

Explicit solution of a class of quartic Thue equations

by

NIKOS TZANAKIS (Iraklion)

1. Introduction. In this paper we deal with the efficient solution of a certain interesting class of quartic Thue equations. In recent years general powerful methods have been developed for the explicit solution of Thue equations; see e.g. [TW], [PS] and the references given there. As these methods depend on rather heavy numerical computations, we think that methods for the solution of special classes of Thue equations which, on the one hand, depend as little as possible on such heavy computations and, on the other hand, are as elementary as possible, have always a theoretical as well as a practical interest.

The Thue equations with which we deal in this paper are those equations

$$(1) \quad \begin{aligned} f(x, y) &= m, \\ f(x, y) &= a_0x^4 + 4a_1x^3y + 6a_2x^2y^2 + 4a_3xy^3 + a_4y^4 \in \mathbb{Z}[x, y], \quad a_0 > 0, \end{aligned}$$

whose corresponding quartic field \mathbb{K} is Galois and non-cyclic. This condition on \mathbb{K} is equivalent with \mathbb{K} having three quadratic subfields (see [N], at the beginning of no. 6), which in turn happens exactly when the cubic resolvent of the quartic Thue equation has three distinct rational roots ([N], Theorem 1). If \mathbb{K} is totally complex, then elementary estimates imply small upper bounds for $|x|$ and $|y|$; thus, the efficient solution in this case is easy and, as a consequence, we may assume that \mathbb{K} is not totally complex. Then, by the classification of Nagell (Table in page 351 of [N]), \mathbb{K} is totally real; in fact, it is the compositum of two real quadratic fields and it contains exactly three quadratic subfields, all of which are real.

In §§2–4 we prove that solving (1), under the above assumptions on \mathbb{K} , reduces to solving a system of two Pellian equations having one common unknown. Such a reduction has certain advantages:

- Dealing with Pellian equations, the only algebraic-arithmetical data needed are units and factorization in orders $\mathbb{Z}[\sqrt{m}]$, $m > 0$, and this sort of data is easily accessible.

• It is not unusual that a system of Pellian equations can be solved by completely elementary means; see §§5 and 6, where examples are given.

• If an elementary method does not work for the solution of a system as above, there is a highly promising method of R. G. E. Pinch [P] which, though based on the *theory of linear forms in logarithms of algebraic numbers*, does not require high precision computations with algebraic numbers and their logarithms, nor does it require any sort of a reduction process, like those usually following the application of that theory, for reducing the very large theoretical upper bounds ⁽¹⁾; examples are given in §7.

• Even if the aforementioned methods do not work, another one, based again on the theory of linear forms in logarithms, is always possible; this is due to A. Baker and H. Davenport [BD] and is also described as “Method 1” in D. Zagier’s paper [Z]. This method leads, in general, to a linear form in *three* logarithms and *two* unknown integral coefficients, whereas any direct attack on the problem of solving (1) by applying the known general methods would, in general, lead to a linear form in *four* logarithms and *three* unknown integral coefficients.

In §§5–7 we discuss methods of solution of systems of two Pellian equations and give applications to various numerical examples.

2. Instead of the cubic resolvent of the quartic equation $f(x, 1) = 0$, it is more convenient to consider the cubic equation

$$(2) \quad \varrho^3 - g_2\varrho - g_3 = 0$$

with roots opposite to those of the cubic resolvent; here g_2 and g_3 are the invariants of the form:

$$g_2 = a_0a_4 - 4a_1a_3 + 3a_2^2, \quad g_3 = \begin{vmatrix} a_0 & a_1 & a_2 \\ a_1 & a_2 & a_3 \\ a_2 & a_3 & a_4 \end{vmatrix},$$

and, as mentioned in §1, in the case that we study, (2) has three distinct rational roots, which we denote by ϱ_i ($i = 1, 2, 3$). According to no. 2 of Nagell’s [N] (some symbolic computations are needed) the typical root of $f(x, 1) = 0$ is of the form

$$(3) \quad -\frac{a_1}{a_0} + \sum_{i=1}^3 \sqrt{\left(\frac{a_1}{a_0}\right)^2 - \frac{a_2 + \varrho_i}{a_0}},$$

where the symbol $\sqrt{(\cdot)}$ denotes one of the two square roots of the quantity under it (not known *a priori* which of the two). It is easy to see, however,

⁽¹⁾ Such reduction processes are usually based on continued fractions techniques or on the LLL basis reduction algorithm.

that a number of the form (3) can be real only if all three quantities under the square root symbol are non-negative; for the proof of this it is important to notice that the three quadratic fields $\mathbb{Q}(\sqrt{\varrho_i})$ ($i = 1, 2, 3$) are distinct (see no. 2 in [N]). Thus, *the Thue equations we will deal with in this paper are characterized by the fact that the cubic equation (2) corresponding to f has three distinct rational roots $\varrho_1, \varrho_2, \varrho_3$ and*

$$\frac{a_1^2}{a_0} - a_2 \geq \max\{\varrho_1, \varrho_2, \varrho_3\}.$$

3. We have

$$g_2 \in \frac{1}{12}\mathbb{Z}, \quad g_3 \in \frac{1}{432}\mathbb{Z}.$$

Let $H(x, y)$ and $G(x, y)$ be the quartic and sextic covariants of $f(x, y)$, respectively (see Chapter 25 of Mordell's book [M*]), i.e.

$$(4) \quad \begin{aligned} H(x, y) &= -\frac{1}{144} \begin{vmatrix} \frac{\partial^2 f}{\partial x^2} & \frac{\partial^2 f}{\partial x \partial y} \\ \frac{\partial^2 f}{\partial y \partial x} & \frac{\partial^2 f}{\partial y^2} \end{vmatrix}, \\ G(x, y) &= -\frac{1}{8} \begin{vmatrix} \frac{\partial f}{\partial x} & \frac{\partial f}{\partial y} \\ \frac{\partial H}{\partial x} & \frac{\partial H}{\partial y} \end{vmatrix}. \end{aligned}$$

We have

$$H(x, y) \in \frac{1}{48}\mathbb{Z}[x, y], \quad G(x, y) \in \frac{1}{96}\mathbb{Z}[x, y]$$

and

$$(5) \quad 4H^3 - g_2 H f^2 - g_3 f^3 = G^2$$

(Theorem 1, Chapter 25 of [M*]).

PROPOSITION 1. *f and H are relatively prime in $\mathbb{Q}[x, y]$.*

PROOF. If not then, since f and H are of the same degree and f is irreducible in $\mathbb{Q}[x, y]$, we would have

$$(6) \quad H = r \cdot f, \quad r \in \mathbb{Q}.$$

Then, by the definition of G (see (4)), $G = 0$; hence, by (5) and (6)

$$(7) \quad 4r^3 - g_2 r - g_3 = 0$$

and it follows that $r \in \{\varrho_1, \varrho_2, \varrho_3\}$. Let now g'_2, g'_3 be the invariants of the quartic form H . It is easy to check that

$$g'_2 = \frac{1}{12}g_2^2, \quad g'_3 = \left(\frac{g_2}{6}\right)^3 - \left(\frac{g_3}{2}\right)^2$$

and, on the other hand, in view of $H = r \cdot f$, it follows that

$$g'_2 = r^2 \cdot g_2, \quad g'_3 = r^3 \cdot g_3,$$

therefore

$$(8) \quad r^2 \cdot g_2 = \frac{1}{12}g_2^2, \quad r^3 \cdot g_3 = \left(\frac{g_2}{6}\right)^3 - \left(\frac{g_3}{2}\right)^2.$$

If $g_2 = 0$, then $g_3 \neq 0$ (because (2) has distinct roots) and the second relation in (8) implies $g_3 = -4r^3$; by (7) and $g_2 = 0$ it follows that $g_3 = 4r^3$, hence $g_3 = 0$, a contradiction. Thus, $g_2 \neq 0$ and the first relation in (8) implies $g_2 = 12r^2$; then, by (7), $g_3 = -8r^3$ and equation (2) becomes $\varrho^3 - 3r^2\varrho + 2r^3 = 0$; this equation has $\varrho = r$ as a double root, which is a contradiction (see the end of §2); this completes the proof.

4. Now we show how the solution of (1) reduces to the solution of a system of two Pellian equations. We put

$$H = \frac{1}{48}H_0, \quad G = \frac{1}{96}G_0, \quad \varrho_i = \frac{1}{12}r_i \quad (i = 1, 2, 3);$$

$$H_0, G_0 \in \mathbb{Z}[x, y], \quad r_i \in \mathbb{Z} \quad (i = 1, 2, 3).$$

Then, in view of (5),

$$(H_0 - 4r_1f)(H_0 - 4r_2f)(H_0 - 4r_3f) = 3G_0^2$$

and the three factors in the left-hand side are pairwise relatively prime in $\mathbb{Z}[x, y]$, by Proposition 1. Then there exist non-zero, square-free integers k_1, k_2, k_3 and quadratic forms $G_i \in \mathbb{Z}[x, y]$, $i = 1, 2, 3$, such that

$$(9) \quad H_0 - 4r_i f = k_i G_i^2, \quad i = 1, 2, 3,$$

and

$$(10) \quad k_1 k_2 k_3 (G_1 G_2 G_3)^2 = 3G_0^2.$$

Then, if $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ is a solution of (1), we get from (9),

$$(11) \quad k_2 G_2^2 - k_1 G_1^2 = 4(r_1 - r_2)m, \quad k_3 G_3^2 - k_1 G_1^2 = 4(r_1 - r_3)m.$$

Clearly, if $k_1 k_2$ or $k_1 k_3$ is a square of an integer, then the first or the second equation, respectively, is trivially soluble (with a finite number of solutions (x, y) , which can be explicitly found), therefore we will assume that both $k_1 k_2$ and $k_1 k_3$ are not squares of an integer. Moreover, we show that k_1, k_2, k_3 are positive and thus we see that (11) is indeed a system of Pellian equations with one common unknown.

From (10), either exactly one of the k_i 's or all three of them are positive. We exclude the first alternative: If this were the case, we could suppose without loss of generality that $k_1 > 0$ and $k_2, k_3 < 0$. Then, by (9), we

would have the polynomial identity

$$4(r_1 - r_2)f = k_2G_2^2 - k_1G_1^2$$

and the right-hand side would be negative for every real pair (x, y) , which contradicts the fact that the equation $f(x, 1) = 0$ has real solutions.

EXAMPLES

5. Congruence considerations and quadratic reciprocity. We consider the Thue equation

$$(12) \quad f(x, y) = \mu, \quad f(x, y) = x^4 - 4x^3y + 8xy^3 - y^4, \quad \mu = \pm 1.$$

Here

$$(13) \quad \begin{aligned} g_2 = 7, \quad g_3 = -3; \quad \varrho_1 = 1, \quad \varrho_2 = \frac{1}{2}, \quad \varrho_3 = -\frac{3}{2}; \\ H(x, y) = x^4 - 4x^3y + 5x^2y^2 - 2xy^3 + 4y^4, \\ H - f = 5[y(x - y)]^2, \quad H - \frac{1}{2}f = \frac{1}{2}(x^2 - 2xy + 3y^2)^2, \\ H + \frac{3}{2}f = \frac{5}{2}(x^2 - 2xy - y^2)^2. \end{aligned}$$

Let (x, y) be a solution of (12). On putting

$$U = x^2 - 2xy + 3y^2, \quad V = x^2 - 2xy - y^2, \quad Z = y(x - y)$$

we get, in view of (13),

$$(14) \quad U^2 - 5V^2 = -4\mu, \quad U^2 - 10Z^2 = \mu.$$

This is a system of two Pellian equations with one common unknown and can be solved by Pinch's method; see Section 7, where, after Proposition 5 we solve system (14). An alternative approach, which sometimes might be proven successful, is to replace the system of the Pellian equations by one in which the first equation results from the elimination of the constant term in the right-hand sides. In our example we replace (14) by

$$V^2 + 2(2Z)^2 = U^2, \quad U^2 - 10Z^2 = \mu.$$

The first equation implies

$$\pm V = m^2 - 2n^2, \quad Z = mn, \quad U = m^2 + 2n^2, \quad (m, 2n) = 1,$$

and substitution in the second gives

$$(15) \quad m^4 - 6m^2n^2 + 4n^4 = \mu, \quad \text{i.e.} \quad (m^2 - 3n^2)^2 - 5n^4 = \mu.$$

A number of general, ready-to-apply results on diophantine equations of the form

$$(16) \quad X^2 - d \cdot Y^4 = k$$

due to J. H. E. Cohn [C1]–[C5] might prove useful at this point; it is interesting to note that the proofs of these results are based only on some elementary theory of quadratic number fields, congruence arguments and quadratic reciprocity. By Section 4 of [C1], the only integral solutions of (16) when $d = 5$ are given by $Y^2 = 0$ or 4 if $k = 1$, and by $Y^2 = 1$ if $k = -1$. From this we see that the only solutions to (15) are given by $(m^2, n^2) = (1, 0)$ if $\mu = 1$, and by $(m^2, n^2) = (1, 1)$ if $\mu = -1$, and then, by the definition of U, V and Z , we easily conclude that the following result holds:

PROPOSITION 2. *The only solutions to (12) are*

$$(x, y) = \pm(1, 0) \quad \text{if } \mu = 1, \quad \text{and} \quad (x, y) = \pm(0, 1), \pm(2, 1) \quad \text{if } \mu = -1.$$

6. The Mohanty–Ramasamy method. This method for solving a system of Pellian equations

$$(17) \quad U^2 - D \cdot V^2 = N, \quad Z^2 - g \cdot V^2 = h$$

is due to S. P. Mohanty and A. M. S. Ramasamy [MR]. We describe it now, by making the following assumptions:

- (a, b) is the least positive solution of $A^2 - DB^2 = 1$.
- (u, v) is the fundamental solution of the first equation (17), which belongs to a certain class of solutions. Note that more than one classes may exist, but since their number is always finite, we have a finite number of choices for (u, v) ; see e.g. [N*].

- $(U_r)_{r \in \mathbb{Z}}$ is the recurrence sequence defined by

$$U_0 = u, \quad U_1 = au + Dbv, \quad U_{r+2} = 2aU_{r+1} - U_r.$$

- (a_t) and (b_t) , $t = 1, 2, \dots$, are the sequences defined by

$$a_1 = a, \quad a_{t+1} = 2a_t^2 - 1; \quad b_1 = b, \quad b_{t+1} = 2a_t b_t.$$

Next, choose a modulus m , which has one of the forms

$$2^\alpha \cdot 6, \quad 2^\alpha \cdot 10, \quad 2^\alpha \cdot 30; \quad \alpha \geq 0.$$

If the system (17) is solvable, then there exists an integer n such that both

$$D \cdot V_n^2 + N, \quad g \cdot V_n^2 + h$$

are perfect squares; here V_n is a term of the recurrence sequence defined by

$$(18) \quad V_0 = v, \quad V_1 = av + bu, \quad V_{r+2} = 2aV_{r+1} - V_r.$$

Let \mathcal{M} be a complete system of residues modulo m . If $n \equiv i \pmod{m}$,

$i \in \mathcal{M}$ and $n \neq i$ put

$$\begin{aligned} n &= i + 3 \cdot 2^t(2\lambda + 1), & t \geq 1 & \text{ if } m = 2^\alpha \cdot 6, \\ n &= i + 5 \cdot 2^t(2\lambda + 1), & t \geq 1 & \text{ if } m = 2^\alpha \cdot 10, \\ n &= i + 15 \cdot 2^t(2\lambda + 1), & t \geq 1 & \text{ if } m = 2^\alpha \cdot 30. \end{aligned}$$

PROPOSITION 3 [MR]. *Consider the following Jacobi symbols:*

$$\begin{aligned} &\left(\frac{gU_i^2 - Dh}{a_i^2 + Db_i^2}\right), \quad \left(\frac{gU_i^2 - Dh}{4Db_{t+1}^2 + 1}\right) \quad \text{if } m = 2^\alpha \cdot 6, \\ &\left(\frac{gU_i^2 - Dh}{16D^2b_{t+1}^4 + 12Db_{t+1}^2 + 1}\right) \quad \text{if } m = 2^\alpha \cdot 10, \\ &\left(\frac{gU_i^2 - Dh}{256D^4b_{t+1}^8 + 576D^3b_{t+1}^6 + 416D^2b_{t+1}^4 + 96Db_{t+1}^2 + 1}\right) \quad \text{if } m = 2^\alpha \cdot 30. \end{aligned}$$

If, for each $t \geq 1$: in the first case, at least one of the first two symbols equals -1 and, in the second or third case, the third or fourth symbol, respectively, equals -1 , then the system (17) has no solution with $V = V_n$ and $n \equiv i \pmod{m}$, except possibly $V = V_i$.

Now we show by an example how this proposition is applied in practice. Consider the Thue equation

$$(19) \quad f(x, y) = -4, \quad f(x, y) = x^4 - 4x^3y - 3x^2y^2 + 14xy^3 - 4y^4.$$

In this example

$$\begin{aligned} g_2 &= \frac{43}{4}, \quad g_3 = -\frac{21}{8}; \quad \varrho_1 = \frac{3}{2}, \quad \varrho_2 = \frac{1}{4}, \quad \varrho_3 = -\frac{7}{4}; \\ H - \frac{3}{2}f &= \frac{65}{4}[y(x - y)]^2, \quad H - \frac{1}{4}f = \frac{5}{4}(x^2 - 2xy + 3y^2)^2, \\ H + \frac{7}{4}f &= \frac{13}{4}(x^2 - 2xy - y^2)^2. \end{aligned}$$

Eliminating H and putting $f = -4$, we obtain

$$(20) \quad U^2 - 5V^2 = -4, \quad Z^2 - 13V^2 = -4,$$

where $U = x^2 - 2xy - y^2$, $V = y(x - y)$, $Z = x^2 - 2xy + 3y^2$. With the previous notations we have $D = 5$, $g = 13$, $N = h = -4$, $a = 9$, $b = 4$, $u = v = 1$ (only one class of solutions exists for the first equation). In (19) the cases $x \equiv y \equiv 0 \pmod{2}$ and $x \equiv 1, y \equiv 0 \pmod{2}$ are trivially excluded. Also, if $x \equiv y \equiv 1 \pmod{2}$, then, on putting $x = 2X + Y$, $y = Y$ we transform (19) into $4X^4 - 9X^2Y^2 + Y^4 = -1$, which is impossible mod 4. Therefore, $x \equiv 0, y \equiv 1 \pmod{2}$, hence V is odd. We take $m = 6$. We will show that $V = V_n$ with $n \equiv 0 \pmod{6}$ is the only possibility, i.e., in the notations preceding Proposition 3, $i = 0$. If n is odd, then it is easy to see, in view of (19), that $V_n \equiv \pm 4 \pmod{9}$, hence, from the second equation (20),

$Z^2 \equiv -3 \pmod{9}$, which is impossible, concluding thus that n is even. Let $n \equiv 2 \pmod{6}$. Then, in view of (18),

$$(21) \quad V_n \equiv -19 \pmod{107}$$

and the second equation (20) implies $Z^2 \equiv 13 \cdot 19^2 - 4 \equiv -19 \pmod{107}$, which is impossible. Also, if $n \equiv 4 \pmod{6}$, then, by (18),

$$(22) \quad V_n \equiv -6 \pmod{19}$$

and the second equation (20) is impossible mod 19. We conclude that $n \equiv 0 \pmod{6}$ ($i = 0$) is the only possibility.

A remark should be made about (21) and (22), which did not come out as arbitrarily as it seems at first glance; indeed, in [MR] the following recurrence sequences are considered:

$$\begin{aligned} A_0 &= 1, & A_1 &= a, & A_{r+2} &= 2a \cdot A_{r+1} - A_r, \\ B_0 &= 0, & B_1 &= b, & B_{r+2} &= 2a \cdot B_{r+1} - B_r, \end{aligned}$$

and a number of useful equalities and congruences relating terms of the sequences (A_r) , (B_r) , (U_r) , and (V_r) are displayed in Section 2. Among them are $V_{r+2s} \equiv -V_r \pmod{A_s}$ and $V_{r+2s} \equiv V_r \pmod{B_s}$, hence $V_{2+6k} \equiv -V_2 \pmod{A_{3k}}$ and $V_{4+6k} \equiv V_4 \pmod{B_{3k}}$. Another pair of relation says that $A_3 \mid A_{3k}$ and $B_3 \mid B_{3k}$. Since $A_3 = 2889 \equiv 0 \pmod{107}$ and $B_3 = 1292 \equiv 0 \pmod{19}$, we obtain (21) and (22).

Now we consider the number $g \cdot U_i^2 - D \cdot h = 13U_0^2 - 5(-4) = 33$ and the Jacobi symbol

$$\left(\frac{33}{4 \cdot 5 \cdot b_{t+1}^2 + 1} \right) = \left(\frac{20b_{t+1}^2 + 1}{33} \right), \quad t \geq 1.$$

We compute the sequences $(a_t), (b_t) \pmod{33}$:

$$\begin{aligned} a_t &: 9, -4, -2, 7, -2, 7, -2, 7, \dots \pmod{33}, \\ b_t &: 4, 6, -15, -6, 15, 6, -15, -6, 15, \dots \pmod{33}. \end{aligned}$$

Thus, the Jacobi symbol under consideration is equal to either $\left(\frac{-5}{33}\right)$ or $\left(\frac{13}{33}\right)$ and both are equal to -1 . By Proposition 3 we conclude that $V = \pm V_0 = \pm 1$ is the only possible solution. Since $V = y(x - y)$, we have proved:

PROPOSITION 4. *The only solutions to (19) are $\pm(x, y) = (2, 1), (0, 1)$.*

7. Application of a method of R. G. E. Pinch. In this section we describe a method of R. G. E. Pinch [P] for solving simultaneous Pellian equations

$$(23) \quad (x + f)^2 - ay^2 = b, \quad (x - f)^2 - cz^2 = d,$$

and we apply it for solving quartic Thue equations belonging to the class under discussion. The advantage of Pinch's method is that it is general, in

the sense that it is almost independent of *ad hoc* properties of each particular instance of the system (23) and, although there is no theoretical guarantee that it always works, the experience shows that it is very unlikely to be proved unsuccessful in a certain particular instance. Another important feature of the method is that, although it is based on the *theory of linear forms in logarithms of algebraic numbers*, it does not demand any multi-length computations like those which are usually needed in the practical applications of this theory.

Now we sketch the method. The system (23) leads to a finite number of problems of the sort: Given two second-order linear recurrence sequences (X_n) , (Y_m) , whose recursive relations are respectively

$$X_{n+1} = sX_n - X_{n-1}, \quad Y_{m+1} = tY_m - Y_{m-1},$$

prove that the only non-negative indices m and n satisfying

$$(24) \quad X_n = Y_m + g,$$

with g a prescribed integer, are $m = 0, n = 0$. The first step is to compute an upper bound B of $\max\{m, n\}$, for those pairs (m, n) satisfying (24); this is accomplished by Theorem 2.6 of [P]. Then an algorithm is applied (Section 3 of [P]) which does the following: It finds arbitrarily large moduli M and N such that

$$(25) \quad X_n = Y_m + g \Rightarrow N \mid n \ \& \ M \mid m.$$

Starting from the initial values $M = N = 1$, it adds prime factors to M and N (*which ones* are “added” each time in M and N depends, of course, on g and the particular recurrences appearing in (24)), until $\min\{M, N\} > B$. Then, the combination of the three relations

$$(26) \quad \max\{m, n\} \leq B; \quad M \mid m \ \& \ N \mid n; \quad \min\{M, N\} > B,$$

implies $m = n = 0$. For a description of the algorithm we refer the reader to Section 3 of [P]; in Section 4 of the same paper, some examples are given. We have implemented Pinch’s algorithm independently on a PC (80386, but even on a PC 80286 the program runs very well) using Fortran (Pinch’s implementation uses Algol-68C on an IBM 3081) and, as a first example, we apply it for solving a “random” equation of the class we study, namely

$$(27) \quad f(x, y) = -23, \quad f(x, y) = 4x^4 - 24x^3y - 16x^2y^2 + 60xy^3 + 25y^4.$$

In this example

$$g_2 = \frac{2^2 \cdot 361}{3}, \quad g_3 = \frac{-2^3 \cdot 5291}{27}; \quad \varrho_1 = \frac{11}{3}, \quad \varrho_2 = \frac{26}{3}, \quad \varrho_3 = -\frac{37}{3};$$

$$3H - 11f = 6[2(2x^2 + 5y^2)]^2, \quad 3H - 26f = [3(2x^2 + 10xy - 5y^2)]^2,$$

$$3H + 37f = 2[6(2x^2 - 4xy - 5y^2)]^2.$$

On putting

$$X = 3(2x^2 + 10xy - 5y^2), \quad Y = 2(2x^2 + 5y^2), \quad Z = 6(2x^2 - 4xy - 5y^2)$$

we are led to the simultaneous Pellian equations

$$(28) \quad X^2 - 6Y^2 = 3 \cdot 5 \cdot 23, \quad X^2 - 2Z^2 = 3^2 \cdot 7 \cdot 23.$$

By standard arguments (see also Section 1 of [P]), we are led to the following problems: Find n, m such that $x_n = y_m$, where $(x_n)_{n \geq 0}, (y_m)_{m \geq 0}$ are the recurrence sequences with

$$x_{n+1} = 10x_n - x_{n-1}, \quad y_{m+1} = 6y_m - y_{m-1}$$

and initial values

$$(29) \quad \begin{aligned} (x_0, x_1) &\in \{(19, 183), (9, 77), (13, 121), (7, 51)\}, \\ (y_0, y_1) &\in \{(31, 173), (17, 83), (19, 97), (13, 47)\}. \end{aligned}$$

If $x_n = y_m$ for a pair (n, m) of non-negative integers, then $\pm X = 3x_n$ satisfies both equations (28) and conversely: if X is a solution to the system of equations (28), then there exists a pair of nonnegative integers (m, n) such that $x_n = y_m$ and $\pm X = 3x_n$. From (29) we see that we have 16 pairs of recurrences $(x_n)_{n \geq 0}$ and $(y_m)_{m \geq 0}$ to consider. However, it is easy to see that the set of values x_{-1}, x_{-2}, \dots corresponding to the initial values $(x_0, x_1) = (13, 121)$, coincides with the set of values x_1, x_2, \dots corresponding to the initial values $(x_0, x_1) = (9, 77)$ and similarly for the remaining sequences, which correspond to the initial values $(19, 183)$ and $(7, 51)$. It suffices therefore to consider only the two sequences (x_n) with initial values $(19, 183)$ and $(13, 121)$, but with n ranging over *all* integers. Analogously, we consider only the two sequences $(y_m)_{m \in \mathbb{Z}}$ corresponding to the initial values $(19, 97)$ and $(13, 47)$.

Let $(x_0, x_1) = (19, 183)$ and $(y_0, y_1) = (13, 47)$. The sequence $(x_n) \pmod{11}$ is periodic with period $-3, -4, -4$. Since $y_m \pmod{11}$ never takes the value -4 , we conclude that $n \equiv 0 \pmod{3}$. Next we work modulo 17: (x_n) has a period of length 18 and since we already know that $3|n$, we are interested in the values $x_0, x_3, x_6, x_9, x_{12}, x_{15} \pmod{17}$, which are $2, -8, 7, -2, 8, -7$, respectively. It is easy to check that $y_m \pmod{17}$ never takes any of these values, hence an equality $x_n = y_m$ can never occur and the case we consider is thus impossible.

Once we had implemented Pinch's algorithm, it was easy to modify it so that it was able to detect impossibilities of equations of the form (24) by automatic application of arguments of the above type. In this way, the computer found the right moduli 11 and 17 and working modulo 11 and 17 it showed the impossibility of the case above, as well as the impossibility of the case $(x_0, x_1) = (13, 121)$ & $(y_0, y_1) = (19, 97)$.

We are left with the two cases

$$\begin{aligned} (x_0, x_1) &= (13, 121) \ \& \ (y_0, y_1) = (13, 47); \\ (x_0, x_1) &= (19, 183) \ \& \ (y_0, y_1) = (19, 97). \end{aligned}$$

We feed Pinch’s algorithm with a set consisting of the first 35 primes $2, 3, \dots, 149$ (this is the set P in the notation of Section 3 of [P]; the “auxiliary” set Q of that section in our present application includes the primes from 3 to 547). In the first case, the values of M and N (cf. (25)) which result out of this set P after the application of Pinch’s algorithm are

$$\begin{aligned} M &= 2^6 \cdot 3^4 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 53 \cdot 61 \cdot 71 \cdot 73 \cdot 101, \\ N &= 2^5 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43 \cdot 47 \cdot 59 \cdot 61 \cdot 67 \cdot 79 \cdot 103 \cdot 107, \end{aligned}$$

from which it follows that $M > 9.56 \times 10^{28}$ and $N > 1.58 \times 10^{31}$. On the other hand, by Theorem 2.6 of [P], we have $\max\{m, n\} < 10^{28}$ in the case we study. Thus, in the notation of (26), $B = 10^{28}$, and we conclude that $m = n = 0$ in this case, which implies that the system (28) is possible only if $\pm X = 3x_0 = 3y_0 = 39$, from which $Y = \pm 14, Z = \pm 6$. In the second case we work in a completely analogous way (with the same sets P and Q); now

$$\begin{aligned} M &= 2^6 \cdot 3^4 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 53 \cdot 61 \cdot 71 \cdot 73 \cdot 83 \cdot 101 \cdot 113, \\ N &= 2^5 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43 \cdot 47 \cdot 59 \cdot 61 \cdot 67 \cdot 79 \cdot 97 \cdot 103 \cdot 107, \end{aligned}$$

so that $M > 8.97 \times 10^{32}$ and $N > 1.539 \times 10^{33}$, while Theorem 2.6 of [P] implies $\max\{m, n\} < 10^{28}$; again we conclude that $m = n = 0$ is the only possibility and thus, in this case, $\pm X = 3x_0 = 3y_0 = 57$ is the only solution to the system (28) and this implies $Y = \pm 22, Z = \pm 30$. By the definition of X, Y, Z it is now an easy task to find all possible values pairs (x, y) , which in our case turn out to be $\pm(x, y) = (5, 2), (10, 3), (1, -1), (3, -4)$ and we check that only the pairs $(x, y) = \pm(1, -1)$ satisfy (27). We have thus proved

PROPOSITION 5. *The only integers satisfying (27) are $(x, y) = \pm(1, -1)$.*

As another application of the above method we give an alternative proof of Proposition 2. By (14) and the definition of U , we have to prove that the only solutions with positive U are those with $U = 1$ if $\mu = +1$ and $U = 3$ if $\mu = -1$. In the notations of (23) we have

$$\begin{aligned} x &\leftarrow U, \quad y \leftarrow V, \quad z \leftarrow Z, \\ f &= 0, \quad a = 5, \quad b = -4\mu, \quad c = 10, \quad d = \mu. \end{aligned}$$

By standard arguments (cf. Section 1 of [P]), we have to consider the following couples of recurrence sequences:

$$\begin{aligned} \mu = +1 : x_0 &= 1, \quad x_1 = 4, \quad x_{n+1} = 3x_n - x_{n-1}; \\ y_0 &= 1, \quad y_1 = 19, \quad y_{m+1} = 38y_m - y_{m-1}, \end{aligned}$$

$$\begin{aligned} \mu = -1 : x_0 = 2, \quad x_1 = 3, \quad x_{n+1} = 3x_n - x_{n-1}; \\ y_0 = 3, \quad y_1 = 117, \quad y_{m+1} = 38y_m - y_{m-1} \end{aligned}$$

and prove that $x_n = y_m$ is possible only if $n = m = 0$ in case $\mu = 1$, and only if $(n, m) = (-1, 0), (1, 0)$ in case $\mu = -1$. In both cases, Theorem 2.6 of [P] implies that

$$x_n = y_m \Rightarrow \max\{m, n\} < 1.206 \times 10^{27}.$$

We run Pinch's algorithm exactly as before, but now with somewhat larger sets P and Q ; now P is the set of 40 primes from 2 to 173 and Q is the set of 145 primes from 3 to 997. When $\mu = +1$ we find

$$\begin{aligned} M = 2^5 \cdot 3^5 \cdot 5^3 \cdot 7^2 \cdot 11^2 \cdot 13^2 \cdot 17^2 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 47 \cdot 53 \cdot 59 \cdot 61 \cdot 67 \\ \cdot 71 \cdot 73 \cdot 79 \cdot 83 \cdot 97 \cdot 103 \cdot 107 \cdot 113 \cdot 137 \cdot 173, \\ N = 2^6 \cdot 3^4 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13^2 \cdot 17^2 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 53 \\ \cdot 59 \cdot 61 \cdot 67 \cdot 71 \cdot 73 \cdot 79 \cdot 89 \cdot 97 \cdot 103, \end{aligned}$$

so that $\min\{M, N\} > 2.03 \times 10^{42}$ and by (26) we conclude that $m = n = 0$ is the only possibility, as claimed. When $\mu = -1$ we replace the sequence (x_n) by its three "disjoint" subsequences $(x_n^{(i)})$, $i = -1, 0, 1$, where $x_n^{(i)} = x_{3n+i}$. Then, we have to show that the relation $x_n^{(i)} = y_m$ is true only for $(n, m) = (0, 0)$ if $i = \pm 1$; and it is impossible if $i = 0$. This is accomplished exactly as before, applying Pinch's algorithm with the same sets P and Q . Our program checked automatically the impossibility of $x_n^{(0)} \equiv y_m \pmod{61}$; for $i = \pm 1$ it run and found the following values for M and N :

$$\begin{aligned} M = 2^5 \cdot 3^5 \cdot 5^3 \cdot 7^2 \cdot 11^2 \cdot 13^2 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 47 \cdot 53 \cdot 59 \\ \cdot 61 \cdot 71 \cdot 73 \cdot 79 \cdot 83 \cdot 107 \cdot 113 \cdot 157 \cdot 173, \\ N = 2^6 \cdot 3^3 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13^2 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 47 \\ \cdot 53 \cdot 61 \cdot 67 \cdot 71 \cdot 73 \cdot 79 \cdot 97, \end{aligned}$$

hence $M > 2.7 \times 10^{44}$, $N > 3.466 \times 10^{36}$. By (26), it follows now that $(m, n) = (0, 0)$ is the only possibility in each case, as claimed.

References

- [BD] A. Baker and H. Davenport, *The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$* , Quart. J. Math. Oxford Ser. (2) 20 (1969), 129–137.
- [C1] J. H. E. Cohn, *Eight Diophantine equations*, Proc. London Math. Soc. (3) 16 (1966), 153–166.
- [C2] —, *The Diophantine equation $y^2 = Dx^4 + 1$* , J. London Math. Soc. 42 (1967), 475–476.
- [C3] —, *Some quartic Diophantine equations*, Pacific J. Math. 26 (1968), 233–243.
- [C4] —, *The Diophantine equation $y^2 = Dx^4 + 1$, II*, Acta Arith. 28 (1975), 273–275.

- [C5] J. H. E. Cohn, *The Diophantine equation $y^2 = Dx^4 + 1$, III*, Math. Scand. 42 (1978), 180–188.
- [M*] L. J. Mordell, *Diophantine Equations*, Pure Appl. Math. 30, Academic Press, London 1969.
- [MR] S. P. Mohanty and A. M. S. Ramasamy, *The characteristic number of two simultaneous Pell's equations and its applications*, Simon Stevin 59 (1985), 203–214.
- [N] T. Nagell, *Sur quelques questions dans la théorie des corps biquadratiques*, Ark. Mat. 4 (1961), 347–376.
- [N*] —, *Introduction to Number Theory*, Chelsea, New York 1964.
- [PS] A. Pethő and R. Schulenberg, *Effektives Lösen von Thue Gleichungen*, Publ. Math. Debrecen 34 (1987), 189–196.
- [P] R. G. E. Pinch, *Simultaneous Pellian equations*, Math. Proc. Cambridge Philos. Soc. 103 (1988), 35–46.
- [TW] N. Tzanakis and B. M. M. de Weger, *On the practical solution of the Thue equation*, J. Number Theory 31 (1989), 99–132.
- [Z] D. Zagier, *Large integral points on elliptic curves*, Math. Comp. 48 (1987), 425–436.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF CRETE
IRAKLION, GREECE
E-mail: TZANAKIS@GREARN.BITNET

*Received on 6.10.1992
and in revised form on 13.1.1993*

(2313)