On the diophantine equation \( x^2 - p^m = \pm y^n \)

by

YANN BUGEAUD (Strasbourg)

1. Introduction. In all what follows, we denote by \( \mathbb{N} \) the set of strictly positive integers. Let \( p \) be an odd prime number, and let \( D \) be a non-power integer with \( D > 1 \) and \( \gcd(p, D) = 1 \). Toyoizumi [16] and Maohua Le [10] (see also [11]) studied the number of solutions of the diophantine equation

\[
  x^2 + D^n = p^m, \quad x, m, n \in \mathbb{N}.
\]

More precisely, Maohua Le [10] proved that if \( \max\{p, D\} \) is larger than an explicit constant, then equation (1) has at most two solutions, except when, for a positive integer \( a \), we have \( D = 3a^2 + 1 \) and \( p = 4a^2 + 1 \). In the latter case, there are at most three solutions, including the trivial one \((x, m, n) = (a, 1, 1)\). Further, he gave [9] an analogous result for the diophantine equation \( x^2 - D^n = p^m \). His method being essentially ineffective, Maohua Le does not obtain computable upper bounds for the solutions of equation (1).

In this work, we deal with a generalization of equation (1), namely, we study the diophantine equation

\[
  x^2 \pm y^n = p^m, \quad x, y, m, n \in \mathbb{N}, \quad \gcd(p, y) = 1.
\]

We show that, under some not very restrictive conditions, (2) has only finitely many solutions \((x, y, m, n)\), and we provide a small explicit upper bound for \( n \) which only depends on \( p \).

As in [1], where the author investigated the diophantine equation \( x^2 - 2^m = \pm y^n \) (see also the work of Yongdong Guo & Maohua Le [4]), the proofs mainly depend on the sharp estimates for linear forms in two logarithms in archimedean and non-archimedean metrics, due to Laurent, Mignotte & Nesterenko [8] and Bugeaud & Laurent [2], respectively.

2. Statement of the results. Let \( p \) be an odd prime number. In this work, we consider the diophantine equations

\[
  x^2 - p^m = y^n, \quad x, y, m, n \in \mathbb{N}, \quad \gcd(x, y) = 1, \quad n \geq 3,
\]

\[213\]
and
\[(4) \quad x^2 + y^n = p^m, \quad x, y, m, n \in \mathbb{N}, \gcd(x, y) = 1, \quad n \geq 3.\]

We state our main result, depending only on the value of \( p \) modulo 4, in the following two theorems.

**Theorem 1.** If \( p \equiv 3 \mod 4 \), then (3) and (4) have only finitely many solutions \((x, y, m, n)\). Moreover, those solutions satisfy
\[n \leq 4.5 \cdot 10^6 p^2 \log^2 p \quad \text{and} \quad n \leq 5.6 \cdot 10^5 p^2 \log^2 p,
\]
respectively.

**Theorem 2.** If \( p \equiv 1 \mod 4 \), then (3) and (4) have only finitely many solutions \((x, y, m, n)\) with even \( m \) or odd \( y \). Moreover, those solutions satisfy
\[n \leq 4.5 \cdot 10^6 p^2 \log^2 p \quad \text{and} \quad n \leq 5.6 \cdot 10^5 p^2 \log^2 p,
\]
respectively.

**Remarks.** The main interest of Theorems 1 and 2 is the small size of the upper bound for \( n \). Indeed, if we apply a theorem of Shorey, Van der Poorten, Tijdeman & Schinzel [15, Theorem 2], we can also show that there exists some effective constant \( c_0(p) \), depending only on \( p \), such that \( n < c_0(p) \) for any solution \((x, y, m, n)\) of (3) or (4). However, their result does not provide an explicit value for \( c_0(p) \), which has to be very large, in view of the method of proof.

The hypothesis \( n \geq 3 \) in the statement of equations (3) and (4) cannot be replaced by \( n \geq 2 \). Indeed, \(( p^m + 1)/2 - p^m = ((p^m - 1)/2)^2 \) for any positive integer \( m \), and, furthermore, it is well known (see e.g. Hardy & Wright [5, Theorem 366]) that \( p^m \) (resp. \( p^{2m} \)) is the sum of two squares if \( p \equiv 1 \mod 4 \) (resp. \( p \equiv 3 \mod 4 \)).

In the course of the proof of Theorems 1 and 2, we need some information about prime powers in binary recurrence sequences with integer roots. To this end, we state the following result.

**Theorem 3.** Let \( p \) be a prime number. Let \( a := a_1/a_2 \) and \( b := b_1/b_2 \) be two irreducible rational numbers satisfying \( v_p(a) = v_p(b) = 0 \) and put \( A := \max\{a_1, a_2, b_1, b_2, 3\} \). Consider the diophantine equation
\[(5) \quad p^m = ax^n + by^n, \quad x, y, m, n \in \mathbb{N}, \gcd(x, y) = 1, \quad n \geq 2.
\]
Then \( n \leq 34000 p \log p \log A \).

**3. Auxiliary results**

**Lemma 1.** The equation \( x^2 - y^n = \pm 1 \) has no solution with \( y > 2 \) and \( n \geq 2 \).

**Proof.** See Chao Ko [6].
The diophantine equation $x^2 - p^m = \pm y^n$

For any integer $x$, we denote by $P[x]$ the greatest prime factor of $x$.

**Lemma 2.** Let $a$, $b$, $x$, and $y$ be non-zero integers with $\gcd(x, y) = 1$. Put $X = \max\{|x|, |y|\}$. For any integer $n \geq 3$, there exist effectively computable constants $c_1$ and $X_1$ such that

$$P[ax^2 + by^n] \geq c_1 (\log \log X \log \log \log X)^{1/2} \quad \text{whenever} \quad X \geq X_1.$$

**Proof.** This is a particular case of a theorem due to Kotov [7].

The next lemma is very close to Lemma 6 of Maohua Le [12]. For similar results, we refer the reader to [14].

**Lemma 3.** Let $d > 1$ be a squarefree integer, and let $k$ be a positive odd integer, coprime to $d$. Denote by $\varrho > 1$ the fundamental unit of the field $\mathbb{Q}(\sqrt{d})$. If $X$, $Y$ and $Z$ are three positive integers satisfying

$$X^2 - dY^2 = \pm kZ,$$

then there exist positive integers $a$, $b$, $t$ and $v$, with $a \equiv b \mod 2$ and $a$ and $b$ even if $d \not\equiv 1 \mod 4$, such that

$$X + Y\sqrt{d} = \varrho - t\left(\frac{a + b\sqrt{d}}{2}\right)^v.$$

Moreover, $0 < t \leq v$ and the integer $Z/v$ divides $h_d$, the class number of the field $\mathbb{Q}(\sqrt{d})$.

**Proof.** For any $\alpha$ in $\mathbb{Q}(\sqrt{d}) =: \mathbb{K}$, we denote by $[\alpha]$ the principal ideal of $\mathbb{K}$ generated by $\alpha$. We infer from $\gcd(k, d) = 1$ that $\gcd([X - \sqrt{d}], [X + \sqrt{d}])$ divides $[2]$. Moreover, $\gcd([X - \sqrt{d}], [X + \sqrt{d}]) = [1]$, since $k$ is assumed to be odd. Working in $\mathbb{K}$, we have the following equalities between ideals:

$$[X - \sqrt{d}] \cdot [X + \sqrt{d}] = [k]^2 = (a\overline{a})^2,$$

where $a$ is an integer ideal in $\mathbb{K}$ and $\overline{\cdot}$ denotes the Galois transformation $\sigma : \sqrt{d} \rightarrow -\sqrt{d}$. There exist $Z_1$ and an algebraic integer $\alpha$ in $\mathbb{K}$ such that $Z_1 | h_d$ and $\alpha Z_1$ is the principal ideal generated by $\alpha$. Thus, putting $v = Z/Z_1$, we have

$$X + Y\sqrt{d} = \eta\alpha^v \quad \text{and} \quad X - Y\sqrt{d} = \varpi\overline{\alpha}^\nu,$$

where $\eta$ is a unit in $\mathbb{K}$.

Put $\omega = \sqrt{d}$ if $d \not\equiv 1 \mod 4$ and $\omega = (1 + \sqrt{d})/2$ otherwise and recall that $\mathbb{Z}[\omega]$ is the ring of integers of $\mathbb{K}$. Modifying $\alpha$ if necessary, we can assume that $\eta = \varrho^{-t}$, with $0 < t \leq v$. Thus we get

$$X + Y\sqrt{d} = \varrho^{-t}\left(\frac{a + b\sqrt{d}}{2}\right)^v,$$
where \( a \) and \( b \) are two integers satisfying \( a \equiv b \mod 2 \) and \( a \) and \( b \) are even if \( d \neq 1 \mod 4 \). From \( X + Y\sqrt{d} > |X - Y\sqrt{d}| \) and \( q^{-1} < q \), we infer that
\[
a + b\sqrt{d} > |a - b\sqrt{d}|
\]
Hence \( a \) and \( b \) are positive, and the lemma is proved.

**Lemma 4.** Let \( p \) be an odd prime. Denote by \( h_p \) and \( R_p \) the class number and the regulator of the quadratic field \( \mathbb{Q}(\sqrt{p}) \). Then we have the upper bounds
\[
h_p \leq 0.5p^{1/2} \quad \text{and} \quad 0.4812 < R_p \leq h_p R_p \leq p^{1/2} \log(4p).
\]

**Proof.** We refer respectively to Maohua Le [13] and to Faisant [3], p. 199.

The next two propositions deal with lower bounds for linear forms in two logarithms. Let \( \alpha = \alpha_1 \) be a non-zero algebraic number with minimal defining polynomial \( a_0(X - \alpha_1) \ldots (X - \alpha_n) \) over \( \mathbb{Z} \). The logarithmic height of \( \alpha \), denoted by \( h(\alpha) \), is defined by
\[
h(\alpha) = \frac{1}{n} \log \left( \prod_{i=1}^{n} \max\{1, |\alpha_i|\} \right).
\]

For any prime number \( p \), let \( \overline{\mathbb{Q}}_p \) be an algebraic closure of the field \( \mathbb{Q}_p \) of \( p \)-adic numbers. We denote by \( v_p \) the unique extension to \( \overline{\mathbb{Q}}_p \) of the standard \( p \)-adic valuation over \( \mathbb{Q}_p \), normalized by \( v_p(p) = 1 \).

**Proposition 1.** Let \( p \) be a prime number. Let \( \alpha_1 \) and \( \alpha_2 \) be two algebraic numbers which are \( p \)-adic units. Denote by \( f \) the residual degree of the extension \( \mathbb{Q}_p \hookrightarrow \mathbb{Q}_p(\alpha_1, \alpha_2) \) and put \( D = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}] / f \). Let \( b_1 \) and \( b_2 \) be two positive integers and put
\[
A_u = \alpha_1^{b_1} - \alpha_2^{b_2}.
\]

Denote by \( A_1 > 1 \) and \( A_2 > 1 \) two real numbers such that
\[
\log A_i \geq \max\{h(\alpha_i), (\log p)/D\}, \quad i = 1, 2,
\]
and put
\[
b' = \frac{b_1}{D \log A_2} + \frac{b_2}{D \log A_1}.
\]

If \( \alpha_1 \) and \( \alpha_2 \) are multiplicatively independent, then we have the lower bound
\[
v_p(A_u) \leq \frac{24p(p^f - 1)}{(p - 1)(\log p)^4} D^4 \left( \max \left\{ \log b' + \log \log p + 0.4, \frac{10\log p}{D}, 5 \right\} \right)^2 \times \log A_1 \log A_2.
\]

**Proof.** This is Théorème 4 of [2] with the choice \((\mu, \nu) = (10, 5)\).

**Proposition 2.** Let \( \alpha_1 \geq 1 \) and \( \alpha_2 \geq 1 \) be two real algebraic numbers. Let \( b_1 \) and \( b_2 \) be two positive integers and put
\[
A_u = b_1 \log \alpha_1 - b_2 \log \alpha_2.
\]
The diophantine equation $x^2 - p^m = \pm y^n$

Set $D = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}]$ and denote by $A_1 > 1$ and $A_2 > 1$ two real numbers satisfying

$$\log A_i \geq \max\{h(\alpha_i), 1/D\}, \quad i = 1, 2.$$

Finally, put

$$b' = \frac{b_1}{D \log A_2} + \frac{b_2}{D \log A_1}.$$

If $\alpha_1$ and $\alpha_2$ are multiplicatively independent, then we have the lower bound

$$\log |A_u| \geq -32.31 D^4 (\max\{\log b' + 0.18, 0.5, 10/D\})^2 \log A_1 \log A_2.$$

Proof. This is Corollaire 2 of [8], where the numerical constants are given in Tableau 2 and correspond to the choice $h_2 = 10$. Notice that the hypotheses of the proposition imply that $h(\alpha_i) \leq \log |\alpha_i|/D$.

4. Proof of Theorem 3. Let $(x, y, m, n)$ be a solution of (5). Without loss of generality, we may suppose that $|y| \geq |x|$ and we set $Y := |y|$.

First, we make the assumption $p^m \geq Y^{n/1.4}$, whence

$$1.4m \log p \geq n \log Y.$$

Putting

$$A_u := \frac{p^m}{ay^n} = \left(\frac{x}{y}\right)^n - \frac{b}{a},$$

we have $v_p(A_u) = m$. In order to bound $m$, we apply Proposition 1 to (7) with the parameters

$$\alpha_1 = x/y, \quad \alpha_2 = -b/a, \quad b_1 = n, \quad b_2 = 1, \quad f = D = 1.$$

Since $p \geq 2$ and $Y \geq 2$ we see that we can take

$$\log A_1 = \frac{\log Y}{\log 2} \log p, \quad \log A_2 = 2 \frac{\log p}{\log 2} \log A,$$

and we have

$$b' \leq e^{-0.4} n/(\log p \log A)$$

provided that

$$n \geq 4 \log A.$$

Assuming that $\alpha_1$ and $\alpha_2$ are multiplicatively independent, we get

$$m \leq 100p(\log p)^{-2} \log Y \log A \max\left\{10 \log p, \log \frac{n}{\log A}\right\}^2,$$

whence, by (6),

$$\frac{n}{\log A} \leq 140 \frac{p}{\log p} \max\left\{10 \log p, \log \frac{n}{\log A}\right\}^2.$$
From (9), we deduce the upper bound
\begin{equation}
(10) \quad n \leq 34000p \log p \log A.
\end{equation}

The estimate (10) remains true if \(\alpha_1\) and \(\alpha_2\) are multiplicatively dependent. Indeed, in the latter case, there exist rational integers \(x' > 0, y' > 0, u > 0\) and \(v\) such that \(x = x'^u, y = y'^u\) and \(-b/a = (x'/y')^v\). Hence, we infer from (5) that
\begin{equation*}
\frac{p^m}{ax^uy^{un-v}} = \left(\frac{x'}{y'}\right)^{un-v} - 1,
\end{equation*}
and we conclude as before, using Proposition 1 together with \(1.4m \log p \geq nu \log |y'|\).

We now make the assumptions \(p^m \leq Y^{n/1.4}\) and
\begin{equation}
(11) \quad n \geq 500 \log A.
\end{equation}

Putting
\begin{equation}
(12) \quad A_a := \frac{p^m}{b'y^n} = \frac{a}{b} \left(\frac{x}{y}\right)^n + 1,
\end{equation}
we have
\begin{equation}
(13) \quad \log |A_a| \leq -(2n/7) \log Y - \log |b| \leq -(2n/7) \log Y + \log A
\end{equation}
and we deduce from (11) that \(|A_a| \leq 1/2000\). Hence, by (12), we get
\begin{equation}
(14) \quad \left| n \log \frac{y}{x} - \log \frac{-b}{a} \right| \leq \log(1 - A_a) \leq 1.001|A_a|.
\end{equation}

Applying Proposition 2 to the left-hand side of (14) with the parameters
\begin{equation*}
\alpha_1 = |y/x|, \quad \alpha_2 = |a/b|, \quad b_1 = n, \quad b_2 = 1, \quad \log A_1 = \log Y, \quad \log A_2 = 2 \log A, \quad b' = \frac{n}{2 \log A} + \frac{1}{\log Y} \leq \frac{n}{\log A},
\end{equation*}
we obtain
\begin{equation}
(15) \quad \log |A_a| \geq -0.002 - 32.31 \max \left\{ \log \frac{n}{\log A} + 0.18, 10 \right\}^2 \log A^2 \log Y,
\end{equation}
provided that \(\alpha_1\) and \(\alpha_2\) are multiplicatively independent and \(|\alpha_2| \geq 1\). However, it is easily seen that (15) remains true if one of the latter conditions is not fulfilled. Consequently, subject to the condition (11), we use (13) to get
\begin{equation*}
n \leq 227 \max \left\{ \log \frac{n}{\log A} + 0.18, 10 \right\}^2 \log A + 7 \log A,
\end{equation*}
hence
\begin{equation}
(16) \quad n \leq 24000 \log A.
\end{equation}
Finally, by (8), (10), (11) and (16), we obtain \( n \leq 34000p \log p \log A \), as claimed.

5. Proof of Theorems 1 and 2. The proofs of both Theorems 1 and 2 run parallel. Lemma 1 shows that equations (3) and (4) have no solution \((x, y, m, n)\) with \(y = 1\). Thus, in all this section, we assume that \(y\) is at least 2.

\(\star\) The case \(m\) even. Let \((x, y, m, n)\) be a solution of (3) or (4) with \(m\) even. Thus we have
\[
(x + p^{m/2})(x - p^{m/2}) = \pm y^n,
\]
and, since \(\gcd(x + p^{m/2}, x - p^{m/2})\) divides 2, we get
\[
\begin{align*}
 x + p^{m/2} &= a_1d_1^n, \\
 x - p^{m/2} &= a_2d_2^n,
\end{align*}
\]
where \(a_1, a_2, d_1\) and \(d_2\) are rational numbers satisfying \(|a_1|, |a_2| \in \{1/2, 1, 2\}, \ |a_1a_2| = 1\) and \(\gcd(d_1, d_2) = 1\). From (17) we deduce that
\[
p^{m/2} = \frac{a_1}{2}d_1^n - \frac{a_2}{2}d_2^n,
\]
and, applying Theorem 2 with \(A = 4\), we get the bound \(n \leq 48000p \log p\), which proves the last parts of Theorems 1 and 2 when \(m\) is even.

\(\star\) The case \(m\) odd. Observe that if \(p \equiv 3 \mod 4\) and if \((x, y, m, n)\) is a solution of equation (3) or (4), then \(x^2 - p^m\) is equal to 1 or 2 modulo 4. Hence, \(y\) cannot be even, and, in order to complete the proof of Theorems 1 and 2, we may assume that \(y\) is an odd integer.

- An upper bound for \(m\) valid for the solutions of (3) and (4). Let \((x, y, m, n)\) be a solution of (3) or (4) with odd \(m\). Denote by \(\varrho (> 1)\) the fundamental unit of the field \(\mathbb{Q}(\sqrt{p})\) and by \(h_p\) and \(R_p := \log \varrho\) its class number and regulator, respectively. By Lemma 3, there exist an algebraic integer \(\varepsilon := a + b\sqrt{p}\) in \(\mathbb{Q}(\sqrt{p})\) and positive integers \(t\) and \(v\) such that \(0 < t \leq v\) and
\[
\begin{align*}
 x + p^{(m-1)/2}\sqrt{p} &= \varepsilon^v \varrho^{-t}, \\
 x - p^{(m-1)/2}\sqrt{p} &= \overline{\varepsilon}^v (\overline{\varrho})^t,
\end{align*}
\]
where \(\overline{\varepsilon}\) denotes the conjugate of \(\varepsilon\) over \(\mathbb{Q}\) and \(\tau \in \{\pm 1\}\) is the norm of \(\varrho\). Moreover,
\[
 v \text{ divides } n \quad \text{and} \quad n \text{ divides } h_p v.
\]
From the system (18) we deduce the equation
\[
2p^{(m-1)/2}\sqrt{p} = \varepsilon^v \varrho^{-t} - \overline{\varepsilon}^v (\overline{\varrho})^t,
\]
and we put
\[(21) \quad A_u := (\varepsilon/\varepsilon)^v - (\tau \varrho^2)^t.\]

Since \(\varepsilon/\varepsilon\) is a root of the irreducible polynomial \(\varepsilon X^2 - (\varepsilon^2 + \varepsilon^2)X + \varepsilon \varepsilon\), we have \(h(\varepsilon/\varepsilon) = \log \varepsilon\) and \(\varepsilon/\varepsilon\) is not a unit. Thus \(\varepsilon/\varepsilon\) and \(\tau \varrho^2\) are multiplicatively independent algebraic numbers, which, moreover, are \(p\)-adic units, since \(\gcd(x, y) = 1\). By (20), we have \(v_p(A_u) = m/2\). In order to bound \(m\), we apply Proposition 1 to (21) with the following parameters:

\[\alpha_1 = \varepsilon/\varepsilon, \quad \alpha_2 = \tau \varrho^2, \quad b_1 = v, \quad b_2 = t, \quad p = 2, \quad D = 2, \quad f = 1.\]

Using Lemma 4 and the upper bound \(\log \sqrt{p} \leq 1.54 \log \varepsilon\) deduced from Lemma 3 (the worst case occurs for \(p = 13\) and \(\varepsilon = (1 + \sqrt{13})/2\)), we see that we can set

\[\log A_1 = 1.54 \log \varepsilon, \quad \log A_2 = \frac{R_p \log p}{0.96} \quad \text{and} \quad b' = \frac{t}{3.08 \log \varepsilon} + \frac{0.48v}{R_p \log p}.\]

Thus, by Proposition 1 and the estimate \(b' \leq 2v/\log p\), we get
\[(22) \quad m \leq 1232p(\log p)^{-3}R_p \max\{\log v + 1.1, 5 \log p\}^2 \log \varepsilon.\]

• The case of equation (4). The result is clearly true if \(m = 1\), thus we assume \(m \geq 3\). From (18), we infer that \(\varepsilon^v \varrho^{-t} \leq 2p^{m/2}\), whence
\[2v \log \varepsilon \leq 2t \log \varrho + \log 4 + m \log p.\]

Together with (22), it yields
\[(23) \quad 2vm \leq 1232p(\log p)^{-3}R_p (m \log p + \log 4 + 2tR_p) \times \max\{\log v + 1.1, 5 \log p\}^2.\]

From \(p^m > y^n \geq 2^n\) and (19), we deduce that
\[\frac{t}{m} \leq \frac{v}{m} \leq \frac{n}{m} \leq \frac{\log p}{\log 2},\]

hence, using (23) and \(m \geq 3\), we get
\[v \leq 616p(\log p)^{-3}R_p \left(\log p + \frac{\log 4}{3} + \frac{2}{\log 2}R_p \log p\right) \max\{\log v + 1.1, 5 \log p\}^2\]

and
\[(24) \quad v \leq 1778p(\log p)^{-2}R_p (R_p + 0.5) \max\{\log v + 1.1, 5 \log p\}^2.\]

Assume first that \(\max\{\log v + 1.1, 5 \log p\} = 5 \log p\). Then we infer from (19) and (24) that
\[n \leq 4450p h_p R_p (R_p + 0.5),\]

and, using \(p \geq 3\) and the upper bounds for \(R_p\) and \(h_p R_p\) given by Lemma 4, we obtain
\[(25) \quad n \leq 2.6 \cdot 10^5 p^2 \log^2 p.\]
The diophantine equation $x^2 - p^m = \pm y^n$

Assume now that $\max\{\log v + 1.1, 5\log p\} = \log v + 1.1$. In order to get a better bound for $n$, we treat separately the smallest two values of $p$. Hence, suppose that $p \not\in \{3, 5\}$, and search an upper bound for $v$ of the shape $v \leq \gamma p R_p (R_p + 0.5)$, with a suitable constant $\gamma$. Since $p \geq 7$, we see that $\gamma$ must satisfy the inequality $\gamma \geq 470(\log \gamma + 7.46)^2$. Thus, we may choose $\gamma = 1.8 \cdot 10^5$ and, using (19) and the upper bounds for $R_p$ and $h_p R_p$ given by Lemma 4, we get

$$n \leq 5.6 \cdot 10^5 p^2 \log^2 p.$$  

Finally, we easily see that (26) remains true for $p \in \{3, 5\}$ and it follows from (25) and (26) that (24) leads to the bound

$$n \leq 5.6 \cdot 10^5 p^2 \log^2 p,$$

as claimed.

- The case of equation (3). Dividing (19) by $\varepsilon^\varrho^{-t}$, we obtain

$$\frac{2p^{(m-1)/2} \sqrt{p}}{\varepsilon^\varrho^{-t}} = \frac{2p^{(m-1)/2} \sqrt{p}}{x + p^{(m-1)/2} \sqrt{p}} = 1 - \left(\frac{\tau}{\varepsilon}\right)^{v} (\tau \varrho^2)^t =: A_a.$$  

If $A_a \geq 1/2$, then we have $4p^{(m-1)/2} / \sqrt{p} \geq \varepsilon^\varrho^{-t}$ and

$$2v \log \varepsilon - 2t \log \varrho \leq m \log p + \log 16.$$  

Otherwise $A_a < 1/2$ and we get

$$|\log(1 - A_a)| \leq 2A_a.$$  

We apply Proposition 2 to the linear form

$$\left|v \log \frac{\varepsilon}{\varrho} - t \log (\varrho^2)\right| \leq \left|v \log \left(\frac{\varepsilon}{\varrho}\right) - t \log (\tau \varrho^2)\right| \leq |\log(1 - A_a)|$$

with the following parameters:

$$\alpha_1 = |\varepsilon/\varrho|, \quad \alpha_2 = \varrho^2, \quad b_1 = v, \quad b_2 = t, \quad D = 2, \quad \log A_1 = \log \varepsilon, \quad \log A_2 = \log \varrho = R_p, \quad b' = \frac{t}{2 \log \varepsilon} + \frac{v}{2R_p}.$$  

It follows from Lemma 4 and $\varepsilon \geq (1 + \sqrt{13})/2$ that $b' \leq 1.64v$, and, using (29), we obtain

$$\log 2 + \log A_a \geq -517 R_p \max\{\log v + 0.68, 5\}^2 \log \varepsilon,$$

hence, by (27),

$$v \log \varepsilon - t \log \varrho \leq \log 4 + (m \log p)/2 + 517 R_p \max\{\log v + 0.68, 5\}^2 \log \varepsilon.$$  

From (22), (28) and (30) we infer that

$$v \log \varepsilon - t R_p \leq \log 4 + 517 R_p \max\{\log v + 0.68, 5\}^2 \log \varepsilon + 616p(\log p)^{-2} R_p \max\{\log v + 1.1, 5 \log p\}^2 \log \varepsilon.$$  

First, assume that $\varepsilon < \exp\{2R_p\}$. From (18), we get $\varepsilon^v \varrho^{-t} > y^n/2$, hence
\begin{equation}
(32)\quad v \log \varepsilon - t \log \varrho > (n \log y)/2.
\end{equation}
However, we have
\begin{equation}
(33)\quad \frac{\log \varepsilon}{\log y} \leq \frac{2R_p}{\log 3},
\end{equation}
since $y > 1$ is odd, and we deduce from (31), (32) and (33) that
\begin{equation*}
n \leq 2.6 + 1883R_p^2 \max\{\log n + 0.68, 5\}^2
+ 2243p(\log p)^{-2}R_p^2 \max\{\log n + 1.1, 5 \log p\}^2.
\end{equation*}
As before, we search an upper bound for $n$ of the shape $n \leq \gamma p^2 \log^2 p$. Using Lemma 4 and a few calculation, we show that it suffices that $\gamma$ satisfies
\begin{equation*}
\gamma \geq 0.3 + 3214\{\log \gamma + 3.1\}^2 + 9508\{\log \gamma + 3.5\}^2.
\end{equation*}
Thus, we can choose $\gamma = 4.5 \cdot 10^6$, which gives the bound
\begin{equation}
(34)\quad n \leq 4.5 \cdot 10^6 p^2 \log^2 p.
\end{equation}
Assume now that $\varepsilon \geq \exp\{2R_p\}$. Then we have
\begin{equation}
(35)\quad v \log \varepsilon - tR_p \geq (v \log \varepsilon)/2,
\end{equation}
since $t \leq v$. Using (31), (35) and the lower bound $\varepsilon \geq (1 + \sqrt{13})/2$, we get
\begin{equation*}
v \leq 3.4 + 1034R_p \max\{\log v + 0.68, 5\}^2
+ 1232p(\log p)^{-2}R_p \max\{\log n + 1.1, 5 \log p\}^2,
\end{equation*}
hence, by (19),
\begin{equation*}
n \leq 3.4h_p + 1034(h_pR_p) \max\{\log n + 0.68, 5\}^2
+ 1232p(\log p)^{-2}(h_pR_p) \max\{\log n + 1.1, 5 \log p\}^2
\end{equation*}
and it is easy to show that (34) also holds in this case. Hence, the last statements of Theorems 1 and 2 are proved.

Now, in order to complete the proofs of Theorems 1 and 2, it suffices to apply Lemma 2 to the polynomials $x^2 \pm y^n$, where $3 \leq n \leq 4.5 \cdot 10^6 p^2 \log^2 p$. 

References

The diophantine equation $x^2 - p^m = \pm y^n$


U.F.R. de mathématiques
Université Louis Pasteur
7, rue René Descartes
67084 Strasbourg, France
E-mail: bugeaud@pari.u-strasbg.fr

Received on 28.5.1996
and in revised form on 12.9.1996 (2996)