ACTA ARITHMETICA
XLVI (1986)

On the diophantine equation $x^2 - Dy^4 = k$

by

NIKOS TZANAKIS (Iraklion, Crete)

0. Introduction. There are various interesting results concerning the equation of the title when $|k| \in \{1, 2, 4, 8, 16\}$, as one can see, for example, in [12], Section D24. These are mainly results of Cohn, Ljunggren and Mordell. However, to the best of the author's knowledge, besides the tables of Lal and Dawe [10], there are no results concerning the title equation for other integer values of k.

It is easy to see that if D, k are rational integers, then

$$x^2 - Dy^4 = k, \quad x, y \in \mathbf{Z} \tag{0.1}$$

has at most a finite number of solutions ([17], p. 236), but, in general, no practical procedure is known deciding whether (0.1) has any solutions and finding explicitly them in case it actually has. In Section 1 of the present paper we prove that if k is a positive integer, then for the solution of (0.1) it suffices to solve a finite number of diophantine equations

$$g(u, v) = A^2, \quad u, v \in \mathbf{Z}, \tag{0.2}$$

where g is a semi-real biquadratic form with rational integer coefficients and A is a known integer. For such equations (0.2) the p-adic method, although no proof guarantees its effectiveness, gives a tentative decision procedure, which is comparatively easy to apply and has good chances to work for finding all solutions to (0.2) (and, consequently, to (0.1)), if any (see the Remark following the statement of the Theorem of Section 1 and the references mentioned there).

The ideas of Section 1 are applied to a non-trivial example in Section 2, where it is shown that for the solution of $x^2 - 3y^4 = 46$ it suffices to solve three equations of the form (0.2). These three equations are solved in Section 3 and in Section 4 the complete solution of $x^2 - 3y^4 = 46$ is given. Finally, in Section 5 some details are given concerning the computation of the fundamental units in the biquadratic fields appearing in this paper.

1. On the solution of the diophantine equation $x^2 - Dy^4 = k$. We prove firstly the following

LEMMA. *Let a, b, c be given non-zero integers with $(a, b, c) = 1$ and such that the diophantine equation*

$$ax^2+by^2+cz^2=0 \tag{1.1}$$

has a solution $(x, y, z) \neq (0, 0, 0)$. Then, we can find integers R_i, S_i, T_i $(i = 1, 2)$, z_1, depending only on a, b, c, satisfying the relations

$$R_1 T_2+R_2 T_1 = 2S_1 S_2, \tag{1.2}$$

$$S_1^2-R_1 T_1 = -bcz_1^2, \quad S_2^2-R_2 T_2 = -acz_1^2 \tag{1.3}$$

and a non-zero integer Δ, depending only on a, b, c, such that: For every non-zero solution (x, y, z) of (1.1), there exist integers Q, u, v and a divisor P of Δ, so that

$$Px = Q(R_1 u^2-2S_1 uv+T_1 v^2), \quad Py = Q(R_2 u^2-2S_2 uv+T_2 v^2).$$

Moreover, if the greatest common divisor of (x, y, z) is bounded, then an upper bound for Q can be found.

Proof. Put $a = a_0 A^2$, $b = b_0 B^2$, $c = c_0 C^2$, a_0, b_0, c_0 square-free, so that (1.1) is equivalent to

$$a_0(Ax)^2+b_0(By)^2+c_0(Cz)^2=0 \tag{1.4}$$

Following Nagell ([19], § 61), let us put $(a_0, b_0) = d$, $(a_0, c_0) = e$, $(b_0, c_0) = f$. Then

$$(d, e) = (d, f) = (e, f) = 1$$

and

$$a_0 = dea_1, \quad b_0 = dfb_1, \quad c_0 = efc_1, \quad Ax = fX, \quad By = eY, \quad Cz = dZ.$$

Thus (1.4) becomes

$$a_1 fX^2+b_1 eY^2+c_1 dZ^2=0 \tag{1.5}$$

which has its coefficients pairwise relatively prime and square-free. By hypothesis, (1.5) has a non-zero solution, say (x_1, y_1, z_1) (see the remark after the end of the proof). In the sequel we keep this solution fixed. As it is well-known (see e.g. [19], formulae 20, p. 225), there exist integers u, v, relatively prime, such that

$$\begin{aligned} d\frac{X}{Q} &= -a_1 fx_1 u^2-2b_1 ey_1 uv+b_1 ex_1 v^2, \\ d\frac{Y}{Q} &= a_1 fy_1 u^2-2a_1 fx_1 uv-b_1 ey_1 v^2, \\ \pm d\frac{Z}{Q} &= a_1 fz_1 u^2+b_1 ez_1 v^2 \end{aligned} \tag{1.6}$$

where d is the g.c.d. of the right-hand sides and $Q = (X, Y, Z)$. In (1.6) multiplication of the first relation by fBC and of the second by eAC gives respectively

$$dABCx = Q(-a_1 f^2 BCx_1 u^2-2b_1 efBCy_1 uv+b_1 efBCx_1 v^2),$$

i.e.

$$Px = Q(R_1 u^2-2S_1 uv+T_1 v^2),$$

$$dABC = Q(a_1 efACy_1 u^2-2a_1 efACx_1 uv-b_1 e^2 ACy_1 v^2),$$

i.e.

$$Py = Q(R_2 u^2-2S_2 uv+T_2 v^2),$$

where the meaning of R_i, S_i, T_i $(i = 1, 2)$ and P is obvious. Now

$$\begin{aligned} S_1^2-R_1 T_1 &= B^2 C^2 b_1 ef^2(b_1 ey_1^2+a_1 fx_1^2) = -B^2 C^2 b_1 ef^2 c_1 dz_1^2 \\ &= -B^2 C^2 b_0 c_0 z_1^2 = -bcz_1^2 \end{aligned}$$

and analogously we prove the second relation of (1.3). On the other hand, a direct simple calculation proves (1.2).

Now consider the determinant Δ' of the coefficients of u^2, uv, v^2 in the right-hand sides of (1.6). By the definition of d,

$$\Delta' u^2 \equiv \Delta' uv \equiv \Delta' v^2 \equiv 0 \pmod{d}.$$

From $(u, v) = 1$, it follows that $d|\Delta'$. Since $\Delta' = -2a_1 b_1 c_1 \operatorname{def} z_1^3$, we conclude that $P = dABC$ is a divisor of $\Delta = 2a_1 b_1 c_1 \operatorname{def} ABCz_1^3$.

Finally, since Q is a common divisor of Ax, By, Cz, it follows that if M is an upper bound for the g.c.d. of x, y, z, then $M(A, B, C)$ is an upper bound for Q.

By their definition, R_i, S_i, T_i $(i = 1, 2)$, z_1 and Δ depend only on a, b, c and this completes the proof of the lemma.

Remark. Dedekind's method for studying (1.1) (see e.g. [19]), Theorem 113, [11], Theorem 91) is essentially an algorithm for the finding of a non-zero solution of (1.1). Thus, a solution (x_1, y_1, z_1) to (1.5) can be effectively computed.

THEOREM. *Consider the diophantine equation*

$$x^2-Dy^4=k \tag{1.7}$$

where k and D are positive integers, no one of them a perfect square. Then we can find a finite number of diophantine equations of the form

$$g(u, v) = A^2, \quad u, v \in \mathbf{Z} \tag{1.8}$$

where A is a known integer and g is an integral binary biquadratic form, with $g(9, 1) = 0$ having exactly two real roots, such that, if we can solve all of them, then we can find all solutions to (1.7).

Remark. The basic thing in the above theorem is that $g(\vartheta, 1) = 0$ has exactly two real roots for every form g in (1.8). For, let g be irreducible (otherwise (1.8) is very easily solved). Then, working in $Q(\vartheta)$, we write (1.8) as $\mathrm{Norm}(u-v\vartheta) = A^2$, which is equivalent to a finite number of equations

$$u-v\vartheta = \alpha\varepsilon_1^m\varepsilon_2^n \tag{1.9}$$

where α runs through a finite set of algebraic integers of $Q(\vartheta)$ with $\mathrm{Norm}(\alpha) = A^2$ and ε_1, ε_2 is a pair of fundamental units in some appropriately chosen order of $Q(\vartheta)$ (very often this order is $Z[\vartheta]$, or the ring of integers of $Q(\vartheta)$; see [2], Chapter 2, Section 5, Theorem 1). Now (1.9) is an exponential equation in the unknowns m, n and there are two equations relating them, which are obtained on equating the coefficients of ϑ^2 and ϑ^3 in $\varepsilon_1^m\varepsilon_2^n$ to zero. Thus, the p-adic method (see e.g. [13], [15], [17], Chapter 23) can be attempted for the solution of (1.9).

On applying the p-adic method, a modest use of a computer is often indispensable (see e.g. [3], [5], [7], [8], [25]) but not always (see e.g. [4], [6], [9], [16], [24]). A different approach to (1.9) is found in [21], [22].

After solving (1.9), i.e. after finding all the algebraic integers of $Q(\vartheta)$ which are of the shape $u-v\vartheta$ and have Norm equal to A^2 (for the various ϑ's and A's arising from (1.8)), then we can find all solutions (x, y) to (1.7), for, as it is seen from the proof that follows, y is expressed as a polynomial in u, v with rational coefficients.

Proof of the Theorem. Let us put

$$D = e^2 d, \quad d \text{ square-free} > 1.$$

We work in $Q(\omega)$, where

$$\omega = \begin{cases} \sqrt{d} & \text{if} \quad d \equiv 2, 3 \pmod 4, \\ (1+\sqrt{d})/2 & \text{if} \quad d \equiv 1 \pmod 4 \end{cases}$$

so that an integral basis for $Q(\omega)$ is $Z[\omega]$. Thus (dashes indicate conjugates),

$$\omega' = \begin{cases} -\omega & \text{if} \quad d \equiv 2, 3 \pmod 4, \\ 1-\omega & \text{if} \quad d \equiv 1 \pmod 4 \end{cases}$$

and for $a+b\omega \in Z[\omega]$ we have

$$\mathrm{Norm}(a+b\omega) = (a+b\omega)(a+b\omega') = \begin{cases} a^2-db^2 & \text{if} \quad d \equiv 2, 3 \pmod 4, \\ a^2+ab+(1-d)b^2/4 & \text{if} \quad d \equiv 1 \pmod 4. \end{cases}$$

By (1.7),

$$\mathrm{Norm}(a+b\omega) = k \tag{1.10}$$

where

$$(a, b) = \begin{cases} (x, ey^2) & \text{if} \quad d \equiv 2, 3 \pmod 4, \\ (x-ey^2, 2ey^2) & \text{if} \quad d \equiv 1 \pmod 4. \end{cases} \tag{1.11}$$

Then (see the reference after (1.9)) there exists a finite subset K of $Z[\omega]$ and a unit ε of $Z[\omega]$, such that

$$\mathrm{Norm}(\varkappa) = k \quad \text{for every } \varkappa \in K, \quad \mathrm{Norm}(\varepsilon) = 1$$

and for every $a+b\omega$ satisfying (1.10) we have

$$a+b\omega = \pm\varkappa\varepsilon^\nu \text{ for some } \varkappa \in K \text{ and for some } \nu \in Z.$$

For $\nu = 2N+j$, $j \in \{0, 1\}$ the last equation becomes

$$a+b\omega = \pm\varkappa\varepsilon^j\varepsilon^{2N}. \tag{1.12}$$

Now we put

$$\varkappa\varepsilon^j = s+t\omega, \quad \varepsilon^N = m+n\omega, \quad s, t, m, n \in Z,$$
$$\mathrm{Norm}(s+t\omega) = k, \quad \mathrm{Norm}(m+n\omega) = 1,$$

and s, t run through a finite set of values. Then (1.12) becomes $a+b\omega = \pm(s+t\omega)(m+n\omega)^2$. Equating the coefficients of ω in both sides and using (1.11) we get

$$\pm ey^2 = tm^2+2smn+tdn^2 \quad \text{if} \quad d \equiv 2, 3 \pmod 4,$$
$$\pm 2ey^2 = tm^2+2(s+t)mn+(s+(d+3)t/4)n^2 \quad \text{if} \quad d \equiv 1 \pmod 4,$$

which can be written respectively

$$-(tm+sn)^2+kn^2+\mu tey^2 = 0 \quad (d \equiv 2, 3 \pmod 4), \tag{1.13}$$

$$-(tm+(s+t)n)^2+kn^2+2\mu tey^2 = 0 \quad (d \equiv 1 \pmod 4) \tag{1.14}$$

($\mu = \pm 1$). In these equations the unknowns are the quantities raised to the square. Since, clearly, $(m, n) = 1$, it follows that the g.c.d. of the unknowns is 1 in both equations.

First consider (1.13). We apply the lemma with -1, k, μte in place of a, b, c, respectively. Then,

$$P(tm+sn) = Q(R_1u^2-2S_1uv+T_1v^2),$$
$$Pn = Q(R_2u^2-2S_2uv+T_2v^2) \tag{1.15}$$

where $(u, v) = 1$. Here R_i, S_i, T_i $(i = 1, 2)$ depend on k and te, therefore they run through a finite set of integral values. Note also that, in view of the lemma, P and Q are bounded. Solving (1.15) for m, n and substituting in

$m^2-dn^2=1$ gives

$$[(R_1-sR_2)u^2-2(S_1-sS_2)uv+(T_1-sT_2)v^2]^2- \\ -d(R_2tu^2-2S_2tuv+T_2tv^2)^2=A^2$$

where $A=Pt/Q$. Thus we were led to an equation of the form (1.8), where $g(u, v)$ is the left-hand side of the last equation.

Now we study the roots of $g(\vartheta, 1)=0$. This equation is equivalent to the pair of quadratic equations

$$[R_1-R_2(s+vt\omega)]\vartheta^2-2[S_1-S_2(s+vt\omega)]\vartheta+[T_1-T_2(s+vt\omega)]=0, \\ v=\pm 1.$$

In view of (1.3) we have

$$S_1^2-R_1T_1=-\mu tekz_1^2, \quad S_2^2-R_2T_2=\mu tez_1^2$$

from which, taking also into account (1.2), we find that the discriminants of the above quadratic equations are

$$2\mu vet^2z_1^2\omega(s+v\omega t), \quad v=+1, -1.$$

The product of these two discriminants is $-4e^2t^4z_1^4dk<0$, which means that $g(\vartheta, 1)=0$ has exactly two real roots.

In case of (1.14) we are led in an analogous way to a finite number of equations

$$[(2R_1-2sR_2-R_2t)u^2-2(2S_1-2sS_2-S_2t)uv+ \\ +(2T_1-2sT_2-T_2t)v^2]^2-d(R_2tu^2-2S_2tuv+T_2tv^2)^2=A^2,$$

where now $A=2Pt/Q$ and $d=(2\omega-1)^2$. This is an equation of the form (1.8) and the solutions of $g(\vartheta, 1)=0$ are the roots of

$$[R_1-R_2(s+t\omega)]\vartheta^2-2[S_1-S_2(s+t\omega)]\vartheta+[T_1-T_2(s+t\omega)]=0$$

and of the equation that results from this one on replacing ω by ω'. As before, we find that the discriminants of the two quadratic equations are

$$2\mu t^2ez_1^2d^{1/2}(s+t\omega) \quad \text{and} \quad -2\mu t^2ez_1^2d^{1/2}(s+t\omega')$$

whose product is $-4t^4e^2z_1^4dk<0$. Thus, again $g(\vartheta, 1)=0$ has exactly two real roots and this completes the proof.

2. An application. The diophantine equation

$$x^2-3y^4=46 \tag{2.1}$$

treated by the method of Section 1.

A special case of (2.1) is

$$X^4-4X^2Y^2+Y^4=46. \tag{2.2}$$

The biquadratic form in the left-hand side of (2.2) arises in the study of the following problem (communicated to the author by R. J. Stroeker): Prove that the product of three integers taken from any set of four consecutive positive integers is never a square. This is closely related to some problems on products of integers originated to P. Erdös, R. L. Graham and J. L. Selfridge (see [23], especially p. 37). The above problem is easily reduced in proving that

$$X^4-4X^2Y^2+Y^4=-2 \tag{2.3}$$

has only the solutions given by $(|X|, |Y|)=(1, 1)$.

Easy congruence-arguments show that the diophantine equation

$$X^4-4X^2Y^2+Y^4=c, \quad |c|\leqslant 100 \tag{2.4}$$

has solutions only when $c\in\{-47, -32, -2, 1, 16, 46, 81\}$. The cases $c=-32, 16, 81$ are trivially reduced to the cases $c=-2, 1, 1$, respectively. For $c=1$ it suffices to solve

$$x^2-3y^4=1. \tag{2.5}$$

This can be solved by a method suggested in Section 1 (cf. the solution of (2.1) below). Alternatively, using a result by Ljunggren [14] we know that (2.5) has at most two solutions with x, y positive integers. Since $(x, y)=(2, 1), (7, 2)$ are solutions to (2.5), these are the only ones.

There is a rather elementary solution of (2.4) when $c=-2$ and it is hoped that in a future paper by R. J. Stroeker and the author this solution will be presented together with a solution of the case $c=-47$.

The case $c=46$ remains in (2.5) and, clearly, it suffices to solve (2.1) on applying the ideas of Section 1.

Let $\omega=\sqrt{3}$. In $Q(\omega)$ we have the ideal equation

$$(x+y^2\omega)(x-y^2\omega)=(1+\omega)^2(2+3\omega)(2-3\omega).$$

Therefore $(x\pm y^2\omega)=(1+\omega)(2-3\omega)$. The fundamental unit in $Q(\omega)$ is $2+\omega$. On supposing $x>0$ we have $x\pm y^2\omega>0$, therefore

$$x\pm y^2\omega=(7+\omega)(2+\omega)^j(m+n\omega)^2, \quad j=0 \text{ or } 1 \tag{2.6}$$

where $m+n\omega$ is a unit, so that $(m, 3n)=1$ and m, n are of opposite partities.

I) If $j=0$ then $\pm y^2=m^2+14mn+3n^2$ and the lower sign implies an impossible mod 23 relation. The upper sign implies

$$(m+7n+y)(m+7n-y)=46n^2. \tag{2.7}$$

Since $m+7n$ and y are odd, we may put $(m+7n+y, m+7n-y)=2d$, d odd. Let p be a prime divisor of d. Then $p|m+7n$. On the other hand $p^2|46n^2$, so that $p|n$. Therefore $p|n$ and $p|m$; a contradiction. Thus $(m+7n+y, m+7n-y)$

$= 2$ and without loss of generality we may suppose that $m+7n+y \equiv 0 \pmod 4$. Now it follows from (2.7) that either

(2.8)
$$m+7n+y = \varepsilon 92u^2, \quad m+7n-y = \varepsilon 2v^2, \quad n = 2uv, \quad \varepsilon = \pm 1, \quad (46u, v) = 1$$

or

(2.9)
$$m+7n+y = \varepsilon 4u^2, \quad m+7n-y = \varepsilon 46v^2, \quad n = 2uv, \quad \varepsilon = \pm 1, \quad (2u, 23v) = 1.$$

From (2.8) we get $m = 46u^2 - 14\varepsilon uv + v^2$, $\varepsilon n = 2\varepsilon uv$. On replacing εu by u we get, in view of $m^2 - 3n^2 = 1$,

$$(46u^2 - 14uv + v^2)^2 - 3(2uv)^2 = 1, \tag{2.10}$$

i.e.

$$\mathrm{Norm}(v - u\vartheta) = 1, \tag{2.10'}$$

where

$$(\vartheta^2 - 14\vartheta + 46)^2 - 3(2\vartheta)^2 = 0 \tag{2.11}$$

and this equation has exactly two real roots.

From (2.9) we get as before

$$(2u^2 - 14uv + 23v^2)^2 - 3(2uv)^2 = 1. \tag{2.12}$$

Modulo 8 it is seen that u is even and then, modulo 16, that $4|u$. Now, by (2.12), $(2u^2 - 14uv + 23v^2) + 2uv\omega$ is a unit of $\boldsymbol{Q}(\omega)$ with an even coefficient of ω, so that it must be $\pm$ an even power of $2+\omega$. Thus, we may write

$$2u^2 - 14uv + 23v^2 = \varepsilon(a^2 + 3b^2), \quad uv = \varepsilon ab, \quad \varepsilon = \pm 1 \tag{2.13}$$

where $a + b\omega$ is some unit of $\boldsymbol{Q}(\omega)$. By $(2.13)_1$,

$$-1 \equiv \varepsilon(a^2 + 3b^2) \pmod 8.$$

If $\varepsilon = 1$ then $a \equiv 2 \pmod 4$ and b is odd. Since $4|u$, it follows that $(2.13)_2$ is impossible. If $\varepsilon = -1$ then by $(2.13)_1$, $a^2 + 3b^2 \equiv 1 \pmod 4$, so that a is odd and b is even. By $(2.13)_2$

$$\frac{u}{b} = \frac{-a}{v} = \frac{\mu}{\nu}, \quad (\mu, \nu) = 1, \quad \mu\nu \text{ odd}.$$

Then $u = B\mu$, $b = B\nu$, $a = -A\mu$, $v = A\nu$ and substitution in $(2.13)_1$ gives

$$(A^2 + 2B^2)\mu^2 - 14AB\mu\nu + (23A^2 + 3B^2)\nu^2 = 0,$$

which is impossible, since the discriminant of this form in μ, ν is $-23A^4 - 6B^4 < 0$.

II) If $j = 1$ then by (2.6), $9m^2 + 34mn + 27n^2 = \pm y^2$, which is written

$(9m+17n)^2 - 46n^2 = \pm(3y)^2$, clearly impossible mod 23 with the lower sign. Therefore

$$(9m+17n+3y)(9m+17n-3y) = 46n^2. \tag{2.14}$$

Let $n \not\equiv 0 \pmod 3$. Then $(9m+17n, 3y) = 1$ so that there are essentially two cases to be considered:

$$9m+17n+3y = 92u^2, \quad 9m+17n-3y = 2v^2, \quad n = 2uv, \quad (46u, v) = 1, \tag{2.15}$$

$$9m+17n+3y = 4u^2, \quad 9m+17n-3y = 46v^2, \quad n = 2uv, \quad (2u, 23v) = 1. \tag{2.16}$$

Next, let $n \equiv 0 \pmod 3$. Then, by $9m^2 + 34mn + 27n^2 = y^2$ it follows that $3|y$, therefore $9|n$. Put $y = 3y_1$ and $n = 9n_1$, so that (2.14) becomes

$$(m + 17n_1 + y_1)(m + 17n_1 - y_1) = 46n_1^2,$$

where the factors in the left-hand side are relatively prime. Thus, there are essentially two cases to be considered:

$$m+17n_1+y_1 = 92u^2, \quad m+17n_1-y_1 = 2v^2, \quad n_1 = 2uv, \quad (46u, v) = 1, \tag{2.17}$$

$$m+17n_1+y_1 = 4u^2, \quad m+17n_1-y_1 = 46v^2, \quad n_1 = 2uv, \quad (2u, 23v) = 1. \tag{2.18}$$

Consider (2.15): $9m = 46u^2 - 34uv + v^2$ and mod 3 it is seen that $u + v \equiv 0 \pmod 3$. Thus, we put $v = 3w - u$, so that

$$m = w^2 - 12wu + 9u^2, \quad n = 6wu - 2u^2 \tag{2.19}$$

and substitution in $m^2 - 3n^2 = 1$ gives

$$(w^2 - 12wu + 9u^2)^2 - 3(6wu - 2u^2)^2 = 1, \tag{2.20}$$

i.e.

$$\mathrm{Norm}(w - u\vartheta) = 1, \tag{2.20'}$$

where

$$(\vartheta^2 - 12\vartheta + 9)^2 - 3(6\vartheta - 2)^2 = 0 \tag{2.21}$$

(exactly two real roots).

Now consider (2.16): $9m = 2u^2 - 34uv + 23v^2$ and mod 3 we see that $u \equiv v \pmod 3$. Put $u = v + 3w$ so that $m = 2w^2 - 10wv - v^2$ and $n = 6wv + 2v^2$. As in the case of (2.12), we see that $\pm(m + n\omega)$ is a square of a unit $a + b\omega$ of $\boldsymbol{Q}(\omega)$, so that

$$2w^2 - 10wv - v^2 = \varepsilon(a^2 + 3b^2), \quad \varepsilon ab = 3wv + v^2, \quad \varepsilon = \pm 1. \tag{2.22}$$

On the other hand, $m^2 - 3n^2 = 1$ implies $4w^4 - 40w^3v - 12w^2v^2 - 52wv^3 - 11v^4 = 1$ and mod 8 it is seen that w is odd. Since v is odd we easily see mod 16 that $wv \equiv 1 \pmod 4$. Then, by $(2.22)_1$, $-1 \equiv \varepsilon(a^2 + 3b^2) \pmod 8$.

If $\varepsilon = 1$ then $a \equiv 2 \pmod 4$ and b is odd, so that $(2.22)_2$ is impossible mod 4. If $\varepsilon = -1$ then $a^2+3b^2 \equiv 1 \pmod 4$ and a is odd, b is even. By $(2.22)_2$,

$$\frac{a}{v} = \frac{3w+v}{-b} = \frac{\mu}{\nu}, \quad (\mu, \nu) = 1, \quad \mu\nu \text{ odd},$$

so that $a = A\mu$, $v = A\nu$, $b = -B\nu$, $w = (B\mu - A\nu)/3$. Substitution in $(2.22)_1$ gives $(9A^2+2B^2)\mu^2 - 34AB\mu\nu + (23A^2+27B^2)\nu^2 = 0$, which is impossible since the discriminant of this form in μ, ν is negative.

Next consider (2.17): $m = 46u^2 - 34uv + v^2$, $n = 18uv$ and $m^2 - 3n^2 = 1$ gives

$$(v^2 - 34vu + 46u^2)^2 - 3(18uv)^2 = 1, \tag{2.23}$$

i.e.

$$\mathrm{Norm}(v - u\vartheta) = 1 \tag{2.23'}$$

where

$$(\vartheta^2 - 34\vartheta + 46)^2 - 3(18\vartheta)^2 = 1 \tag{2.24}$$

(exactly two real roots).

Finally, (2.18) is impossible, as it is seen when we work as in the case of (2.16).

Thus, *in order to solve* (2.1) *it suffices to solve* (2.10), (2.20) *and* (2.23).

3. The solution of (2.10), (2.20) and (2.23). As in Section 2, $\omega = \sqrt{3}$.

Consider (2.10). Put $\Theta = (6+14\omega)^{1/2}$, so that in (2.11) $\vartheta = 7+\omega+\Theta$. We work in the order $\boldsymbol{Z}[1, \omega, \Theta, \omega\Theta]$. By (2.10')

$$(v-7u) - u\omega - u\Theta = \pm\varepsilon_1^m \varepsilon_2^n, \tag{3.1}$$

where ε_1, ε_2 is a pair of fundamental units. Such a pair is (see Section 5)

$$\varepsilon_1 = 77+44\omega+14\Theta+8\Theta\omega, \quad \varepsilon_2 = 2+\omega.$$

Now we work p-adically with $p = 61$. A calculation shows that

$$\varepsilon_1^{60} \equiv 1+61(30\Theta - 21\Theta\omega), \quad \varepsilon_2^{30} \equiv -1-61\cdot 27\omega \pmod{61^2}. \tag{3.2}$$

Put $m = 60M+r$, $n = 30N+s$, $0 \leqslant r \leqslant 59$, $0 \leqslant s \leqslant 29$. By (3.1)

$$(v-7u) - u\omega - u\Theta \equiv \pm\varepsilon_1^r \varepsilon_2^s \pmod{61},$$

therefore in $\varepsilon_1^r \varepsilon_2^s$ the coefficient of $\Theta\omega$ must be zero (mod 61) and the coefficients of ω and Θ must be congruent (mod 61). A search in the computer showed that the only pairs (r, s) satisfying both conditions are $(r, s) = (0, 0)$, $(30, 15)$. The second pair must be rejected, for, in this case

m is even and n is odd. On the other hand, $\varepsilon_1^2 \equiv 1$, $\varepsilon_2^2 \equiv -1 \pmod 4$, therefore by (3.1),

$$(v-7u) - u\omega - u\Theta \equiv \pm\varepsilon_2 = \pm(2+\omega) \pmod 4,$$

clearly impossible.

Thus, $m = 60M$, $n = 30N$ and in view of (3.2) we have the 61-adic expansions

$$\varepsilon_1^{60M} = [1+61^2(\ )] + 61^2(\ )\omega + [61\cdot 30M + 61^2(\ )]\Theta + \\ + [-61\cdot 21M + 61^2(\ )]\Theta\omega,$$

$$\pm\varepsilon_2^{30N} = [1+61^2(\ )] + [61\cdot 27N + 61^2(\ )]\omega$$

where every ( ) above stands for some 61-adic integer. Then, equating of the coefficients in (3.1) gives the 61-adic system

$$\begin{aligned} -21M + \quad & +61(\ ) = 0, \\ 30M + 27N & +61(\ ) = 0, \end{aligned} \qquad \begin{vmatrix} -21 & 0 \\ 30 & 27 \end{vmatrix} \not\equiv 0 \pmod{61}.$$

By a well-known result of Skolem ([20], p. 180; see also footnote p. 500 of [3]) $(M, N) = (0, 0)$ is the only solution of the system, proving that $(m, n) = (0, 0)$ is the only solution of (3.1).

We conclude therefore that $(u, v) = (0, \pm 1)$ *is the only solution to* (2.10).

For the solution of (2.20) and (2.23) we work in $\boldsymbol{Q}(\Theta)$, where now $\Theta = (54+34\omega)^{1/2}$ and

$$\vartheta = \begin{cases} 6+3\omega+\Theta & \text{in case of (2.20')–(2.21),} \\ 17+9\omega+3\Theta & \text{in case of (2.23')–(2.24).} \end{cases}$$

We work p-adically as before, but now it is convenient to take $p = 11$. A pair of fundamental units in the order $\boldsymbol{Z}[1, \omega, \Theta, \Theta\omega]$ is

$$\varepsilon_1 = 863+498\omega+81\Theta+47\Theta\omega, \quad \varepsilon_2 = 2+\omega$$

(see Section 5), with

$$\varepsilon_1^5 \equiv 1+11(2\Theta+5\Theta\omega), \quad \varepsilon_2^5 \equiv -1-11\cdot 3\omega \pmod{11^2}.$$

(2.20') and (2.23') are respectively equivalent to

$$(w-6u) - 3u\omega - u\Theta = \pm\varepsilon_1^m \varepsilon_2^n, \quad (v-17u) - 9u\omega - 3u\Theta\omega = \pm\varepsilon_1^m \varepsilon_2^n. \tag{3.3}$$

In both cases we put $m = 5M+r$, $n = 5N+s$, $0 \leqslant r, s \leqslant 4$, and we see that in $\varepsilon_1^r \varepsilon_2^s$ the coefficient of $\Theta\omega$ is zero (mod 11) and the coefficient of ω is 3 times the coefficient of Θ (mod 11). It is readily seen that $(r, s) = (0, 0)$ is the only pair satisfying both conditions and as before we find an 11-adic system in M, N, which has as its only solution $(M, N) = (0, 0)$. Thus, in both relations (3.3) we have $(m, n) = (0, 0)$, proving that $(u, w) = (0, \pm 1)$ *is the only solution to* (2.20) *and* $(u, v) = (0, \pm 1)$ *is the only solution to* (2.23).

4. The complete solution of $x^2-3y^4=46$. We return to Section 2. From (2.10) $u=0$, $|v|=1$ and then (2.8) implies $n=0$, $m+y=0$, $m-y=\pm 2$, so that $|y|=1$ and $|x|=7$.

From (2.20), $u=0$, $|w|=1$ ($|v|=3$) and then from (2.19), $n=0$, $m=1$, while from (2.15) $3m+y=0$, $3m-y=6$, i.e. $y=-3$ and $|x|=17$. In an analogous way, (2.23) produces the solution $y=-3$, $|x|=17$.

We have thus proved the following

THEOREM. *The only solutions to* $x^2-3y^4=46$ *are given by* $(|x|, |y|)=(7, 1), (17, 3)$.

COROLLARY. *The only solutions to* $X^4-4X^2Y^2+Y^4=46$ *are given by*

$$(|X|, |Y|)=(1, 3), (3, 1).$$

5. The fundamental units in the orders of Section 3. Consider the biquadratic field $K=Q(\Theta)$, $\Theta=\sqrt{a+b\sqrt{m}}$, where $a, b, m\in Z$, $m>0$, $\sqrt{m}\notin Q$, $a+b\sqrt{m}>0$, $a-b\sqrt{m}<0$. For any $\alpha\in K$ we denote by α', α'', $\bar{\alpha}''$ its algebraic conjugates (α' is real and α'', $\bar{\alpha}''$ are complex-conjugates). We have used the following result of Berwick [1], conveniently formulated here (see also [26]): *Let R be an order of K containing the ring of integers of $Q(\sqrt{m})$. Then, the set $E=\{\varepsilon:\ \varepsilon$ unit of R, $\varepsilon>1$, $|\varepsilon'|<1$, $|\varepsilon''|\leqslant 1\}$ is a discrete non-empty set. Let ε_1 be the minimum element of E and $\varepsilon_2>1$ the fundamental unit of $Q(\sqrt{m})$. Then $\varepsilon_1\varepsilon_1'=\pm\varepsilon_2$ or ± 1. If $\varepsilon_1\varepsilon_1'=\pm 1$ and $\varepsilon_2<\varepsilon_1$ and $\sqrt{\varepsilon_2}\notin R$, then ε_1, ε_2 is a pair of fundamental units in R.*

The above theorem can be immediately applied for the quartic fields appearing in Section 3. The search of the units ε_1 was made with the aid of a personal computer (Apple). The algorithm used is similar (but rather simpler) to that used in [25]. In both cases the ε_1 found satisfied $\varepsilon_1\varepsilon_1'=1$.

Alternatively, we can use Theorem 7 of Section 12 of Nagell [18]. Note that in Nagell's notation, the $Q(\Theta)$' s of this paper belong to class 7 (Théorème 4 of [18]).

References

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

[2] Z. I. Borevič and I. R. Šafarevič, *Number Theory*, Academic Press, New York, London 1973.

[3] A. Bremner, *Solution of a problem of Skolem*, J. Number Theory 9 (1977), pp. 499–501.

[4] — *A diophantine equation arising from tight 4-designs*, Osaka J. Math. 16 (1979), pp. 353–356.

[5] — *On trinomials of type x^n+Ax^m+1*, Math. Scand. 49 (1981), pp. 145–155.

[6] A. Bremner and P. Morton, *The integer points on three related elliptic curves*, Math. Comp. 39 (1982), pp. 235–238.

[7] A. Bremner and N. Tzanakis, *Integer points on $y^2=x^3-7x+10$*, ibid. 41 (1983), pp. 731–741.

[8] A. Bremner, *Integral generators in a certain quartic field and related diophantine equations*, to appear.

[9] S. Chowla, D. J. Lewis, and T. Skolem, *The diophantine equation $2^{n+2}-7=x^2$ and related problems*, Proc. Amer. Math. Soc. 10 (1959), pp. 663–669.

[10] J. Dawe and M. Lal, *Solutions of the diophantine equation $x^2-Dy^4=k$*, Math. Comp. 22 (1968), pp. 679–682.

[11] L. E. Dickson, *Introduction to the Theory of Numbers*, Dover Publ., New York 1957.

[12] W. Leveque, *Reviews in Number Theory*, Vol. 2, Amer. Math. Soc. 1974.

[13] D. J. Lewis, *Diophantine equations: p-adic methods*, in *Studies in Number Theory*, M.A.A. Studies in Mathematics, Vol. 6, Math. Assoc. of America, 1969.

[14] W. Ljunggren, *Einige Eigenschaften der Einheiten reeller quadratischer und reinbiquadratischer Zahlkörper*, Skr. Norske Vid.-Akad. Oslo I, Mat.-Naturv. Kl. 1936, no 12.

[15] — *Diophantine equations: A p-adic approach*, Notes prepared by R. R. Laxton, Univ. of Nottingham, 1968.

[16] — *On the diophantine equation $y^2-k=x^3$*, Acta Arith. 8 (1963), pp. 451–463.

[17] L. J. Mordell, *Diophantine Equations*, Academic Press, London, New York 1969.

[18] T. Nagell, *Sur quelques questions dans la théorie des corps biquadratiques*, Arkiv för Mat., Band 4, no 26 (1961), pp. 347–376.

[19] — *Introduction to Number Theory*, Chelsea Publ. Co., New York 1964.

[20] T. Skolem, *Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen*, 8$^{\text{de}}$ Skand. Mat. Kongress, Stockholm 1934, pp. 163–188.

[21] R. J. Stroeker, *On the diophantine equation $x^3-Dy^2=1$*, Nieuw Arch. Wisk. (3) 24 (1976), pp. 231–255.

[22] — *On a diophantine equation of E. Bombieri*, Proc. Koninklijke Nederlandse Akad. van Wetenschappen, Amsterdam, series A, 80 (1977), pp. 131–139.

[23] J. W. M. Turk, *Products of integers in short intervals*, Econometric Institute, Erasmus University, Rotterdam, Report 8228/M.

[24] N. Tzanakis, *The diophantine equation $x^3-3xy^2-y^3=1$ and related equations*, J. Number Theory 18 (1984), pp. 192–204. (Corrigendum: ibid. 19 (1984), p. 296.

[25] — *On the diophantine equation $2x^3+1=py^2$*, Manuscripta Math. 54 (1985), pp. 145–164.

[26] — *A remark on a theorem of W. E. H. Berwick*, to appear in Math. Comp. (1986).

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF CRETE
IRAKLION, CRETE, GREECE

Received on 13.9.1984
and in revised form on 22.1.1985 (1454)