ACTA ARITHMETICA
101.2 (2002)

The square-free kernel of $x^{2^n} - a^{2^n}$

by

Paulo Ribenboim (Kingston, Ont.)

Dedicated to my long-time friend and collaborator Wayne McDaniel, at the occasion of his retirement

1. Introduction

A. Statement of the results. We investigate the number $\nu(x^{2^n} - a^{2^n})$ of odd prime factors of the square-free kernel of numbers $x^{2^n} - a^{2^n}$, where $x > a \geq 1$ and $n \geq 2$. The main theorem states that (under a certain assumption) for each $a \geq 1$ the set $T_a = \{(x,n) \mid n \geq 2,\ x > a$ and the square-free kernel of $x^{2^n} - a^{2^n}$ has $n-1$ odd prime factors$\}$ is finite and effectively computable.

In the final section, we show with several examples how to determine explicitly the sets T_a, namely $T_1, T_2, T_3, T_4, T_5, T_6, T_{10}$. As an illustration of the results obtained,

$$\nu(3^{2^n} - 1) \geq n \quad \text{for all } n \geq 4,$$
$$\nu(7^{2^n} - 1) \geq n \quad \text{for all } n \geq 4,$$
$$\nu(99^{2^n} - 1) \geq n \quad \text{for all } n \geq 3,$$

and if $x \neq 3, 7, 99$ then

$$\nu(x^{2^n} - 1) \geq n \quad \text{for all } n \geq 2.$$

The proofs rely on properties of binary linearly recurring sequences and more specifically on a special case of the main theorem in Ribenboim [7].

Now we gather the concepts and facts used in this paper.

B. Binary linearly recurring sequences. Let $P > 0$, $Q \neq 0$ be integers such that $\gcd(P,Q) = 1$ and $D = P^2 - 4Q \neq 0$.

Let $U_0 = 0$, $U_1 = 1$, $V_0 = 2$, $V_1 = P$ and for $n \geq 2$:

$$U_n = PU_{n-1} - QU_{n-2}, \qquad V_n = PV_{n-1} - QV_{n-2}.$$

2000 *Mathematics Subject Classification*: Primary 11B37; Secondary 11A05, 11B39.

We also define $U_{-n} = -U_n/Q^n$, $V_{-n} = V_n/Q^n$ (for $n > 0$); then the above formulas still hold.

$\mathcal{U} = (U_n)_n$, $\mathcal{V} = (V_n)_n$ are called *binary linearly recurring sequences of first kind*, respectively *of second kind*, with parameters (P, Q). We also use the notation $U_n(P, Q)$, $V_n(P, Q)$.

For an expository account of the theory of binary linearly recurring sequences, see Chapter 1 of Ribenboim [6]. Here we limit ourselves to mention explicitly the facts which are used in what follows.

If $P = 2$, $Q = -1$ the numbers U_n, V_n are the Pell numbers of first kind, respectively of second kind. These numbers are (for $n \geq 0$):

$$\begin{array}{ll} U_n: & 0\ 1\ 2\ 5\ 12\ 29\ 70\ 169\ldots, \\ V_n: & 2\ 2\ 6\ 14\ 34\ 82\ 198\ 478\ldots \end{array}$$

Then U_n is even if and only if n is even, $2 \mid V_n$ but $4 \nmid V_n$ for all n.

The symbol $\Box$ denotes any non-zero integer which is a square.

Concerning square and double square Pell numbers, we quote the following important result of Ljunggren [1] (see also Ribenboim [5]); in particular, the proof of (a) is difficult.

(1.1) *For Pell numbers*:

(a) $U_n = \Box$ *if and only if* $n = 1, 7$;
(b) $U_n = 2\Box$ *if and only if* $n = 2$;
(c) $V_n \neq \Box$ *for all* n;
(d) $V_n = 2\Box$ *if and only if* $n = 0, 1$.

C. Pell equations. Let $F > 1$ be a square-free integer, and $\varepsilon = c + d\sqrt{F}$ be the fundamental unit of the ring $\mathbb{Z}[\sqrt{F}]$, so $1 < \varepsilon$. Let $Q = N(\varepsilon) = c^2 - d^2F = \pm 1$ be the norm of ε. We consider the equations

$$x^2 - Fy^2 = \pm 1.$$

(1.2) *Solutions of* $x^2 - Fy^2 = 1$. The solutions (x, y) with $x + y\sqrt{F} > 0$ are given by (x_n, y_n), where

$$x_n + y_n\sqrt{F} = \varepsilon^n \begin{cases} \text{for all } n \text{ if } Q = 1, \\ \text{for all even } n \text{ if } Q = -1. \end{cases}$$

(1.3) *Solutions of* $x^2 - Fy^2 = -1$. The solutions (x, y) with $x + y\sqrt{F} > 0$ are given by (x_n, y_n), where $x_n + y_n\sqrt{F} = \varepsilon^n$ and $Q = -1$, n odd. If $Q = 1$ there are no solutions.

It is possible to express (x_n, y_n) by means of terms of a binary linearly recurring sequence.

Let $\varepsilon = c + d\sqrt{F}$ as before, let $P = 2c$, $Q = N(\varepsilon) = \pm 1$ and consider the sequences $\mathcal{U}$, $\mathcal{V}$ with parameters (P, Q). We note that V_n is even for all n. Then:

(1.4) $x_n = V_n/2$, $y_n = dU_n$ *for all* n.

We shall require the following result (part (a) was first proved by Ljunggren [2] and a simpler proof was given by Samuel [8]; in the same paper, Samuel proved also (b)):

(1.5) *Let* $x > 1$ *and let* p *be any prime.*

(a) *If* $x^4 - 1 = p\Box$ *then* $(x, p) = (3, 5)$ *or* $(99, 29)$.
(b) *If* $x^4 - 1 = 2p\Box$ *then* $(x, p) = (7, 3)$.

In Ribenboim [7] we considered families of systems of two Pell equations. Let $F > 1$ and $G > 0$ be square-free integers, let f, g be non-zero integers. We denote by $(F, f \mid G, g)$ the family of systems—one for each prime p—of Pell equations

$$(F, f \mid G, g) \qquad \begin{cases} x^2 - f = F\Box, \\ x^2 - g = Gp\Box. \end{cases}$$

We proved a theorem for certain families of the above kind. Here we shall only need the following special case:

(1.6) *For each* $b \geq 1$ *the set of solutions* (x, b) *of each family below is finite and effectively computable*: $(2, b^2 \mid 1, -b^2)$, $(2, -b^2 \mid 1, b^2)$, $(2, b^2 \mid 2, -b^2)$, $(2, -b^2 \mid 2, b^2)$.

2. The main theorem. For every $m \geq 1$ let $\nu(m)$ denote the number of odd prime factors of the square-free kernel of m. So $\nu(m) = 0$ if and only if $m = \Box$ or $m = 2\Box$. And $\nu(m) = 1$ if and only if $m = p\Box$ or $m = 2p\Box$, where p is any odd prime. It is immediate that if $\gcd(m, n) = 1$ or 2, then $\nu(mn) = \nu(m) + \nu(n)$.

For all $a \geq 1$ and $n \geq 1$ we define the set

$$S_{a,n} = \{x \mid x > a \text{ and } \nu(x^{2^n} - a^{2^n}) = n - 1\}.$$

In particular, $S_{a,1} = \{x \mid x > a \text{ and } x^2 - a^2 = \Box \text{ or } 2\Box\}$.

We introduce the following notation. Let $x > a \geq 1$ and $n \geq 1$; we define the integers u_n, v_n (which depend on x, a) as follows:

$$u_n = x^{2^n} - a^{2^n}, \qquad v_n = x^{2^n} + a^{2^n}.$$

It is easy to verify the following properties. If $\gcd(x, a) = 1$ then $\gcd(u_n, v_m) = 1$ or 2 (for all n, m), $\gcd(v_n, v_m) = 1$ or 2 (for all $n \neq m$) and $u_n = u_{n-1}v_{n-1}$ for all $n \geq 2$. The integers u_n, v_n may be also defined with the help of a binary linearly recurring sequence. Let $P = x + a$, $Q = xa$; then $\gcd(P, Q) = 1$ and

$$u_n = (x - a) \cdot U_{2^n}(P, Q), \qquad v_n = V_{2^n}(P, Q).$$

We shall need the following facts.

(2.1) Lemma. *Let $x > a \geq 1$ and $n \geq 2$.*

1) $\nu(x^{2^n} + a^{2^n}) \neq 0$.
2) $\nu(x^{2^n} - a^{2^n}) > n - 2$.

Proof. 1) We show that $x^{2^n} + a^{2^n} \neq \Box, 2\Box$. As $n \geq 2$, we have $x^{2^n} + a^{2^n} = (x^{2^{n-2}})^4 + (a^{2^{n-2}})^4 \neq \Box$ by the classical result of Fermat (see for example Ribenboim [4]). Similarly, if $x^{2^n} + a^{2^n} = (x^{2^{n-2}})^4 + (a^{2^{n-2}})^4 = 2\Box$ then again $x^{2^{n-2}} = a^{2^{n-2}}$, so $x = a$ (see Ribenboim [4]) and this has been excluded.

2) We may assume without loss of generality that $\gcd(x, a) = 1$. Indeed, if $\gcd(x, a) = e$, let $x = ze$, $a = be$, hence $x^{2^n} - a^{2^n} = e^{2^n}(z^{2^n} - b^{2^n})$ and $\nu(x^{2^n} - a^{2^n}) = \nu(z^{2^n} - b^{2^n})$.

We prove the statement by induction on n. Let $n = 2$. By the classical theorem of Fermat (see [4]), $x^4 - a^4 \neq \Box$. Next we show that $x^4 - a^4 \neq 2\Box$. We quote the following theorem of Euler: If $u^4 - v^4 = 2w^2$ then $u = v$, $w = 0$. For a proof, see Ribenboim [3], Proposition A14.5. Therefore if $x > a \geq 1$ then $x^4 - a^4 \neq 2\Box$.

Now, let $n \geq 3$ and assume that the statement is true for $n - 1$. We have $x^{2^n} - a^{2^n} = u_n = u_{n-1}v_{n-1}$ with $\gcd(u_{n-1}, v_{n-1}) = 1$ or 2, since $\gcd(x, a) = 1$. So $\nu(u_n) = \nu(u_{n-1}v_{n-1}) = \nu(u_{n-1}) + \nu(v_n) > n - 3 + 1 = n - 2$. ∎

We introduce some sets. For all $a \geq 1$, $n \geq 1$ and for all e dividing a, let

$$S_{a,n}(e) = \{x \in S_{a,n} \mid \gcd(x, a) = e\}.$$

If e, e' divide a and $e \neq e'$ then $S_{a,n}(e) \cap S_{a,n}(e') = \emptyset$ and $S_{a,n} = \bigcup_{e|a} S_{a,n}(e)$. If $x \in S_{a,n}(e)$, let $x = ze$ and $a = be$. Then $z > b$, $\gcd(z, b) = 1$ and $\nu(e^{2^n}(z^{2^n} - b^{2^n})) = n - 1$, so $\nu(z^{2^n} - b^{2^n}) = n - 1$, so $z \in S_{b,n}(1)$. The mapping $x \mapsto z$ is a bijection between $S_{a,n}(e)$ and $S_{b,n}(1)$; moreover the mapping is effectively computable.

Let $a \geq 1$. The set $S_{a,1}$ is infinite. Indeed, let $\varepsilon = 1 + \sqrt{2}$ be the fundamental unit of $\mathbb{Z}[\sqrt{2}]$, and for every even $m \geq 1$, let $z_m + u_m\sqrt{2} = (1 + \sqrt{2})^m$. Hence $z_m^2 - 2u_m^2 = 1$, so if $x_m = az_m$ then $x_m^2 - a^2 = 2\Box$. So $x_m \in S_{a,1}$, showing that this set is infinite.

For $n \geq 2$ we have:

(2.2) Theorem. 1) $S_{a,2} \supseteq S_{a,3} \supseteq \ldots$
2) *$S_{a,2}$ is a finite effectively computable set.*

Proof. 1) Let $n \geq 3$; we show that $S_{a,n} \subseteq S_{a,n-1}$. It suffices to show that, for every $e \mid a$, $S_{a,n}(e) \subseteq S_{a,n-1}(e)$, or equivalently, for every b dividing a, $S_{b,n}(1) \subseteq S_{b,n-1}(1)$.

Let $z \in S_{b,n}(1)$, so $z > b$, $\gcd(z, b) = 1$ and $\nu(z^{2^n} - b^{2^n}) = n - 1$. Let $d = \gcd(z^{2^{n-1}} - b^{2^{n-1}}, z^{2^{n-1}} + b^{2^{n-1}})$, so $d \mid 2b^{2^{n-1}}$; but $\gcd(z, b) = 1$, hence

$d = 1$ or 2. We may write

$$\begin{cases} z^{2^{n-1}} - b^{2^{n-1}} = k, \\ z^{2^{n-1}} + b^{2^{n-1}} = h, \end{cases}$$

with $\gcd(k, h) = 1$ or 2, $n - 1 = \nu(kh) = \nu(k) + \nu(h)$. By (2.1), $\nu(h) \geq 1$, so $\nu(k) \leq n - 2$. By (2.1), $\nu(k) > n - 3$, hence $\nu(k) = n - 2$, showing that $z \in S_{b,n-1}(1)$.

2) To show that $S_{a,2}$ is finite and effectively computable, it suffices to show that for every $e \mid a$, $S_{a,2}(e)$ is finite and effectively computable, or equivalently, for every $b \mid a$, the set $S_{b,2}(1)$ is finite and effectively computable.

Now $z \in S_{b,2}(1)$ if and only if $z > b$, $\gcd(z, b) = 1$ and $\nu(z^4 - b^4) = 1$ and this means that $z^4 - b^4 = p\Box$ or $2p\Box$, for some odd prime p. We have $\gcd(z^2 - b^2, z^2 + b^2) = 1$ or 2, because $\gcd(z, b) = 1$. Then the following cases may happen:

$$\left\{\begin{array}{l} z^2 - b^2 = \\ z^2 + b^2 = \end{array}\right. \begin{array}{c|c|c|c} \Box & p\Box & 2\Box & 2p\Box \\ p\Box & \Box & 2p\Box & 2\Box \\ \scriptstyle(1) & \scriptstyle(2) & \scriptstyle(3) & \scriptstyle(4) \end{array} \quad \text{when } z^4 - b^4 = p\Box,$$

$$\left\{\begin{array}{l} z^2 - b^2 = \\ z^2 + b^2 = \end{array}\right. \begin{array}{c|c|c|c} \Box & 2\Box & p\Box & 2p\Box \\ 2p\Box & p\Box & 2\Box & \Box \\ \scriptstyle(5) & \scriptstyle(6) & \scriptstyle(7) & \scriptstyle(8) \end{array} \quad \text{when } z^4 - b^4 = 2p\Box.$$

In cases (1), (2), (5) and (8), z belongs to a finite and effectively computable set. By (1.6), the families $(2, \pm b^2 \mid 2, \mp b^2)$ and $(2, \pm b^2 \mid 1, \mp b^2)$ have a finite effectively computable set of solutions (z, p). So, in cases (3), (4), (6) and (7), z belongs to a finite and effectively computable set. This shows that $S_{b,2}(1)$ is finite and effectively computable. ∎

Consider the following statement about the pair of integers (b, z):

($\mathrm{H}_{b,z}$) If $z > b \geq 1$, $\gcd(z, b) = 1$ and $\nu(z^4 - b^4) = 1$, there exists an effectively computable $h \geq 2$ (depending on z, b) such that $\nu(z^{2^h} + b^{2^h}) > 1$.

No proof is known for this statement but, of course it holds in every numerical example computed thus far.

(2.3) Theorem. *Assume that the statement* ($\mathrm{H}_{b,z}$) *holds for* $z > b \geq 1$ *with* $\gcd(z, b) = 1$ *and* $\nu(z^4 - b^4) = 1$. *Let* $h \geq 2$ *be the smallest integer such that* $\nu(z^{2^h} + b^{2^h}) > 1$. *Then* $z \notin S_{b,j}(1)$ *for all* $j \geq h + 1$.

Proof. With the notation introduced, we have $\nu(u_2) = \nu(z^4 - b^4) = 1$, and

$$z^{2^j} - b^{2^j} = u_j = v_{j-1} v_{j-2} \ldots v_{h+1} v_h v_{h-1} \ldots v_2 u_2.$$

As already stated, $\gcd(u_2, v_i) = 1$ or 2 (for all i) and $\gcd(v_i, v_l) = 1, 2$ for $i \neq l$. So

$$\nu(u_j) = \nu(v_{j-1}) + \ldots + \nu(v_{h+1}) + \nu(v_h) + \ldots + \nu(v_2) + \nu(u_2).$$

By (2.1) and the hypothesis, $\nu(u_j) \geq (j - 1 - h) + 2 + (h - 2) + 1 = j$, so $z \notin S_{b,j}(1)$. ∎

If $a \geq 1$ let

$$T_a = \{(x, n) \mid n \geq 2,\ x \in S_{a,n}\}.$$

For every e dividing a, let

$$T_a(e) = \{(x, n) \in T_a \mid \gcd(x, a) = e\}.$$

If $e \mid a$, $b = a/e$, $z = x/e$ and $(x, n) \in T_a(e)$ then $(z, n) \in T_b(1)$. The mapping $(x, n) \mapsto (z, n)$ is a bijection between $T_a(e)$ and $T_b(1)$.

(2.4) Theorem. *Let $a \geq 1$ and assume that* $(\mathrm{H}_{b,z})$ *holds for every b dividing a and $z > b$. Then T_a is a finite and effectively computable set.*

Proof. It suffices to show that for every e dividing a, the set $T_a(e)$ is finite and effectively computable. By the above remark it suffices to show that for every b dividing a, the set $T_b(1)$ is finite and effectively computable. By (2.2) the set $S_{b,2}(1)$ is finite and effectively computable. By (2.3) and the hypothesis, for every $z_0 \in S_{b,2}(1)$ there exists an effectively computable integer $h \geq 2$ (depending on b and z_0) such that if $z_0 \in S_{b,i}(1)$ then $i \leq h$. So the set

$$T_b(1)|z_0 = \{(z, n) \in T_b(1) \mid z = z_0\}$$

is finite and effectively computable, hence

$$T_b(1) = \bigcup_{z_0 \in S_{b,2}(1)} T_b(1)|z_0$$

is also finite and effectively computable. ∎

3. Explicit computations. For specific values of $a \geq 1$, it is possible to determine explicitly the finite effectively computable set T_a. This determination requires the actual solution of certain families of systems of Pell equations. We recall that if $a \geq 1$ then

$$T_a = \{(x, n) \mid n \geq 2,\ x > a,\ \nu(x^{2^n} - a^{2^n}) = n - 1\}.$$

The following easy remark will be useful: If $(x, n) \in T_a$ then $(mx, n) \in T_{ma}$.

(3.1) *Let $a = 1$. Then* $T_1 = \{(3, 2), (3, 3), (7, 2), (7, 3), (99, 2)\}$.

Proof. We determine explicitly $S_{1,2} = \{x \mid x > 1,\ \nu(x^4 - 1) = 1\}$. If $x^4 - 1 = p\Box$ for some odd prime p, then by (1.5), $(x, p) = (3, 5)$ or $(99, 29)$.

If $x^4 - 1 = 2p\Box$ for some odd prime p, then by (1.5), $(x, p) = (7, 3)$. This shows that $S_{1,2} = \{3, 7, 99\}$.

Now

$$\begin{aligned}
3^4+1 &= 82 = 2\times 41, &&\text{so}\quad \nu(3^4+1)=1,\\
3^8+1 &= 2\times 17\times 193, &&\text{so}\quad \nu(3^8+1)=2,\\
7^4+1 &= 2\times 1201, &&\text{so}\quad \nu(7^4+1)=1,\\
7^8+1 &= 2\times 17\times 169553, &&\text{so}\quad \nu(7^8+1)=2,\\
99^4+1 &= 2\times 2617\times 18353, &&\text{so}\quad \nu(99^4+1)=2.
\end{aligned}$$

Thus $(3,2),(3,3)\in T_1$, $(3,j)\notin T_1$ for all $j\ge 4$; $(7,2),(7,3)\in T_1$, $(7,j)\notin T_1$ for all $j\ge 4$; $(99,2)\in T_1$, $(99,j)\notin T_1$ for all $j\ge 3$. ■

(3.2) $T_2=\{(6,2),(6,3),(14,2),(14,3),(198,2)\}$.

Proof. Let $x>2$ be such that $x^4-2^4=p\square$ or $2p\square$, for some odd prime p.

First case: x is even. Let $x=2z$. Then $2^4(z^4-1)=p\square$ or $2p\square$, hence $z^4-1=p\square$ or $2p\square$. As stated in (3.1), $z=3,99$ or 7, hence $x=6,198$ or 14. We have $6^4+2^4=2^4(3^4+1)$ so

$$\nu(6^4+2^4)=\nu(3^4+1)=1;$$

similarly

$$\nu(6^8+2^8)=\nu(3^8+1)=2.$$

In the same manner

$$\nu(14^4+2^4)=\nu(7^4+1)=1,\qquad \nu(14^8+2^8)=\nu(7^8+1)=2,$$
$$\nu(198^4+2^4)=\nu(99^4+1)=2.$$

Altogether, only $(6,2),(6,3),(14,2),(14,3),(198,2)\in T_2$.

Second case: x is odd. So $\gcd(x^2-4,x^2+4)=1$. Since x^4-2^4 is odd we have $x^4-2^4\ne 2p\square$ and there are only the following cases:

$$\left\{\begin{array}{l}x^2-4=\\ x^2+4=\end{array}\right.\begin{array}{c|c}\square & p\square\\ p\square & \square\\ \scriptstyle(1) & \scriptstyle(2)\end{array}$$

Subcase (1): there exists $t\ne 0$ such that $x^2-t^2=4$, which is clearly impossible.

Subcase (2): there exists t such that $t^2-x^2=4$, which is again impossible. ■

(3.3) $T_3=\{(9,2),(9,3),(21,2),(21,3),(297,2),(4,2),(4,3),$
$(5,2),(5,3),(5,4)\}$.

Proof. Let $x>3$ be such that $x^4-3^4=p\square$ or $2p\square$, for some odd prime p.

First case: $3 \mid x$. Let $x = 3z$. Then $z^4 - 1 = p\Box$ or $2p\Box$. As already seen, $z = 3, 99, 7$ so $x = 9, 297, 21$. We have, as computed in (3.1),

$$\nu(9^4 + 3^4) = \nu(3^4(3^4 + 1)) = 1, \qquad \nu(9^8 + 3^8) = \nu(3^8(3^8 + 1)) = 2$$

and similarly

$$\nu(21^4 + 3^4) = 1, \qquad \nu(21^8 + 3^8) = 2, \qquad \nu(297^4 + 3^4) = 2.$$

Thus, only $(9, 2), (9, 3), (21, 2), (21, 3)$, and $(297, 2)$ are in T_3.

Second case: $\gcd(x, 3) = 1$. Then $d = \gcd(x^2 - 3^2, x^2 + 3^2) = 1$ or 2, because $d \mid 18$ but $3 \nmid d$.

Case A: $d = 1$. If $x^4 - 3^4 = p\Box$ then

$$\left\{\begin{array}{rcc|c} x^2 - 3^2 = & \Box & p\Box \\ x^2 + 3^2 = & p\Box & \Box \\ & \scriptstyle(1) & \scriptstyle(2) \end{array}\right.$$

(1) is not possible, while (2) gives $(x, p) = (4, 7)$.

We have $4^4 + 3^4 = 337$, prime, $\nu(4^8 + 3^8) = \nu(17 \times 4241) = 2$. Then only $(4, 2)$ and $(4, 3)$ are in T_3.

If $x^4 - 3^4 = 2p\Box$ then x is odd. On the other hand, since $d = 1$, it follows that x is even, a contradiction.

Case B: $d = 2$. If $x^4 - 3^4 = p\Box$ then

$$\left\{\begin{array}{rc|c} x^2 - 3^2 = & 2\Box & 2p\Box \\ x^2 + 3^2 = & 2p\Box & 2\Box \\ & \scriptstyle(1) & \scriptstyle(2) \end{array}\right.$$

Both cases are impossible; this is seen modulo 3:

$$1 \equiv x^2 \mp 3^2 = 2\Box \pmod 3.$$

If $x^4 - 3^4 = 2p\Box$ we have one of the following cases:

$$\left\{\begin{array}{rc|c|c|c} x^2 - 3^2 = & \Box & 2\Box & p\Box & 2p\Box \\ x^2 + 3^2 = & 2p\Box & p\Box & 2\Box & \Box \\ & \scriptstyle(1) & \scriptstyle(2) & \scriptstyle(3) & \scriptstyle(4) \end{array}\right.$$

In (1) we have $(x, p) = (5, 17)$. Since $\nu(5^4 + 3^4) = \nu(2 \times 353) = 1$, $\nu(5^8 + 3^8) = \nu(2 \times 198593) = 1$ and $\nu(5^{16} + 3^{16}) = \nu(2 \times 97 \times 786757409) = 2$, we have only $(5, 2), (5, 3), (5, 4) \in T_3$.

In (2), x is odd, so $2 \equiv x^2 + 3^2 = p\Box \pmod 4$, which is impossible.

In (3), since $3 \nmid x$ we have $1 \equiv x^2 + 3^2 \equiv 2\Box \pmod 3$ and this is impossible.

(4) is also impossible.

The reader may wish to show, with the same method:

(3.4) $T_5 = \{(15, 2), (15, 3), (35, 2), (35, 3), (495, 2), (13, 2), (13, 3)\}$.

$$(3.5)\quad T_4 = \{(12,2),(12,3),(28,2),(28,3),(396,2),(5,2),(5,3)\}.$$

$$(3.6)\quad T_6 = \{(18,2),(18,3),(42,2),(42,3),(594,2),(8,2),(8,3),(10,2),(10,3),(10,4)\}.$$

$$(3.7)\quad T_{10} = \{(30,2),(30,3),(70,2),(70,3),(990,2),(26,2),(26,3)\}.$$

References

[1] W. Ljunggren, *Zur Theorie der Gleichung $x^2 + 1 = Dy^4$*, Avh. Norske Vid. Akad. Oslo 1942, no. 5, 27 pp.

[2] —, *Some remarks on the diophantine equations $x^2 - Dy^4 = 1$ and $x^4 - Dy^2 = 1$*, J. London Math. Soc. 41 (1965), 42–44.

[3] P. Ribenboim, *Catalan's Conjecture*, Academic Press, Boston, 1994.

[4] —, *Fermat's Last Theorem for Amateurs*, Springer, New York, 1999.

[5] —, *Pell numbers: squares and cubes*, Publ. Math. Debrecen 54 (1999), 131–152.

[6] —, *My Numbers, My Friends* (Chapter 1: The Fibonacci numbers and the Arctic Ocean), Springer, New York, 2000.

[7] —, *Solving infinite families of systems of Pell equations with binary recurring sequences*, preprint, 2001.

[8] P. Samuel, *Résultats élémentaires sur certaines équations diophantiennes*, preprint, 2000.

Department of Mathematics and Statistics
Queen's University
Kingston, Ontario
Canada K7L 3N6

Received on 20.2.2001
and in revised form on 8.6.2001 (3980)