R. J. STROEKER

A class of diophantine equations connected with certain elliptic curves over $Q(\sqrt{-13})$

Compositio Mathematica, tome 38, nº 3 (1979), p. 329-346

<http://www.numdam.org/item?id=CM_1979__38_3_329_0>

COMPOSITIO MATHEMATICA, Vol. 38, Fasc. 3, 1979, pag. 329–346

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

R.J. Stroeker

0. Introduction

In a private communication to J.-P. Serre [8], J. Tate indicates how one can construct elliptic curves with good reduction everywhere over certain imaginary quadratic number fields. A full account may be found in [7]. However, the discriminants of these number fields are rather large. In the course of trying to construct an elliptic curve with good reduction everywhere over an imaginary quadratic number field of small discriminant, we came across some interesting Diophantine equations, the solutions of which are related in a certain way to elliptic curves defined over $\mathbb{Q}(\sqrt{-13})$. The choice of the field $\mathbb{Q}(\sqrt{-13})$ is based mainly on the fact that the existence of a curve E/K with good reduction everywhere over the imaginary quadratic number field K, implies that the class number of K is greater than one (cf. [7], p. 16).

In the remainder of this introduction we suppose that $K = \mathbb{Q}(\sqrt{-13})$. Let E/K be an elliptic curve defined over K. Select a Weierstrass model for E/K with coefficients in the ring of integers $\mathcal{O}_K$ of K. If Δ denotes the discriminant of this model, then

$$c_4^3 - c_6^2 = 2^6 3^3 \Delta, \tag{0.1}$$

where c_4 and c_6 are well-known expressions in the coefficients of the Weierstrass model (cf. [3]). If Π is a fixed finite set of prime ideals of $\mathcal{O}_K$ and if the only prime ideal divisors of Δ are elements of Π, then there are only finitely many curves for which (0.1) holds true. These curves have good reduction outside Π. This is essentially Shafarevich's theorem. Moreover, Weierstrass models for these curves can be effectively computed from the solutions of the equations (0.1). The main difficulty lies in solving (0.1) in the unknowns c_4, c_6 and the exponents of the prime divisors of Δ.

0010-437X/79/03/0329-18 $00.20/0

To narrow the field of search, that is to reduce the problem to an easier one, we assume that $\Pi = \{\wp\}$ where $\wp$ is the integral prime ideal above 2. Now if $(x, y) \in \mathbb{A}_K^2$ is an affine point with integral co-ordinates on the elliptic curve E_n/K given by

$$(0.2) \qquad x^3 - y^2 = \pm 2^n 3^3, \quad n \in Z \quad \text{and} \quad n \geqq 0$$

then $(x, y) \dot{+} (\bar{x}, \bar{y})$ is a point on $E_n/\mathbb{Q}$. Here "$\dot{+}$" denotes addition on the curve and "$^-$" is complex conjugation. The group $E_n(\mathbb{Q})$ is known and for each $P \in E_n(\mathbb{Q})$ with integral co-ordinates, the point (x, y) may be recovered from

$$(x, y) \dot{+} (\bar{x}, \bar{y}) = P.$$

In particular, if $E_n(\mathbb{Q})$ is finite, we can find all solutions (x, y) of (0.2) in this way. We should mention here that Siegel's celebrated theorem on integer points on curves [6] shows that (0.2) has at most finitely many solutions (x, y, n) where x and y are required to be co-prime.

From experience we learn that most solutions of (0.2) usually come from the choice $P = \underline{0}$, the neutral element of the group $E_n(\mathbb{Q})$. Starting from $(x, y) \dot{+} (\bar{x}, \bar{y}) = \underline{0}$, we find that $\bar{x} = x$ and $\bar{y} = -y$. The transformation $x \mapsto -x$, $y \mapsto y\sqrt{-13}$ leads to the Diophantine equations

$$(0.3) \qquad x^3 - 13y^2 = \pm 2^n 3^3$$

in rational integers x, y and n ($n \geqq 0$). These equations we plan to solve completely; the resulting solutions give rise to Weierstrass models of elliptic curves E/K with good reduction everywhere, with the possible exception of the prime $\wp$ above 2. For full details of this process we refer to [7]. In table 2 on the next page, Weierstrass models of the 28 elliptic curves (8 "old" curves defined over $\mathbb{Q}$, and 20 "new" ones), constructed as indicated above, are given. Unfortunately, all 28 curves have bad reduction at $\wp$. Because of the restrictions imposed – not all solutions of (0.2) necessarily come from the choice $P = \underline{0}$, and moreover a curve with good reduction outside $\{\wp\}$ does not necessarily have a Weierstrass model with coefficients in $\mathcal{O}_K$ and discriminant divisible by powers of $\wp$ only since $\mathcal{O}_K$ is not a principal ideal domain – we cannot infer that table 2 is complete in the sense of giving all curves E/K with good reduction outside $\{\wp\}$. In a forthcoming paper we hope to fill this gap.

Siegel's theorem tells us that (0.3) has at most finitely many

TABLE 2. Weierstrass models for the elliptic curves E/K corresponding with the solutions of $x^3 - 13y^2 = \tau 2^n 3^3$ (see also Table 1).

E/K: $y^2 = x^3 + a_2x^2 + a_4x + a_6$, $K = \mathbf{Q}(\alpha)$, $\alpha = \sqrt{-13}$

	a_2	a_4	a_6	Δ	j
I_1.	0	1	0	-2^6	12^3
I_2.	0	4	0	-2^{12}	12^3
II_1.	0	2	0	-2^9	12^3
II_2.	0	8	0	-2^{15}	12^3
III_1.	0	-1	0	2^6	12^3
III_2.	0	-4	0	2^{12}	12^3
IV_1.	0	-2	0	2^9	12^3
IV_2.	0	-8	0	2^{15}	12^3
V_1.	α	-5	$-\alpha$	2^9	2^6
V_2.	$-\alpha$	-5	α	2^9	2^6
V_3.	α	-7	α	2^{15}	2^6
V_4.	$-\alpha$	-7	$-\alpha$	2^{15}	2^6
VI_1.	0	7	2α	2^9	-42^3
VI_2.	0	7	-2α	2^9	-42^3
VI_3.	0	28	16α	2^{15}	-42^3
VI_4.	0	28	-16α	2^{15}	-42^3
VII_1.	α	475	-961α	2^9	-2876^3
VII_2.	$-\alpha$	475	961α	2^9	-2876^3
VII_3.	α	1913	9601α	2^{15}	-2876^3
VII_4.	$-\alpha$	1913	-9601α	2^{15}	-2876^3
VIII_1.	α	-8	-4α	2^{15}	$11^3/2^3$
VIII_2.	$-\alpha$	-8	4α	2^{15}	$11^3/2^3$
VIII_3.	α	-19	13α	2^{21}	$11^3/2^3$
VIII_4.	$-\alpha$	-19	-13α	2^{21}	$11^3/2^3$
IX_1.	α	392	988α	2^{27}	$-1189^3/2^{15}$
IX_2.	$-\alpha$	392	-988α	2^{27}	$-1189^3/2^{15}$
IX_3.	α	1581	-6323α	2^{33}	$-1189^3/2^{15}$
IX_4.	$-\alpha$	1581	6323α	2^{33}	$-1189^3/2^{15}$

solutions (x, y, n) with $x, y, n \in Z$ $(n \geqq 0)$ and $(x, y) = 1$. If (x, y, n) is a solution, so is $(2^{2t}x, 2^{3t}y, n + 6t)$ for every $t \in Z$, $t \geqq 0$. This leads to

DEFINITION: A solution $(x, y, n) \in Z^3$ with $n \geqq 0$ of (0.3) is called basic iff

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

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 $x^3 \equiv 0$, ± 1 or ± 8 (mod 13).

In the following sections we shall therefore study the Diophantine equations

$$x^3 - 13y^2 = \tau 2^{3m} 3^3, \quad \tau = \pm 1 \tag{0.4}$$

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

We intend to prove the following

THEOREM: *The Diophantine equation* (0.4) *has precisely nine basic solutions. They are given in table* 1 *below.*

TABLE 1. Basic solutions of the Diophantine equations $x^3 - 13y^2 = \tau 2^n 3^3$.

	x	y	n	τ
I.	3	0	0	+1
II.	6	0	3	+1
III.	−3	0	0	−1
IV.	−6	0	3	−1
V.	−2	4	3	−1
VI.	21	27	3	−1
VII.	1438	15 124	3	−1
VIII.	−11	31	9	−1
IX.	1189	11 561	27	−1

1. Two Lemmas

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*

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

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

$$2^n + 9 \pm 6\sqrt{3} = \epsilon 2^r (4 + \sqrt{3})^s (a + b\sqrt{3})^2, \tag{1.2}$$

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

Now $\eta := 2 - \sqrt{3}$ is a fundamental unit of K. Hence we may take $\epsilon = \pm\eta^t$ 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

$$\pm(2^n + 9) \pm 6\sqrt{3} = (2 - \sqrt{3})(4 + \sqrt{3})(a + b\sqrt{3})^2, \tag{1.3}$$

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

$$\pm(2^n + 9) = 5(a^2 + 3b^2) - 12ab \tag{1.4a}$$

and

$$\pm 6 = -2(a^2 + 3b^2) + 10ab \tag{1.4b}$$

with independent $\pm$signs.

The right-hand side of (1.4a) 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 (1.4a) modulo 3 shows that n has to be odd. Thus $n \geqq 3$. From (1.4a) modulo 8, we deduce that a is odd and $b \equiv 2 \pmod 4$. Combining this result with (1.4b) modulo 8 shows that we must have the $-$sign in (1.4b).

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

$$13uv = 2^{n-1} - 3 \tag{1.5a}$$

and

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

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

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

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

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

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

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

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

because ± 1 are the only units in $\mathcal{O}_L$. 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

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

It is easily seen that

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

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

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

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*

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

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 root of $f(t, 1) = 0$ and put $K := \mathbb{Q}(\theta)$. Now $\omega := -\frac{1}{2}\theta + (\theta^2/26) \in \mathcal{O}_K$, 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 $-2^3 \cdot 13$ and the set $\{1, \omega, \omega^2\}$ is an $\mathcal{O}_K$-basis.

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

$$1 < \epsilon < 5 \text{ and hence } \tfrac{1}{5} < \epsilon' \bar{\epsilon}' < 1.$$

It then easily follows that $0 < |c| \leqq 2$. Checking all possibilities shows that only $c = -1$ satisfies the requirements. This gives $\epsilon = \eta$. 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 $\mathcal{O}_K$-basis.

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

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

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

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

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

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

$I: (r, s) = (3,0)$
From (1.9) we have

$$(u - v\theta) = \wp^3 = (5 - \theta).$$

let $a, b, c \in Z$ 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

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

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

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

and

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

It is an easy exercise to check that

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

In the first case (I_1) we have

$$\begin{aligned} a + b\theta + c\omega &\equiv \pm\eta^{-4}\eta^{2^\lambda T} \equiv \pm\eta^{-4}\{1 - 2^\lambda(1 + 3\theta + 3\omega)\}^T \\ &\equiv \pm(133 - 36\theta - 52\omega)\{1 - 2^\lambda T(1 + 3\theta + 3\omega)\} \\ &\equiv \pm\{133 - 36\theta - 52\omega - 2^\lambda T(1 + 3\theta + 3\omega)\} \pmod{2^{\lambda+3}}. \end{aligned}$$

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

$$\begin{aligned} a + b\theta + c\omega &= \pm\eta^{2^\lambda T} \equiv \pm\{1 - 2^\lambda(1 + 3\theta + 3\omega)\}^T \\ &\equiv \pm\{1 - 2^\lambda T(1 + 3\theta + 3\omega)\} \pmod{2^{\lambda+3}}. \end{aligned}$$

Again $13b = 9c$ implies $3.2^{\lambda+2}T \equiv 0 \pmod{2^{\lambda+3}}$. 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

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

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

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

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

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

Now we have from (1.9)

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

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

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

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, $c \in \mathbf{Z}$ are given in such a way that

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

Then

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

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

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

we again find that $k = 0$. This gives $(u, v) = (6, 1)$.
This completes the proof of the lemma. □

2. The proof of the theorem

Let (x, y, m) be a basic solution of (0.4). We distinguish between the following cases, according as $m \geqq 2$, $m = 1$ or $m = 0$.

In the first case ($m \geqq 2$), we see immediately that x has to be odd. For otherwise, (x, y, m) would not be basic. Write (0.4) 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

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

with $A, B \in Z$, $A, B \geqq 0$ and squarefree (if $\neq 0$), $(A, B) = 1$ or 3 and $a, b \in Z$, $a, b \geqq 0$ 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 $m \geqq 2$ 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

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

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

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

Hence

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

where η is a unit of $\mathcal{O}_K$, $r, s \in \{0, 1\}$ 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 $\mathcal{O}_K$ 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) $x + 3\tau 2^m \rho = \eta(c + d\rho)^2$ with $\eta = \pm 1$, $A = 13$ and $B = 1$,

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

(2.3.3)
$x + 3\tau 2^m \bar{\rho} = \eta(-1 + 4\rho)(c + d\rho)^2$ with $\eta = \pm 1$, $A = 1$ 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) $$\begin{cases} x = \eta(c^2 - d^2) = 3\tau 2^m + 13a^2, \; y = a(c^2 + cd + d^2) \\ 3\tau 2^m = \eta d(2c + d). \end{cases}$$

Now c and d are co-prime, because (x, y, m) is a basic solution. Moreover d is even and c is odd since $m \geqq 2$. 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 $m \geqq 3$. Combining the first and the third equation in (2.4) leads to:

$$13a^2 = (c-d)^2 - 3d^2 \tag{2.5}$$

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

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

Now $2 \parallel d$, since $4 \mid d$ 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:

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

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

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

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

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

The first and the third equation in (2.7) imply that c is odd and d is even. Also a is odd. Since $m \geqq 2$, 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 $2 \parallel d$ and consequently $m = 2$. Then

$$\begin{aligned} a^2 = c^2 + 8cd + 3d^2 - 12\tau &= c^2 + 8cd + 3d^2 - 12\tau \\ &+ 3(4c^2 + 6cd - d^2 + 12\tau) = 13c^2 + 26cd + 24\tau \equiv -2\tau \pmod{13}. \end{aligned}$$

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 (0.4) in case $m \geqq 2$.

We now wish to solve (0.4) 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 (0.4), with $m = 1$ and $\tau = 1$, in the form

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

Thus

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

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:

$$2^3 3^3 = a^3 - 234ab^2, \quad 6y = 3a^2 b - 78b^3. \tag{2.9}$$

We see immediately that $6 \mid a$ and $2 \mid b$. 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

$$(x, y, m) = (6, 0, 1).$$

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

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

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

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

$$(x, y, m) = (-6, 0, 1).$$

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

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

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

$$u^3 - 91uv^2 + 338v^3 = 8. \tag{2.12}$$

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 (0.4):

$$(x, y, m) = (-2, 4, 1), (21, 27, 1) \textit{ and } (1438, 15124, 1).$$

Finally, we are left to solve (0.4) when $m = 0$. We first deal with the case $\tau = 1$. Let $F := \mathbb{Q}(\sqrt{-39})$, then $h_F = 4$, $(2) = \wp_1\wp_2$ with $\wp_1 = (2, \frac{1}{2}(1+\sqrt{-39}))$, $\wp_2 = (2, \frac{1}{2}(1-\sqrt{-39}))$ and $(3) = \mathfrak{q}^2$. The ideals $\wp_1$, $\wp_2$ and $\mathfrak{q}$ are prime ideals. From (0.4) with $m = 0$ and $\tau = 1$, it follows that

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

and thus

$$(9 + y\sqrt{-39}) = \wp_1^{r_1}\wp_2^{r_2}\mathfrak{q}^s\mathfrak{A}^3 \tag{2.13}$$

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) $\qquad r_1 = r_2 = 0, \quad s = 1$ in (2.13).

We have

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

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

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

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

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

(2.13.2) $\qquad r_1 = 1, \quad r_2 = 2, \quad s = 1$ in (2.13),

Since y is odd in this case, we have

$$\left(\frac{9 + y\sqrt{-39}}{2}\right) = \wp_2\mathfrak{q}\mathfrak{A}^3.$$

Now $\wp_1$ belongs to the same ideal class as $(\mathfrak{q}\mathfrak{A})^3$, for

$$(2.15)\ \wp_1\left(\frac{27+3y\sqrt{-39}}{2}\right)=\wp_1\mathfrak{q}^2\left(\frac{9+y\sqrt{-39}}{2}\right)=\wp_1\wp_2(\mathfrak{q}\mathfrak{A})^3=(2)(\mathfrak{q}\mathfrak{A})^3.$$

The prime ideal $\wp_1$ is non-principal. However, $\wp_1\mathfrak{q}\mathfrak{A}$ is principal, because $h_F=4$ and thus $\wp_1\mathfrak{q}\mathfrak{A}$ belongs to the same ideal class as $(\mathfrak{q}\mathfrak{A})^4$ which is the principal one. Put $\wp_1\mathfrak{q}\mathfrak{A}=((a+b\sqrt{-39})/2)$ with $a,b\in Z$ and $a\equiv b \pmod 2$.

Since $\wp_1^4=((5+\sqrt{-39})/2)$, we obtain from (2.15) in integers of F,

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

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

We have, equating coefficients in (2.16):

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

Clearly $3\mid a$ and $3\mid b$. 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) $\qquad r_1=2,\quad r_2=1,\quad s=1$ in (2.13).

In this case we have the ideal equation

$$(9+y\sqrt{-39})=(2)\wp_1\mathfrak{q}\mathfrak{A}^3,$$

the conjugate of which is

$$(9-y\sqrt{-39})=(2)\wp_2\mathfrak{q}\mathfrak{A}^3.$$

This equation shows that we are in the same situation as in case (2.13.2). This means that no further solutions of (0.4) with $m=0$ and $\tau=1$ are found.

Finally we consider equation (0.4) with $m=0$ and $\tau=-1$. Put $G:=\mathbb{Q}(\sqrt{39})$, then $h_G=2$, $(2)=\wp^2$, $(3)=\mathfrak{q}^2$ and $\eta:=25+4\sqrt{39}$ is a fundamental unit of G.

As before we have

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

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 $a, b \in Z$. Then we have in integers of G:

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

with $\epsilon = \pm\eta^t$, $t \in \{0, 1, 2\}$. 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 $\epsilon = 1$ and $\epsilon = \eta$.

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

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

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

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

When $\epsilon = \eta$, 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 $3 \mid a$ and $3 \mid b$: Inserting $a =: 3a_1$ 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 [5] and [2] Nagell and Delaunay show that a binary cubic with negative discriminant represents 1 in at most 3 distinct 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 result mentioned above 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.

Acknowledgement

The author wishes to express his gratitude to the referee for his valuable comments.

REFERENCES

[1] Z.I. BOREVICH and I.R. SHAFAREVICH: Number Theory. *Pure and Appl. Maths. Ser. 20.* Acad. Press, New York and London, 1966.
[2] B. DELAUNAY: Ueber die Darstellung der Zahlen durch die binäre kubische Formen mit negativer Diskriminante. *Math. Zeitschr. 31* (1930) 1–26.
[3] P. DÉLIGNE: Courbes elliptiques: Formulaire (d'après J. Tate). In: Modular functions of one variable IV. *Lecture Notes in Maths. 476.* Springer, Berlin–Heidelberg–New York, 1975, 53–73.
[4] L.J. MORDELL: Diophantine Equations. *Pure and Appl. Maths. Ser. 30.* Acad. Press, New York and London, 1969.
[5] T. NAGELL: Darstellungen ganzer Zahlen durch binäre kubische Formen mit negativer Diskriminante. *Math. Zeitschr. 28* (1928) 10–29.
[6] C.L. SIEGEL: Ueber einige Anwendungen Diophantischer Approximationen. Abh. Preuss. Akad. Wiss. *Phys.-Math. Kl. 1929 nr. 1.*
[7] R.J. STROEKER: Elliptic curves defined over imaginary quadratic number fields. *Doct. thesis,* Univ. Amsterdam, 1975.
[8] J.T. TATE: Letter to J.-P. Serre, dated July 24th 1971.

(Oblatum 21-I-1977 & 6-VI-1978)

Erasmus University
Econometric Institute
Burg. Oud-laan 50
Rotterdam, The Netherlands