Solving the Diophantine Equation $y^2 = x(x^2 - n^2)$

Konstantinos Draziotis and Dimitrios Poulakis

Abstract

In this paper we give some necessary conditions satisfied by the integer solutions of the Diophantine equation $y^2 = x(x^2 - n^2)$. Next, using these conditions, we develop an algorithm for solving the equation.

1 Introduction

Let n be a positive integer and E_n be the elliptic curve defined by the equation

$$y^2 = x(x^2 - n^2). \tag{1}$$

The equation (1) has always the integer solutions $(0,0), (\pm n, 0)$ which we shall call trivial. These couples and the point at infinity are all the torsion points of E_n over $\mathbb{Q}$. In [8, Lemma 1.1], some sufficient conditions on n are listed for the rank of $E_n(\mathbb{Q})$ to be zero. Furthermore, if n is a perfect square, then, it is easily seen, that the rank of $E_n(\mathbb{Q})$ is zero. The integer points of E_n can be determined by the elliptic logarithm method [18], [11], if one knows a full set of generators for the group $E_n(\mathbb{Q})$, modulo torsion. Algorithms for finding such generators exist but are not guaranteed to give always an answer [5], [10]. Finally, note that the elliptic curves E_n are closely related with the congruent number problem (see [3] and [13]).

In [6], the integer solutions of (1), in the case where $n = p^a$ with p prime, are determined. When $n = 2^a p^b$ where p is an odd prime and $a > 0$, $b > 0$, an algorithm is given in [7] for the calculation of the integer solutions of (1) which does not use the structure of the group $E_n(\mathbb{Q})$. The aim of this paper is to generalize the approach of [7] and develop an algorithm for the determination of the integer solutions of (1), for any n. We use the "multiplication by 2" on E_n and we reduce the problem of the determination of integer solutions of (1) to the solution of a finite number of unit equations over some bicyclic biquadratic fields.

Let a be an integer and p be a prime. We denote by $\mathrm{ord}_p(a)$ the greatest integer $r \geq 0$ such that p^r divides a. Let Σ_n be the set consisting of the following positive integers:

1. The integers of the form $(a-b)^2/4$, where a, b are positive integers with $ab = n$.

2. The integers of the form $(a+b)/2$, where a, b are positive integers with $ab = n^2$.

3. The integers of the form $d(a \pm b)^2/4$, where d is a positive divisor of n such that $\mathrm{ord}_p(d) = \mathrm{ord}_p(n)$ for every odd prime divisor p of d with odd exponent and a, b are positive integers with $ab = n/d$.

Let D be the set of positive divisors of n, $d = d_1\delta^2$, where $d_1, \delta \in \mathbb{Z}$ and d_1 is square-free, such that for every prime divisor p of d_1 we have $\mathrm{ord}_p(d) = \mathrm{ord}_p(n)$. For every element $d = d_1\delta^2$ of D we consider the negative integers x with $|x| < n$, $x = -daA^2$, where $a, A \in \mathbb{Z}$, $a|d_1$, for every odd prime divisor q of n/d we have $(-(d_1/a)/q) = 1$ and $a((n/d)^2 - (x/d)^2)/d_1$ is a square. We denote the set of all these integers by Λ_n.

Let K be a number field of degree k. For $a \in K$ we denote by $\Delta(a)$ the discriminant of the elements $1, a, \ldots, a^{k-1}$. Furthermore, we denote by N_K, Tr_K and O_K the norm, the trace and the ring of integers of K, respectively.

Theorem 1 *Let $(x, y) \in \mathbb{Z}^2$ be a nontrivial integer solution of (1) with $x \notin \Sigma_n \cup \Lambda_n$. Then $x > n$ and there is a divisor d of n with $d = wuvA^2$, where $A \in \mathbb{Z}$ and w, u, v are pairwise relatively prime, square free, positive integers such that the field $K = \mathbb{Q}(\sqrt{uv}, \sqrt{2^e wv})$, where $e \in \{0, 1\}$, has degree 4 and contains a primitive element $r \in O_K$ such that*

$$x = \frac{d(r^2 + m^2)^2}{4r(r^2 - m^2)},$$

where $m = n/d$. We have $N_K(r) = m^4$, $N_K(r \pm m) = 4m^4$ and $Tr_K(r) = 4x/d$. If $\sqrt{2} \in K$, then $(r \pm m)/\sqrt{2} \in O_K$ and $N_K((r \pm m)/\sqrt{2}) = m^4$. The numbers w, u, and v satisfy the following equalities:

1. $\mathrm{ord}_p(d) = \mathrm{ord}_p(n)$, *for every odd prime divisor p of wuv.*
2. $(wu2^e/p) = 1$ *and* $(wv2^e/p) = 1$, *for every odd prime divisor p of m.*
3. $(mu2^e/p) = 1$ *and* $(-mv2^e/p) = 1$, *for every odd prime divisor p of w.*
4. $(-wm/p) = 1$ *and* $(-mv2^{e+1}/p) = 1$, *for every odd prime divisor p of u.*
5. $(wm/p) = 1$ *and* $(mu2^{e+1}/p) = 1$, *for every odd prime divisor p of v.*

($(\cdot/p)$ denotes the usual Legendre symbol.) Furthermore, there is a primitive element $\eta \in O_K$ satisfying $\Delta(\eta) = 2^{14}n^6$, $Tr_K(\eta) = 0$ and

$$(\eta^4 - 6x\eta^2 - 3x^2 + 4n^2)^2 - 64\eta^2(x^3 - n^2x) = 0.$$

Moreover, if $d = n$, then $x = nwA^2$, where (A, B) is an integer solution to the equation $w^2X^4 - uvY^2 = 1$.

Let R and S be maximal sets of pairwise non associate $z \in O_K$ with $N_K(z) = m^4$ and $N_K(z) = 4m^4$, respectively. By [2, Theorem 5, page 90], R and S are finite. Since $N_K(r) = m^4$ and $N_K(r \pm m) = 4m^4$, there are $a \in R$, $b \in S$ and units $u, v \in K$ such that $r = au$ and $r - m = bv$. It follows that u, v is a solution of the unit equation

$$aU - bV = m.$$

If $\sqrt{2} \in K$, then there are $a, b \in R$ and units $u, v \in K$ such that $r = au$ and $(r - m)/\sqrt{2} = bv$. Thus, u, v is a solution of the unit equation

$$aU - b\sqrt{2}V = m.$$

Note that the sets R and S can be easily determined using the computational algebraic systems KANT/KASH [21] and MAGMA [22]. An efficient method for the solution of the unit equation is the Wildanger's algorithm [19]. It is also implemented in the systems KANT/KASH and MAGMA and so provides easily the solutions of the above equations.

On the other hand, [12] implies that there exists an effectively determined finite set $T \subset O_K$ such that for every $v \in O_K$ with $\Delta(v) = 2^{16}n^6$ there are $w \in T$ and $z \in \mathbb{Z}$ with $v = w + z$. Thus, for the algebraic integer η of Theorem 1 there are $b \in T$ and $k \in \mathbb{Z}$ such that $\eta = b + k$. Since $Tr_K(\eta) = 0$, we have $Tr_K(b) = -4k$. Hence, η is among the primitive elements $b+k$ with $b \in T$, $k \in \mathbb{Z}$ and $Tr_K(b) = -4k$. Note that the solvability of the discriminant form equation is equivalent to the solvability of the index form equation $I_K(\eta) = 2^7n^3/\sqrt{D_K}$. A method for the solution of the index form equation is implemented in the systems KANT/KASH and MAGMA.

Finally, the equation $b^2x^4 - dy^2 = 1$ can be solved using the results of [4] and [1].

Taking in account the efficiency of the implemented algorithms, we combine the above approaches and we develop an algorithm for the solution of the equation (1). Firstly, for every divisor d of n, using the relations (1)-(5) of Theorem 1, we obtain the possible cases for the field K and checking the solvability of the index form equation $I_K(\eta) = 2^7n^3/\sqrt{D_K}$ we reduce further their number. Next, for every such field K, we determine maximal sets R and S of pairwise non associate $z \in O_K$ with $N_K(z) = m^4$ and $N_K(z) = 4m^4$, respectively, and solving a family of unit equations $aU - bV = m$, where $(a,b) \in R \times S$, we find the solutions of (1) (if $\sqrt{2} \in K$, then we solve unit equations $aU - b\sqrt{2}V = m$, where $a, b \in R$). In case where $d = n$ we can alternatively solve some equations of the form $b^2x^4 - dy^2 = 1$.

The paper is organized as follows. In Section 2 we give some auxiliary results useful for the proof of Theorem 1. Section 3 is devoted in the proof of Theorem 1. For the convenience of the reader, some results on the index form equations and the equation $b^2x^4 - dy^2 = 1$ are presented in Sections 4 and 5, respectively. In Section 6 we specialize our results in case of integers n with only two odd prime divisors and we develop two algorithms for the solution of the equation (1). Finally, in Section 7, we give an algorithm for the case where n has more than two prime factors.

2 Auxiliary Lemmata

In this section we give some lemmata which are useful for the proof of Theorem 1.

Lemma 1 *Let $(x, y) \in \mathbb{Z}^2$ be an integer solution of (1) with $y \neq 0$ and $d = \gcd(x, n)$. If $d = d_1\delta^2$, where d_1, δ are positive integers and d_1 is square-free, then for every prime divisor p of d_1 we have $\operatorname{ord}_p(d) = \operatorname{ord}_p(n)$.*

Proof. Since $d = \gcd(x, n)$, we have $x = dz$ and $n = dm$, where z and m are positive integers with $\gcd(z, m) = 1$. Let p be a prime divisor of d_1 with $\operatorname{ord}_p(d) < \operatorname{ord}_p(n)$. Then $p|m$ and so $p \not| z$. On the other hand, the equality

$$(y/d_1\delta^3)^2 = d_1z(z^2 - m^2)$$

implies that $p|m^2-z^2$ and so $p|z$ which is a contradiction. Thus, for every prime divisor p of d_1 we have $\mathrm{ord}_p(d)=\mathrm{ord}_p(n)$.

Lemma 2 *Let $(x,y)\in\mathbb{Z}^2$ be an integer solution of (1) with $x<0$ and $\gcd(x,n)=d$. If $d=d_1\delta^2$, where d_1, δ are positive integers and d_1 is square-free, then $(n/d,d_1)=1$, $x=-daA^2$, where a, A are positive integers with $a|d_1$, such that for every odd prime divisor q of n/d we have $(-(d_1/a)/q)=1$. Furthermore, $|x|\leq n$ and $a((n/d)^2-(x/d)^2)/d_1$ is a square.*

Proof. We set $x=-z$, where z is a positive integer. Let $\gcd(z,n)=d$ and $d=d_1\delta^2$, where d_1, δ are positive integers and d_1 is square-free. We have $z=dz_1$ and $n=dm$, where m and z_1 are positive integers with $\gcd(z_1,m)=1$. Since $\gcd(z_1,m^2-z_1^2)=1$, the equality

$$(y/d\delta)^2=d_1z_1(m^2-z_1^2)$$

implies that there are positive integers a, b, A, B with $d_1=ab$ such that

$$z_1=aA^2,\quad m^2-z_1^2=bB^2.$$

Thus $m^2=z_1^2+bB^2$ and $\gcd(z_1,B)=1$. By Lemma 1, for every prime divisor p of d_1, we have $\mathrm{ord}_p(d)=\mathrm{ord}_p(n)$ and so $\gcd(d_1,m)=1$, whence $\gcd(b,m)=1$. It follows that for every prime odd divisor q of m we have $(-b/q)=1$.

Lemma 3 *Let $(x,y)\in\mathbb{Z}^2$ be an integer solution of (1) such that $x>n$. Put $\gcd(x,n)=d$, $m=n/d$ and $d=d_1\delta^2$, where δ, d_1 are positive integers and d_1 is square free. Then*

$$x=dwA^2,\quad x+n=d2^euB^2,\quad x-n=d2^evC^2,$$

where w, u, v, A, B and C are positive integers with $wuv=d_1$. We have $e=1$ if m and x/d have the same parity and $e=0$ otherwise. Furthermore, the following equalities are satisfied:

1. *For every odd prime divisor p of m we have*

$$(wu2^e/p)=1,\quad (wv2^e/p)=1.$$

2. *For every odd prime divisor p of w we have*

$$(mu2^e/p)=1,\quad (-mv2^e/p)=1.$$

3. *For every odd prime divisor p of u we have*

$$(-wm/p)=1,\quad (-mv2^{e+1}/p)=1.$$

4. *For every odd prime divisor p of v we have*

$$(wm/p)=1,\quad (mu2^{e+1}/p)=1.$$

Proof. Putting $x = dz$, where z is an integer, we obtain

$$(y/d\delta^3)^2 = d_1 z(z^2 - m^2).$$

Since $\gcd(z, m) = 1$, we have $\gcd(z, z \pm m) = 1$ and $\gcd(z + m, z - m) = 2^e$, where $e = 1$, if z and m have the same parity and $e = 0$, otherwise. It follows that

$$z = wA^2, \quad z + m = 2^e uB^2, \quad z - m = 2^e vC^2,$$

where w, u, v, A, B and C are positive integers with $wuv = d_1$. Finally, combining the above equalities, we obtain

$$wA^2 + m = 2^e uB^2, \quad wA^2 - m = 2^e vC^2, \quad 2m = 2^e uB^2 - 2^e vC^2,$$

whence we deduce the equalities (1)-(4).

The following lemma is a version of Proposition 20 of [13]. We denote by $\bar{\mathbb{Q}}$ an algebraic closure of $\mathbb{Q}$.

Lemma 4 *Let E be the elliptic curve $Y^2 = (X - e_1)(X - e_2)(X - e_3)$ with $e_1, e_2, e_3 \in \mathbb{Q}$. If $(x, y) \in \mathbb{Q}^2$ and $(s, t) \in \bar{\mathbb{Q}}^2$ are two points on E such that $(x, y) = [2](s, t)$, then $\mathbb{Q}(s, t) = \mathbb{Q}(\sqrt{x - e_i}, \sqrt{x - e_j})$, for every pair $i, j \in \{1, 2, 3\}$ with $i \neq j$.*

Proof. Consider the change of variables $Z = X - x$. We set $w_i = e_i - x$ $(i = 1, 2, 3)$ and $v = s - x$. Then $P = (0, y)$ and $Q = (v, t)$ are two points on the elliptic curve E_1 defined by $Y^2 = (Z - w_1)(Z - w_2)(Z - w_3)$ such that $P = [2]Q$. The tangent line to E_1 at Q passes through $-P = (0, -y)$ and hence its equation is $Y = mZ - y$. If $v = 0$, then $t = -y$ and we have $m = 0$. Suppose that $v \neq 0$. Then v is the double root of the cubic $(mZ - y)^2 = (Z - w_1)(Z - w_2)(Z - w_3)$. Since the third root of the cubic is zero, we have $v = (w_1 + w_2 + w_3 + m^2)/2$. Also, we have $t = mv - y$. Thus $v, t \in \mathbb{Q}(m)$. Conversely, since $m = (t + y)/v$, we have $m \in \mathbb{Q}(v, t)$. Therefore $\mathbb{Q}(m) = \mathbb{Q}(v, t)$.

Next, note that the points $Q_i = Q \bigoplus (w_i, 0)$ $(i = 1, 2, 3)$ of E_1 satisfy $[2]Q_i = P$ and Q, Q_1, Q_2 and Q_3 are all the points of E_1 having this property ($\bigoplus$ denotes the addition on E). Let $Q_i = (v_i, t_i)$ $(i = 1, 2, 3)$. The tangent line to E_1 at Q_i has equation $Y = m_i Z - y$ $(i = 1, 2, 3)$. We have, as previously, $\mathbb{Q}(m_i) = \mathbb{Q}(v_i, t_i)$. The formulas of addition on E_1 imply that $v_i, t_i \in \mathbb{Q}(v, t)$ and so $m_i \in \mathbb{Q}(m)$. Hence $\mathbb{Q}(m_i) \subseteq \mathbb{Q}(m)$. Changing the role of m and m_i we have $\mathbb{Q}(m) \subseteq \mathbb{Q}(m_i)$. Therefore $\mathbb{Q}(m_i) = \mathbb{Q}(m)$ $(i = 1, 2, 3)$.

Put $m = m_0$. For every $i = 0, 1, 2, 3$ the equation

$$(m_i Z - y)^2 = Z^3 + aZ^2 + bZ + c,$$

where

$$a = -w_1 - w_2 - w_3, \quad b = w_1 w_2 + w_1 w_3 + w_2 w_3, \quad c = -w_1 w_2 w_3 = y^2$$

has a double root. Simplifying and factor out Z, we deduce that the equation

$$Z^2 + (a - m_i^2)Z + (b + 2m_i y) = 0$$

has a double root. This is equivalent to

$$(a - m_i^2)^2 - 4(b + 2m_i y) = 0 \quad (i = 0, 1, 2, 3).$$

Next, we introduce f_i satisfying $f_i^2 = -w_i$ and $f_1 f_2 f_3 = y$. There are two possible chooses for f_i, unless $w_i = 0$. If all the w_i are nonzero, then the condition $f_1 f_2 f_3 = y$ implies that the signs of f_1 and f_2 can be arbitrary and the sign of f_3 is chosen so that y and $f_1 f_2 f_3$ are the same square root of $-w_1 w_2 w_3$. If, say, $w_3 = 0$, then either choose can be made for the sign of f_1, f_2, and $f_3 = 0$. Suppose, without loss of generality that w_1 and w_2 are nonzero. So, once we fix f_1, f_2, f_3, we have the following four choices: f_1, f_2, f_3; $f_1, -f_2, -f_3$; $-f_1, f_2, -f_3$; $-f_1, -f_2, f_3$.

Setting $s_1 = f_1 + f_2 + f_3$, $s_2 = f_1 f_2 + f_1 f_3 + f_2 f_3$ and $s_3 = f_1 f_2 f_3$, we get

$$a = s_1^2 - 2s_2, \quad b = s_2^2 - 2s_1 s_3, \quad y = s_3.$$

Thus, we have

$$\begin{aligned}(a - T^2)^2 - 4(b + 2Ty) &= (T^2 - s_1^2 + 2s_2)^2 - 4(s_2^2 - 2s_1 s_3 + 2Ts_3) \\ &= (T^2 - s_1^2)^2 + 4s_2(T^2 - s_1^2) - 8s_3(T - s_1).\end{aligned}$$

It follows that s_1 is a root of the above polynomial. Since we could have made three other choices for the signs of the f_i, the other roots must correspond to these choices. Hence, the roots of this polynomial are

$$M_1 = f_1 + f_2 + f_3, \quad M_2 = f_1 - f_2 - f_3, \quad M_3 = -f_1 + f_2 - f_3, \quad M_4 = -f_1 - f_2 + f_3$$

and of course we have $\{m, m_1, m_2, m_3\} = \{M_1, M_2, M_3, M_4\}$. We deduce that $f_1 = (M_1 + M_2)/2$, $f_2 = (M_1 + M_3)/2$ and $f_3 = (M_1 + M_4)/2$, whence $\mathbb{Q}(f_1, f_2) \subseteq \mathbb{Q}(m)$. Conversely, it is obvious that $\mathbb{Q}(m) \subseteq \mathbb{Q}(f_1, f_2)$. Hence $\mathbb{Q}(m) = \mathbb{Q}(f_1, f_2)$. The result follows.

3 Proof of Theorem 1

By Lemma 1, we have $x > 0$. We consider $(s, t) \in \bar{\mathbb{Q}}^2$ such that $[2](s, t) = (x, y)$. Let $K = \mathbb{Q}(s, t)$. Suppose that $d = \gcd(x, n)$ is not a perfect square. There are relatively prime integers z and m such that $x = dz$ and $n = dm$. Set $d = d_1 \delta^2$, where $d_1, \delta \in \mathbb{Z}$ and d_1 is square free. By Lemmata 1 and 3, for every odd prime divisor p of d with odd exponent, we have $\mathrm{ord}_p(d) = \mathrm{ord}_p(n)$ and

$$x = dwA^2, \quad x + n = d2^e uB^2, \quad x - n = d2^e vC^2,$$

where w, u, v, A, B and C are positive integers with $wuv = d_1$. Further, $e = 1$ if m and z have the same parity and $e = 0$ otherwise. Moreover, the following equalities are satisfied:

1. For every odd prime divisor p of m we have

$$(wu2^e/p) = 1, \quad (wv2^e/p) = 1.$$

2. For every odd prime divisor p of w we have

$$(mu2^e/p) = 1, \quad (-mv2^e/p) = 1.$$

3. For every odd prime divisor p of u we have

$$(-wm/p) = 1, \quad (-mv2^{e+1}/p) = 1.$$

4. For every odd prime divisor p of v we have

$$(wm/p) = 1, \quad (mu2^{e+1}/p) = 1.$$

Then Lemma 4 yields

$$K = \mathbb{Q}(\sqrt{uv}, \sqrt{2^e wv}) = \mathbb{Q}(\sqrt{uv}, \sqrt{2^e wu}) = \mathbb{Q}(\sqrt{2^e wu}, \sqrt{2^e wv}).$$

Suppose first that $K = \mathbb{Q}$. Then there are integers U, V and W such that $x = U^2$, $x + n = V^2$ and $x - n = W^2$. It follows that $x = (\alpha - \beta)^2/4$, where α and β are positive integers with $\alpha > \beta$ and $\alpha\beta = n$.

Next, we suppose that K is a quadratic field. We have the following cases:
1. $uv = 1$. Then $u = v = 1$. It follows that $x = U^2$, where U is positive integer, and equation (1) implies that there is a positive integer V such that $V^2 = U^4 - n^2$. Hence we have $x = (\alpha + \beta)/2$, where α and β are positive integers with $\alpha\beta = n^2$.
2. $2^e wv = 1$. Then $e = 0$, $w = v = 1$. We deduce that $A^2 - m = C^2$, whence we get $A = (\alpha + \beta)/2$, where α and β are positive integers with $\alpha\beta = m$. Thus $x = d(\alpha + \beta)^2/4$.
3. $uv \neq 1$ and $2^e wv \neq 1$. If d_1 is odd, then $e = 0$, $u = w = 1$. It follows that $B^2 - A^2 = m$, whence $A = (\alpha - \beta)/2$, where α and β are positive integers with $\alpha > \beta$ and $\alpha\beta = m$ and so $x = d(\alpha - \beta)^2/4$. If d_1 is even, then exactly one of w, u, v is even. Suppose that u is even. Then $e = 1$, $u = 2$ and $w = 1$. So, we have $(2B)^2 - A^2 = m$ and we deduce that x is as in the previous case. If v is even, then we obtain $A^2 - m = (2C)^2$ and we get $x = d(\alpha + \beta)^2/4$, where α and β are positive integers with $\alpha\beta = m$. If w is even, then $e = 1$, $w = 2$ and $v = 1$. It follows that $\gcd(z, m)$ is even which is a contradiction.

Finally, we suppose that $[K : \mathbb{Q}] = 4$. We have $[2](s,t) = (\phi(s,t), \psi(s,t))$, where

$$\phi(s,t) = -2s + \left(\frac{3s^2 - n^2}{2t}\right)^2, \quad \psi(s,t) = -t + \left(\frac{3s^2 - n^2}{2t}\right)(s - \phi(s,t)).$$

Putting $\eta = (3s^2 - n^2)/2t$, we get

$$x = -2s + \eta^2, \quad y = -\frac{3s^2 - n^2}{2\eta} + \eta(3s - \eta^2). \tag{2}$$

We eliminate s between these two equalities and we obtain that η satisfies the equation

$$h(U) = U^4 - 6xU^2 - 8yU - 3x^2 + 4n^2 = 0. \tag{3}$$

From the equality $s = (\eta^2 - x)/2$ we obtain $K \subseteq \mathbb{Q}(\eta)$ and since $[\mathbb{Q}(\eta) : \mathbb{Q}] \leq 4$, we have $K = \mathbb{Q}(\eta)$. Thus, $h(U)$ is the minimal polynomial of η. The discriminant of $h(T)$ is equal to $2^{14}n^6$ and so $\Delta(\eta) = 2^{14}n^6$. Eliminating y between $y^2 = x^3 - n^2x$ and (3), we obtain

$$(\eta^4 - 6x\eta^2 - 3x^2 + 4n^2)^2 = 64\eta^2(x^3 - n^2x).$$

Furthermore, we remark that $Tr(\eta) = 0$.

Next, substituting the values of x and y given by (6) in (7) and replacing η^2 by $2s + x$, we obtain that s is a root of the equation

$$f(T) = T^4 - 4xT^3 + 2n^2T^2 + 4n^2xT + n^4 = 0. \tag{4}$$

We shall prove that $K = \mathbb{Q}(s)$ and hence $f(T)$ is the irreducible polynomial of s. Since $s \neq 0$ we have

$$0 = \frac{f(s)}{s^2} = (s - \frac{n^2}{s})^2 - 4x(s - \frac{n^2}{s}) + 4n^2$$

and so, we get

$$s - \frac{n^2}{s} = 2(x \pm \sqrt{x^2 - n^2}),$$

whence

$$s^2 - 2(x \pm \sqrt{x^2 - n^2})s - n^2 = 0.$$

Therefore, we obtain

$$s = x \pm \sqrt{x^2 - n^2} \pm \sqrt{2x^2 \pm 2x\sqrt{x^2 - n^2}}.$$

We remark that $[\mathbb{Q}(s) : \mathbb{Q}] < 4$ if and only if $\sqrt{x^2 - n^2}$ is the square of an integer or $2x^2 \pm 2x\sqrt{x^2 - n^2}$ is the square of an element of $\mathbb{Z}[\sqrt{x^2 - n^2}]$. If $x^2 - n^2 = a^2$, where $a \in \mathbb{Z}$, then $a^2 = uvd^2 2^{2e} B^2 C^2$, whence $uv = 1$ and so, $[K : \mathbb{Q}] < 4$ which is a contradiction. Suppose that $2x^2 \pm 2x\sqrt{x^2 - n^2} = (a + b\sqrt{x^2 - n^2})^2$, where $a, b \in \mathbb{Z}$. It follows that $2x^2 = a^2 + b^2(x^2 - n^2)$ and $x = |a||b|$. Eliminating x, we deduce $a^2(b^2 - 1)^2 = n^2b^2$, whence $|a|(b^2 - 1) = nb$. Multiplying the two members of the last equality by $|a|$, we get $a^2(b^2 - 1) = nx$. Replacing ab by x, we obtain $a^2 = x^2 - nx = y^2/(x + n)$ and hence $x + n$ is a perfect square. Since $K = \mathbb{Q}(\sqrt{x}, \sqrt{x + n})$, we deduce that $[K : \mathbb{Q}] \leq 2$ which is a contradiction. Hence $K = \mathbb{Q}(s)$ and $f(T)$ is the irreducible polynomial of s.

Since $r = s/d$ is a root of the equation

$$f_1(T) = T^4 - 4zT^3 + 2m^2T^2 + 4m^2zT + m^4 = 0,$$

we get $N_K(r) = m^4$. Further, $r \pm m$ are roots of the irreducible polynomial

$$f_2(T) = f_1(T \mp m) = T^4 + 4(\mp m - z)T^3 + 4m(2m \pm 3z)T^2 + 8m^2(\mp m - z)T + 4m^4,$$

and so, we obtain $N_K(r \pm m) = 4m^4$. If $\sqrt{2} \in K$, then from the equation $f_2(r \pm m) = 0$ we deduce that $\sqrt{2}$ divides $r \pm m$. It follows that $(r \pm m)/\sqrt{2}$ is an algebraic integer with $N_K((r \pm m)/\sqrt{2}) = m^4$. Further, from (8) we have

$$x = \frac{(s^2 + n^2)^2}{4s(s^2 - n^2)} = \frac{d(r^2 + m^2)^2}{4r(r^2 - m^2)}.$$

Finally, suppose that $d = n$. Then $x = nwA^2$ and $x^2 - n^2 = n^2uv(2^eBC)^2$. It follows that $w^2A^4 - uv(2^eBC)^2 = 1$.

4 Index Form Equations

Let a, b be two distinct square-free positive integers > 1. If $l = \gcd(a, b)$, then $a = la_1$ and $b = lb_1$, where a_1, b_1 pairwise prime positive integers. We consider the field $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$. We denote by D_K the discriminant of K and by $I_K(x_2, x_3, x_4)$ the index form over K. Following [9] and [20], we list an integral basis, the discriminant and the index form for K. We have the following cases:

Case 1. $a \equiv b \equiv a_1 \equiv b_1 \equiv 1 \pmod 4$. Integral basis: 1, $(1+\sqrt{a})/2$, $(1+\sqrt{b})/2$, $(1+\sqrt{a}+\sqrt{b}+\sqrt{a_1b_1})/4$. Discriminant: $D_K = (la_1b_1)^2$. Index form:

$$I_K(x_2, x_3, x_3) = (l(x_2 + x_4/2)^2 - b_1x_4^2/4)(l(x_3 + x_4/2)^2 - a_1x_4^2/4)$$
$$\times((b_1(x_3 + x_4/2)^2 - a_1(x_2 + x_4/2)^2).$$

Case 2. $a \equiv b \equiv 1 \pmod 4$, $a_1 \equiv b_1 \equiv 3 \pmod 4$. Integral basis: 1, $(1+\sqrt{a})/2$, $(1+\sqrt{b})/2$, $(1-\sqrt{a}+\sqrt{b}+\sqrt{a_1b_1})/4$. Discriminant: $D_K = (la_1b_1)^2$. Index form:

$$I_K(x_2, x_3, x_3) = (l(x_2 - x_4/2)^2 - b_1x_4^2/4)(l(x_3 + x_4/2)^2 - a_1x_4^2/4)$$
$$\times(b_1(x_3 + x_4/2)^2 - a_1(x_2 - x_4/2)^2).$$

Case 3. $a \equiv 1 \pmod 4$, $b \equiv 2 \pmod 4$. Integral basis: 1, $(1+\sqrt{a})/2$, $\sqrt{b}$, $(\sqrt{b}+\sqrt{a_1b_1})/2$. Discriminant: $D_K = (4la_1b_1)^2$. Index form:

$$I_K(x_2, x_3, x_3) = (lx_2^2 - b_1x_4^2)(l(x_3 + x_4/2)^2 - a_1x_4^2/4)(4b_1(x_3 + x_4/2)^2 - a_1x_2^2).$$

Case 4. $a \equiv 2 \pmod 4$, $b \equiv 3 \pmod 4$. Integral basis: 1, $\sqrt{a}$, $\sqrt{b}$, $(\sqrt{a}+\sqrt{a_1b_1})/2$. Discriminant: $D_K = (8la_1b_1)^2$. Index form:

$$I_K(x_2, x_3, x_3) = ((2x_2+x_4)^2/2 - b_1x_4^2/2)(2lx_3^2 - a_1x_4^2/2)(2b_1x_3^2 - a_1(2x_2+x_4)^2/2)$$

Case 5. $a \equiv b \equiv 3 \pmod 4$. Integral basis: 1, $\sqrt{a}$, $(\sqrt{a}+\sqrt{b})/2$, $(1+\sqrt{a_1b_1})/2$. Discriminant: $D_K = (4la_1b_1)^2$. Index form:

$$I_K(x_2, x_3, x_3) = (l(2x_2 + x_3)^2 - b_1x_4^2)(lx_3^2 - a_1x_4^2)(b_1x_3^2/4 - a_1(x_2 + x_3/2)^2).$$

Consider now the index form equation

$$I_K(x_2, x_3, x_3) = \pm\mu,$$

where μ is a positive integer.

Proposition 1 *If the above index form equation has a solution, then there are integers F_1, F_2, F_3 with $F_1F_2F_3 = \mu$ such that, according to cases 1-5, we have:*

Case 1: The system $lx^2 - b_1y^2 = 4F_1$, $lz^2 - a_1y^2 = 4F_2$, $b_1z^2 - a_1x^2 = 4F_3$ has an integer solution and $-F_1a_1 + F_2b_1 = F_3l$.

Case 2: The system $lx^2 - b_1y^2 = 4F_1$, $lz^2 - a_1y^2 = 4F_2$, $n_1z^2 - a_1x^2 = 4F_3$ has an integer solution and $-F_1a_1 + F_2b_1 = F_3l$.

Case 3: The system $lx^2 - b_1y^2 = F_1$, $lz^2 - a_1y^2 = 4F_2$, $b_1z^2 - a_1x^2 = F_3$ has an integer solution and $F_1a_14F_2b_1 = F_3l$.

Case 4: The system $x^2 - b_1y^2 = 2F_1$, $2lz^2 - a_1/2y^2 = F_2$, $2b_1z^2 - a_1/2x^2 = F_3$ has an integer solution and $-F_1a_1 + F_2b_1 = F_3l$.

Case 5: The system $lx^2 - b_1y^2 = F_1$, $lz^2 - a_1y^2 = F_2$, $b_1z^2 - a_1x^2 = 4F_3$ has an integer solution and $-F_1a_1 + F_2b_1 = 4F_3l$.

Proof. See [9, pages 103-104].

Note that we can check the solvability of Pell equations in Proposition 6 using the computational system MAPLE. Furthermore, in [15] elementary necessary and sufficient conditions for the solvability of the equation $x^2 - Dy^2 = a$, where $D, a \in \mathbb{Z}$ and $D > 0$, are given.

5 The equation $b^2x^4 - dy^2 = 1$

In this section, we give some results on the integer solutions of the above equation useful for the determination of the integer points of E_n. We call trivial solutions of this equation the solutions given by $x^2 = 1$.

Theorem 2 *Let $a+b\sqrt{d}$ be the fundamental solution of the equation $x^2-dy^2 = 1$. Then the only possible non trivial integer solutions of the equation $x^4-dy^2 = 1$ are given by $x^2 = a$ and $x^2 = 2a^2 - 1$; both solutions occur in only one case, $d = 1785$.*

Proof. See [4].

Theorem 3 *If d is a prime number or the double of a prime number, then the equation $x^4 - dy^2 = 1$ has only the trivial solutions, unless $d = 5, 29, 6$ in which cases there is also the solutions $(x, y) = (\pm 3, \pm 4)$, $(\pm 99, \pm 1820)$ and $(\pm 7, \pm 20)$, respectively.*

Proof. See [17, Th. 2.1].

Theorem 4 *If p is a prime number, then the equation $4x^4 - py^2 = 1$ has only the trivial solutions, unless $p = 3, 7$ in which cases there is also the solutions $(x, y) = (\pm 1, \pm 1)$ and $(\pm 2, \pm 3)$, respectively.*

Proof. See [17, Th. 2.2].

Let now b and d be two square-free relatively prime integers > 1. We denote by $\epsilon = T + U\sqrt{d}$ the fundamental solution to the Pell equation $x^2 - dy^2 = 1$, and, for $k \geq 1$, we put $T_k + U_k\sqrt{d} = \epsilon^k$. The divisibility index $\alpha(b)$ of b in the sequence T_k is the smallest positive integer k for which $b|T_k$. If, for all k, b do not divides T_k, then we set $\alpha(b) = \infty$.

Theorem 5 *There is at most one index k for which $T_k = bx^2$ for some $x \in \mathbb{Z}$, and consequently, the equation $b^2x^4 - dy^2 = 1$ has at most one solution in positive integers x, y. Moreover, if such solution exists, then $k = \alpha(b)$.*

Proof. See [1, Theorem 1.2].

A useful corollary is the following:

Corollary 1 *Let $b = 2^r3^s5^t7^u11^v$ for some integers $r, s, t, u, v \in \{0, 1\}$, not all zero. Then any solution of $T_k = bx^2$ with $x \in \mathbb{Z}$ implies $k = 1$ unless*

1. *$b = 7$, in which case $k = 1$ or $k = 2$ (but not both),*

2. *$b = 11$ and $d = 2$, in which case $T_3 = 11 \cdot 3^2$,*

3. *$b = 55$ and $d = 1139$, in which case $T_3 = 55 \cdot 423^2$.*

Proof. See [1, Corollary 1.3].

The following Proposition is stated without proof in [1, page 3486]. Professor Gary Walsh kindly communicated to us its proof.

Proposition 2 *Suppose that p is a prime. If $p = 2$, then $\alpha(p) = 1$ or ∞ and if $p > 2$, then either $\alpha(p)|(p - (d/p))/2$ or $\alpha(p) = \infty$.*

Proof. If $p = 2$, then it is easily seen that $\alpha(p) = 1$ or ∞. Suppose that $p > 2$. If p divides d or U, then $\alpha(p) = \infty$. Suppose now that p does not divides d or U. We have $U_n = u_n U$ and $T_n = t_n/2$, where $u_n = (\epsilon^n - \epsilon^{-n})/(\epsilon - \epsilon^{-1})$ and $t_n = \epsilon^n + \epsilon^{-n}$ are the Lucas sequences associated to polynomial $X^2 - 2T + 1$ with discriminant equal to $4(T^2 - 1) = 4dU^2$. By [16, page 44], we have $u_{2k} = u_k t_k$. Thus, if r is the highest power of 2 dividing $p - (d/p)$, then we have

$$u_{p-(d/p)} = u_{(p-(d/p))/2^r} t_{(p-(d/p))/2} \cdots t_{(p-(d/p))/2^r}.$$

By [16, page 49], $p|u_{p-(d/p)}$. So, either p divides $u_{(p-(d/p))/2^r}$ or p divides one of the $t_{(p-(d/p))/2^i}$. Suppose first that $p|u_{(p-(d/p))/2^r}$. If p divides some t_k, then p divides $u_{2k} = u_k t_k$. By [16, page 51], we have $\gcd(u_{2k}, u_{(p-(d/p))/2^r}) = u_{\gcd(2k,(p-(d/p))/2^r)}$ and so p divides $u_{\gcd(2k,(p-(d/p))/2^r)}$. Since $(p - (d/p))/2^r$ is odd, $\gcd(2k, (p - (d/p))/2^r)$ divides k. By [16, page 47], $u_{\gcd(2k,(p-(d/p))/2^r)}$ divides u_k and hence $p|u_k$. Further, [16, page 51] implies $\gcd(u_k, t_k) = 1$ or 2 and so $p|2$ which is a contradiction. Therefore, p does not divide t_k which implies $\alpha(p) = \infty$. Suppose next that p divides one of the $t_{(p-(d/p))/2^i}$. Since the set of k for which $p|T_k$ is precisely the set $\{t\alpha(p)/\ t \text{ is odd}\}$, we deduce that $\alpha(p)$ is a divisor of $(p - (d/p))/2^i$ which is a divisor of $(p - (d/p))/2$. The result follows.

Proposition 3 *Let b be a square-free integer > 1 and $b = p_1 \cdots p_k$ the prime decomposition of b. If $\alpha(b) < \infty$, then $\alpha(p_i) < \infty$ $(i = 1, \ldots, k)$ and $\alpha(b) = \mathrm{lcm}(\alpha(p_1), \ldots, \alpha(p_k))$. Furthermore, if b is even, then $\alpha(b)$ is odd.*

Proof. The set of k for which $p_i|T_k$ is precisely the set $\{t\alpha(p_i)/\ t \text{ is odd}\}$ $(i = 1, \ldots, k)$. Since $\alpha(b) < \infty$, then $\alpha(p_i) < \infty$ $(i = 1, \ldots, k)$ and there are odd integers $t_1, \ldots, t_k$ such that

$$\alpha(b) = \alpha(p_1)t_1 = \ldots = \alpha(p_k)t_k.$$

It follows that $\mathrm{ord}_2(\alpha(p_1)) = \ldots = \mathrm{ord}_2(\alpha(p_k))$. Therefore, we deduce that $\alpha(b) = \mathrm{lcm}(\alpha(p_1), \ldots, \alpha(p_k))$. If b is even, Proposition 2 implies that $\alpha(2) = 1$ and so the equality $\mathrm{ord}_2(\alpha(p_1)) = \ldots = \mathrm{ord}_2(\alpha(p_k))$ yields that $\alpha(p_i)$ $(i = 1, \ldots, k)$ are odd. Hence $\alpha(b)$ is odd.

6 The Case $n = p^a q^b$

In this section we consider the case $n = p^a q^b$, where p, q are distinct primes and a, b positive integers with a odd.

Proposition 4 *Let $n = p^a q^b$, where p, q are odd primes and a, b positive integers with a odd and b even. Let $(x, y) \in \mathbb{Z}^2$ be an nontrivial integer solution of (1) with $x \notin \Sigma_n \cup \Lambda_n$. Then we have $(x, p) = (9n, 5), (9801n, 29)$ or*

$$x = \frac{p^a q^{2c} (r^2 + q^{(b-2c)2})^2}{4r(r^2 - q^{(b-2c)2})}, \quad 0 \leq 2c < b,$$

where r is a primitive element of $K = \mathbb{Q}(\sqrt{p}, \sqrt{2})$, $r, (r \pm q^{b-2c})/\sqrt{2} \in O_K$ with $N_K(r) = N_K((r \pm q^{b-2c})/\sqrt{2}) = q^{(b-2c)4}$, $q \equiv \pm 1 \pmod 8$ and $(p/q) = 1$.

Proof. We follow the notations of Theorem 1. By Theorem 1, $\mathrm{ord}_p(d) = \mathrm{ord}_p(n)$. Thus $d = p^a q^{2c}$, where $0 \leq 2c \leq b$. Suppose first that $2c < b$. Since $wvu = p$, we have the following cases:

1. $(w, u, v) = (p, 1, 1)$. Thus $K = \mathbb{Q}(\sqrt{2^e p})$ which is a contradiction.

2. $(w, u, v) = (1, p, 1)$. If $e = 0$, then $K = \mathbb{Q}(\sqrt{p})$ which is a contradiction. If follows that $e = 1$ and $K = \mathbb{Q}(\sqrt{p}, \sqrt{2})$. Theorem 1 gives $(2p/q) = (2/q) = (-1/p) = 1$. It follows that $q \equiv \pm 1 \pmod 8$, $p \equiv 1 \pmod 4$, $(p/q) = 1$.

3. $(w, u, v) = (1, 1, p)$. If $e = 0$, then we have again $K = \mathbb{Q}(\sqrt{p})$ which is a contradiction. Thus, $e = 1$ and $K = \mathbb{Q}(\sqrt{p}, \sqrt{2})$. From Theorem 1, we have $(2p/q) = (2/q) = 1$. Hence $q \equiv \pm 1 \pmod 8$ and $(p/q) = 1$.

Suppose next $2c = b$. Then $d = n$ and $wuv = p$. If $w = p$, then $K = \mathbb{Q}(\sqrt{2^e p})$ which is a contradiction. Hence $uv = p$. By Lemma 3, we have $x = nA^2$ and $x^2 - n^2 = n^2 pD^2$, where $A, D \in \mathbb{Z}$. Thus $A^4 - 1 = pD^2$. By Theorem 3, we have either $p = 5$ and $x = 9n$ or $p = 29$ and $x = 9801n$.

We remark that all the conjugates of r give the same x. So it is enough to determine one of them. The solvability of the index form equation $I(\eta) = \pm 2^7 n^3/\sqrt{D_K}$ can be checked using Proposition 1. We use MAPLE for testing the solvability of the associated Pell equations. In case where all equations have solution we try to check the solvability of system. If we cannot easily decide we continue in the next steps of our algorithms.

Thus, we have the following algorithm.

Algorithm 1.
Input: $n = p^a q^b$, where p, q are odd primes and a, b positive integers with a odd and b even.
Output: The integer solutions of (1).

1. Determine the integer solutions (x, y) of (1) with $x \in \Sigma_n$.

2. Determine the integer solutions (x, y) of (1) with $x \in \Lambda_n$.

3. If $p = 5, 29$, then determine respectively the integer solution (x, y) of (1) with $x = 9n, 9801n$.

4. If we have one of the following three cases: $q \not\equiv \pm 1 \pmod 8$, $(p/q) = -1$, the equation $I_K(x_2, x_3, x_4) = \pm 2^7 n^3/\sqrt{D_K}$, where $K = \mathbb{Q}(\sqrt{p}, \sqrt{2})$, has no integer solution, then go to step 8. Otherwise, go to the next step.

5. For every integer c with $0 \leq 2c < b$, determine a maximal set R_p^c of pairwise non associate algebraic integers of $\mathbb{Q}(\sqrt{p}, \sqrt{2})$ with norm $q^{4(b-2c)}$ and a maximal subset S_p^c of R_p^c containing pairwise non conjugate elements of R_p^c.

6. For every integer c with $0 \leq 2c < b$, determine the units u in $\mathbb{Q}(\sqrt{p}, \sqrt{2})$ for which there are $\alpha \in S_p^c$ and $\beta \in R_p^c$ such that $(\alpha u - q^{b-2c})/\beta\sqrt{2}$ is also a unit. Denote by W_c the set of elements αu.

7. For every integer c with $0 \leq 2c < b$ determine the integer solutions (x, y) of (1) with $x > n$ and
$$x = p^a q^{2c} \frac{(q^{2(b-2c)} + r^2)^2}{4r(r^2 - q^{2(b-2c)})},$$
where $r \in W_c$.

8. The integer solutions of (1) are the couples $(0, 0)$, $(\pm n, 0)$ and the couples obtained in steps 1, 2, 3 and 7.

Proposition 5 *Let $n = p^a q^b$, where p, q are odd primes and a, b odd positive integers. Let $(x, y) \in \mathbb{Z}^2$ be a nontrivial integer solution of (1) with $x \notin \Sigma_n \cup \Lambda_n$. Then we have one of the following cases:*

1. $x = n\alpha, n(2\alpha^2 - 1)$, where (α, β) is the fundamental solution of the Pell equation $x^2 - pqy^2 = 1$.

2.
$$x = \frac{p^a q^{2c}(r^2 + q^{(b-2c)2})^2}{4r(r^2 - q^{(b-2c)2})}, \quad 0 \leq 2c < b,$$
where r is a primitive integer element of $K = \mathbb{Q}(\sqrt{p}, \sqrt{2})$ with $N_K(r) = p^{(a-2c)4}$, $q \equiv \pm 1 \pmod 8$, $(p/q) = 1$ and $(r \pm q^{b-2c})/\sqrt{2} \in O_K$ with $N_K((r \pm q^{b-2c})/\sqrt{2}) = q^{(b-2c)4}$.

3.
$$x = \frac{p^{2c} q^b (r^2 + p^{(a-2c)2})^2}{4r(r^2 - p^{(a-2c)2})}, \quad 0 \leq 2c < a,$$
where r is a primitive integer element of $K = \mathbb{Q}(\sqrt{q}, \sqrt{2})$ with $N_K(r) = p^{(a-2c)4}$, $p \equiv \pm 1 \pmod 8$, $(q/p) = 1$ and $(r \pm p^{a-2c})/\sqrt{2} \in O_K$ with $N_K((r \pm p^{a-2c})/\sqrt{2}) = p^{(a-2c)4}$.

4. $x = nT_l$, where $T_l + U_l\sqrt{q} = (T + U\sqrt{q})^l$, $T + U\sqrt{q}$ is the fundamental solution of the Pell equation $x^2 - qy^2 = 1$ and $l|(p - (q/p))/2$. Further, $(p/q) = (-q/p) = 1$.

5. $x = nV_h$, where $V_h + W_h\sqrt{p} = (V + W\sqrt{p})^h$, $V + W\sqrt{p}$ is the fundamental solution of the Pell equation $x^2 - py^2 = 1$ and $h|(q - (p/q))/2$. Further, $(-p/q) = (q/p) = 1$.

Proof. We follow the notations of Theorem 1. Suppose first that $d_1 = p$. By Theorem 1, $\mathrm{ord}_p(d) = \mathrm{ord}_p(n)$. Thus $d = p^a q^{2c}$, where $0 \leq 2c < b$. On the other hand, $wvu = p$ and so we have the following cases:

1. $(w, u, v) = (p, 1, 1)$. Thus $K = \mathbb{Q}(\sqrt{2^e p})$ which is a contradiction.

2. $(w, u, v) = (1, p, 1)$. If $e = 0$, then $K = \mathbb{Q}(\sqrt{p})$ which is a contradiction. If follows that $e = 1$ and $K = \mathbb{Q}(\sqrt{p}, \sqrt{2})$. Theorem 1 gives $(2p/q) = (2/q) = (-q/p) = 1$. It follows that $q \equiv \pm 1 \pmod 8$ and $(p/q) = (-q/p) = 1$.

3. $(w,u,v)=(1,1,p)$. If $e=0$, then we have again $K=\mathbb{Q}(\sqrt{p})$ which is a contradiction. Thus, $e=1$ and $K=\mathbb{Q}(\sqrt{p},\sqrt{2})$. From Theorem 1, we have $(2p/q)=(2/q)=(q/p)=1$. Hence $q\equiv\pm1 \pmod 8$ and $(p/q)=(q/p)=1$.

If $d_1=q$, then we have the same results by changing the role of p and q.

Suppose now that $d_1=pq$. By Theorem 1, we have $d=n$ and $wuv=pq$. Thus, we have the following cases:

1. $w=1$, $uv=pq$. By Lemma 3, we have $x=nA^2$ and $x^2-n^2=n^2pqD^2$, where $A,D\in\mathbb{Z}$. Thus $A^4-1=pqD^2$. By Theorem 2, we have $x=n\alpha, n(2\alpha^2-1)$, where $\alpha+\beta\sqrt{pq}$ is the fundamental solution of the equation $x^2-pqy^2=1$.

2. $w=pq$, $u=v=1$. By Theorem 1, $K=\mathbb{Q}(\sqrt{2^epq})$ which is a contradiction.

3. $w=p$, $uv=q$. Lemma 3 implies that $x=npA^2$ and $x^2-n^2=n^2qD^2$, where $A,D\in\mathbb{Z}$. Further, we have $p^2A^4-qD^2=1$. Let $T+U\sqrt{q}$ be the fundamental solution of the Pell equation $x^2-qy^2=1$ and put $T_k+U_k\sqrt{q}=(T+U\sqrt{q})^k$, $k\geq1$. By Theorem 3 and Proposition 1, we have $pA^2=T_l$ and l divides the quantity $(p-(q/p))/2$. Hence $x=nT_l$. Furthermore, Theorem 1 implies that $(p/q)=(-q/p)=1$.

4. $w=q$, $uv=p$. Let $V+W\sqrt{p}$ be the fundamental solution of the Pell equation $x^2-py^2=1$ and put $V_k+W_k\sqrt{p}=(V+W\sqrt{p})^k$, $k\geq1$. We deduce, as in the previous case, that $x=nV_h$ with h divides $(q-(p/q))/2$ and $(-p/q)=(q/p)=1$.

Proposition 5 leads to the following algorithm.

Algorithm 2.
Input: $n=p^aq^b$, where p, q are odd primes and a, b positive odd integers.
Output: The integer solutions of (1).

1. Determine the integer solutions (x,y) of (1) with $x\in\Sigma_n$.
2. Determine the integer solutions (x,y) of (1) with $x\in\Lambda_n$.
3. Determine the integer solutions (x,y) of (1) with $x=n\gamma, n(2\gamma^2-1)$, where $\gamma+\delta\sqrt{pq}$ is the fundamental solution of the equation $x^2-pqy^2=1$.
4. If $(p/q)=(-q/p)=1$, then determine the set G_q of positive integers T_l such that $T_l+U_l\sqrt{q}=(T+U\sqrt{q})^l$, where $T+U\sqrt{q}$ is the fundamental solution of the Pell equation $x^2-qy^2=1$ and l is a positive integer with $l|(p-(q/p))/2$.
5. Determine the integer solutions (x,y) of (1) with $x=nT_l$ and $T_l\in G_q$.
6. If $(-p/q)=(q/p)=1$, then determine the set G_p of positive integers V_h such that $V_h+W_h\sqrt{p}=(V+W\sqrt{p})^h$, where $V+W\sqrt{p}$ is the fundamental solution of the Pell equation $x^2-py^2=1$ and h is a positive integer with $h|(q-(p/q))/2$.
7. Determine the integer solutions (x,y) of (1) with $x=nV_h$ and $V_h\in G_p$.
8. If $q\equiv\pm1 \pmod 8$, $(p/q)=1$ and $(-q/p)=1$ or $(q/p)=1$ and the equation $I_K(x_2,x_3,x_4)=\pm2^7n^3/\sqrt{D_K}$, where $K=\mathbb{Q}(\sqrt{p},\sqrt{2})$, has an integer solution, then for every integer c with $0\leq 2c<b$, determine a

maximal set R_p^c of pairwise non associate algebraic integers of K with norm $q^{4(b-2c)}$ and a maximal subset S_p^c of R_p^c containing the pairwise non conjugate elements of R_p^c.

9. For every integer c with $0 \leq 2c < b$, determine the units u in $\mathbb{Q}(\sqrt{p}, \sqrt{2})$ for which there are $\alpha \in S_p^c$ and $\beta \in R_p^c$ such that $(\alpha u - q^{b-2c})/\beta\sqrt{2}$ is also a unit. Denote by W_p^c the set of elements αu.

10. For every integer c with $0 \leq 2c < b$ determine the integer solutions (x, y) of (1) with $x > n$ and
$$x = p^a q^{2c} \frac{(q^{2(b-2c)} + r^2)^2}{4r(r^2 - q^{2(b-2c)})},$$
where $r \in W_p^c$.

11. If $p \equiv \pm 1 \pmod 8$, $(q/p) = 1$ and $(-p/q) = 1$ or $(p/q) = 1$ and the equation $I_K(x_2, x_3, x_4) = \pm 2^7 n^3/\sqrt{D_K}$, where $K = \mathbb{Q}(\sqrt{2}, \sqrt{q})$, for every integer c with $0 \leq 2c < b$, determine a maximal set R_q^c of pairwise non associate algebraic integers of K with norm $q^{4(b-2c)}$ and a maximal subset S_q^c of R_q^c containing the pairwise non conjugate elements of R_q^c.

12. For every integer c with $0 \leq 2c < a$, determine the units $u \in \mathbb{Q}(\sqrt{q}, \sqrt{2})$ for which there are $\alpha \in S_q^c$ and $\beta \in R_q^c$ such that $(\alpha u - p^{a-2c})/\beta\sqrt{2}$ is also a unit. Denote by W_q^c the set of elements αu.

13. For every integer c with $0 \leq 2c < a$ determine the integer solutions (x, y) of (1) with $x > n$ and
$$x = p^{2c} q^b \frac{(p^{2(a-2c)} + r^2)^2}{4r(r^2 - p^{2(a-2c)})},$$
where $r \in W_q^c$.

14. The integer solutions of (1) are the couples $(0, 0)$, $(\pm n, 0)$ and the couples obtained in steps 1, 2, 3, 5, 7, 10 and 13.

The following proposition in many cases helps us to eliminate the number of unit equations which have to solve.

Proposition 6 *Let p, q be distinct odd primes and $K = \mathbb{Q}(\sqrt{2}, \sqrt{p})$. Suppose that there are exactly four elements $A_1, A_2, A_3, A_4 \in O_K$, pairwise no associate, with norm q. Then for every $r \in O_K$ with $(r - q^\epsilon)/\sqrt{2} \in O_K$ and $N_K(r) = N_K((r - q^\epsilon)/\sqrt{2}) = q^{4\epsilon}$, a conjugate of r is equal to au, where (u, v) is a solution of unit equation $aU - b\sqrt{2}V = q^\epsilon$ and (a, b) is one of the following couples:*

1. $(A_1^\epsilon A_j^{3\epsilon}, A_1^{3\epsilon} A_j^\epsilon)$, $j = 2, 3, 4$,

2. $(A_1^i A_k^\epsilon A_l^{3\epsilon - i}, A_1^i A_k^{3\epsilon - i} A_l^\epsilon)$, $i = 1, \ldots, \epsilon$, *and* $(k, l) = (2, 3), (3, 2), (2, 4), (4, 2), (3, 4), (4, 3)$,

3. $(A_1^i A_2^{3\epsilon - i} A_3^\epsilon, A_1^\epsilon A_2^\epsilon A_3^{2\epsilon})$, $(A_1^e A_2^e A_3^{2\epsilon}, A_1^i A_2^{3\epsilon - i} A_3^\epsilon)$, $i = \epsilon + 1, \ldots, 2\epsilon - 1$,

4. $(A_1^\epsilon A_2^\epsilon A_3^\epsilon A_4^\epsilon, A_1^\epsilon A_2^\epsilon A_3^e A_4^e)$,

5. $(A_1^iA_2^jA_3^{3\epsilon-i-j}A_4^\epsilon, A_1^iA_2^jA_3^\epsilon A_4^{3\epsilon-i-j})$, $(A_1^iA_3^jA_2^{3\epsilon-i-j}A_4^\epsilon, A_1^iA_3^jA_2^\epsilon A_4^{3\epsilon-i-j})$, $i=1,\dots,\epsilon$, $j=1,\dots,\epsilon$ *and* $2\epsilon > i+j$,

6. $(A_1^iA_2^jA_3^{3e-i-j}A_4^\epsilon, A_1^iA_2^\epsilon A_3^\epsilon A_4^{2\epsilon-i})$, $(A_1^iA_2^\epsilon A_3^jA_4^{3\epsilon-i-j}, A_1^iA_2^{2\epsilon-i}A_3^\epsilon A_4^\epsilon)$, $(A_1^iA_2^jA_3^\epsilon A_4^{3\epsilon-i-j}, A_1^iA_2^\epsilon A_3^{2\epsilon-i}A_4^\epsilon)$, $i=1,\dots,\epsilon-1$, $j=\epsilon+1,\dots,2\epsilon-2$ *and* $2\epsilon-i > j$.

Proof. Since $N_K(A_i) = q$, we deduce that the principal ideals (A_i) $(i = 1,2,3,4)$ of O_K are prime. If $W \in O_K$ with $N_K(W) = q^{4\epsilon}$, then $(W) = (A_1)^i(A_2)^j(A_3)^k(A_4)^l$, where i, j, k, l are no negative integers with $i+j+k+l = 4\epsilon$. It follows that $W = A_1^iA_2^jA_3^kA_4^lU$, where U is a unit of O_K. Hence, the set R of elements $A_1^iA_2^jA_3^kA_4^l$, with $i+j+k+l = 4\epsilon$, is a maximal set of pairwise non associate elements of O_K with norm $q^{4\epsilon}$.

Put $r = au$, $(r-q^\epsilon)/\sqrt{2} = bv$, where $a, b \in R$ and u, v are units of O_K. Then (u,v) is a solution of the unit equation $aU - b\sqrt{2}V = q^\epsilon$. Since $q = A_1A_2A_3A_4U$, where U is a unit of O_K, it follows that A_s, $s \in \{1,2,3,4\}$, divides a if and only if A_s divides b. Further, if A_s^j divides a and A_s^k divides b, then we easily see that either $j \neq k$ and $\min\{j,k\} = \epsilon$ or $j = k \leq \epsilon$. Then, we have the following cases:

1. $a = b = A_s^{4\epsilon}$, $s \in \{1,2,3,4\}$. Then $A_s^{4\epsilon}$ divides q^c which a contradiction.

2. $a = A_s^{i_1}A_t^{j_1}$, $b = A_s^{i_2}A_t^{j_2}$, $s,t \in \{1,2,3,4\}$ and $s \neq t$. If $i_1 = i_2 \leq \epsilon$, then $j_1 = j_2 \geq 3\epsilon$ which is a contradiction. Similarly, if $j_1 = j_2 \leq \epsilon$ we have a contradiction. Thus $i_1 \neq i_2$, $j_1 \neq j_2$ and $\min\{i_1,i_2\} = \min\{j_1,j_2\} = \epsilon$. So, we have $(i_1,j_1,i_2,j_2) = (\epsilon,3\epsilon,3\epsilon,\epsilon),(3\epsilon,\epsilon,\epsilon,3\epsilon)$.

3. $a = A_s^{i_1}A_t^{j_1}A_u^{l_1}$, $b = A_s^{i_2}A_t^{j_2}A_u^{l_2}$, $s,t,u \in \{1,2,3,4\}$ and s,t,u are pairwise distinct. If $i_1 = i_2$ and $j_1 = j_2$, then $l_1 = l_2$ and so $i_1 + j_1 + l_1 \leq 3\epsilon$ which is a contradiction. Thus, $(i_1,j_1) \neq (i_2,j_2)$. Similarly, $(i_1,l_1) \neq (i_2,l_2)$ and $(j_1,l_1) \neq (j_2,l_2)$. Next, suppose that $i_1 = i_2 \leq e$. If $\epsilon = j_1 < j_2$ and $l_1 > l_2 = \epsilon$, then $l_1 = j_2$ and $i_1 + l_1 = 3\epsilon$. Hence $(i_1,j_1,l_1) = (i_1,\epsilon,3\epsilon-i_1)$, $(i_2,j_2,l_2) = (i_1,3\epsilon-i_1,\epsilon)$ and $i_1 = 1,\dots,\epsilon$. Similarly, if $j_1 > j_2 = \epsilon$ and $c = l_1 < l_2$, then $(i_1,j_1,l_1) = (i_1,3\epsilon-i_1,\epsilon)$, $(i_2,j_2,l_2) = (i_1,\epsilon,3\epsilon-i_1)$ and $i_1 = 1,\dots,\epsilon$. Now suppose that $i_1 \neq i_2$, $j_1 \neq j_2$ and $l_1 \neq l_2$. Note that in this case we have $\epsilon > 1$. If $i_1 > i_2 = \epsilon$, $j_1 > j_2 = \epsilon$ and $\epsilon = l_1 < l_2$, then $l_2 = 2\epsilon$ and $j_1 = 3\epsilon - i_1$, where $i_1 = \epsilon+1,\dots,2\epsilon-1$. Similar results we obtain in other cases.

4. $a = A_1^{i_1}A_2^{j_1}A_3^{k_1}A_4^{l_1}$, $b = A_1^{i_2}A_2^{j_2}A_3^{k_2}A_4^{l_2}$. First, suppose that $i_1 \neq i_2$, $j_1 \neq j_2$, $k_1 \neq k_2$, $l_1 \neq l_2$. If $\epsilon = i_1 < i_2$, $j_1 > j_2 = \epsilon$, $k_1 > k_2 = \epsilon$, $l_1 > l_2 = \epsilon$, then $i_2 = \epsilon$ which is a contradiction. Similarly, in other cases we also obtain a contradiction. Next, suppose that $i_1 = i_2 \leq \epsilon$, $j_1 > j_2 = \epsilon$, $k_1 > k_2 = \epsilon$, $\epsilon = l_1 < l_2$. Then $l_2 = 2\epsilon - i_1$ and $j_1 + k_1 = 3\epsilon - i_1$. Similar results we obtain in other cases where exactly one pair of exponents for the same A_i are equals. Suppose now that $i_1 = i_2 \leq \epsilon$, $j_1 = j_2 \leq e$, $k_1 > k_2 = \epsilon$, $\epsilon = l_1 < l_2$. Then $k_1 = l_1 = 3\epsilon - i_1 - j_1 > \epsilon$. Similar results we deduce also in other cases. Finally, we have the case where $i_s = j_s = k_s = l_s = \epsilon$ $(s = 1,2)$.

We remark that for every $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ we have $\sigma(A_j) = A_{\mu(j)}U_j$, where U_j is a unit of O_K and $\mu(j) \in \{1,2,3,4\}$. Furthermore, we have $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Considering the action of $\mathrm{Gal}(K/\mathbb{Q})$ on the unit equations of cases (2)-(4), we deduce that there is $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma(r) = au$, where (u,v) is the solution of the unit equation $aU - b\sqrt{2}V = q^{4\epsilon}$ and (a,b) is one of the couples (1)-(6).

Example 1 *The integer points of the elliptic curve* E_{469409} *are*

$$(x, y) = (0, 0), (\pm 469409, 0), (9628609, \pm 29842047480).$$

Proof. The mwrank program of Cremona gives that E_{469409} has rank 2. We have $469409 = 41 \cdot 107^2$. So, we can use Algorithm 1. Since $107 \equiv 3 \pmod 8$, the integer solutions of E_{469409} are $(0, 0)$, $(\pm 469409, 0)$ and the couples obtained in steps 1, 2 and 3. We have $\Lambda_{469409} = \emptyset$ and Σ_{469409} gives the solutions $(9628609, \pm 29842047480)$.

Example 2 *The integer points of the elliptic curve* E_{1127} *are*

$$(x, y) = (0, 0), (\pm 1127, 0).$$

Proof. The mwrank programm of Cremona implies that the rank of E_{1127} is 1. We have $1127 = 23 \cdot 7^2$. Thus, we shall use Algorithm 1. We easily deduce that the elements of Σ_{1127} and Λ_{1127} do not give any no trivial solution. Next, since $(23/7) = 1$ and $7 \equiv -1 \pmod 8$, we have to check the solvability of the index form equation $I_K(x_2, x_3, x_4) = \pm 2^7 1127^3 / \sqrt{D_K}$, where $K = \mathbb{Q}(\sqrt{23}, \sqrt{2})$. By Section 4, $D_K = 2^8 23^2$ and so we have the equation $I_K(x_2, x_3, x_4) = \pm 2^3 23^2 7^6$. We shall apply Proposition 1. The triples (F_1, F_2, F_3) satisfying $-2F_1 + 23F_2 = F_3$ and $F_1 F_2 F_3 = \pm 2^3 23^2 7^6$ are:

$$(e1127, -e98, -e4508), \quad (e2254, e98, -e2254), \quad (e1127, e196, e2254),$$

where $e = \pm 1$. For the first triple we have the following two systems of Pell equations:

$$x^2 - 23y^2 = e2254, \quad 2z^2 - y^2 = -e98, \quad 46z^2 - x^2 = -e4508.$$

Since the equation $x^2 - 23y^2 = 2254$ has no solution, the system with $e = 1$ has no solution. For $e = -1$, we see that every equation has a solution. So, we investigate the system. If $(x, y, z) \in \mathbb{Z}^3$ is a solution, then the first and second equation imply that x and y are even and so we obtain $4 | 2254$ which is a contradiction. Hence the system has no solution. For the second triple we obtain the following two systems:

$$x^2 - 23y^2 = e4508, \quad 2z^2 - y^2 = -e98, \quad 46z^2 - x^2 = e2254.$$

The equations $x^2 - 23y^2 = 4508$ and $46z^2 - x^2 = -2254$ have no solution. Thus, the two system have no solution. Finally, the last triple yields the following two systems:

$$x^2 - 23y^2 = e2254, \quad 2z^2 - y^2 = e196, \quad 46z^2 - x^2 = e2254.$$

Since $x^2 - 23y^2 = 2254$ and $46z^2 - x^2 = -2254$ have no solution the system has no solution. Therefore, the index form equation has no solution and so, the only integer points on E_{1127} are the couples $(0, 0)$ and $(\pm 1127, 0)$.

Example 3 *The integer solutions to the equation* E_{16241} *are*

$$(x, y) = (0, 0), (\pm 16241, 0).$$

Proof. The mwrank programm of Cremona implies that the rank of E_{16241} is 2. We have $16241 = 149 \cdot 109$ and 109, 149 are primes with $149 \equiv 109 \equiv 5 \pmod 8$ and $(149/109) = (109/149) = -1$. We shall use Algorithm 2. We easily see that the fundamental solution (γ, δ) to $x^2 - 16241y^2 = 1$ does not give integer point (x, y) on E_{16241} with $x = 16241\gamma$ or $16241(2\gamma^2 - 1)$. Finally, we easily verify that Σ_{16241} and Λ_{16241} do not give any integer point of E_{16241}.

Example 4 *The integer solutions to the equation E_{11659} are*

$$(x, y) = (0, 0), (\pm 11659, 0).$$

Proof. By the mwrank programm of Cremona the rank of E_{11659} is 2. We have $11659 = 131 \cdot 89$ and 131, 89 are primes with $89 \equiv 1 \pmod 8$, $131 \equiv 3 \pmod 8$, $(89/131) = (131/89) = (-131/89) = 1$ and $(-89/131) = -1$. We apply Algorithm 2. We easily see that the sets Λ_{11659} and Σ_{11659} give no nontrivial integer point on E_{11659}. The fundamental solution (γ, δ) to $x^2 - 11659y^2 = 1$ has $\gamma = 161558523925453228690$. We see that there is no integer point (x, y) to E_{11659} with $x = 11659\gamma$ or $11659(2\gamma^2 - 1)$. Since $(89/131) = (-131/89) = 1$, we consider the set $\Pi = \{1, 2, 4, 11, 22, 44\}$ and the fundamental solution $10610 + 927\sqrt{131}$ to $x^2 - 131y^2 = 1$. We determine the quantities T_l with $T_l + U_l\sqrt{131} = (10610 + 927\sqrt{131})^l$, $l \in \Pi$, and we deduce that there is not an integer point (x, y) on E_{11659} with $x = 11659T_l$, $l \in \Pi$.

Finally, since $89 \equiv 1 \pmod 8$ and $(131/89) = 1$ we have to examine the solvability of the index form equation $I_K(x_2, x_3, x_4) = \pm 2^3 89^3 131^2$, where $K = \mathbb{Q}(\sqrt{2}, \sqrt{131})$. We shall use Proposition 1. The triples $(F_1, F_2, F_3) = (e89 \cdot 131, e2 \cdot 89, e2^2 \cdot 89 \cdot 131)$, where $e = \pm 1$ satisfy $F_1F_2F_3 = 2^3 89^3 131^2$ and $2F_1 + 131F_2 = F_3$. The associate systems of Pell equations are:

$$x^2 - 131y^2 = -e2 \cdot 89 \cdot 131, \quad 2z^2 - y^2 = e2 \cdot 89, \quad 2 \cdot 131z^2 - x^2 = e2^2 \cdot 89 \cdot 131.$$

For $e = -1$, all the equations of the system have a solution. Thus, we cannot deduce that the above index form equation has not a solution and so, we continue our work in the field K.

Let $\omega = \sqrt{2} + \sqrt{131}$. Using MAGMA we obtain the following integral basis of K:

$$y_0 = 1, \quad y_1 = \omega, \quad y_2 = \frac{1}{2}(\omega^2 + 1), \quad y_3 = \frac{1}{516}(y^3 + 129y^2 + 379y + 387).$$

We represent an algebraic integer of K, $Z = \sum_{i=0}^{3} z_i y_i$, where $z_i \in \mathbb{Z}$ $(i = 0, 1, 2, 3)$, by $Z = [z_0, z_1, z_2, z_3]$. Furthermore, we obtain that a maximal set of pairwise non associate algebraic integers of K with norm 89 is given by the elements:

$$\begin{aligned} A_1 &= [5074606605, -2320452103, -1372644189, 2496425047], \\ A_2 &= [-311, 134, 68, -127], \\ A_3 &= [-438, -134, -59, 127], \\ A_4 &= [15807, -7223, -4273, 7771]. \end{aligned}$$

By Proposition 6, we have to solve the following unit equations:

$$A_1^3 A_j U - \sqrt{2} A_1 A_j^3 V = 89 \quad (j = 2, 3, 4),$$

$$\begin{aligned}
A_1^2A_kA_lU-\sqrt{2}A_1A_k^2A_lV &= 89 \quad ((k,l)=(2,3),(2,4),(3,4)),\\
A_1^2A_kA_lU-\sqrt{2}A_1A_kA_l^2V &= 89 \quad ((k,l)=(2,3),(2,4),(3,4)),\\
A_1A_2A_3A_4U-\sqrt{2}A_1A_2A_3A_4V &= 89.
\end{aligned}$$

Using MAGMA we see that only the equation

$$A_1A_2A_3A_4U-\sqrt{2}A_1A_2A_3A_4V=89$$

has a solution. Further, if (U,V) is a solution to this equation, then U is equal to one of the following numbers:

$$\pm[20959927732,-8086833265,-4130709548,7665345784],$$

$$\pm[122163411326,-47133518355,-24075539574,44676909288].$$

We easily deduce that none of these solutions yields a nontrivial integer point on E_{11659}. The result follows.

Let $n=2^ap^b$, where p is an odd prime and a, b are positive integers not both even. In this case, we developed in [7], an algorithm for the calculation of the integer solutions of (1). Here, we give an alternative method using the above ideas.

Let $a\geq 3$. If a is even, then we put

$$S_n=\{p^b(2^{a-2}+1)^2,p^b(2^{a-2}-1)^2,p^b(2^{2(a-1)}+1),2^{a-1}(p^{2b}+1)\}.$$

Let a be odd. If b is even, then we set

$$S_n=\{2^{a-2}(p^b+1)^2,p^b(2^{2(a-1)}+1)\}.$$

If b is odd, then we put

$$S_n=\{2^{a-2}(p^b+1)^2,p^b(2^{2(a-1)}+1),p^b(2^{a-2}+1)^2,p^b(2^{a-2}-1)^2\}\cup L_n,$$

where $L_n=\{2^{a-3}25\}$ when $(p,b)=(3,1)$, $L_n=\{3^{b-1}25\}$ when $(p,a)=(3,3)$ and $L_n=\emptyset$ otherwise. Finally, for $a=2$ we put $S_n=\{2(p^{2b}+1),p^b5\}$ and for $a=1$, $S_n=\{(p^b+1)^2/2,(p^b-1)^2/2\}$.

Proposition 7 *Let $n=2^ap^b$, where p is an odd prime and a, b are positive integers not both even. Let $(x,y)\in\mathbb{Z}^2$ be an integer solution of (1) with $x>n$ and $x\notin S_n\cup L_n$. Then, either a is even, b is odd and $(p,x)=(5,9n),(29,9801n)$ or a, b are odd and we have one of the following cases:*

1. *$(x,p)=(2n,3),(49n,3),(8n,7)$.*
2. *$x=nA_l$, where $A_l+B_l\sqrt{2}=(3+2\sqrt{2})^l$ and l is a positive integer with $l|(p-(2/p))/2$.*

Proof. By [7, Lemma 1], we have $x=nz$ and z is a positive integer. Then $(y/n)^2=zn(z^2-1)$. We have the following cases:

1. a odd, b even. Then $y_1^2=2z(z^2-1)$ with $y_1=y/n2^{(a-1)/2}p^{b/2}$. If z is even, then $z^2-1=L^2$, where $L\in\mathbb{Z}$, and so $z=1$ which is a contradiction. Suppose that z is odd. Then $z=M^2$ and $z^2-1=2N^2$, where $M,N\in\mathbb{Z}$. It follows that $M^4-2N^2=1$. By [4], this equation has no nontrivial solution.

2. a even, b odd. We have $y_1^2 = pz(z^2-1)$ with $y_1 \in \mathbb{Z}$. If $p|z$, then we obtain, as in the previous case, a contradiction. Suppose next that $p \not| z$. Then $z = M^2$ and $z^2 - 1 = pN^2$, where $M, N \in \mathbb{Z}$. Thus $M^4 - pN^2 = 1$. By Theorem 3, $p = 5, 29$ and $x = 9n, 9801n$, respectively.

3. a odd, b odd. We have $y_1^2 = 2pz(z^2-1)$ with $y_1 \in \mathbb{Z}$. If $2p|z$, then we obtain, as above, a contradiction. If $2|z$ and $p \not| z$, then we have $z = 2M^2$ and $z^2 - 1 = pN^2$, where $M, N \in \mathbb{Z}$. It follows that $4M^4 - pN^2 = 1$. By Theorem 4, we have $(p, z) = (3, 2), (7, 8)$. If $p|z$ and $2 \not| z$, then $z = pM^2$ and $z^2 - 1 = 2N^2$, where $M, N \in \mathbb{Z}$, and so $p^2M^4 - 2N^2 = 1$. By Theorem 5 and Proposition 2, we have $z = A_l$, where $A_l + B_l\sqrt{2} = (3 + 2\sqrt{2})^l$ and l is a positive integer with $l|(p - (2/p))/2$. Finally, if $p \not| z$ and $2 \not| z$, then $z = M^2$ and $z^2 - 1 = 2pN^2$, where $M, N \in \mathbb{Z}$. Thus $M^4 - 2pN^2 = 1$ and so Theorem 3 implies that $p = 3$ and $z = 49$.

The integer points (x, y) of E_n, in the above case, with $x < 0$ are given by [7, Lemma 2].

Example 5 *The integer points of E_6 are*

$$(x, y) = (0, 0), (\pm 6, 0), (-3, \pm 9), (-2, \pm 8), (12, \pm 36), (18, \pm 72), (294, \pm 5040).$$

Proof. This equation has been solved already in [7]. We shall solve it using Proposition 7. First, we remark that $(294, \pm 5040)$ and $(12, \pm 36)$ are integers points on E_6. Next, since $(3-(2/3))/2 = 2$, we deduce that $A_1 = 3$ and $A_2 = 17$ and so we obtain the integer point $(18, 72)$. Further, we have $S_6 = \{2, 8\}$, whence we do not obtain any integer point. Finally, we easily verified that the integer points (x, y) with $x < 0$ are: $(-6, 0), (-3, \pm 9), (-2, \pm 8)$.

7 The General Case

In this section we present an algorithm for the solution of (1) in case where n has more than three prime divisors. Using Theorem 1, we obtain the following algorithm:

Algorithm 3.
Input: An integer $n > 1$ which is not a square and of the form $p^a q^b$, where p, q are distinct primes and a, b integers ≥ 0.
Output: The integer solutions of (1).

1. Determine the integer solutions (x, y) of (1) with $x \in \Sigma_n$.
2. Determine the integer solutions (x, y) of (1) with $x \in \Lambda_n$.
3. Determine the set D of positive divisors d of n having primes in its prime decomposition with odd exponent and for every such prime p we have $\mathrm{ord}_p(d) = \mathrm{ord}_p(n)$.
4. For every $d \in D$ we put $m = n/d$ and $d = d_1\delta^2$, where $d_1, \delta \in \mathbb{Z}$ and d_1 is square free. We determine the set $D(d)$ of quadruples of integers (w, u, v, e) with $wuv = d_1$, $w, u, v > 0$ and $e \in \{0, 1\}$ such that we have
$$\mathbb{Q}(\sqrt{uv}, \sqrt{2^e wv}) = \mathbb{Q}(\sqrt{uv}, \sqrt{2^e wu}) = \mathbb{Q}(\sqrt{2^e wu}, \sqrt{2^e wv}),$$
$[\mathbb{Q}(\sqrt{uv}, \sqrt{2^e wv}) : \mathbb{Q})] = 4$ and the following equalities are satisfied:

- For every odd prime divisor p of m we have

$$(wu2^e/p) = 1, \quad (wv2^e/p) = 1.$$

- For every odd prime divisor p of w we have

$$(mu2^e/p) = 1, \quad (-mv2^e/p) = 1.$$

- For every odd prime divisor p of u we have

$$(-wm/p) = 1, \quad (-mv2^{e+1}/p) = 1.$$

- For every odd prime divisor p of v we have

$$(wm/p) = 1, \quad (mu2^{e+1}/p) = 1.$$

5. For every $d \in D$, determine the subset $G(d)$ of $D(d)$ which contains the quadruples $(w, u, v, e) \in D(d)$ such that the equation $I_K(x_2, x_3, x_4) = \pm 2^7 n^3/\sqrt{D_K}$, where $K = \mathbb{Q}(\sqrt{uv}, \sqrt{2^e wv})$, has an integer solution.

6. For every $d \in D$ and for every $\lambda = (w, u, v, e) \in G(d)$ determine maximal sets $R_{d,\lambda}$ and $S_{d,\lambda}$ of pairwise non associate algebraic integers of $\mathbb{Q}(\sqrt{uv}, \sqrt{2^e wv})$ with norm m^4 and $4m^4$, respectively.

7. For every $d \in D$ and for every $\lambda = (w, u, v, e) \in G(d)$ determine the units η in $\mathbb{Q}(\sqrt{uv}, \sqrt{2^e wv})$ for which there are $\alpha \in R_{d,\lambda}$ and $\beta \in S_{d,\lambda}$ such that $(\alpha\eta - m)/\beta$ is also a unit. Denote by $W_{d,\lambda}$ the set of elements $\alpha\eta$.

8. For every $d \in D$ and for every $\lambda \in G(d)$ determine the integer solutions (x, y) of (1) with $x > n$ and

$$x = d\frac{(m^2 + r^2)^2}{4r(r^2 - m^2)},$$

where $r \in W_{d,\lambda}$.

9. The integer solutions of (1) are the couples $(0, 0)$, $(\pm n, 0)$ and the couples obtained in steps 1, 2 and 8.

Remark 1 If $d = n$ and $G(n) \neq \emptyset$, then the solutions given by steps 6, 7 and 8 can be also obtained by $x = nwA^2$, where (A, B) are the integer solutions of $w^2X^4 - uvY^2 = 1$, for every $(w, u, v, e) \in G(n)$.

Remark 2 In Step 6, if $\sqrt{2} \in \mathbb{Q}(\sqrt{uv}, \sqrt{2^e wv})$, then we can alternatively take $S_{d,\lambda}$ to be a maximal set of pairwise non conjugate elements of $R_{d,\lambda}$ and in Step 7 to consider the units η in $\mathbb{Q}(\sqrt{uv}, \sqrt{2^e wv})$ for which there are $\alpha \in R_{d,\lambda}$ and $\beta \in S_{d,\lambda}$ such that $(\alpha\eta - m)/\beta\sqrt{2}$ is also a unit.

Example 6 *The integer points of* E_{30} *are*

$$(x, y) = (0, 0), (\pm 30, 0), (-6, \pm 72), (-20, \pm 100), (45, \pm 225), (150, \pm 1800).$$

Proof. The mwrank program of Cremona implies that the rank of E_{30} is 1. We easily obtain that the set Σ_{30} does not gives any nontrivial integer point and the set Λ_{30} gives the points $(-6, \pm 72)$ and $(-20, \pm 100)$. For $d = 30$ we have the quadruples: $(w, u, v, e) = (1, 1, 30, 1), (1, 2, 15, 0), (5, 3, 2, 1), (5, 6, 1, 0), (6, 5, 1, 1)$.

We shall apply Remark 1. The two first quadruples correspond to the equation $x^4 - 30y^2 = 1$. Using Theorem 2 we deduce that this equation has no nontrivial solution. The other two give the equation $25x^4 - 6y^2 = 1$. The fundamental solution to $x^2 - 6y^2 = 1$ is $(5, 2)$. So, Corollary 1 yields that $(1, 2)$ is the only nontrivial solution of $25x^4 - 6y^2 = 1$. This gives the integer point $(150, \pm 1800)$ of E_{30}. Similarly, for the last quadruple we examine the equation $36x^4 - 5y^2 = 1$. By Corollary 1, this equation has no nontrivial solution.

Let $d = 15$. The only quadruple satisfying the equalities of step 7 is $(w, u, v, e) = (3, 5, 1, 0)$ which yields the field $K = \mathbb{Q}(\sqrt{5}, \sqrt{3})$. In order to apply Proposition 1, we write $K = \mathbb{Q}(\sqrt{15}, \sqrt{3})$ and so we have the case 5 with $l = 3$, $a_1 = 5$ and $b_1 = 1$. The triples $(F_1, F_2, F_3) = (-e24, e120, e20)$, where $e = \pm 1$, satisfy the equalities $5F_1 + F_2 = 12F_3$ and $F_1F_2F_3 = \pm 2^8 3^2 5^2 = \pm 2^7 30^3/\sqrt{D_K}$. We have the following systems:

$$3x^2 - y^2 = -e24, \quad 3z^2 - 5x4^2 = e120, \quad z^2 - 5x^2 = e80.$$

Using MAPLE, we see that all the above Pell equations have a solution. Thus, we cannot deduce that the associated index form equation has no solution and so, we continue to the next steps of Algorithm 3. We use the computational system KANT 2.5 and we obtain the following integral basis for the field K:

$$\omega_0 = 1, \ \omega_1 = \theta, \ \omega_2 = (-2 - 2\theta + \theta^2)/4, \ \omega_3 = (-4 - 2\theta + \theta^3)/8,$$

where $\theta = \sqrt{3} + \sqrt{5}$. We represent an algebraic integer of K, $z = \sum_{i=0}^{3} z_i \omega_i$, where $z_i \in \mathbb{Z}$ $(i = 0, 1, 2, 3)$, by $z = [z_0, z_1, z_2, z_3]$. A maximal set of pairwise non associate algebraic integers of K with norm 16 and 64 is given by the elements $\alpha = [2, 0, 0, 0]$ and $\beta = [32, -110, 0, 64]$, respectively. Using KANT 2.5 we obtain the solutions of the unit equation

$$\alpha U - \beta V = 2$$

which are listed in the following table:

TABLE 1

$([-16, 22, 3, -12], [1, 2, 2, 1])$,	$([3, 13, -2, -8], [-1, -2, -4, 2])$,
$([-11, 15, 2, -8], [-1, -1, -4, 2])$,	$([-4, 7, 1, -4], [2, 3, 6, -1])$,
$([-2, -1, -3, -2], [33, 29, 47, 25])$,	$([0, 2, -1, -2], [10, 9, 15, 7])$,
$([2, 3, -1, -2], [1, 0, -1, 3])$,	$([1, 3, 0, -2], [2, 3, 7, -2])$,
$([-4, 4, 1, -2], [0, 0, -1, 1])$,	$([-1, -3, -2, 0], [23, 20, 32, 18])$,
$([-1, 1, -2, 0], [-5, -12, -32, 18])$,	$([0, -1, -1, 0], [8, 6, 8, 9])$,
$([0, 0, -1, 0], [1, -2, -8, 9])$,	$([0, 0, 1, 0], [1, 3, 8, -5])$,
$([0, 1, 1, 0], [-6, -5, -8, -5])$,	$([1, -1, 2, 0], [7, 13, 32, -14])$,
$([1, 3, 2, 0], [-21, -19, -32, -14])$,	$([0, -2, -3, 2], [-8, -18, -47, 25])$,
$([4, -4, -1, 2], [2, 1, 1, 3])$,	$([2, -3, -1, 2], [-3, -6, -15, 7])$,
$([3, -3, 0, 2], [-4, -4, -7, -2])$,	$([-2, -3, 1, 2], [1, 1, 1, 1])$,
$([0, -6, 1, 4], [-3, -3, -6, -1])$,	$([11, -15, -2, 8], [3, 2, 4, 2])$,
$([-3, -13, 2, 8], [3, 3, 4, 2])$,	$([-4, -19, 3, 12], [0, 0, -2, 1])$

The above solutions yield the integer point $(45, \pm 225)$ of E_{30}. For if $(u, v) = ([0,0,1,0],[1,3,8,-5])$, then putting $r = 2u$ we obtain

$$x = 15\frac{(4+r^2)^2}{4r(r^2-4)} = 45.$$

For $d = 1,2,3,5,6,10$ the set $G(d)$ is empty.

Example 7 *The integer points of E_{110} are*

$$(x,y) = (0,0), (\pm 110, 0), (-90, \pm 600), (-11, \pm 363), (1100, \pm 36300).$$

Proof. The mwrank program implies that the rank of E_{110} is 1. It is easily seen that Σ_{110} does not give any nontrivial integer point and Λ_{110} yields the points $(-11, \pm 363)$ and $(-90, \pm 600)$. For $d = 110$ we have: $(w, u, v, e) = (1,1,110,1)$, $(1,2,55,0)$, $(2,5,11,1)$, $(11,10,1,1)$, $(11,5,2,0)$ and $(10,11,1,0)$.

The first two quadruples give the equation $x^4 - 110y^2 = 1$. Using Theorem 2, we see that the fundamental solution $(21,2)$ to $x^2 - 110y^2 = 1$ does not yield a solution for $x^4 - 110y^2 = 1$ and consequently an integer point for E_{110}. The third quadruple corresponds to the equation $4x^4 - 55y^2 = 1$. The fundamental solution of $x^2 - 55y^2 = 1$ is $(89,12)$ and so, Corollary 1 implies that $x^4 - 110y^2 = 1$ has no nontrivial solution. The other two quadruples yield the equation $11^2x^4 - 10y^2 = 1$. The fundamental solution to $x^2 - 10y^2 = 1$ is $(19,6)$. By Corollary 1, we see that $11^2x^4 - 10y^2 = 1$ does not have a nontrivial solution. The last quadruple gives the equation $10^2x^4 - 11y^2 = 1$. The fundamental solution to $x^2 - 11y^2 = 1$ is $(10,3)$. By Corollary 1 the equation $10^2x^4 - 11y^2 = 1$ has only the solution $(x,y) = (1,3)$. Thus, we obtain the integer point $(1100, \pm 36300)$ of E_{110}.

For $d < 110$, we get $D(55) = \{(5,11,1,1)\}$ and $D(d) = \emptyset$ for $d \neq 55, 110$. Thus, we obtain the field $K = \mathbb{Q}(\sqrt{10}, \sqrt{11})$. The triples (F_1, F_2, F_3) satisfying the equalities $-10F_1 + 11F_2 = F_3$ and $F_1F_2F_3 = \pm 2^6 5^2 11^2$ are $(-e22, e20, e440)$ and $(e44, e20, -e220)$, where $e = \pm 1$. For the first triple we have the following systems:

$$x^2 - 11y^2 = -e22, \quad 2z^2 - 5y^2 = e20, \quad 22z^2 - 5x^2 = e440.$$

Since the equations $x^2 - 11y^2 = -22$ and $22z^2 - 5x^2 = -440$ have no solution, the above systems have no solution. The second triple yield the systems

$$x^2 - 11y^2 = e44, \quad 2z^2 - 5y^2 = e20, \quad 22z^2 - 5x^2 = -e220.$$

The equations $x^2 - 11y^2 = 44$ and $22z^2 - 5x^2 = 220$ do not have solution and hence the two systems do not have solution. Thus, the the associated index form equation has also no solution. The result follows.

Example 8 *The integer points of E_{255} are*

$$(x,y) = (0,0), (\pm 255, 0), (-225, \pm 1800), (289, \pm 2312), (4080, \pm 260100).$$

Proof. By the mwrank program, the rank of E_{255} is 1. We have $n = 255 = 5 \cdot 3 \cdot 17$. We easily see that Σ_{255} gives the integer point $(289, \pm 2312)$ and Λ_{255} gives $(-225, \pm 1800)$.

For $d = 255$ we have the quadruples: $(w, u, v, e) = (1, 1, 255, 1),\ (1, 17, 15, 0)$. The two quadruples give the equation $x^4 - 255y^2 = 1$. The fundamental solution of $x^2 - 255y^2 = 1$ is $(16, 1)$. By Theorem 2, we obtain that the only nontrivial solution of $x^4 - 255y^2 = 1$ is $(4, 1)$ which gives the integer points $(x, y) = (4080, \pm 260100)$ on E_{255}. Furthermore, we deduce that $E(d) = \emptyset$ for $d < 255$.

Example 9 *The integer points of $E_{8428033}$ are*

$$(x, y) = (0, 0), (\pm 8428033, 0).$$

Proof. The mwrank program implies that the rank of $E_{8428033}$ is ≤ 2. We have $n = 337 \cdot 281 \cdot 89 = 8428033$. We easily deduce that the sets Σ_n and Λ_n do not provide us with nontrivial integer points of $E_{8428033}$. For $d = 8428033$ we have the quadruple $(w, u, v, e) = (1, 1, 8428033, 1)$ which gives the equation $x^4 - 8428033y^2 = 1$. Following Theorem 2, we compute the fundamental solution of $x^2 - 8428033y^2 = 1$ and we see that it does not give a nontrivial solution of $x^4 - 8428033y^2 = 1$. Thus, this equation has no nontrivial solution. Finally, we obtain $G(d) = \emptyset$ for $d < n$. The result follows.

Example 10 *The integer points of E_{1131} are*

$$(x, y) = (0, 0), (\pm 1131, 0), (-117, \pm 12168), (10933, \pm 1137032).$$

Proof. First note that the rank of E_{1131} is 2. We have $n = 3 \cdot 13 \cdot 29$. The set Σ_{1131} does not give nontrivial integer point of E_{1131} and the set Λ_{1131} yields the point $(-117, \pm 12168)$. Only for $d = 1131, 377, 87$ we obtain quadruples (w, u, v, e).

If $d = 1131$, then we get $(w, u, v, e) = (1, 1, 1131, 1), (1, 13, 87, 1), (13, 29, 3, 0)$. We shall apply Remark 1. For the first two quadruples, we have to find the solutions of $x^4 - 1131y^2 = 1$. The fundamental solution of the equation $x^2 - 1131y^2 = 1$ is $(a, b) = (268185, 10948)$ and $\sqrt{a}, \sqrt{2a^2 - 1}$ are not integers. So Theorem 2 implies that the equation $x^4 - 1131y^2 = 1$ has no integer solution. Thus, the first two quadruples do not give an integer point of E_{1131}. For $(w, u, v, e) = (13, 29, 3, 0)$ we have to solve $13^2x^4 - 87y^2 = 1$. Using Theorem 5 and Proposition 2 we deduce that this equation has no solution and so the last quadruple does not give an integer point of E_{1131}.

For $d = 377$ we have the quadruples $(w, u, v, e) = (29, 13, 1, 1), (29, 1, 13, 1)$. Both quadruples yield the field $K = \mathbb{Q}(\sqrt{58}, \sqrt{13})$. The triples $(F_1, F_2, F_3) = (e348, e39, e4524)$, where $e = \pm 1$, satisfy $-13F_1 + 4 \cdot 58F_2 = F_3$ and $F_1F_2F_3 = \pm 2^4 3^3 13^2 29^2 = \pm 2^7 1131^3/\sqrt{D_K}$. Thus, we have the systems

$$x^2 - 58y^2 = e348, \quad z^2 - 13y^2 = e156, \quad 58z^2 - 13x^2 = e4524.$$

For $e = 1$, every equation of the system has a solution. So we continue to the next steps of Algorithm 3.

Set $\theta = \sqrt{13} + \sqrt{58}$. The computational system MAGMA gives the following integral basis for the field $K = \mathbb{Q}(\sqrt{58}, \sqrt{13})$:

$$\omega_0 = 1, \quad \omega_1 = \theta, \quad \omega_2 = (\theta^2 + 2\theta + 3)/4, \quad \omega_3 = (\theta^3 + 83\theta + 90)/180.$$

If $z = \sum_{i=0}^{3} z_i\omega_i$, where $z_0, z_1, z_2, z_3 \in \mathbb{Z}$, is an element of O_K, then we write $z = [z_0, z_1, z_2, z_3]$. A maximal set of pairwise non associate elements of O_K with norm 3^4 is given by MAGMA. Its elements are listed in the following table.

TABLE 3

$[46, -30, -17, 70]$
$[4, 2, -1, -4]$
$[4, 1, 0, -1]$
$[28, -16, -1, 14]$
$[646, 236, -17, -196]$
$[-19, -2, 4, 0]$
$[-167254, 78936, 55361, -193688]$
$[8, 3, 0, -2]$
$[-116, -47, 17, 70]$
$[12, 5, -2, -8]$
$[3, 0, 0, 0]$
$[54, -27, -2, 24]$
$[-123378, 33167, 35564, -92558]$
$[-6, 3, 0, -2]$
$[-1330901358, 626185105, 49998419, -561048396]$
$[129, 2, -4, 0]$
$[3, -1, 0, 1]$
$[-2352490266, 1106839766, 88376795, -991704638]$
$[-450, 219, 17, -196]$

Furthermore, MAGMA provides a maximal set of pairwise non associate elements of O_K with norm $4 \cdot 3^4$ given in the table below.

TABLE 4

$[-78, 39, 3, -35]$
$[18, 7, -1, -7]$
$[75450997426395, 26966216894344, -1993938001999, -22374625065691]$
$[9874766665, 3529245596, -260959765, -2928313929]$
$[-9, 6, 3, -13]$
$[-64259, 39638, 23153, -92919]$
$[498, 191, -13, -159]$
$[30, -3, -1, 3]$
$[-18, 9, 1, -9]$
$[1856475641909, 663505142760, -49060946289, -550528791509]$
$[27, 10, -1, -9]$
$[-391, 234, 125, -515]$
$[4671, 1670, -125, -1389]$
$[-11, 6, 1, -7]$
$[875811, 313018, -23153, -259737]$
$[113, 42, -3, -35]$

Next we solve, using MAGMA, the units equations $aU - bV = 3$, where a is an element of TABLE 3 and b an element of TABLE 4. The equation with $a = [12, 5, -2, -8]$ and

$$b = [75450997426395, 26966216894344, -1993938001999, -22374625065691]$$

has only the solution

$$\begin{aligned} U &= [-1, 0, 0, 0] \\ V &= [290305319644, -179246403758, -104979192791, 420989904480] \end{aligned}$$

which yields the integer points $(10933, \pm 1137032)$ of E_{1131}. None of the other equations gives another integer point of E_{1131}.

For $d = 87$ we have the quadruple $(w, u, v, e) = (1, 29, 3, 0)$. It yields the field $\mathbb{Q}(\sqrt{3}, \sqrt{87})$. The triples (F_1, F_2, F_3) satisfying $F_1F_2F_3 = \pm 2^5 3^2 13^3 29^2 = \pm 2^7 1131^3/\sqrt{D_K}$ and $-F_1 - 29F_2 = 12F_3$ are $(-e9048, 156, 377)$,$(-e4524, e156, e754)$ and $(e4524, e312, e377)$, where $e = \pm 1$. For the first triple we have the systems:

$$3x^2 - 29y^2 = -e9048, \quad 3z^2 - y^2 = e156, \quad 29z^2 - x^2 = e377.$$

The two systems have no solution since the equations $3x^2 - 298y^2 = -9048$ and $3z^2 - y^2 = -156$ have no solution. The second triple yields the systems:

$$3x^2 - 29y^2 = -e4524, \quad 3z^2 - y^2 = e156, \quad 29z^2 - x^2 = e754.$$

The equations $3x^2 - 29y^2 = \pm 4524$ have no solution and so, the systems have no solution. The last triple gives the systems

$$3x^2 - 29y^2 = e4524, \quad 3z^2 - y^2 = e312, \quad 29z^2 - x^2 = e377$$

which have no solution, since $3x^2 - 29y^2 = \pm 4524$ do not. The result follows.

Acknowledgements. The authors wishes to thank the referee for helpful comments.

References

[1] M. A. Bennett and P.G. Walsh, The Diophantine equation $b^2X^4 - dY^2 = 1$. Proc. of the Amer. Math. Soc. 127 (1999), 3481-3491.

[2] Z. I. Borevich and I. R. Shafarevich, *Number Theory,* Academic Press Inc. 1966.

[3] J. S. Chahal, *Topics in number theory,* The University Series in Mathematics. Plenum Press, New York, 1988.

[4] J. H. E. Cohn, The Diophantine Equation $x^4 - Dy^2 = 1$. II, *Acta Arith.* 78 no. 4 (1997), 401-403.

[5] J. E. Cremona, *Algorithms for modular elliptic curves,* Cambridge University Press, Cambridge, 1992.

[6] K. Draziotis, Integral solutions of the equation $Y^2 = X^3 \pm p^kX$, *Mathematics of Computation* Vol. 75, no 255 (2006), 1493-1505.

[7] K. Draziotis and D. Poulakis, Practical Solution of the Diophantine Equation $y^2 = x(x + 2^ap^b)(x - 2^ap^b)$, *Mathematics of Computation* Vol. 75, no 255 (2006), 1585-1593.

[8] K. Feng and M. Xiong, On elliptic curves $y^2 = x^3 - n^2x$ with rang zero, *J. Number Theory* 109 (2004), 1-26.

[9] I. Gaál, A. Pethö, M. Pohst, On the Resolution of Index Form Equations in Biquadratic Fields III. The Bicyclic Biquadratic case, *J. Number Theory,* 53 (1995), 100-114.

[10] J. Gebel and H. G. Zimmer, Computing the Mordell-Weil group of an elliptic curve over $\mathbb{Q}$, pp. 61-83 in *Elliptic curves and related topics,* edited by H. Kisilevsky and M. R. Murty, CRM Proc. Lecture Notes 4, Amer. Math. Soc., Providence, RI, 1994.

[11] J. Gebel, A. Pethö and H. G. Zimmer, Computing integral points on elliptic curves, *Acta Arith.* 68(2) (1994), 171-192.

[12] K. Győry, Sur les polynômes à coefficients entiers et de discriminant donné III, *Publ. Math. Debrecen,* 23 (1976), 141-165.

[13] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms,* Springer-Verlag 1984.

[14] S. Lang, *Algebraic Number Theory,* Addison-Wesley 1970.

[15] R. A. Mollin, Simple Continued Fraction Solutions for Diophantine Equations, *Expo. Math.* 19 (2001), 55-73.

[16] P. Ribenboim, *Nombres premiers: mystères et records,* Presses Universitaires de France 1994.

[17] P. Samuel, Résultats élémentaires sur certaines équations diophantiennes, *J. Number Theory Bordaux,* 14, 2002, 629-646.

[18] R. J. Stroeker and N. Tzanakis, Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms, *Acta Arith.* 67(2) (1994), 177-196.

[19] K. Wildanger, Uber das Losen von Einheiten- und Indexformgleichungen in algebraischen Zahlkorpern. *J. Number Theory* 82(2) (2000), 188–224.

[20] K. S. Williams, Integers of biquadratic fields, *Canad. Math. Bull.* 13 (1970), 519-526.

[21] http://www.math.tu-berlin.de/ kant/

[22] http://magma.maths.usyd.edu.au/magma/.

Dimitrios Poulakis
Aristotle University of Thessaloniki,
Department of Mathematics,
54124 Thessaloniki, Greece
e.mail: poulakis@math.auth.gr

Konstantinos Draziotis
Kromnis 33
54454 Thessaloniki
Greece