ACTA ARITHMETICA
153.4 (2012)

On the system of Diophantine equations $a^2+b^2=(m^2+1)^r$ and $a^x+b^y=(m^2+1)^z$

by

Florian Luca (Morelia and Johannesburg)

1. Introduction. Given a triple (a,b,c) of positive integers, several authors have looked for positive integers (x,y,z) such that

$$a^x+b^y=c^z. \tag{1}$$

Mahler [11] proved that there are only finitely such triples (x,y,z). His method was ineffective. Gel'fond [6] used Baker's method to give an effective version of Mahler's result. Terai [15] (see also [4], [5], [8]) conjectured that with a few exceptions such as

$$1+2^3=3^2,\quad 2^5+7^2=3^4,\quad \text{and}\quad 2^p+(2^{p-2}-1)^2=(2^{p-2}+1)^2$$

for which also

$$1+2=3,\quad 2+7=3^2,\quad \text{and}\quad 2+(2^{p-2}-1)=2^{p-2}+1,$$

equation (1) has at most one positive integer solution (x,y,z) whenever (a,b,c) are relatively prime, a condition which we will assume throughout the paper. Many papers treated various particular cases, but the general conjecture remains open. The particular case in which there exists a solution with $(x,y)=(2,2)$ has received a lot of attention. In this case, Terai's conjecture amounts to the statement that if $r\ge 2$ is some integer and m and n are coprime positive integers of different parities, then writing

$$A+Bi=(m+in)^r\qquad (i=\sqrt{-1}), \tag{2}$$

the equation

$$a^x+b^y=(m^2+n^2)^z$$

with $(a,b)=(|A|,|B|)$ has only the solution $(x,y,z)=(2,2,r)$. The case when $r=2$ was conjectured by Jeśmanowicz [7].

2010 *Mathematics Subject Classification*: Primary 11D61.
Key words and phrases: exponential Diophantine equation, Terai conjecture, applications of linear forms in logarithms of algebraic numbers.

DOI: 10.4064/aa153-4-3

Many authors have proved the above conjecture in the special case when $n = 1$ and some additional conditions hold. For example, when $n = 1$, then the above conjecture has been verified for $r = 2$ in [10] and for $r \in \{3, 5\}$ in [5]. It has also been verified recently when r is congruent to one of 4, 5 or 6 modulo 8, except for a finite number of pairs (m, r) (see [9] and [13]), and when m and r satisfy certain inequalities.

Here, we show that for $n = 1$, there can only be finitely many pairs (m, r) which fail the above conjecture. Furthermore, they are all effectively computable. We recall that in this case

$$A + Bi := (m + i)^r. \tag{3}$$

Also, since n and m should be of different parities in (2) and $n = 1$, the number m is even. Our result is the following.

THEOREM 1. *Let $m \geq 2$ be an even integer and $r \geq 1$ be an integer. Let A and B be as in* (3) *and set $a := |A|$ and $b := |B|$. Then equation* (1) *with $c := m^2 + 1$ admits a solution $(x, y, z) \neq (2, 2, r)$ only in finitely many instances (m, r). Moreover, there exists a computable constant c_0 such that all such solutions satisfy* $\max\{m, r, x, y, z\} \leq c_0$.

Throughout the paper, we write $c_0, c_1, \ldots$ for computable constants which are absolute. We also use the Landau symbols O and o as well as the Vinogradov symbols $\ll$, $\gg$, $\asymp$ and $\sim$ with their regular meaning. Recall that $F = O(G)$, $F \ll G$ and $G \gg F$ are all equivalent and mean that the inequality $|F| < cG$ holds with some constant c. Moreover, $F \asymp G$ means that both $F \ll G$ and $G \ll F$ hold, whereas $F \sim G$ and $F = o(G)$ mean that F/G tends to 1 and 0, respectively. The constants implied by the above Landau and Vinogradov symbols in our arguments are effective.

2. Tools. Our main tools are linear forms in complex and p-adic logarithms. Recall that for a nonzero algebraic number η whose minimal polynomial over the integers is

$$F(X) := a_0 \prod_{i=1}^{d} (X - \eta^{(i)}) \in \mathbb{Z}[X],$$

its *logarithmic height* is defined as

$$h(\eta) := \frac{1}{d}\Big(\log a_0 + \sum_{i=1}^{d} \log \max\{1, |\eta^{(i)}|\}\Big).$$

For us, η will be either in $\mathbb{Q}$ or in $\mathbb{Q}(i)$. If $\eta := u/v$ with coprime integers u and v, then

$$h(\eta) = \log(\max\{|u|, |v|\}),$$

whereas if $\eta := (u+iv)/w \in \mathbb{Q}(i)$, where u, v, w are integers satisfying $\gcd(u, v, w) = 1$, then

$$h(\eta) \le \log(\max\{w, \sqrt{u^2+v^2}\}).$$

Let η_1 and η_2 be nonzero elements of $\mathbb{Q}(i)$, and b_1 and b_2 be integers. Put $B := \max\{3, |b_1|, |b_2|\}$ and $A_i := \max\{1, h(\eta_i)\}$ for $i = 1, 2$. Put also

$$\Lambda := \eta_1^{b_1}\eta_2^{b_2} - 1. \tag{4}$$

The following result is a simplified version of a lower bound for a linear form in logarithms of algebraic numbers (see [12], for example).

LEMMA 2. *With the above notation, there exists a constant c_1 such that if $\Lambda \ne 0$, then*

$$\log|\Lambda| > -c_1 A_1 A_2 \log B. \tag{5}$$

The above statement is interesting only when $|\Lambda|$ is small. Putting

$$\Gamma := b_1 \log \eta_1 + b_2 \log \eta_2,$$

where log stands for any determination of the logarithm, and using the fact that $|\Lambda| = |e^{\Gamma} - 1| \asymp |\Gamma|$ for $|\Gamma|$ small (say $|\Gamma| < 1/2$), it follows that estimate (5) holds with Λ replaced by Γ assuming that $\Gamma \ne 0$ (and with some appropriate constant c_1). In what follows, we shall use inequality (5) with either Γ or Λ.

We now move on to linear forms in p-adic logarithms. Let q be a prime either in $\mathbb{Z}$ or in $\mathbb{Z}[i]$. As a matter of convention, we write $q = p$ when we mean that $p \in \mathbb{Z}$, and $q = \pi$ to mean that q is a prime in $\mathbb{Z}[i]$ which is not associated to a prime in $\mathbb{Z}$. In this last case, $|\pi|^2 = p$ is a prime in $\mathbb{Z}$ which is a multiple of π as an element of $\mathbb{Z}[i]$. For a nonzero r in $\mathbb{Q}(i)$ we write $v_q(r)$ for the exponent of q in the factorization of r. The following is a simplified version of the classical lower bound for linear forms in p-adic logarithms (see [16], for example).

LEMMA 3. *Assume that η_1 and η_2 are in $\mathbb{Q}$ and $q = p \in \mathbb{Z}$. There exists a constant c_2 such that if $\Lambda \ne 0$, then*

$$v_q(\Lambda) < c_2 p A_1 A_2 \log B.$$

Somewhat better inequalities are due to Bugeaud [2] and Bugeaud and Laurent [3]. To formulate these bounds, let again η_1 and η_2 be rational or in $\mathbb{Q}(i)$. Let q be a prime in $\mathbb{Z}$ or in $\mathbb{Z}[i]$. Assume that g and E are positive integers such that

$$v_q(\eta_1^g - 1) \ge E \quad \text{and} \quad v_q(\eta_2^g - 1) > 0. \tag{6}$$

Under condition (6), Bugeaud and Bugeaud and Laurent proved:

Lemma 4.

(i) *Assume that* η_1 *and* η_2 *are multiplicatively independent rational numbers and* $q = p \in \mathbb{Z}$. *Assume further that* $H_i \ge \max\{h(\eta_i), E \log p\}$ *for* $i = 1, 2$. *Then there exists a constant* c_3 *such that if* $\Lambda \neq 0$, *then*

$$v_q(\Lambda) < c_3 \frac{g}{E^3 (\log p)^4} (\max\{\log B, E \log p\})^2 H_1 H_2. \tag{7}$$

(ii) *Assume that* η_1 *and* η_2 *are multiplicatively independent in* $\mathbb{Q}(i)$ *and* $q = \pi \in \mathbb{Z}[i]$ *is a prime of norm* $p = |\pi|^2$. *Then* (7) *holds with* $E = 1$, *the corresponding value of* g, *and an appropriate constant* c_3.

3. The proof. We proceed in several stages.

3.1. Eliminating degenerate cases

Lemma 5. *Every positive integer solution* (m, r, x, y, z) *satisfies the following conditions:*

(i) a *and* b *are coprime;*
(ii) $r \ge 2$;
(iii) $z > r/2$, *in particular,* $z \ge 2$;
(iv) $a \ge 2$ *and* $b \ge 2$;
(v) $x \neq y$.

Proof. (i) If a and b are not coprime, let p be any of their common prime factors. By (3), we get $p \mid (m+i)^r$. If $p > 2$, then p is squarefree in $\mathbb{Z}[i]$, so $p \mid m + i$. This is impossible because $p \nmid 1$. If $p = 2$, then $2 \mid (m+i)^r$, and taking norms in $\mathbb{Z}[i]$ we see that $4 \mid (m^2+1)^r$, which is false because m is even. Hence, a and b are coprime.

(ii) Assume that $r = 1$. Then $(a, b) = (m, 1)$. In this case, equation (1) becomes

$$m^x + 1 = (m^2+1)^z. \tag{8}$$

Since $(x, y, z) \neq (2, 2, 1)$, we must have $z > 1$, and clearly $x > 1$. However, (8) has no positive integer solutions $m \ge 2$, $x \ge 2$, $z \ge 2$ by known results on the Catalan equation.

(iii) Observe that

$$c^z = a^x + b^y \ge a + b > \sqrt{a^2 + b^2} = c^{r/2},$$

so that $z > r/2$. In particular, $z > 1$ by (ii) above.

(iv) Observe first that if we put $\alpha := m + i$ and $\beta := m - i$, then

$$A = \frac{\alpha^r + \beta^r}{2} \quad \text{and} \quad B = \frac{\alpha^r - \beta^r}{\alpha - \beta}.$$

Furthermore, $\alpha+\beta=2m$ and $\alpha\beta=m^2+1$ are coprime. Moreover,

$$\frac{\alpha}{\beta}=\frac{m+i}{m-i}=\frac{m^2-1}{m^2+1}+i\frac{2m}{m^2+1}$$

is not a root of unity because the only roots of unity in $\mathbb{Z}[i]$ are ± 1 and $\pm i$, and neither $(m^2-1)/(m^2+1)$ nor $2m/(m^2+1)$ is zero.

Hence, $B=u_r$ is the rth member of the Lucas sequence with roots (α,β). This Lucas sequence is nondegenerate. Furthermore, $A=u_{2r}/(2u_r)$. Assume now that either $a=1$ or $b=1$. Then either $u_r=\pm 1$, or $u_{2r}=\pm 2u_r$. In particular, either u_r has no prime factors, or every prime factor of u_{2r} divides u_r, or 2 divides the discriminant $\Delta:=(\alpha-\beta)^2=-4$ of our sequence. By the Primitive Divisor Theorem of Bilu, Hanrot and Voutier [1], this is possible only if $r\in\{2,3,4,6\}$, or if the triple $(r,m+i,m-i)$ belongs to a finite list of triples all of which can be found in Table 1 of [1]. A quick look at that table convinces one that no pair (α,β) of roots in that table belongs to $\mathbb{Q}(i)$. Thus, $r\in\{2,3,4,6\}$. For these r, we compute a and b to get

$$(a,b)=(m^2-1,2m),\ (m^3-3m,3m^2-1),\ (m^4-6m^2+1,4m^3-4m),$$
$$(m^6-15m^4+15m^2-1,6m^5-20m^3+6m),$$

respectively, so $\min\{a,b\}$ is never 1, contrary to assumption.

(v) Assume that $x=y$. Let v_n be the nth term of the Lucas sequence of roots a and b. That is, $v_n:=(a^n-b^n)/(a-b)$ for all $n\geq 0$. This is nondegenerate since a and b are coprime and their ratio is not a root of unity. Then $c^r=a^2+b^2=v_4/v_2$ and $c^z=a^x+b^x=v_{2x}/v_x$. It is clear that $x\neq 1$, because $a+b$ is coprime to a^2+b^2. It is also clear that $x\neq 2$, for if $x=2$, then $(x,y,z)=(2,2,r)$. Hence, $x\geq 3$. All prime factors of v_{2x} are either prime factors of v_x, or of c, so in particular of v_4. Thus, v_{2x} has no primitive prime factors. This is impossible for $x\geq 4$ by Table 1 in [1]. Thus, $x=3$, but then $a^3+b^3=(a+b)(a^2+b^2-ab)$ is coprime to a^2+b^2, a contradiction. ∎

As a byproduct of Lemma 5(iii), we see that if $r_1:=\lceil r/2\rceil$, then

$$a^2+b^2\equiv a^x+b^y\equiv 0 \pmod{c^{r_1}}, \tag{9}$$

a congruence which we shall exploit later.

Note also that a is a multiple of m when r is odd, and b is a multiple of m when r is even. In particular, since m is even, a or b is even according to whether r is odd or even.

3.2. Upper bounds for x and y in terms of r and m. Here, we prove the following lemma.

Lemma 6. *We have*

$$\max\{x,y\}=O(r^3(\log m)^4)\quad \textit{and}\quad z=O(r^4(\log m)^4). \tag{10}$$

Proof. Assume that r is odd. Then a is even. Suppose first that $a^x < b^{y/2}$. Then

$$\Lambda := c^z b^{-y} - 1 = a^x b^{-y} < \frac{1}{b^{y/2}}.$$

Observe that $\Lambda > 0$. Taking logarithms, we get

$$y \log b < -2 \log \Lambda = O(\log c \log b \log(\max\{y, z\}))$$

by Lemma 2 with $\eta_1 := c$, $\eta_2 := b$, $b_1 := x$, and $b_2 := -y$. In our case, $B = \max\{|b_1|, |b_2|\} = \max\{x, y\}$. Thus,

$$y = O(\log c \log(\max\{y, z\})). \tag{11}$$

Observe that

$$(m^2 + 1)^z = a^x + b^y < 2b^y \le b^{y+1}.$$

Since

$$b = \left|\frac{\alpha^r - \beta^r}{2i}\right| \le \frac{|\alpha|^r + |\beta|^r}{2} = |\alpha|^r = (m^2 + 1)^{r/2},$$

we have

$$z \le (y + 1)\, \frac{\log b}{\log(m^2 + 1)} \le \frac{r(y + 1)}{2} \le ry. \tag{12}$$

We thus get, by (11) and (12),

$$y = O(\log(m^2 + 1) \log(ry)) = O(\log m \log(ry)). \tag{13}$$

We now distinguish the cases $y \le r$ and $r \le y$. In case $r \le y$, (13) yields

$$y < c_4 \log m \log y \tag{14}$$

for some constant c_4 which we can assume to be larger than 10. It is well known that for $A > 3$,

$$\frac{y}{\log y} < A \quad \text{implies} \quad y < 2A \log A. \tag{15}$$

Hence taking $A := c_4 \log m > 3$ and using (14) gives

$$y < 2c_4 \log m \log(c_4 \log m) = O((\log m)^2).$$

Since $r \ge 1$, we also have

$$y = O(r(\log m)^2). \tag{16}$$

All this was in case $r \le y$. However, (16) also holds trivially when $y \le r$.

Since $a^x < b^{y/2}$, (16) yields

$$x < \frac{y \log b}{2 \log a} \le \frac{y \log b}{2 \log 2} \le \frac{yr \log(m^2 + 1)}{4 \log 2} = O(r^2(\log m)^3), \tag{17}$$

where we also used estimate (3.2) and Lemma 5(iv).

All this was under the assumption that $a^x < b^{y/2}$. Suppose now that $a^x > b^{y/2}$. Then

$$y < \frac{2\log a}{\log b} x \le \left(\frac{2\log(m^2+1)^{r/2}}{\log 2}\right) x = O(rx\log m). \tag{18}$$

Since

$$a^x = c^z - b^y = b^y(c^z b^{-y} - 1),$$

and b and c are odd, we get

$$\begin{aligned} x \le v_2(a^x) = v_2(c^z b^{-y} - 1) &= O(\log b \log c \log(\max\{y, z\})) \\ &= O(r(\log m)^2 \log(ry)). \end{aligned} \tag{19}$$

The middle estimate above follows from Lemma 3 with respect to the prime $p = 2$, where Λ is given by (3.2); we have also used (12). Comparing (19) and (18), we get

$$y = O(rx\log m) = O(r^2(\log m)^3 \log(ry)).$$

We now distinguish again the cases $y \le r$ and $r \le y$. In case $r \le y$, we have

$$y = O(r^2(\log m)^3 \log y),$$

and applying the argument from implication (15) we arrive at

$$y = O(r^2(\log m)^3(\log r + \log\log m)) = O(r^3(\log m)^4). \tag{20}$$

This obviously holds in the case $y \le r$ as well. Going back to (19), we get

$$x = O(r(\log m)^2(\log r + \log\log m)) = O(r^2(\log m)^3). \tag{21}$$

Comparing (16), (17), (20) and (21), we reach the first inequality of (10). The second follows from the first and (12).

The case of r even can be treated similarly. Namely, b is then even and we repeat the above argument with (a, x) and (b, y) interchanged. That is, we distinguish between the cases $b^y < a^{x/2}$ and $b^y > a^{x/2}$. We give no further details. ∎

3.3. A useful divisibility relation. Let p be any prime factor of $m^2 + 1$. Note that $p \ge 5$. Let $e_p := \mathrm{ord}_p(2)$ be the multiplicative order of 2 modulo p; that is, e_p is the minimal positive integer k such that $2^k \equiv 1 \pmod{p}$. Recall that $r_1 = \lceil r/2 \rceil$. With this notation, we have the following result.

LEMMA 7. *The following divisibility relations and estimates hold:*

(i) $2^{4(r-1)(x-y)} \equiv 1 \pmod{c}$;
(ii) $e_p \mid 4(r-1)(x-y)$;
(iii) $r = O(e_p(\log m)^3/(\log p)^3)$;
(iv) $r = O(m^2)$.

Proof. (i) We start with (9),

$$a^2+b^2\equiv a^x+b^y\equiv 0 \pmod{c^{r_1}}.$$

The first congruence implies that $a^4\equiv b^4 \pmod{c^{r_1}}$, so $a^{4x}\equiv b^{4x} \pmod{c^{r_1}}$; the second yields $a^{4x}\equiv b^{4y} \pmod{c^{r_1}}$. So, $b^{4x}\equiv b^{4y} \pmod{c^{r_1}}$. Since a, b and c are pairwise coprime, we conclude that

$$b^{4(x-y)}\equiv 1 \pmod{c^{r_1}}.$$

Observe that β divides c and $r\ge r_1$ (in fact, $r>r_1$ because $r\ge 2$ by Lemma 5(ii)). Hence, in $\mathbb{Z}[i]$, we have

$$\pm b=B=\frac{\alpha^r-\beta^r}{\alpha-\beta}\equiv\frac{(m-i+(2i))^r}{2i}\equiv(2i)^{r-1} \pmod{\beta}. \tag{22}$$

Thus,

$$b^{4(x-y)}\equiv 2^{4(r-1)(x-y)}\equiv 1 \pmod{\beta}.$$

The same argument applies with β replaced by α. Since α and β are coprime in $\mathbb{Z}[i]$ and their product is c, we get (i).

(ii) This is an immediate consequence of (i).

(iii) Observe that, as in (22), we have

$$\pm b=B=\frac{\alpha^r-\beta^r}{\alpha-\beta}\equiv\frac{\alpha^r}{2i} \pmod{\beta^r}.$$

Hence,

$$b^{4y}\equiv\frac{\alpha^{4ry}}{2^{4y}} \pmod{\beta^r}.$$

A similar argument shows that

$$a^{4x}\equiv\frac{\alpha^{4rx}}{2^{4x}} \pmod{\beta^r}.$$

Since $c^{r_1}\mid a^x+b^y\mid a^{4x}-b^{4y}$, we get

$$\frac{\alpha^{4rx}}{2^{4x}}\equiv\frac{\alpha^{4ry}}{2^{4y}} \pmod{\beta^{r_1}},$$

so $\alpha^{4r(x-y)}-2^{4(x-y)}\equiv 0 \pmod{\beta^{r_1}}$. Now let π be any prime factor of β in $\mathbb{Z}[i]$ and write $p=|\pi|^2$ for the corresponding prime factor of $c=m^2+1$ in $\mathbb{Z}$ such that $\pi\mid p$. We apply Lemma 4(ii) with $\eta_1:=\alpha$, $\eta_2:=2$, $E:=1$. It is clear that η_1 and η_2 are multiplicatively independent. Observe also that since $\alpha=\beta+2i\equiv 2i \pmod{\beta}\equiv 2i \pmod{\pi}$, we can take $g=4e_p$. Furthermore, $h(\eta_1)=O(\log m)$, $h(\eta_2)=O(1)$, and we can take $B:=4r(x+y)$. We get, by (7),

$$\begin{aligned} r/2\le r_1 &\le \Lambda_\pi(\alpha^{4r(x-y)}-2^{4(x-y)})\\ &=O\biggl(\frac{e_p(\max\{\log(r(x+y)),\log p\})^2\max\{\log m,\log p\}}{(\log p)^3}\biggr). \end{aligned}$$

Since $p \le m^2+1$, we have $\max\{\log m, \log p\} = O(\log m)$. Furthermore, by Lemma 6,

$$\log(r(x+y)) = O(\log r + \log\log(m+2)) = O(\log r + \log m).$$

Thus

$$r = O\biggl(\frac{e_p(\log m)(\log r+\log m)^2}{(\log p)^3}\biggr). \tag{23}$$

Since $e_p < p \le m^2+1$, we have $e_p/(\log p)^3 = O(m^2/(\log m)^3)$. Hence,

$$r = O\biggl(\frac{m^2(\log r+\log m)^2}{(\log m)^2}\biggr), \tag{24}$$

which implies that $r = O(m^2)$, so $\log r = O(\log m)$. Inserting this into (23), we get the desired upper bound (iii).

(iv) Follows immediately from (24). ∎

Lemma 7(iv) together with Lemma 6 shows that there are only finitely many computable possibilities for r, x, y, z once m is fixed. Thus, from now on, we assume that m is larger than any effectively computable number that will show up along the way. The goal is to close the loop and show that m must nevertheless be bounded by some computable number.

3.4. Some congruences modulo m. From now on, we assume that $m \ge 3$.

LEMMA 8. *Assume that r is odd. Then the following congruences hold:*

(i) *if $x = 1$, then*

$$r \equiv 0 \pmod{m}; \tag{25}$$

(ii) *if $x = 2$, then*

$$z + y\binom{r}{2} - r^2 \equiv 0 \pmod{m^2}; \tag{26}$$

(iii) *if $x \ge 3$, then*

$$z + y\binom{r}{2} \equiv 0 \pmod{m}. \tag{27}$$

Moreover, none of the integers appearing in the left-hand sides of (25)–(27) *is zero. When r is even, then* (i)–(iii) *hold with x and y interchanged, and with the same conclusion about nonzero left-hand sides.*

Proof. Suppose that r is odd. Then

$$\begin{aligned} A &= \frac{1}{2}((m+i)^r + (m-i)^r) = (-1)^{(r-1)/2}\biggl(rm - \binom{r}{3}m^3 + \cdots\biggr),\\ B &= \frac{1}{2i}((m+i)^r - (m-i)^r) = (-1)^{(r-1)/2}\biggl(1 - \binom{r}{2}m^2 + \cdots\biggr). \end{aligned} \tag{28}$$

Writing $a = \varepsilon A$ and $b = \eta B$, where $\varepsilon, \eta \in \{\pm 1\}$, we get, from (28),

$$
\begin{aligned}
a^x &= \varepsilon^x (-1)^{x(r-1)/2} m^x \left(r - \binom{r}{3} m^2 + \cdots \right)^x \equiv \varepsilon_1 m^x r^x \pmod{m^{x+2}},\\
b^y &= \eta^y (-1)^{y(r-1)/2} \left(1 - \binom{r}{2} m^2 + \cdots \right)^y \\
&\equiv \eta_1 \left(1 - y\binom{r}{2} m^2 \right) \pmod{m^4},\\
c^z &= (1+m^2)^z \equiv 1 + zm^2 \pmod{m^4},
\end{aligned} \tag{29}
$$

where $\varepsilon_1 := \varepsilon^x (-1)^{x(r-1)/2}$ and $\eta_1 := \eta^y (-1)^{y(r-1)/2}$ are both in $\{\pm 1\}$.

Reducing equation (1) modulo m and using (29) together with the fact that $x \geq 1$, we get $\eta_1 \equiv 1 \pmod{m}$. Since $m > 2$, we conclude that $\eta_1 = 1$.

(i) Assume that $x = 1$. Reducing (1) modulo m^2 and using (29) and the fact that $\eta_1 = 1$, we get

$$\varepsilon_1 mr + 1 \equiv 1 \pmod{m^2},$$

which leads to (25). It is also clear that $r \neq 0$.

(ii) Assume that $x = 2$. Reducing (1) modulo m^2, using (29) and observing that $\varepsilon_1 = 1$ and $\eta_1 = 1$, we get

$$r^2 m^2 + 1 - y\binom{r}{2} m^2 \equiv 1 + zm^2 \pmod{m^4},$$

or

$$z + y\binom{r}{2} - r^2 \equiv 0 \pmod{m^2}, \tag{30}$$

which is exactly (26). Let us show that the left-hand side of (30) is nonzero. If $y \geq 3$, then this number is at least

$$z + 3\binom{r}{2} - r^2 = z + \frac{r(r-3)}{2} \geq z > 0$$

(because $r \geq 3$, as $r > 1$ is odd). The case $y = 2$ is not allowed since it leads to $(x, y, z) = (2, 2, r)$. Finally, if $y = 1$, then

$$c^z = a^2 + b < a^2 + b^2 = c^r,$$

therefore $z < r$. Now the left-hand side of (30) is

$$z + \binom{r}{2} - r^2 = z - \frac{r(r+1)}{2} < r - \frac{r(r+1)}{2} = \frac{r(1-r)}{2} < 0,$$

so it is not zero either.

(iii) Assume that $x \geq 3$. Reducing (1) modulo m^3, and using (29) as well as the fact that $\eta_1 = 1$, we get

$$1 - y\binom{r}{2} m^2 \equiv 1 + zm^2 \pmod{m^3},$$

which leads to the congruence (27). The left-hand side of this congruence is positive.

We shall just sketch the argument when r is even, since it is entirely similar. In this case, formulas (28) become

$$A = \frac{1}{2}((m+i)^r + (m-i)^r) = (-1)^{r/2}\left(1 - \binom{r}{2}m^2 + \cdots\right),$$
$$B = \frac{1}{2i}((m+i)^r - (m-i)^r) = (-1)^{(r-2)/2}m\left(r - \binom{r}{3}m^2 + \cdots\right),$$

so that the analogs of the first two congruences (29) are

$$a^x = \varepsilon^x(-1)^{xr/2}\left(1 - \binom{r}{2}m^2 + \cdots\right)^x = \varepsilon_1\left(1 - x\binom{r}{2}m^2\right) \pmod{m^4},$$
$$b^y = \eta^y(-1)^{y(r-2)/2}m^y\left(r - \binom{r}{3}m^2 + \cdots\right)^y = \eta_1 r m^y \pmod{m^{2+y}},$$

where again ε_1 and η_1 are in $\{\pm 1\}$. Reducing equation (1) modulo m, we get $\varepsilon_1 = 1$. Reducing (1) modulo m^2 when $y = 1$ and modulo m^3 for $y \geq 3$ gives congruences (25) and (27) (with y replaced by x), respectively, and the left-hand sides of these congruences are positive. Finally, for $y = 2$, reducing (1) modulo m^4 and using the fact that $\eta_1 = 1$ and $\varepsilon_1 = 1$, we get

$$1 - x\binom{r}{2}m^2 + r^2m^2 \equiv 1 + zm^2 \pmod{m^4},$$

leading to

$$z + x\binom{r}{2} - r^2 \equiv 0 \pmod{m^2}. \tag{31}$$

If $x \geq 3$, then the left-hand side above is at least

$$z + 3\binom{r}{2} - r^2 = z + \frac{r(r-3)}{2},$$

and this is again positive when $r \geq 3$, as well as when $r = 2$, because it is then $z - 1 > 0$ (by Lemma 5(iii)).

The case $x = 2$ leads to $(x, y, z) = (2, 2, r)$. Finally, when $x = 1$, the left-hand side of (31) is

$$z + \binom{r}{2} - r^2 = z - \frac{r(r+1)}{2}. \tag{32}$$

Similar to the case when r is odd, we have

$$c^z = a + b^2 < a^2 + b^2 = c^r,$$

so $z < r$, which implies that the right-hand side of (32) is negative. ∎

3.5. A lower bound for r

Lemma 9. *We have*

$$r \gg m^{1/6}. \tag{33}$$

Proof. If $x = 1$ or $y = 1$, then Lemma 8(i) shows that $r \geq m$, which is better than (33). When $\min\{x, y\} \geq 2$, (ii), (iii) and the remaining statements of Lemma 8 show that m divides

$$z + x\binom{r}{2} + \delta r^2 \quad \text{or} \quad z + y\binom{r}{2} + \delta r^2 \qquad \text{for some } \delta \in \{0, -1\},$$

and none of these is 0. Hence,

$$m \leq \left| z + (x+y)\binom{r}{2} + \delta r^2 \right| \leq z + (x+y)\binom{r}{2} + r^2 = O(r^5 (\log m)^4),$$

by Lemma 6. This easily implies the desired estimate (33). ∎

3.6. An upper bound for $\Omega(m^2+1)$. We use the standard notation $\Omega(n)$ for the number of prime factors of n including repetitions.

Lemma 10.

(i) *Let p be any prime factor of $m^2 + 1$. Then $p \gg m^{1/6}$.*
(ii) $r = O(e_p)$.
(iii) $\Omega(m^2 + 1) \leq 12$ *if m is sufficiently large.*

Proof. (i) Lemma 9 together with Lemma 7(iii) and the fact that $e_p \leq p - 1$ leads to

$$m^{1/6} \ll r = O\left(\frac{e_p (\log m)^3}{(\log p)^3}\right) = O\left(\frac{p (\log m)^3}{(\log p)^3}\right),$$

which implies (i).

(ii) By (i), we have $\log p \asymp \log m$, so by Lemma 7(iii),

$$r = O\left(\frac{e_p (\log m)^3}{(\log p)^3}\right) = O(e_p).$$

(iii) If $\Omega(m^2+1) \geq 13$, then, by (i),

$$m^2 + 1 \geq (\min\{p \mid m\})^{13} \gg m^{13/6},$$

which implies that $m = O(1)$. ∎

3.7. Accurate estimates for $\log a$ and $\log b$

Lemma 11. *We have*

$$\log a = \frac{r}{2}\log(m^2+1) + O((\log m)^2), \tag{34}$$

and a similar estimate holds for $\log b$.

Proof. We write

$$\log a = \log|\alpha|^r - \log 2 + \log\left|1+\left(\frac{\beta}{\alpha}\right)^r\right| \tag{35}$$
$$= \frac{r}{2}\log(m^2+1) - \log 2 + \log\left|1+\left(\frac{\beta}{\alpha}\right)^r\right|.$$

The number $\gamma := \beta/\alpha = (m^2-1)/(m^2+1) - i(2m)/(m^2+1)$ is quadratic. Since γ is not a root of unity, the expression inside the last logarithm is nonzero. The minimal polynomial of γ over $\mathbb{Z}[X]$ is

$$f(X) := (m^2+1)X^2 - 2(m^2-1)(m^2+1)X + (m^2+1),$$

so that the logarithmic height of γ is precisely $h(\gamma) = (1/2)\log(m^2+1)$. Now by Lemma 2 with $\eta_1 := \beta/\alpha$, $\eta_2 := -1$, $b_1 := r$, and $b_2 := 1$, for which $B = \max\{|b_1|, |b_2|\} = r$, we have

$$\left|\log\left|1+\left(\frac{\beta}{\alpha}\right)^r\right|\right| = O(h(\gamma)\log r) = O((\log m)^2), \tag{36}$$

where for the last inequality we also used Lemma 7(iv). The desired estimate (34) follows now from (35) and (36). ∎

3.8. Bounding $\max\{x,y\}$**.** We put $X := \max\{x,y\}$.

LEMMA 12. *We have*

$$X = O((\log m)^2). \tag{37}$$

Proof. Suppose that $b^y > a^x$ since the remaining case can be dealt with similarly. We start with (1) written in the form

$$\exp(x\log a - b\log y) = a^x b^{-y} = \Lambda := c^z b^{-y} - 1.$$

Observe that $\Lambda \in (0,1)$. Taking logarithms, we get

$$|x\log a - y\log b| = |\log\Lambda| = O(\log c\log b(\log\max\{y,z\})) \tag{38}$$

by Lemma 2. Observe that

$$\log b < r\log(m+1) \quad \text{and} \quad \log c < 2\log(m+1) \tag{39}$$

(see (3.2) for the left inequality; the right one is obvious).

From Lemma 6, Lemma 10(ii), and the fact that $e_p < p \le m^2+1$ for all primes p dividing m^2+1, we get

$$\max\{y,z\} = O(r^4(\log m)^4) = O(m^8(\log m)^4).$$

Thus, from Lemma 11,

$$(40)\qquad \begin{aligned}|\log \Lambda| &= |x\log a - y\log b| \\ &= \left|\frac{1}{2}(x-y)r\log(m^2+1) + O(X(\log m)^2)\right| \\ &= \frac{1}{2}|x-y|r\log(m^2+1) + O(X(\log m)^2),\end{aligned}$$

while by (38), (39) and (10),

$$(41)\qquad |\log \Lambda| = O(r(\log m)^3).$$

Now comparing (40) and (41) gives

$$(42)\qquad |x-y| = O\biggl(\frac{X\log m}{r} + (\log m)^2\biggr).$$

We also note that

$$\max\{a^x, b^y\} < c^z \le 2\max\{a^x, b^y\},$$

and taking logarithms in the above inequality and using Lemma 11, we get

$$\begin{aligned}z\log(m^2+1) = z\log c &= \max\{x\log a, y\log b\} + O(1) \\ &= \frac{Xr}{2}\log(m^2+1) + O(X(\log m)^2).\end{aligned}$$

This yields

$$(43)\qquad 2z - Xr = O(X\log m).$$

Since $r \gg m^{1/6}$ by Lemma 9, the term under the O-symbol in (43) is indeed an error. In particular,

$$(44)\qquad c_5 Xr < z < c_6 Xr$$

for large m with $c_5 := 1/3$ and $c_6 := 2/3$.

Now we observe that letting p be any prime factor of c, the form

$$(45)\qquad \Gamma := a^{4x} - b^{4y} = b^{4y}((a^4/b^4)^x b^{4(x-y)} - 1)$$

is divisible by p^z. Put $\eta_1 := a^4/b^4$, $\eta_2 := b^4$, $b_1 := x$, and $b_2 := x-y$. The rational numbers η_1 and η_2 are multiplicatively independent because $a \ge 2$ and $b \ge 2$ are coprime. Furthermore, put $E := r_1 \ge r/2$ and note that

$$v_p(\eta_1 - 1) \ge E \quad\text{and}\quad v_p(\eta_2^{x-y} - 1) \ge E.$$

We set $g := |x-y|$ and apply Lemma 4(i) to the form Γ given by (45), getting

$$(46)\qquad z \le v_p(\Gamma) < \frac{c_7 g}{E^3(\log p)^4}(\max\{\log(4X), E\log p\})^2 H_1 H_2,$$

where c_7 is some absolute constant and where we must take

$$(47)\qquad H_i \ge \max\{4\log a, 4\log b, E\log p\} \quad \text{for } i = 1, 2.$$

Since $p \gg m^{1/6}$ for large m (see Lemma 9) and $E = r_1 \geq r/2$, it follows, by Lemma 11, that all three terms $\log a$, $\log b$ and $E \log p$ under the max above are of the same order of magnitude, namely $r \log p$. So, if we take $H_1 = H_2 := c_8 r \log p$ for a suitable constant c_8, then inequalities (47) hold. Now (46) gives

$$z \ll \frac{g(E\log p)^4}{E^3(\log p)^4} = gE \ll |x-y|r.$$

Since $z \gg Xr$ (see (44)), we get

$$X \ll |x-y|.$$

Combining this with (42), we get

$$X \ll \frac{X\log m}{r} + (\log m)^2,$$

implying

$$r = O\left(\log m + \frac{r(\log m)^2}{X}\right).$$

Since $r \gg m^{1/6}$, we can omit the $\log m$ term above, getting

$$r \ll \frac{r(\log m)^2}{X},$$

which implies (37). ∎

LEMMA 13.

(i) $z = O(r(\log m)^2)$.
(ii) $r \gg m^{1/2}/\log m$.
(iii) $\Omega(m^2+1) \leq 5$ *for all sufficiently large* m.
(iv) $|2z - Xr| = O((\log m)^3)$.

Proof. (i) This follows from (44) and Lemma 12.

(ii) The argument from the proof of Lemma 9, based on Lemma 8, shows that either $r \geq m$ (that is, if $\min\{x,y\} = 1$), or m divides one of the expressions appearing in (3.5) which are nonzero (if $\min\{x,y\} \geq 2$). Hence,

$$m = O(z + Xr^2) = O(r^2(\log m)^2). \tag{48}$$

This immediately implies (ii).

(iii) This follows by noting that if p is an arbitrary prime factor of m^2+1, then (48) together with Lemma 10(ii) gives

$$m \ll r^2(\log m)^2 \ll e_p^2(\log m)^2 \ll p^2(\log m)^2,$$

so $p \gg m^{1/2}/\log m$. Since p is an arbitrary prime factor of m^2+1, (iii) follows for all sufficiently large m by an argument similar to the one used in the proof of Lemma 10(iii).

(iv) This follows from (43) and Lemma 12. ∎

3.9. The greatest common divisor of $r-1$ and m^2. Put $D := \gcd(r-1, m^2)$. Here, we show that D is large.

LEMMA 14. *We have*

$$D \gg \frac{r}{(\log m)^{10}} \gg \frac{m^{1/2}}{(\log m)^{11}}. \tag{49}$$

Proof. Let $p \mid m^2+1$. Then $e_p \mid 4|x-y|(r-1)$ by Lemma 7(ii). Since

$$4|x-y| = O(X) = O((\log m)^2)$$

by Lemma 12, it follows that

$$d_p := \gcd(r-1, e_p) \gg \frac{e_p}{(\log m)^2} \gg \frac{r}{(\log m)^2}, \tag{50}$$

where the last inequality follows from Lemma 10(ii). Now write $m^2+1 = p_1 \cdots p_s$ with primes $p_1 \le \cdots \le p_s$, not necessarily distinct. For large m, we have $s \le 5$ by Lemma 13(iii). Since (50) holds for $p = p_i$ and $i = 1, \ldots, s$, it follows that

$$e := \gcd(d_1, \ldots, d_s) \gg \frac{r}{(\log m)^{10}}. \tag{51}$$

To maybe better see why this holds, observe that if we write $r-1 =: d_{p_i} a_i$ for $i = 1, \ldots, s$, then

$$a_i = O((\log m)^2) \quad \text{for all } i = 1, \ldots, s$$

(by (50)), and

$$\frac{r-1}{e} \le a_1 \cdots a_s = O((\log m)^{2s}) = O((\log m)^{10}).$$

However, $p \equiv 1 \pmod{e_p}$ for all primes p by Fermat's Little Theorem. In particular, $p_i \equiv 1 \pmod{e}$ for all $i = 1, \ldots, s$. Thus, $m^2+1 \equiv 1 \pmod{e}$, showing that $m^2 \equiv 0 \pmod{e}$. In particular, $D \ge e$. The first inequality of (49) now follows from (51), while the second follows from Lemma 13(ii). ■

3.10. Finding a linear relation among r, m and z. Assume that m is large.

LEMMA 15. *If r is odd, then one of the following holds:*

(i) $x = 1$, $r = m\lambda$ *and* $z = \pm\lambda + m\lambda y/2$;
(ii) $x = 2$ *and* $z = 1 + y(r-1)/2$;
(iii) $x \ge 3$ *and* $z = y(r-1)/2$.

If r is even, then one of the analogs of (i)–(iii) *with x and y interchanged must hold.*

Proof. We revisit the arguments from the proof of Lemma 8. We keep the notation from that lemma. Assume that r is odd. Then congruences (29) hold.

Assume first that $x = 1$. Then, by Lemma 8(i), we have $r = m\lambda$. Also, $\eta_1 = 1$. Reducing equation (1) modulo m^4, we have

$$\varepsilon_1\left(rm - \binom{r}{3}m^3\right) + 1 - y\binom{r}{2}m^2 = 1 + zm^2 \pmod{m^4}$$

(see (29)). Observe that $6\binom{r}{3}$ is a multiple of r, which in turn is a multiple of m. Hence,

$$3(2z + yr(r-1) - 2\varepsilon_1\lambda) \equiv 0 \pmod{m^2}.$$

Since r^2 is a multiple of m^2, we get

$$6z - 6\varepsilon_1\lambda - 3yr \equiv 0 \pmod{m^2}.$$

Since $X = y$, the left-hand side above is of size

$$O(|2z - Xr| + \lambda) = O(r/m + (\log m)^3) = O(m + (\log m)^3) = O(m)$$

(see Lemma 13(iv)), so for large m it can be a multiple of m^2 only if it is zero. This leads to (i).

(ii) Assume that $x = 2$. By reducing (1) modulo m^2, we get

$$z - y\binom{r}{2} - r^2 \equiv 0 \pmod{m^2}.$$

Since $D \mid r - 1$, we see that D divides $2z - 2$. Suppose first that $y \geq 3$. Then $X = y$ and

$$\frac{|2z - 2 - y(r-1)|}{D} \leq \frac{|2z - yr| + (y-2)}{D} = O\left(\frac{(\log m)^3}{D}\right) \tag{52}$$

by Lemmas 12 and 13(v). Since $2z - 2 - y(r-1)$ is a multiple of D, the left-hand side of (52) is an integer, while the right-hand side is, by (49), of order $O((\log m)^{14}/m^{1/2})$. Hence, for large m the left-hand side is zero, and we get (ii).

If on the other hand $y = 1$, we get $X = 2$, so, again by Lemma 13(iv), we have

$$2z - 2r = O((\log m)^3).$$

Thus,

$$(2z - 2) - (2r - 2) = O((\log m)^3).$$

The left-hand side above is a multiple of $D \gg m^{1/2}/(\log m)^{11}$, so by a previous argument, it must be 0. Hence, $z = r$, which is false since then $c^r = a^2 + b^2 = a^2 + b = c^z$, so $b = b^2$, which is impossible because $b > 1$ by Lemma 5(v).

(iii) Assume that $x \geq 3$. Put $d := \gcd(m, D)$. Observe that $d \geq D^{1/2}$. Then, by reducing (1) modulo m^3, we get

$$m \mid 2z + 2y\binom{r}{2}$$

(see Lemma 8(iii)). Now both m and $2\binom{r}{2} = r(r-1)$ are divisible by d, so d also divides $2z$. Thus,

$$\frac{|2z - X(r-1)|}{d} \le \frac{|2z - Xr| + X}{d} = O\bigg(\frac{(\log m)^3}{d}\bigg), \tag{53}$$

by Lemmas 12 and 13(v). The left-hand side of (53) is an integer, and the right-hand side is of order

$$\frac{(\log m)^3}{d} \le \frac{(\log m)^3}{D^{1/2}} \ll \frac{(\log m)^9}{m^{1/4}} = o(1)$$

as m becomes large. Thus, the left-hand side must be 0, proving (iii).

This completes the analysis when r is odd.

The case of r even is almost identical. We give no further details. ∎

3.11. The end of the proof. We assume that r is odd, since the case of r even is similar. Let us look at each of the situations described in Lemma 15.

(i) Let $x = 1$ and $r = m\lambda$, $z = \pm\lambda + yr/2$. We write

$$a^2 + b^2 = c^{m\lambda} \quad \text{and} \quad a + b^y = c^{\pm\lambda + yr/2}.$$

We reduce these equations modulo a to get $b^{2y} \equiv c^{m\lambda y} \pmod{a}$ and $b^{2y} \equiv c^{\pm 2\lambda + m\lambda y} \pmod{a}$. Since a and c are coprime, we are led to $c^{2\lambda} \equiv 1 \pmod{a}$. Observe that since $r = m\lambda$ and $r \ll m^2$ (by Lemma 7(iv)), we have $\lambda \ll r^{1/2}$. Now since $a \mid c^{2\lambda} - 1$, and this last number is nonzero, we have

$$\log a \le \log c^{2\lambda} = 2\lambda \log c = O(r^{1/2} \log m).$$

Comparing this with Lemma 11, we get

$$\frac{r}{2}\log(m^2+1) + O((\log m)^2) = O(r^{1/2}\log m),$$

which leads to

$$r = O(r^{1/2}\log m).$$

This implies that $r = O((\log m)^2)$, and since also $r \gg m^{1/6}$ by Lemma 9, we get only finitely many solutions.

(ii) Let $x = 2$ and $z = 1 + y(r-1)/2$. Then

$$a^2 + b^2 = c^r \quad \text{and} \quad a^2 + b^y = c^{1+y(r-1)/2}.$$

Reducing modulo a^2 implies $b^{2y} \equiv c^{yr} \pmod{a^2}$ and $b^{2y} \equiv c^{yr+2-y} \pmod{a^2}$. Hence, $c^{y-2} \equiv 1 \pmod{a^2}$. Clearly, $y \ne 2$, otherwise we would get $c^z = a^2 + b^2 = c^r$, so $r = z$, which is not allowed. We thus get $a^2 \mid c^{y-2} - 1$ and this last integer is nonzero. So,

$$\log a \le \log c^y = y \log c = O(X \log m) = O((\log m)^3).$$

Using again (34), we get $r \ll (\log m)^2$, which via Lemma 9 leads to $m^{1/6} \ll (\log m)^2$, having only finitely many solutions.

(iii) Let $x \geq 3$ and $z = y(r-1)$. Then

$$a^x + b^y = c^{y(r-1)/2} \quad \text{and} \quad a^2 + b^2 = c^r.$$

Reducing modulo a^2 gives $b^y \equiv c^{y(r-1)/2} \pmod{a^2}$, so $b^{2y} \equiv c^{yr-y} \pmod{a^2}$, and $b^2 \equiv c^r \pmod{a^2}$, so $b^{2y} \equiv c^{yr} \pmod{a^2}$. From these two congruences, we see that $c^y \equiv 1 \pmod{a^2}$. Thus, a^2 divides $c^y - 1$, which is not zero. Hence

$$2\log a = \log(a^2) \leq \log c^y = y \log c = O((\log m)^3),$$

and we conclude that m is bounded as in the previous case.

This finishes the proof.

Acknowledgments. I thank Professor Arnold Knopfmacher for useful advice and the referee for a careful reading of the paper. This paper was written while the author was on a sabbatical leave from the Mathematical Institute of UNAM from January 1 to June 30, 2011 and supported by a PASPA fellowship from DGAPA.

References

[1] Yu. F. Bilu, G. Hanrot and P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers* (with an appendix by M. Mignotte), J. Reine Angew. Math. 539 (2001), 75–122.

[2] Y. Bugeaud, *Linear forms in p-adic logarithms and the Diophantine equation* $(x^n - 1)/(x - 1) = y^q$, Math. Proc. Cambridge Philos. Soc. 127 (1999), 373–381.

[3] Y. Bugeaud et M. Laurent, *Minoration effective de la distance p-adique entre puissances de nombres algébriques*, J. Number Theory 61 (1996), 311–342.

[4] Z. F. Cao, *A note on the Diophantine equation* $a^x + b^y = c^z$, Acta Arith. 91 (1999), 85–93.

[5] Z. F. Cao and X. Dong, *On the Terai–Jeśmanowicz conjecture*, Publ. Math. Debrecen 22 (2002), 1–13.

[6] A. O. Gel'fond, *Sur la divisibilité de la différence des puissances des deux nombres entiers par une puissance d'un idéal premier*, Mat. Sb. 7 (1940), 7–25.

[7] L. Jeśmanowicz, *Several remarks on Pythagorean numbers*, Wiadom. Mat. 1 (1955/1956), 196–202 (in Polish).

[8] M. H. Le, *A conjecture concerning the exponential Diophantine equation* $a^x + b^y = c^z$, Acta Arith. 106 (2003), 345–353.

[9] —, *A note on the Diophantine system* $a^2 + b^2 = c^r$ *and* $a^x + b^y = c^z$, Acta Math. Sinica (Chinese Ser.) 52 (2008), 677–684 (in Chinese).

[10] W. T. Lu, *On the Pythagorean numbers* $4n^2 - 1, 4n$ *and* $4n^2 + 1$, Acta Sci. Natur. Univ. Szechuan 2 (1959), 39–42 (in Chinese).

[11] K. Mahler, *Zur Approximation algebraischer Zahlen I: Über den grössten Primteiler binärer Formen*, Math. Ann. 107 (1933), 691–730.

[12] E. M. Matveev, *An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers, II*, Izv. Ross. Akad. Nauk Ser. Mat. 64 (2000), 125–180 (in Russian); English transl: Izv. Math. 64 (2000), 1217–1269.

[13] T. Miyazaki, *Terai's conjecture on exponential Diophantine equations*, Int. J. Number Theory 7 (2011), 981–999.
[14] T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Univ. Press, 1986.
[15] N. Terai, *The Diophantine equation* $a^y + b^y = c^z$, Proc. Japan Acad. Ser. A Math. Sci. 70 (1994), 22–26.
[16] K. Yu, *p-adic logarithmic forms and group varieties II*, Acta Arith. 89 (1999), 337–378.

Florian Luca
Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58089, Morelia, Michoacán, México
and
The John Knopfmacher Centre
for Applicable Analysis and Number Theory
University of the Witwatersrand
P.O. Wits 2050, Johannesburg, South Africa
E-mail: fluca@matmor.unam.mx

Received on 30.3.2011
and in revised form on 27.9.2011 (6653)