\pm6\sqrt{3} = (2-\sqrt{3})(4+\sqrt{3})(a+b\sqrt{3})^2,$$

where the $\pm$ signs are independent. Equating coefficients in (1.3) leads to

$$(1.4)_1\qquad \pm(2^n+9) = 5(a^2+3b^2) - 12ab$$

and

$(1.4)_2$ $$\pm 6 = -2\,(a^2+3b^2) + 10\,ab$$

with independent $\pm$ signs.

The right-hand side of $(1.4)_1$ is positive definite, whence the + sign is the correct one. It is easy to check that, in case $n=1$, (1.4) is only possible when $a=2b$ and $b^2=1$. This gives $(x,n)=(1,1)$.

Considering $(1.4)_1$ modulo 3 shows that n has to be odd. Thus $n\geq 3$. From $(1.4)_1$ modulo 8, we deduce that a is odd and $b\equiv 2 \pmod 4$. Combining this result with $(1.4)_2$ modulo 8 shows that we must have the - sign in $(1.4)_2$.

Put $a=u$, $b=2v$ then both u and v are odd.
In terms of u and v, (1.4) reads

$(1.5)_1$ $$13uv = 2^{n-1} - 3$$

and $(n \geq 3)$

$(1.5)_2$ $$(2u+3v)^2+39v^2 = 2^{n+1}\,.$$

Equation $(1.5)_1$ then implies $2^{n-1}\equiv 3 \pmod{13}$ and thus $n\equiv 5 \pmod{12}$.
Put $n=:\ 5+12T$ ($T\in\mathbb{Z}, T\geq 0$).

Consider the number field $L:=\mathbb{Q}(\sqrt{-39})$. The class number of L equals 4 and $(2)=\mathfrak{p}\mathfrak{p}'$ with prime ideals $\mathfrak{p}:=(2,\theta)$, $\mathfrak{p}':=(2,\bar{\theta})$ where $\theta:=\frac{1}{2}(1+\sqrt{-39})$.
We write $(1.5)_2$ in the form

(1.6) $$\mathrm{Norm}_{L/\mathbb{Q}}(u+v+v\theta)=2^{n-1},\ n=5+12T.$$

Because both u and v are odd, (1.6) implies that

$$(u+v+v\theta) = \wp^{4(1+3T)} \text{ or } \wp'^{4(1+3T)}$$

Now $\wp^4 = (2+\theta)$ and $\wp'^4 = (2+\bar{\theta}) = (3-\theta)$. Hence

$$u+v+v\theta = \pm(2+\theta)^{1+3T} \text{ or } \pm(3-\theta)^{1+3T},$$

because ± 1 are the only units in O_L. Now $u+v+v\theta = \pm(3-\theta)^{1+3T}$ gives $\theta \equiv 1+\theta \pmod 2$ since both u and v are odd. This is clearly impossible. Choosing the sign of u and v appropriately, we arrive at

$$u+v+v\theta = (2+\theta)^{1+3T}.$$

Put $\xi := 2+\theta$, then (1.5) takes the form

$$(1.7) \qquad \begin{cases} u-v+v\xi = \xi^{1+3T} \\ 13uv = 2^{4+12T}-3 \end{cases} \qquad (T \geq 0)$$

It is easily seen that

$$\xi^{3^\lambda} \equiv 1+3^{\lambda+1}\xi \pmod{3^{\lambda+2}}, \ \lambda=1,2,\ldots$$

Let $T =: 3^{\lambda-1}t$, $\lambda \geq 1$. Then

$$\xi^{1+3T} = \xi^{1+3^\lambda t} \equiv \xi(1+3^{\lambda+1}\xi)^t \equiv -3^{\lambda+1}t + (1-3^{\lambda+1}t)\xi \pmod{3^{\lambda+2}}$$

and we deduce from (1.7) that

$$u-v \equiv -3^{\lambda+1}t \pmod{3^{\lambda+2}} \text{ and } v \equiv 1-3^{\lambda+1}t \pmod{3^{\lambda+2}}$$

and thus $uv \equiv 1 \pmod{3^{\lambda+2}}$. Combining this with the second equation in (1.7) gives

$$2^{4.3^{\lambda}t} \equiv 1 \pmod{3^{\lambda+2}}.$$

The implication is that $t \equiv 0 \pmod 3$, since the multiplicative cyclic group of $\mathbb{Z}_{3^\lambda}$ is generated by 2 for each $\lambda=1,2,\ldots$

By means of induction it is then easy to show that $T \equiv 0 \pmod{3^{\lambda}}$ for all $\lambda \in \mathbb{N}$. Hence $T=0$. This given $n=5$, $u=v=1$, which leads to $(x,n)=(11,5)$. This completes the proof of the lemma. □

LEMMA 2. The Diophantine equation

(1.8)
$$x^3-91xy^2+338y^3=8 \quad x,y \in \mathbb{Z}$$

has exactly four solutions viz. $(x,y)=(2,0),(5,1),(6,1)$ and $(-11,1)$.

PROOF. Let $f \in \mathbb{Z}[x,y]$ be given by $f(x,y):=x^3-91xy^2+338y^3$. The discriminant of f equals $-2^5 13^3$. Let θ be the real voot of $f(t,1)=0$ and put $K:=\mathbb{Q}(\theta)$. Now $\omega := -\frac{1}{2}\theta + \frac{\theta^2}{26} \in O_K$, the ring of integers of K and $\theta=-13-10\omega+\omega^2$. Hence K and $\mathbb{Q}(\omega)$ coincide. The absolute discriminant of K equals $-2^3.13$ and the set $\{1,\omega,\omega^2\}$ is an O_K-basis.

Further, we claim that the unit $\eta:=17+9\omega-\omega^2$ is fundamental. We prove this as follows. Because $1<\eta\lesssim 4,85$ let $\varepsilon := a+b\omega+c\omega^2$ with $a,b,c \in \mathbb{Z}$ be a unit, satisfying

$$1 < \varepsilon < 5 \text{ and hence } \frac{1}{5} < \varepsilon'\bar{\varepsilon}' < 1.$$

It then easily follows that $0<|c|\leq 2$. Checking all possibilities shows that only $c=-1$ satisfies the requirements. This gives $\varepsilon=\eta$. Consequently η is the unit >1 of minimal size.

Finally, $(2)=\mathfrak{p}^2\mathfrak{q}$ with $\mathfrak{p}:=(2+\omega)$ and $\mathfrak{q}:=(15+8\omega-\omega^2)$. This gives us sufficient information on the number field K to tackle equation (1.8) successfully. We note that $\{1,\theta,\omega\}$ also is an $\mathfrak{O}_K$-basis.

Let (x,y) be a solution of (1.8). Then

$$\mathrm{Norm}_{K/\mathbb{Q}}(u-v\theta) = 8$$

for some rational integers u and v. This gives the ideal equation

$$(1.9) \qquad (u-v\theta) = \mathfrak{p}^r\mathfrak{q}^s$$

with $r, s \in \mathbb{Z}$, $r, s \geq 0$ and $r+s=3$.

We consider the four cases $(r,s)=(3,0)$, $(2,1)$, $(1,2)$ and $(0,3)$ separately.

<u>I : $(r,s)=(3,0)$.</u>

From (1.9) we have

$$(u-v\theta) = \mathfrak{p}^3 = (5-\theta).$$

Let $a,b,c \in \mathbb{Z}$ be given in such a way that

$$u-v\theta=(5-\theta)(a+b\theta+c\,\omega).$$

Then $u \equiv v \pmod 4$. Put $u-5v=:4t$. It is easily established that $a = -33t+v$, $b=9t$ and $c=13t$. Hence

$$(1.10) \quad \begin{cases} a+b\theta+c\omega = \pm\eta^k, \quad k \in \mathbb{Z} \\ \text{and} \\ 13b = 9c \quad . \end{cases}$$

Considering (1.10) modulo 8, we deduce that $13b=9c$ can only be satisfied if $k \equiv 0 \pmod 4$. There are two possibilities to be considered, namely

$I_1 : k = -4+2^\lambda T$ with $\lambda \in \mathbb{N}$, $\lambda \geq 3$ and T odd if $T \neq 0$

and

$I_2 : k = 2^\lambda T$ with $\lambda \in \mathbb{N}$, $\lambda \geq 3$ and T odd if $T \neq 0$.

It is an easy exercise to check that

$$\eta^{2^\lambda} \equiv 1-2^\lambda(1+3\theta+3\omega) \pmod{2^{\lambda+3}}, \ \lambda \geq 3.$$

In the first case (I_1) we have

$$a+b\theta+c\omega \equiv \pm\eta^{-4} \cdot \eta^{2^\lambda T} \equiv \pm\,\eta^{-4}\,\{1-2^\lambda(1+3\theta+3\omega)\}^T \equiv$$

$$\equiv \pm(133-36\theta-52\omega)\{1-2^\lambda T(1+3\theta+3\omega)\} \equiv$$

$$\equiv \pm\{133-36\theta-52\omega-2^\lambda T(1+3\theta+3\omega)\} \pmod{2^{\lambda+3}}.$$

It now follows from $13b = 9c$ that $3.2^{\lambda+2}T \equiv 0 \pmod{2^{\lambda+3}}$. Hence T is even, which implies $T=0$. Then $k=-4$ and $(u,v) = (-11,1)$.

Similarly, in case I_2 we find

$$a+b\theta+c\omega = \pm\ \eta^{2^{\lambda}T} \equiv \pm\{1-2^{\lambda}(1+3\theta+3\omega)\}^{T} \equiv$$

$$\equiv \pm\{1-2^{\lambda}T(1+3\theta+3\omega)\}(\mathrm{mod}\ 2^{\lambda+3}).$$

Again $13b = 9c$ implies $3.2^{\lambda+2}T \equiv 0\ (\mathrm{mod}\ 2^{\lambda+3})$. Thus T is even $\Rightarrow T = 0$. This gives $k=0$, $(u,v)=(5,1)$.

II: $(r,s) = (2,1)$.

From (1.9) we deduce

$$(u-v\theta) = 2$$

and thus

$$u-v\theta = \pm\ 2\eta^{k}\ ,\ k \in \mathbb{Z}.$$

In an entirely analogous way (see I), we deduce that $k = 0$, making use of

$$\eta^{2^{\lambda}} \equiv 1 + 2^{\lambda}(1+\theta+\omega)(\mathrm{mod}\ 2^{\lambda+2}),\ \lambda \geq 2.$$

This gives $(u,v) = (2,0)$.

III: $(r,s) = (1,2)$.

Now we have from (1.9)

$$(u-v\theta) = \wp\mathfrak{q}^{2}$$

and thus $u-v\theta = \pm\eta^{k}(2+\omega)(2-\theta-2\omega)^{2}\ ,\ k \in \mathbb{Z}$.

This implies modulo 2 that

$$u-v\theta \equiv \eta^{k}\omega\theta^{2} \equiv \eta^{k}(1+\theta+\omega) \equiv \eta^{k}+\eta^{k+1} \equiv 1+\theta+\omega, \text{ because}$$

$$\eta \equiv \theta+\omega\ (\mathrm{mod}\ 2) \text{ and } \eta^{2} \equiv 1\ (\mathrm{mod}\ 2).$$

Clearly, we have arrived at an impossibility.

IV: $(r,s) = (0,3)$.

Finally, (1.9) gives in this case

$$(u-v\theta) = \mathfrak{q}^3 = (6-\theta).$$

Suppose $a,b,c \in \mathbb{Z}$ are given in such a way that

$$u-v\theta = (6-\theta)(a+b\theta+c\omega).$$

Then

$$(1.11)\begin{cases} a+b\theta+c\omega = \pm\eta^k, \quad k \in \mathbb{Z} \\ \text{and} \\ 26b = 19c. \end{cases}$$

As in I, we deduce from (1.11) that $k \equiv 0 \pmod 4$.

Making use of

$$\eta^{2^\lambda} \equiv 1+2^\lambda(1+\theta+\omega) \pmod{2^{\lambda+1}}, \quad \lambda \geq 2$$

we again find that $k=0$. This gives $(u,v)=(6,1)$.

This completes the proof of the lemma.

$\square$

2. THE PROOF OF THE THEOREM.

Let (x,y,m) be a basic solution of (0.2). We distinguish between the following cases, according as $m\geq 2$, $m=1$ or $m=0$.

In the first case ($m\geq 2$), we see immediately that x has to be odd. For otherwise, (x,y,m) would not be basic. Write (0.2) in the form

$$(2.1)\qquad (x-3\tau 2^m)(x^2+3\tau 2^m x+3^2 2^{2m}) = 13y^2.$$

The only possible common prime divisor of the two factors in the left-hand side of (2.1) is the prime 3. Hence

$$(2.2)\begin{cases} x - 3\tau 2^m = Aa^2 \\ \text{and} \\ x^2+3\tau 2^m x+3^2 2^{2m} = Bb^2, \end{cases}$$

with $A,B \in \mathbb{Z}$, $A,B\geq 0$ and squarefree (if $\neq 0$), $(A,B) = 1$ or 3 and $a,b \in \mathbb{Z}$, $a,b\geq 0$ with $(a,b) = 1$. Since $AB(ab)^2 = 13y^2$, we have $AB = 13$ in case $(A,B)=1$ and $AB = 9.13$ in case $(A,B) = 3$. From the quadratic equation of (2.2), we deduce that

$$(3\tau 2^m)^2 - 4\,(3^2 2^{2m}-Bb^2) = \text{square}$$

and thus

$$Bb^2-3^3 2^{2m-2} = \text{square}\ .$$

This gives, because of $m\geq 2$ and the fact that both b and B are odd, that

$$B \equiv 1+2^{2m-2} \pmod 8).$$

Hence $B \equiv 1$ or $5 \pmod 8$. Since $B \in \{1,3,13,39\}$ it follows that $B \in \{1,13\}$ and consequently $(A,B) = 1$. This leaves the two possibilities

$$A = 1,\ B = 13 \text{ and } A = 13,\ B = 1.$$

Put K: = $\mathbb{Q}(\rho)$ with $\rho := \frac{1}{2}+\frac{1}{2}\sqrt{-3}$. The second equation of (2.2) may be written as

$$\mathrm{Norm}_{K/\mathbb{Q}}(x+3\tau 2^m\rho) = Bb^2, \text{ with } B = 1 \text{ or } 13.$$

Hence

$$(2.3) \qquad x+3\tau 2^m\rho = \eta(-1+4\rho)^r(-1+4\bar{\rho})^s(c+d\rho)^2,$$

where η is a unit of O_K, $r,s \in \{0,1\}$ and c,d are rational integers.

Taking norms in (2.3) yields:

$$\mathrm{Norm}_{K/\mathbb{Q}}(\eta)13^{r+s}(c^2+cd+d^2)^2 = Bb^2,$$

which implies that we may take $\eta = \pm 1$ in (2.3) - every unit in O_K may be written as $\pm$ the square of a unit - and $(r,s) = (0,0)$, $(1,0)$ or $(0,1)$.

This leaves the following cases to be investigated:

$$(2.3.1) \qquad x+3\tau 2^m\rho = \eta(c+d\rho)^2 \text{ with } \eta = \pm 1, A = 13 \text{ and } B = 1,$$

$$(2.3.2) \qquad x+3\tau 2^m\rho = \eta(-1+4\rho)(c+d\rho)^2 \text{ with } \eta = \pm 1, A = 1 \text{ and } B = 13,$$

$$(2.3.3) \qquad x+3\tau 2^m\bar{\rho} = \eta(-1+4\rho)(c+d\rho)^2 \text{ with } \eta = \pm 1, A = 1 \text{ and } B = 13.$$

We first consider (2.3.1). Equating coefficients of 1 and ρ in (2.3.1) we obtain, taking also the first equation in (2.2) into consideration,

$$(2.4) \qquad \begin{cases} x = \eta(c^2-d^2) = 3\tau 2^m+13a^2, \; y = a(c^2+cd+d^2) \\ 3\tau 2^m = \eta d(2c+d). \end{cases}$$

Now c and d are co-prime, because (x,y,m) is a basic solution. Moreover d is even and c is odd since $m \geq 2$. If we consider the first equation in (2.4) modulo 4, we find $\eta \equiv a^2 \equiv 1 \pmod 4$ and hence $\eta = 1$. Then the third equation modulo 8 gives:

$$2^m \equiv d(2+d) = (d+1)^2-1 \equiv 0 \pmod 8).$$

Thus $m\geq 3$. Combining the first and the third equation in (2.4) leads to:

$$(2.5) \qquad 13a^2 = (c-d)^2-3d^2$$

and consequently, $3|a$ if $3|2c+d$. However, this gives $3|d$ and hence also $3|c$, a contradiction.

Hence $3\nmid 2c+d$, which implies that $3|d$.

Now $2||d$, since $4|d$ would imply (see (2.5)) that

$$-3 \equiv (c-d)^2 \pmod 8),$$

which is clearly contradictory. Because of (2.4), the third equation, we deduce that $|d| = 6$. Then (2.4) and (2.5) yield :

$$(2.6) \qquad 13a^2 = (-\tau.2^{m-2}+9)^2-108.$$

Considering (2.6) modulo 13 shows that $m \equiv 0$ or $1 \pmod 3)$. But then $a^2 \equiv 3-(2(\tau-1))^2 \equiv 3 \pmod 7)$ in case $\tau = 1$. But 3 is a quadratic non-residue mod 7. Hence $\tau = -1$ and (2.6) becomes equation (1.1) of lemma 1. Thus $(a,m) = (1,3)$ or $(11,7)$ and this leads to the solutions

$$\underline{(x,y,m) = (-11,31,3), (1189,11561,7)}.$$

Next we look at (2.3.2). This time we find

$$(2.7) \quad \begin{cases} x = -\eta(c^2+8cd+3d^2) = 3\tau 2^m+a^2, \; y = a(c^2+cd+d^2) \\ 3\tau 2^m = \eta(4c^2+6cd-d^2). \end{cases}$$

The first and the third equation in (2.7) imply that c is odd and d is even. Also a is odd. Since $m \geq 2$, we have $a^2 \equiv -\eta \pmod 4$ and thus $\eta = -1$. Considering the first and third equation modulo 8, it is an easy exercise to show that $2 \| d$ and consequently m = 2. Then

$$a^2 = c^2+8cd+3d^2-12\tau = c^2+8cd+3d^2-12\tau+3(4c^2+6cd-d^2+12\tau) =$$

$$= 13c^2+26cd+24\tau \equiv -2\tau \pmod{13}.$$

However 2 and -2 are quadratic non-residues mod. 13. It is not difficult to show that (2.3.3.) can be treated in a completely analogous fashion, so that no solutions are found in either case.

This completes the discussion of (0.2) in case $m \geq 2$.

We now wish to solve (0.2) in case m = 1, and again the cases $\tau = 1$ and $\tau = -1$ will be treated separately. First, let $\tau = 1$. If $K := \mathbb{Q}(\sqrt{-78})$, then the class number $h_K = 4$ and $(2) = \mathfrak{p}^2$, $(3) = \mathfrak{q}^2$, where $\mathfrak{p}$ and $\mathfrak{q}$ are prime ideals. We write (0.2), with m = 1 and $\tau = 1$, in the form

$$\mathrm{Norm}_{K/\mathbb{Q}}(2^3 3^3+6y\sqrt{-78}) = (6x)^3.$$

Thus

$$(2.8) \qquad (2^3 3^3+6y\sqrt{-78}) = \mathfrak{p}^r \mathfrak{q}^s \mathfrak{a}^3,$$

where $r,s \in \{0,1,2\}$ and $\mathfrak{a}$ is an integral ideal of K. Taking norms, we deduce that we may take r = s = 0, in the ideal equation (2.8). Apparently, $\mathfrak{a}^3$ is a principal ideal, and since $(h_K,3) = 1$, also $\mathfrak{a}$ is principal. Put $\mathfrak{a} = (a+b\sqrt{-78})$ with $a,b \in \mathbb{Z}$. We have

$$2^3 3^3+6y\sqrt{-78} = (a+b\sqrt{-78})^3$$

and equating coefficients of 1 and $\sqrt{-78}$ yields:

$$(2.9) \qquad 2^3 3^3 = a^3-234ab^2 \ , \ 6y = 3a^2b-78b^3.$$

We see immediately that $6|a$ and $2|b$. Put $a =: 6a_1$ and $b =: 2b_1$, then from (2.9) we obtain:

$$1 = a_1(a_1^2-26b_1^2).$$

Hence $a_1 = 1$, $b_1 = 0$ which leads to the solution

$$\underline{(x,y,m) = (6,0,1)}.$$

Next, $\tau = -1$ in (0.2) with $m = 1$. Put $L := \mathbb{Q}(\sqrt{78})$, then $h_L = 2$, $(2) = \mathfrak{p}^2$, $(3) = \mathfrak{q}^2$ and $\eta := 53+6\sqrt{78}$ is a fundamental unit of L. As in the previous case, we write

$$\mathrm{Norm}_{L/\mathbb{Q}}(2^3 3^3+6y\sqrt{78}) = (6x)^3,$$

and we deduce, since $(h_L,3) = 1$ and because of the factorization of 2 and 3, that

$$(2.10) \qquad 2^3 3^3+6y\sqrt{78} = \varepsilon\ (a+b\sqrt{78})^3,$$

where $a,b \in \mathbb{Z}$ and $\varepsilon = \pm\eta^t$ with $t = 0,1$ or 2. If we do not specify the sign of y, it is sufficient to consider only the possibilities $\varepsilon = 1$ and $\varepsilon = \eta$.

Let $\varepsilon = 1$ in (2.10). As before, see (2.9), we find immediately that $a = 6$ and $b = 0$. This gives the solution

$$\underline{(x,y,m) = (-6,0,1)}.$$

If $\varepsilon = \eta$ in (2.10), we find by equating coefficients, noting that again $a = 6a_1$, for some rational integer a_1,

$$(2.11) \quad \begin{cases} x = -6a_1^2+13b^2 \\ y = 216a_1^3+954a_1^2b+1404a_1b^2+689b^3 \\ 2 = 106a_1^3+468a_1^2b+689a_1b^2+338b^3. \end{cases}$$

The last equation of (2.11) has the following solutions $(a_1,b) = (3,-2)$, $(-4,3)$ and $(35,-26)$. We also note that a_1 and b do not have the same parity

The substitution

$$u = 19a_1+26b$$
$$v = 3a_1+4b$$

transforms the third equation of (2.11) into

$$(2.12) \qquad u^3-91uv^2+338v^3 = 8.$$

We stress that the substitution used is not unimodular, so that the number of solutions (u,v) of (2.12) could be different from the number of solutions (a_1,b) of equation $(2.11)_3$. In fact, we have to solve (2.12) under the condition that u and v have the same parity. (See also the remark at the end of this section.)

Lemma 2 supplies the answer to our question. The solutions (u,v) of (2.12), where u and v have the same parity, are $(u,v) = (2,0)$, $(5,1)$ and $(-11,1)$. This gives the following basic solutions of (0.2):

<u>$(x,y,m) = (-2,4,1)$, $(21,27,1)$ and $(1438,15124,1)$</u>.

Finally, we are left to solve (0.2) when $m = 0$. We first deal with the case $\tau = 1$. Let $F := \mathbb{Q}(\sqrt{-39})$, then $h_F = 4$, $(2) = \mathfrak{p}_1\mathfrak{p}_2$ with $\mathfrak{p}_1 = (2,\frac{1}{2}(1+\sqrt{-39}))$, $\mathfrak{p}_2 = (2,\frac{1}{2}(1-\sqrt{-39}))$ and $(3) = \mathfrak{q}^2$. The ideals $\mathfrak{p}_1$, $\mathfrak{p}_2$ and $\mathfrak{q}$ are prime ideals. From (0.2) with $m = 0$ and $\tau = 1$, it follows that

$$\mathrm{Norm}_{F/\mathbb{Q}}(9+y\sqrt{-39}) = 3x^3$$

and thus

(2.13) $$(9+y\sqrt{-39}) = \mathfrak{p}_1^{r_1}\mathfrak{p}_2^{r_2}\mathfrak{q}^s\mathfrak{A}^3$$

with $r_1, r_2, s \in \{0,1,2\}$ and integral ideal $\mathfrak{A}$. On taking norms in (2.13) we see that $r_1+r_2 \equiv 0 \pmod 3$ and $s \equiv 1 \pmod 3$. Hence $r_1+r_2 = 0$ or 3 and $s = 1$.

We shall treat the three possibilities in turn.

(2.13.1) $r_1 = r_2 = 0$, $s = 1$ in (2.13).

We have

(2.14) $$(27+3y\sqrt{-39}) = \mathfrak{q}^2(9+y\sqrt{-39}) = (\mathfrak{q}\mathfrak{A})^3.$$

Since $(h_F, 3) = 1$, we deduce that $\mathfrak{q}\mathfrak{A}$ is a principal ideal, say $\mathfrak{q}\mathfrak{A} = (\frac{1}{2}a+\frac{1}{2}b\sqrt{-39})$ with $a, b \in \mathbb{Z}$ and $a \equiv b \pmod 2$. Inserting the expression for $\mathfrak{q}\mathfrak{A}$ in (2.14) and equating coefficients, gives

$$216 = a(a^2-117b^2),\ 24y = 3b(a^2-13b^2).$$

It easily follows that $a = 6$ and $b = 0$. Hence, the corresponding basic solution is

$(x,y,m) = (3,0,0)$.

(2.13.2) $r_1 = 1, r_2 = 2, s = 1$ in (2.13).

Since y is odd in this case, we have

$$\left(\frac{9+y\sqrt{-39}}{2}\right) = \mathfrak{p}_2\mathfrak{q}\mathfrak{A}^3.$$

Now $\mathfrak{p}_1$ belongs to the same ideal class as $(\mathfrak{q}\mathfrak{a})^3$, for

(2.15) $$\mathfrak{p}_1\left(\frac{27+3y\sqrt{-39}}{2}\right) = \mathfrak{p}_1\mathfrak{q}^2\left(\frac{9+y\sqrt{-39}}{2}\right) = \mathfrak{p}_1\mathfrak{p}_2(\mathfrak{q}\mathfrak{a})^3 = (2)(\mathfrak{q}\mathfrak{a})^3.$$

The prime ideal $\mathfrak{p}_1$ is non-principal. However, $\mathfrak{p}_1\mathfrak{q}\mathfrak{a}$ is principal, because $h_K=4$ and thus $\mathfrak{p}_1\mathfrak{q}\mathfrak{a}$ belongs to the same ideal class as $(\mathfrak{q}\mathfrak{a})^4$ which is the principal one. Put $\mathfrak{p}_1\mathfrak{q}\mathfrak{a} = \left(\frac{a+b\sqrt{-39}}{2}\right)$ with $a,b \in \mathbb{Z}$ and $a \equiv b \pmod 2$.

Since $\mathfrak{p}_1^4 = \left(\frac{5+\sqrt{-39}}{2}\right)$, we obtain from (2.15) in integers of F,

(2.16) $$\left(\frac{5+\sqrt{-39}}{2}\right)\left(\frac{27+3y\sqrt{-39}}{2}\right) = 2\left(\frac{a+b\sqrt{-39}}{2}\right)^3.$$

Note that the units i.e. ± 1 may be obsorbed in the cube.

We have, equating coefficients in (2.16):

(2.17) $$135-117y = a(a^2-117b^2),\quad 27+15y = 3b(a^2-13b^2).$$

Clearly $3|a$ and $3|b$. Put $a =: 3a_1$, $b =: 3b_1$. Then elimination of y from the equations (2.17) yields:

$$64 = 5a_1^3+117a_1^2b_1-585a_1b_1^2-1521b_1^3,$$

which implies the impossible congruence

$$5a_1^3 \equiv 1 \pmod 9.$$

(2.13.3) $\underline{r_1 = 2,\ r_2 = 1,\ s = 1 \text{ in } (2.13).}$

In this case we have the ideal equation

$$(9+y\sqrt{-39}) = (2)\,\mathfrak{p}_1\mathfrak{q}\mathfrak{a}^3,$$

the conjugate of which is

$$(9-y\sqrt{-39}) = (2)\mathfrak{p}_2\mathfrak{q}\mathfrak{A}'^3.$$

This equation shows that we are in the same situation as in case (2.13.2) This means that no further solutions of (0.2) with $m = 0$ and $\tau = 1$ are found.

Finally we consider equation (0.2) with $m = 0$ and $\tau = -1$. Put $G: = \mathbb{Q}(\sqrt{39})$, then $h_G = 2$, $(2) = \mathfrak{p}^2$, $(3) = \mathfrak{q}^2$ and $\eta: = 25+4\sqrt{39}$ is a fundamental unit of G.

As before we have

$$\mathrm{Norm}_{G/\mathbb{Q}}(9+y\sqrt{39}) = 3(-x)^3$$

and thus

$$(9+y\sqrt{39}) = \mathfrak{p}^r\mathfrak{q}^s\mathfrak{A}^3, \tag{2.18}$$

with $r,s \in \{0,1,2\}$ and integral ideal $\mathfrak{A}$. Taking norms we find that $r \equiv 0 \pmod 3$ and $s \equiv 1 \pmod 3$. Hence we may take $r = 0$ and $s = 1$ in (2.18). Multiplication by $\mathfrak{q}^2$ yields:

$$(27+3y\sqrt{39}) = (\mathfrak{q}\mathfrak{A})^3$$

and consequently $\mathfrak{q}\mathfrak{A}$ is a principal ideal, since $(\mathfrak{q}\mathfrak{A})^3$ is principal and $(h_G, 3) = 1$. Put $\mathfrak{q}\mathfrak{A} = (a+b\sqrt{39})$ with $a,b \in \mathbb{Z}$. Then we have in integers of G:

$$(27+3y\sqrt{39} = \varepsilon(a+b\sqrt{39})^3, \tag{2.19}$$

with $\varepsilon = \pm\eta^t$, $t \in \{0,1,2\}$. Since $\eta^2 = \eta'\eta'^{-3}$, where η' denotes the conjugate of η, and since ± 1 may be absorbed in the cube, we only need to consider $\varepsilon = 1$ and $\varepsilon = \eta$.

Equating coefficients of 1 and $\sqrt{39}$ in (2.19) in case $\varepsilon = 1$, gives

$$27 = a(a^2+117b^2),\ 3y = 3b(a^2+13b^2).$$

We see immediately that $3|a$. It is a small step to deduce that $a = 3$ and $b = 0$. This leads to the basic solution

$$\underline{(x,y,m) = (-3,0,0)}.$$

When $\varepsilon = \eta$, we have

$$27+3y\sqrt{39} = (25+4\sqrt{39})(a+b\sqrt{39})^3.$$

We find that

$$27 = 25a^3+468a^2b+2925ab^2+6084b^3, \tag{2.20}$$

and it follows that $3|a$ and $3|b$: Insenting $a =: 3a_1$ and $b =: 3b_1$ in (2.20) yields the impossible congruence

$$-2a_1^3 \equiv 1 \pmod 9.$$

This completes the proof of the theorem. □

REMARK. In [4] and [2] Nagell and Delaunay show that a binary cubic with negative discriminant represents 1 in at most 3 disinct ways with a few exceptions, in which there are 4 or 5 such representations. Now solving $(2.11)_3$ i.e. the third equation of (2.11)(the cubic involved does not belong to any of the exceptional classes), is the same as solving two equations of the type $f(x,y) = 1$, where the two f's are binary cubics belonging to different classes. It is clear from the above proof that one of these cubics represents 1 only once and that the other represents 1 twice. So neither achieves the maximum possible number of representations of 1. Consequently, the application of the above mentioned result does not bring us any closer to solving $(2.11)_3$ completely. This is the reason why we have chosen to solve equation (2.12)(or rather (1.8)), given by a cubic inequivalent to the cubic of $(2.11)_3$, but with the advantage of determining all solutions in one go.

REFERENCES

[1] Z.I. Borevich & I.R. Schafarevich - Number Theory. Pure and Appl. Maths. Series 20. Academic Press, New York and London 1966.

[2] B. Delaunay - Über die Darstellung der Zahlen durch die binäre kubische Formen mit negativer Diskriminante. Math. Zeitschr. 31 (1930), 1-26.

[3] L.J. Mordell - Diophantine Equations, Pure and Appl. Math. Series 30. Acad. Press, New York and London 1969.

[4] T. Nagell - Darstellungen ganzer Zahlen durch binäre kubische Formen mit negativer Diskriminante. Math. Zeitschr. 28 (1928), 10-29.

[5] R.J. Stroeker - Elliptic curves defined over imaginary quadratic number fields. Doct. thesis, Univ. of Amsterdam, 1975.

REPORTS 1976

7600 List of Reprints, nos. 172-178; List of Reports, 1975.

7601/ES "Profit Structure in Retailing", by B. Nooteboom.

7602/M "On a Diophantine Equation of E. Bombieri", by R.J. Stroeker.

7603/S "Limit Theory for Multivariate Sample Extremes", by L. de Haan and S.I. Resnick.

7604/S "On Typical Characteristics of Economic Time Series and the Relative Qualities of Five Autocorrelation Tests", by C. Dubbelman, A.P.J. Abrahamse and A.S. Louter.

7605/E "The Two-Level C.E.S. Production Function in Input-Output Analysis: Some Preliminary Results of an Emperical Study for the Netherlands, 1948-1958", by P.M.C. de Boer.

7606/E "Solution of Econometric Equation Systems by Means of a Modified Gauss-Seidel Procedure", by A. Kunstman and T. Kloek.

7607/E "Linearization and Estimation of the Leser-Somermeyer-Houthakker Model of Optimal Allocation of Consumer Expenditure", by P.M.C. de Boer.

7608/O "A Study on Maintenance Systems for Locomotives", by J. Telgen.

7609/M "Moduli and Canonical Forms for Linear Dynamical Systems. II: The Topological Case", by M. Hazewinkel.

7610/M "Moduli and Canonical Forms for Linear Dynamical Systems. III: The Algebraic-Geometric Case", by M. Hazewinkel.

7611/M "On n-Isoclinic Groups", by M. Hazewinkel.

7612/S "Sample Extremes: An Elementary Introduction", by L. de Haan.

7613/ES "Production Functions and Mark-Up Pricing: with a Methodological Enquiry and an Emperical Study of Grocers", by B. Nooteboom.

7614/E "Predictive Moments of Simultaneous Econometric Models, A Bayesian Approach", by H.K. van Dijk and T. Kloek.

7615/ES "Economics of Scale in Retailing", by B. Nooteboom.

7616/E "Efficient Estimation of Income Distribution Parameters", by T. Kloek and H.K. van Dijk.

7617/S "A Characterization of Multidimensional Extreme-Value Distribution", by L. de Haan.

7618/E "On Bayesian and Non-Bayesian Estimation of C.E.S. Production Functions within the Context of Two Alternative Models of Firm Bahaviour", by S. Schim van der Loeff and R. Harkema.

7619/O "A Reduction Method for Nonlinear Programming", by G. van der Hoek.

7620/O "Projective Methods to Find a Feasible Solution to Systems of Linear Constraints", by J. Telgen and G. van der Hoek.

7621/M "A Class of Diophantine Equations Connected with Certain Elliptic Curves over $Q(\sqrt{-13})$", by R. Stroeker.