On a conjecture on exponential Diophantine equations

by

Mihai Cipu (Bucureşti and Strasbourg)
and Maurice Mignotte (Strasbourg)

1. The problem. Let a, b, c be fixed coprime integers with $\min(a, b, c)$ > 1. As an application of his p-adic analogue of the Thue–Siegel method, Mahler [15] proved in 1933 that the equation

$$(1) \qquad a^x + b^y = c^z$$

has finitely many solutions (x, y, z) in positive integers. His method is ineffective in the sense that it gives no indication on the number of possible solutions for a fixed triple (a, b, c). Such an information has been obtained only in particular instances. Thus, Sierpiński [20] showed that $(2, 2, 2)$ is the unique solution in positive integers to the equation $3^x + 4^y = 5^z$. In the same journal, Jeśmanowicz [10] conjectured the uniqueness of the solution to (1) in case (a, b, c) is a Pythagorean triple. This conjecture is still open, despite the efforts of many authors.

In analogy to Jeśmanowicz's conjecture, Terai [23] claimed that (1) always has at most one solution. Simple counterexamples to this statement have been found by Cao [4], who attempted to correct it by adding the hypothesis $\max(a, b, c) > 7$. It turns out that this condition is not sufficient to entail the sought-for uniqueness. A family of counterexamples has been found by Le (see [14]), who also stated the following form of Terai's conjecture.

CONJECTURE 1.1. *For given coprime integers $a, b, c > 1$, the Diophantine equation* (1) *has at most one solution in integers $x, y, z > 1$.*

Starting with [23] and [24], much work has been devoted to the case when (1) has a solution of the form $(2, 2, r)$, with r greater than 1 and odd. This implies in particular that c is odd and exactly one of a, b is even. For definiteness, suppose that a is even and therefore b is odd. Most of the recent

results concern the case

(2) $a \equiv 2 \pmod 4$, $b \equiv 3 \pmod 4$, $\gcd(a, b) = 1$, $r > 1$ odd, $a^2 + b^2 = c^r$.

The conjecture is established in this case under one of the following additional hypotheses:

(α) (Terai [25]) $b \equiv 3 \pmod 8$, $b \geq 30a$ and $\left(\frac{a}{d}\right) = -1$, where $d > 1$ is a divisor of b and $\left(\frac{a}{d}\right)$ denotes the Jacobi symbol,

(β) (Cao [4]) c is a prime power,

(γ) (Cao–Dong [5]) $b \geq 25.1a$,

(δ) (Le [14]) $c > 3 \cdot 10^{27}$ and $r > 7200$.

Further partial confirmations of the conjecture are referred to in the papers cited above.

Contrary to what is claimed in [14], the last result quoted above does not imply that the conjecture holds with the exception of finitely many pairs (c, r). One of the aims of this paper is to prove that indeed there are at most finitely many values for which the conjecture can be refuted. On the way we shall prove other results for the positive solutions to the Diophantine simultaneous equations

(3) $a^2 + b^2 = c^r$, $a^2 + b^y = c^z$,

where

(4) $r, z > 1$ are odd, $a \equiv 2 \pmod 4$, $b \equiv 3 \pmod 4$, $\gcd(a, b) = 1$.

As a consequence of our deliberations, several improvements on the results (α)–(δ) are obtained. Thus, we prove that, if the conditions stated in (2) hold, in any hypothetical counterexample to Conjecture 1.1 each of a, b, c must have at least two prime divisors. Moreover, we strengthen (α) and (γ) by showing that the inequality $b > 0.218\,a$ entails the truth of Terai's conjecture. With regard to (δ), we are able to improve the bound on r to 770. Our proofs approach these cases from a different perspective and are much shorter than the published ones, although they involve a harder computational component.

We give here a rough description of our procedure. In the hypotheses of our work, c is a sum of two coprime squares. We generate all such decompositions for c up to $4 \cdot 10^{10}$ with the help of Cornacchia's algorithm (see [18] and [2] for very simple proofs of its correctness). We notice that, when compared to the obvious method (for c fixed and $1 \leq u < \sqrt{c}$ test whether $c - u^2$ is a square), for our range of values Cornacchia's algorithm is more than ten times faster. To each such decomposition of c one associates values a and b as in (2). We show that the existence of a solution to system (3)–(4) implies that a and b are comparatively big in comparison to c. The resulting inequalities relating a, b and c impose stringent restrictions on y, r, and z.

This description is vague; details are given in Section 3, after we recall classical facts, some of them going back at least to Lagrange. Additional information on the putative solutions of (3) are given in Section 3. Section 4 contains the proofs of our main results, among which are the following.

THEOREM 1.2. *There are at most finitely many quadruples (a, b, c, r) for which (2) holds and (1) has more than one solution in integers $x, y, z > 1$. For all of these quadruples, we have $r < 770$.*

The method of proof is ineffective since it gives no explicit bound on c beyond which Terai's conjecture holds in case (2).

THEOREM 1.3. *Let u and r be positive integers with $u \equiv 2 \pmod 4$ and $r \equiv 3 \pmod 4$. Put*

$$a = \sum_{j=0}^{(r-1)/2} (-1)^j \binom{r}{2j} u^{r-2j}, \ \ b = \sum_{j=0}^{(r-1)/2} (-1)^j \binom{r}{2j+1} u^{r-1-2j}, \ \ c = u^2 + 1.$$

Then (1) has a unique solution in integers $x, y, z > 1$.

THEOREM 1.4. *If a or b is a prime power then the system (3) has no solutions subject to the restrictions from (4).*

The last part of the paper is devoted to improvements of bounds on the parameters associated to a putative solution to system (3). They are meant to shrink the search domains for the components of a solution to a manageable size according to the present-day technology.

Although Terai's conjecture remains open, we have pushed the analysis further than ever before; and there is significant hope that our results can be improved by either complementing them with brand new ideas or dedicated computations.

2. Arithmetic restrictions. We use a result of Lagrange (1741), *Leçons sur le calcul des fonctions*, which makes recurrent appearance in the study of Diophantine equations, as well as in the theory of finite fields, Chebyshev polynomials and many other areas of mathematics. For the sake of completeness, we sketch its proof.

LEMMA 2.1. *Let X and Y two commuting indeterminates and let $n \geq 1$ be a positive integer. Then*

$$X^n + Y^n = \sum_{j=0}^{\lfloor n/2 \rfloor} c_{n,j} (-XY)^j (X+Y)^{n-2j},$$

where the $c_{n,j}$ are nonnegative integers which are defined recursively by

$$c_{n,j} = 0 \quad if \quad j < 0 \ or \ j > \lfloor n/2 \rfloor,$$
$$c_{1,0} = 1, \ c_{2,0} = 1, \ c_{2,1} = 2, \quad c_{n+1,j} = c_{n,j} + c_{n-1,j-1} \ for \ n \geq 2.$$

More precisely,

$$c_{n,j} = \frac{(n-j-1)!\,n}{(n-2j)!\,j!}.$$

Proof. The result is obvious for $n \leq 2$, including the initial values $c_{1,0} = 1$, $c_{2,0} = 1$, $c_{2,1} = 2$. The general case can be obtained by induction from the formula

$$X^{n+1} + Y^{n+1} = (X^n + Y^n)(X+Y) - XY(X^{n-1} + Y^{n-1}),$$

which implies the recursive relation

$$c_{n+1,j} = c_{n,j} + c_{n-1,j-1} \quad \text{for } n \geq 2.$$

By completely working out the details, one can get the closed form for the coefficients $c_{n,j}$. ∎

We shall repeatedly use the well-known structure of integers satisfying the first equation from (3).

LEMMA 2.2. *If X, Y and Z are coprime positive integers such that*

$$X^2 + Y^2 = Z^n,$$

where n is an odd integer and X is even, then there exist coprime positive integers u and v, with u even and v odd, and $\lambda_1, \lambda_2 \in \{-1, 1\}$ such that

$$X + Yi = \lambda_1 \varepsilon^n, \quad \varepsilon = u + v\lambda_2 i, \quad Z = u^2 + v^2.$$

Moreover, if $\varepsilon = |\varepsilon| e^{\theta i/2}$ then

$$X = Z^{n/2}|\cos(n\theta/2)|, \quad Y = Z^{n/2}|\sin(n\theta/2)|.$$

The former part is proved as in Mordell's book [17, pp. 122–123]; the latter assertion is an obvious consequence of the preceding formulas.

In the present case, using the relations $a^2 + b^2 = c^r$ and $a^2 + b^y = c^z$, we get exponential expressions for a, b and $b^{y/2}$.

COROLLARY 2.3. *There are positive integers u, v, u_1, v_1, with u, u_1 even and v, v_1 odd, such that $c = u^2 + v^2 = u_1^2 + v_1^2$ and*

$$a = \tfrac{1}{2}|\varepsilon^r + \bar{\varepsilon}^r| = c^{r/2}|\cos(r\xi)|, \quad b = \tfrac{1}{2}|\varepsilon^r - \bar{\varepsilon}^r| = c^{r/2}|\sin(r\xi)|$$

and

$$a = \tfrac{1}{2}|\varepsilon_1^z + \bar{\varepsilon}_1^z| = c^{z/2}|\cos(z\xi_1)|, \quad b^{y/2} = \tfrac{1}{2}|\varepsilon_1^z - \bar{\varepsilon}_1^z| = c^{z/2}|\sin(z\xi_1)|,$$

where $\varepsilon = u + vi$, $\varepsilon_1 = u_1 + v_1 i$, $\tan \xi = v/u$, and $\tan \xi_1 = v_1/u_1$.

On combining the previous results, we get alternative expressions for a, b and $b^{y/2}$.

COROLLARY 2.4. *The values of a and b satisfy*

$$a = \pm u \sum_{j=0}^{(r-1)/2} c_{r,j}(-c)^j(4u^2)^{(r-1)/2-j}, \quad b = \pm v \sum_{j=0}^{(r-1)/2} c_{r,j}c^j(-4v^2)^{(r-1)/2-j}$$

and

$$a = \pm u_1 \sum_{j=0}^{(z-1)/2} c_{z,j}(-c)^j(4u_1^2)^{(r-1)/2-j},$$

$$b^{y/2} = \pm v_1 \sum_{j=0}^{(z-1)/2} c_{z,j}c^j(-4v_1^2)^{(z-1)/2-j}.$$

From the last formula it follows that

$$b^{y/2} \equiv \pm v_1 z c^{(z-1)/2} \pmod{v_1^3},$$

in particular

$$p \,|\, v_1 \;\Rightarrow\; \mathrm{v}_p(v_1) \ge y/2 \ge 3 \text{ if } \gcd(p, z) = 1.$$

3. Bounds for a, b, c. From our standard hypotheses on a, b, c stated in (3) and (4) it follows that $c \equiv 5 \pmod 8$. As recalled in Lemma 2.2, the first equation from (3) implies that there exist positive integers u and v such that

$$(5) \qquad\qquad c = u^2 + v^2.$$

By [4], we may also suppose that c has at least two prime divisors. Then it is easily seen that one has $c \ge 85$. Much better lower bounds on c are derived as follows. With the help of Corollary 2.3, from each decomposition (5) of c we get values of a and b satisfying (2) for a suitable r. If the corresponding system (3) has a solution, we find that $a > c^{z/\mu}$ and $b > c^{r/\lambda}$ for certain positive reals μ, λ. Such inequalities allow for comparison of the exponents r, y, z. The resulting inequalities involve these values μ, λ. Changing the point of view, we reverse the reasoning and infer from $\mu\lambda \le 2y$ that either $a < c^{z/\mu}$ or $b < c^{r/\lambda}$. This game is easily played on a computer and consists of computations of suitable continued fractions and of bounds for linear forms in the logarithms of algebraic numbers.

To put this strategy at work, additional information is needed. Useful facts are given by the next result, proved in several places, for instance in [14].

LEMMA 3.1. *With the above notation and hypotheses, let (x, y, z) be a solution to (1) with $(x, y, z) \ne (2, 2, r)$. Then $x = 2$, $y \equiv 2 \pmod 4$, $y \ge 6$ and z is odd.*

Let us come back to the notation of Lemma 2.2 and put $\varepsilon = e^{i\theta/2}$ and

$$\alpha := \varepsilon/\bar{\varepsilon} = \frac{u^2 - v^2 + 2uvi}{u^2 + v^2}\, e^{\theta i}.$$

Since α is a root of the irreducible integer polynomial

$$(u^2 + v^2)T^2 - 2(u^2 - v^2)T + u^2 + v^2,$$

whose Mahler's measure is equal to $u^2 + v^2$, the absolute logarithmic height of α is

$$\mathrm{h}(\alpha) = \tfrac{1}{2}\log(u^2 + v^2) = \tfrac{1}{2}\log Z.$$

We also have

$$\min\{X, Y\} \geq \frac{Z^{n/2}}{\pi}\, \min_{k' \in \mathbb{Z}} |n\theta - k'\pi|.$$

Let k be an integer such that $\min_{k' \in \mathbb{Z}} |n\theta - k'\pi| = |n\theta - k\pi|$ and put

$$\Lambda = n\log\alpha - k\log(-1).$$

Then

$$\min\{X, Y\} \geq \frac{Z^{n/2}}{\pi}\, |\Lambda| \quad \text{and} \quad \min\{X, Y\} \geq 0.99\, Z^{n/2} \min\{|\Lambda|, 0.001\},$$

where Λ is a linear form in two logarithms of algebraic numbers.

3.1. *A first application of linear forms.* In a number field K embedded in the complex field, containing a root of unity $\zeta = e^{i\pi/m}$, where m is maximal, and a number α of modulus one which is not a root of unity, a linear form

$$\Lambda = n\log\alpha - ik\pi$$

as above can be written as

$$\Lambda = n\log\alpha - mk\log\zeta.$$

We remark that changing α into a suitable $\alpha\zeta^\ell$ if necessary we can assume that $|\log\alpha| \leq \pi/(2m)$. We may work under this hypothesis without changing the notation because $\mathrm{h}(\zeta^\ell\alpha) = \mathrm{h}(\alpha)$.

On using the main result of Laurent–Mignotte–Nesterenko [12], it is possible to prove that

(6) $$z > 55000 \quad \text{implies} \quad a > c^{z/(2\sqrt{3})}.$$

On using relations $a^2 + b^y = c^z$ and $c = u_1^2 + v_1^2$, by a computation of a suitable continued fraction we verify that

(7) $$\text{for } 85 \leq c < 4 \cdot 10^{10}, \quad z > 10 \quad \text{implies} \quad a > c^{z/(2\sqrt{3})}.$$

Similarly, from $a^2 + b^2 = c^r$ and $c = u^2 + v^2$ for some integers u, v which may be different from u_1, v_1, we obtain

(8) $$\text{for } 85 \leq c < 4 \cdot 10^{10}, \quad r > 10 \quad \text{implies} \quad b > c^{r/(2\sqrt{3})}.$$

This information is exploited in conjunction with the following remarks.

LEMMA 3.2. *Assume both conditions* (3) *and* (4) *hold. Then*:

(a) *If for some* $\mu > 0$ *one has* $a \geq c^{z/\mu}$ *then* $2z < \mu r$.
(b) *If for some* $\lambda > 0$ *one has* $b \geq c^{r/\lambda}$ *then* $yr < \lambda z$.
(c) *If* $\mu_1, \mu_2 > 0$ *are such that* $\mu_1 \mu_2 \leq 2y$ *then* $a \geq c^{z/\mu_1}$ *and* $b \geq c^{r/\mu_2}$ *cannot simultaneously hold. In particular*,

$$a < c^{z/(2\sqrt{3})} \quad or \quad b < c^{r/(2\sqrt{3})}.$$

Proof. (a) From $a \geq c^{z/\mu}$ and $a^2 + b^2 = c^r$ it readily follows that $c^{2z/\mu} < c^r$.

(b) If $b \geq c^{r/\lambda}$ then $c^{yr/\lambda} \leq b^y < c^z$.

(c) The first assertion follows directly from (a) and (b). The last part follows from this because $y \geq 6$ by Lemma 3.1. ∎

Using this lemma, we ruled out the small values of r and z (precisely, those with $2 < r < z < 10$) and prove that c cannot be comparatively small. After around two weeks of computation we verified the following result.

LEMMA 3.3. *Assume the system of equations* (3) *has solutions satisfying* (4). *Then* $c > 4 \cdot 10^{10}$.

3.2. *A second application of linear forms.* From now on we consider $c > 4 \cdot 10^{10}$ without further explicitly mentioning it. In order to improve the bounds on r and z obtained in the previous subsection, we apply a very recent result of Laurent [11].

LEMMA 3.4. *Consider a nonzero linear form*

$$\Lambda = b_1 \log \alpha_1 - b_2 \log \alpha_2,$$

where α_1 *and* α_2 *are nonzero algebraic numbers, both different from* 1, *and* b_1 *and* b_2 *are positive integers. Put*

$$D = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}]/[\mathbb{R}(\alpha_1, \alpha_2) : \mathbb{R}].$$

Let K *be an integer* ≥ 3, L *an integer* ≥ 2, *and* R_1, R_2, S_1, S_2 *positive integers. Let* ρ *and* μ *be real numbers with* $\rho > 1$ *and* $1/3 \leq \mu \leq 1$. *Put* $R = R_1 + R_2 - 1$, $S = S_1 + S_2 - 1$, $N = KL$, *and*

$$g = \frac{1}{4} - \frac{N}{12RS}, \quad \sigma = \frac{1 + 2\mu - \mu^2}{2},$$

$$b = \frac{((R-1)b_2 + (S-1)b_1)}{2} \left(\prod_{k=1}^{K-1} k! \right)^{-2/(K^2-K)}.$$

Let a_1, a_2 *be positive real numbers such that*

$$a_i \geq \rho |\log \alpha_i| - \log |\alpha_i| + 2D \, \mathrm{h}(\alpha_i),$$

for $i = 1, 2$. Suppose that

(I) $\mathrm{Card}\{\alpha_1^r \alpha_2^s;\ 0 \le r < R_1,\ 0 \le s < S_1\} \ge L,$

(II) $\mathrm{Card}\{rb_2 + sb_1;\ 0 \le r < R_2,\ 0 \le s < S_2\} > (K - 1)L$

and also that

(III) $K(\sigma L - 1)\log\rho - (D + 1)\log N - D(K - 1)\log b$
$$- gL(Ra_1 + Sa_2) > c(N),$$

where

$$c(N) = \frac{2}{N}\,\log(N!\,N^{-N+1}(e^N + (e-1)^N)).$$

Then

$$|\Lambda'| \ge \rho^{-\mu K L},$$

where

$$\Lambda' = \Lambda \max\left\{ \frac{LSe^{LS|\Lambda|/(2b_2)}}{2b_2},\ \frac{LRe^{LR|\Lambda|/(2b_1)}}{2b_1} \right\}.$$

In our case $\alpha_1 = \alpha$ (up to a power of i), $\alpha_2 = i$, $b_1 = r$ or z, and $b_2 = k$. (To work with the linear form associated to the relation $a^2 + b^y = c^z$ we only need to take above $b_1 = z$ instead of $b_1 = r$.) For $c = 4 \cdot 10^{10} + 5$, we choose the parameters as follows: $L = 8$, $\rho = 7.7$, $\mu = 0.56$, $K = \lceil mLa_1a_2 \rceil$, $R_1 = 4$, $S_1 = 2$, $R_2 = \lceil \sqrt{m}\,La_2 \rceil$, and $S_2 = \lceil (1 + (K-1)L)/R_2 \rceil$, where $m = 0.1166$, and we get

$$|\Lambda| > c^{-0.2113r} \quad \text{for } r \ge 771,$$

which implies

$$a > c^{z/(2\sqrt{3})} \quad \text{and} \quad b > c^{r/(2\sqrt{3})} \quad \text{for } r \ge 771.$$

Taking into account Lemma 3.2(b), one concludes that $r \le 769$.

Now, combining Lemma 3.2(a) and Lemma 3.2(c), we see that if the system has a solution then $r \le 769$ and $z \le 983$. The detailed argument is the following: we apply Laurent's result twice, a first computation for $z \ge 985$ gives an upper bound for μ_2 which combined with part (a) implies $r \ge 641$; then a second computation for $r \ge 641$ gives an upper bound for μ_1 with $\mu_1\mu_2 < 12$, and part (c) leads to a contradiction. Thus $z \le 983$. Moreover, it is easy to check that the greater c, the better our estimates, so that the conclusion holds for all $c > 4 \cdot 10^{10}$.

Arguing in the same way, we can establish tighter bounds for r and z, provided a higher lower bound on y is available.

LEMMA 3.5. *If the Diophantine system* (3) *has solutions satisfying* (4) *then in all cases*

$$r \le 769 \quad \text{and} \quad z \le 983.$$

Moreover,

$$y \geq 10 \;\Rightarrow\; r \leq 539 \text{ and } z \leq 759,$$
$$y \geq 14 \;\Rightarrow\; r \leq 461 \text{ and } z \leq 681,$$
$$y \geq 18 \;\Rightarrow\; r \leq 419 \text{ and } z \leq 647,$$
$$y \geq 22 \;\Rightarrow\; r \leq 395 \text{ and } z \leq 627,$$
$$y \geq 602 \;\Rightarrow\; r \leq 263 \text{ and } z \leq 539.$$

3.3. *Elementary lower bounds on b.* Let $\varepsilon = u + iv = |\varepsilon|e^{i\xi}$, where $c = u^2 + v^2$, with u even, and $|\varepsilon| = \sqrt{c}$. Then $\tan\xi = v/u$ and

$$b = \tfrac{1}{2}|\varepsilon^r - \bar\varepsilon^r| = c^{r/2}|\sin(r\xi)|$$

with $r \geq 3$. In this subsection we derive lower bounds on b from lower bounds on v.

LEMMA 3.6. *With the above notation*,

$$r \leq \pi/\xi - 1 \;\Rightarrow\; b \geq vc^{(r-1)/2} \geq vc.$$

In particular, $b \geq vc^{(r-1)/2}$ *whenever* $r \leq u\pi/v - 1$.

Proof. The hypothesis $3 \leq r \leq \pi/\xi - 1$ implies that $\xi \leq \pi/4$ and $3\xi \leq r\theta \leq \pi - \xi$, and therefore $\sin(r\xi) \geq \sin\xi = v/\sqrt{c}$.

For the last part, note that the hypothesis $r \leq \pi/\xi - 1$ holds if $r \leq u\pi/v - 1$ because $0 < \xi < \tan\xi = v/u$. ∎

Despite its innocuous appearance, the lemma just proved plays an important role in subsequent reasonings. Thus, $v \leq 925$ implies $u/v > 216$ (recall our standing hypothesis $c > 4 \cdot 10^{10}$) and then the previous lemma gives $b \geq vc^{(r-1)/2} \geq c^{r/3}$ (since $3 \leq r$). In view of Lemma 2.1, it follows that one always has $b \geq v$. Therefore, $b \geq 925$.

More importantly, with the help of Lemma 3.6 we shall derive a strikingly sharp bound for the quotient y/z.

LEMMA 3.7. *We always have*

$$b \geq \frac{\pi}{r+1}\left(1 + \frac{\pi^2}{(r+1)^2}\right)^{-1/2}\sqrt{c}$$

and

$$y < z\left(2 + \frac{9.982}{\log b}\right).$$

Moreover, if $y > 600$ then

$$y < z\left(2 + \frac{8.863}{\log b}\right).$$

In particular, always

$$y < 1778.$$

Proof. From our previous study we know that

(9)
$$b \geq \begin{cases} c^{(r-1)/2} \geq c & \text{if } (r+1)v < \pi u, \\ v & \text{otherwise.} \end{cases}$$

Notice that $(r+1)v \geq \pi u$ implies

$$c \leq \left(1 + \frac{(r+1)^2}{\pi^2}\right)v^2,$$

so that in all cases b satisfies

$$b \geq \frac{\pi}{r+1}\left(1 + \frac{\pi^2}{(r+1)^2}\right)^{-1/2}\sqrt{c}.$$

Now we consider the upper bounds for y. From (9) we get

$$c \leq \begin{cases} b & \text{if } (r+1)v < \pi u, \\ v^2 + \dfrac{(r+1)^2}{\pi^2}\,v^2 & \text{otherwise.} \end{cases}$$

Hence,

$$c \leq \left(1 + \frac{(r+1)^2}{\pi^2}\right)b^2.$$

Using the inequality $b^y < c^z$ one gets

(10)
$$y < z\left(2 + \frac{\log(1 + (r+1)^2/\pi^2)}{\log b}\right).$$

If $y \leq 10$ the second estimate of the lemma is trivial, hence we suppose $y \geq 14$. Then $r < 462$, and after a simple computation we get the stated inequality.

When $y > 600$ we know from Lemma 3.5 that $r \leq 263$ and the third estimate follows. The last one is deduced by using the fact that $b \geq 925$ and $z < 540$ whenever $y \geq 600$. ∎

3.4. *Estimates on a.* Our next goal is to obtain some estimates on a. Put $b = c^\lambda$. The information we have up to know allows us to conclude that $1/2 - (\log 1800)/\log c < \lambda < r/2$. We use this knowledge to prove the following.

LEMMA 3.8. *Put $a = b^{(y-\lambda')/2}$. Then λ' is positive and satisfies*

$$\lambda' > \frac{\log c}{\log b}\,(z - r - 10^{-22}) > \frac{2}{r}\,(2 - 10^{-22}).$$

Proof. From the second equation in (3) we get

$$c^z(1 - c^{-z+r}) < b^y < c^z$$

and since $z \geq r + 2$ this implies

$$z \log c + \log(1 - c^{-2}) < y \log b < z \log c,$$

while the first equation in (3) and the definition of λ' imply

$$(y - \lambda') \log b < r \log c.$$

Hence

$$z \log c - 10^{-21} < r \log c + \lambda' \log b,$$

and therefore

$$2 \leq z - r < 10^{-22} + \lambda' \frac{\log b}{\log c} 10^{-22} + \lambda'\lambda,$$

by the definition of λ. In other words

$$\lambda' > \frac{1}{\lambda} (z - r - 10^{-22}),$$

and in particular

$$\lambda' > \frac{2}{r} (2 - 10^{-22}) > 0. \quad \blacksquare$$

4. Main results. Recall the result of Corollary 2.3: we have seen that $c = u^2 + v^2 = u_1^2 + v_1^2$ for some positive integers, with u, u_1 even and v, v_1 odd, and that

$$a = \tfrac{1}{2}|\varepsilon^r + \bar{\varepsilon}^r| = \tfrac{1}{2}|\varepsilon_1^z + \bar{\varepsilon}_1^z|, \quad b = \tfrac{1}{2}|\varepsilon^r - \bar{\varepsilon}^r|, \quad b^{y/2} = \tfrac{1}{2}|\varepsilon_1^z - \bar{\varepsilon}_1^z|,$$

where $\varepsilon = u + vi$ and $\varepsilon_1 = u_1 + v_1 i$. It follows that, up to sign, a, b and $b^{y/2}$ are values of binary linear recursive sequences. If $(u, v) = (u_1, v_1)$ then the term $b^{y/2}$ has no primitive divisors, so that on checking tables of binary Lucas sequences having terms without primitive divisors given in [3] and [1] we recover Cao's result [4] mentioned in Introduction.

THEOREM 4.1. *If c is a prime power then the system* (3) *has no solutions subject to restrictions from* (4).

Now we are in a position to prove that the conjecture holds perhaps with the exception of finitely many pairs (c, r).

Subtracting the two equations from (3) results in the Diophantine equation

(11) $$b^y - b^2 = c^z - c^r.$$

Since $6 \leq y$ and $5 \leq z$, for fixed exponents (y, r, z) one gets an algebraic curve of positive genus. The absolute irreducibility and the genus of the curve defined by (11) are given by a theorem of Davenport, Lewis and Schinzel [9].

LEMMA 4.2. *Let $f(X)$ and $g(Y)$ be polynomials with integral coefficients of degree $n > 1$ and respectively $m > 1$. Let $D(\lambda) = \mathrm{disc}(f(X) + \lambda)$ and $E(\lambda) = \mathrm{disc}(g(Y) + \lambda)$. Suppose there are at least $n/2$ distinct roots of $D(\lambda) = 0$ for which $E(\lambda) \neq 0$. Then $f(X) - g(Y)$ is irreducible over the complex field. Further, the genus of the curve $f(x) - g(y) = 0$ is positive*

except possibly when $m = 2$ or $m = n = 3$. Apart from these possible exceptions, the equation $f(x) - g(y) = 0$ has at most finitely many integral solutions.

Stickelberger's formula [21] (cf. [22]) for the discriminant of a trinomial gives

$$\operatorname{disc}(b^y - b^2 + \lambda) = -\lambda(y^{y/2}\lambda^{y/2-1} - 2(y-2)^{y/2-1})^2,$$
$$\operatorname{disc}(c^z - c^r + \lambda) = (-1)^{z(z-1)/2}\lambda^{r-1}(z^z\lambda^{z-r} - (z-r)^{z-r}r^r),$$

so that the last quoted result applies.

Combining these classical facts with some of our results in the previous sections, we obtain the main result of the paper.

THEOREM 4.3. *There are at most finitely many quadruples (a, b, c, r) for which* (2) *holds and* (1) *has more than one solution in integers $x, y, z > 1$. For all of these quadruples, we have $r < 770$.*

Proof. For each fixed pair of odd numbers (r, z), $1 < r < z$, any solution to the system (3) subject to (4) corresponds to an integer point on a curve (11) of positive genus. By Siegel's seminal paper [19], such an equation has only finitely many integral solutions. According to Lemma 3.5, in any compatible system (3) one has $r < 770$ and $z \leq 983$. Moreover, y is bounded from above by 1800 (see Lemma 3.7). Therefore, a compatible system (3) gives rise to finitely many nonrational plane curves, each of which can have only finitely many integer points. ∎

The case when c is the successor of a perfect square has received a lot of attention from people working on Terai's conjecture (cf. [6] and the references therein). Our next result improves on all published results on this case.

THEOREM 4.4. *If in the representation for c derived from Lemma 2.2 one has $v = 1$, then the system* (3) *has no solutions subject to the restrictions from* (4).

Proof. We argue by reduction to absurd. Assume that $c = u^2 + 1$, and consequently $b = \pm\sum_{j=0}^{(r-1)/2} c_{r,j} c^j (-4)^{(r-1)/2-j}$. Suppose that (x, y, z) is a solution to the simultaneous equations (3) satisfying all the conditions from (4). From Lemma 2.2 applied for $n = r$ we know that $a + ib = \eta_1(u + \eta_2 i)^r$ with $\eta_1, \eta_2 \in \{\pm 1\}$, thus

$$a \equiv \pm ru \pmod{u^3}, \quad b \equiv \pm\left(1 - \binom{r}{2}u^2\right) \pmod{u^4},$$

and it follows that

$$c^z = a^2 + b^y \equiv r^2 u^2 + \left(1 - \tfrac{1}{2}r(r-1)yu^2\right) \equiv 1 + zu^2 \pmod{u^4},$$

that is, $\frac{1}{2}r(r-1)\,y + z \equiv r^2 \pmod{u^2}$. On noting that the left-hand side of this relation is greater than the right-hand side (because $y \geq 6$), one obtains the first inequality from the chain

$$(12) \qquad u^2 + r^2 \leq \tfrac{1}{2}r(r-1)y + z < \tfrac{1}{2}r^2 y.$$

The second inequality holds since $z < ry/2$. Indeed, $c^{ry/2} = (a^2 + b^2)^{y/2} > a^2 + b^y = c^z$. Since in this case $u^2 \geq 4 \cdot 10^{10}$, (12) readily contradicts the bounds $r < 770$ and $y < 1800$ already obtained. ∎

We are now in a position to prove Terai's conjecture when b is a prime power. The proof relies on the observation that b is of the form $\pm v U_r$, where

$$U_r = U_r(\alpha, \beta) = \frac{\alpha^r - \beta^r}{\alpha - \beta}$$

is the rth Lucas number associated to the pair $(\alpha, \beta) = (u + vi, u - vi)$. In a subsequent proof we shall use the fact that $a = \pm u \tilde{U}_r$, with

$$\tilde{U}_r = \tilde{U}_r(\tilde{\alpha}, \tilde{\beta}) = \frac{\tilde{\alpha}^r - \tilde{\beta}^r}{\tilde{\alpha} - \tilde{\beta}}$$

the rth Lehmer number associated to the pair $(\tilde{\alpha}, \tilde{\beta}) = (u + vi, -u + vi)$. Recall that a prime divisor of U_r, respectively $\tilde{U}_r$, is called *primitive* if it does not divide

$$(13) \qquad (\alpha - \beta)^2 U_1 \cdots U_{r-1} = -4v^2 U_1 \cdots U_{r-1},$$

respectively

$$(14) \qquad (\tilde{\alpha}^2 - \tilde{\beta}^2)^2 \tilde{U}_1 \cdots \tilde{U}_{r-1} = -16u^2 v^2 \tilde{U}_1 \cdots \tilde{U}_{r-1}.$$

Bilu, Hanrot and Voutier [3] showed that for $n > 30$, the nth Lucas and Lehmer numbers have primitive divisors. Moreover, together with Abouzaid [1] they gave a complete list of n and (α, β), respectively $(\tilde{\alpha}, \tilde{\beta})$, for which $U_r(\alpha, \beta)$ or $\tilde{U}_r(\tilde{\alpha}, \tilde{\beta})$ does not have a primitive divisor.

THEOREM 4.5. *If b is a prime power then the system* (3) *has no solutions subject to the restrictions from* (4).

Proof. Let p be an odd prime and s a positive integer such that $b = p^s$. In view of the result just proved, we conclude that if the system (3) has a solution satisfying (4), then p divides v. Therefore, either $U_r = 1$ or its only prime divisor p is not primitive (see (13)). Checking the relevant tables from [3] and [1], one finds that necessarily $r = 3, 5, 7$ or 13. Moreover, when $r = 3$, c would be even, in contradiction with (4). For $r = 5$, no candidates for (α, β) yield an integer value for v, while for $r = 7$ or 13 the resulting value for u is not an integer. ∎

To the best of our knowledge, the literature contains nothing of the kind of our next result.

THEOREM 4.6. *If a is a prime power then the system* (3) *has no solutions subject to the restrictions from* (4).

Proof. As explained before, we use the equality $a = \pm u\tilde{U}_r$ with $u \geq 2$. We proceed as in the previous proof, reasoning about the Lehmer pair $(\tilde{\alpha}, \tilde{\beta})$ instead of the Lucas pair (α, β). Since the differences are insignificant, the details can be safely left to the reader. ∎

5. Further results. In subsequent reasonings we shall need to know that $v_1 \neq 1$. This fact follows from the following.

LEMMA 5.1. *With the notation of the previous section we have the following two results*:

$$\min\{u_1/v_1, v_1/u_1\} \leq 0.01 \ \Rightarrow \ r \leq 659 \text{ and } z \leq 845$$

and

$$\min\{u_1/v_1, v_1/u_1\} \geq 0.001856.$$

In particular,

$$\min\{u_1, v_1\} \geq 372.$$

Proof. With the notation $\varepsilon_1 = u_1 + iv_1 = |\varepsilon|e^{i\xi_1}$ and $\xi_1' = \pi/2 - \xi_1$, the corresponding linear form is

$$\Lambda = z(2i\xi_1) - k(i\pi/2) = z(-2i\xi_1') - k'(i\pi/2)$$

and when ξ_1 or ξ_1' is small we can get much better estimates in the application of Laurent's lower bound. Technically, we can take a much larger radius of interpolation and we obtain the above upper bounds for r and z.

The proof of the second result is elementary. We have $a = c^{z/2}|\cos(z\xi_1)| = c^{z/2}|\sin(z\xi_1')|$. Hence the condition $(z+1)\xi_1 < \pi/2$ implies

$$|\cos(z\xi_1)| \geq \cos(\pi/2 - \xi_1) = \sin\xi_1 = v_1/\sqrt{c},$$

where $0 < \xi_1 < \tan\xi_1 = v_1/u_1$. It follows that

$$\frac{v_1}{u_1} < \frac{\pi}{2 \cdot 846} = 0.001856733\dots \ \Rightarrow \ a > c^{z/2-1} \geq c^{r/2}.$$

Since $a^2 + b^2 = c^r$, this is a contradiction that proves the lower bound $v_1/u_1 \geq 0.001856$. A similar reasoning leads to the inequality $u_1/v_1 \geq 0.001856$.

Now, since $u_1^2 + v_1^2 > 4 \cdot 10^{10}$, a simple computation gives $\min\{u_1, v_1\} \geq 372$. ∎

In a similar way we can prove partially analogous results concerning the pair (u, v).

LEMMA 5.2. *The following implication holds*:

$$\min\{u/v, v/u\} \leq 0.01 \ \Rightarrow \ r \leq 553 \text{ and } z \leq 705.$$

If the Diophantine system (3) *has solutions satisfying* (4) *with*

$$b \geq c^{(r-1)/2}$$

(*which is true if* $v(r+1) < \pi u$) *then*

$$y \geq 6 \; \Rightarrow \; r \leq 101 \; and \; z \leq 299.$$

Moreover, again under the hypothesis $b \geq c^{(r-1)/2}$,

$$y \geq 10 \; \Rightarrow \; r \leq 47 \; and \; z \leq 227, \quad y \geq 14 \; \Rightarrow \; r \leq 31 \; and \; z \leq 209,$$
$$y \geq 18 \; \Rightarrow \; r \leq 23 \; and \; z \leq 197, \quad y \geq 22 \; \Rightarrow \; r \leq 19 \; and \; z \leq 189,$$
$$y \geq 30 \; \Rightarrow \; r \leq 13 \; and \; z \leq 185, \quad y \geq 50 \; \Rightarrow \; r \leq 7 \; and \; z \leq 161,$$
$$y \geq 70 \; \Rightarrow \; r \leq 5 \; and \; z \leq 155, \quad y \geq 98 \; \Rightarrow \; r \leq 3 \; and \; z \leq 147,$$

and there is no solution for $y \geq 142$.

We add some other estimates related to b.

LEMMA 5.3. *If the Diophantine system* (3) *has solutions satisfying* (4) *then*

$$ry/2 = z + 2t \quad with \; t \geq 1,$$

and

$$b < c^{r/2 - 2/y}.$$

Moreover, if

$$b \geq (1 + 10^{-20}) \, c^{r/2 - 4/y}$$

then

$$ry/2 = z + 2.$$

If $ry/2 = z + 2$ *then*

$$y \geq 6 \; \Rightarrow \; r \leq 101, \quad y \geq 10 \; \Rightarrow \; r \leq 47, \quad y \geq 14 \; \Rightarrow \; r \leq 29,$$
$$y \geq 18 \; \Rightarrow \; r \leq 19, \quad y \geq 22 \; \Rightarrow \; r \leq 17, \quad y \geq 26 \; \Rightarrow \; r \leq 13,$$
$$y \geq 30 \; \Rightarrow \; r \leq 11, \quad y \geq 38 \; \Rightarrow \; r \leq 9, \quad y \geq 42 \; \Rightarrow \; r \leq 7,$$
$$y \geq 50 \; \Rightarrow \; r \leq 5, \quad y \geq 66 \; \Rightarrow \; r = 3,$$

and there is no solution for $y \geq 102$.

Proof. We give a proof just for the first two assertions. From the relations

$$(a^2 + b^2)^{y/2} > a^2 + b^y = c^z$$

we deduce $ry/2 > z$ and the first assertion follows since $ry/2$ and z are both odd.

If $b \geq (1 + 10^{-20})c^{r/2 - 4/y}$ then, since $b^y > (1 - 10^{-21})c^z$, we see that $z > ry/2 - 4$ and the relation $z = ry/2 - 2$ follows from the first assertion.

The remaining estimates result from computation with the help of lower bounds on linear forms. ∎

Our next result improves upon the main results of [25], [5] (see (α) and respectively (γ) in Introduction) and [13] (the reader is warned that in Le's paper b denotes the unique even number among a and b).

PROPOSITION 5.4. *If system* (3) *has solutions subject to the restrictions from* (4) *then*

$$a > 4.608\,b, \quad c > 3^{y-10}, \quad y \le 2z + 4.$$

Moreover,

$$y \le 2z - 4 \quad for \; y \ge 34$$

and

$$y \ge 602 \;\Rightarrow\; r \le 149 \; and \; z \le 319.$$

In particular,

$$y \le 634.$$

Proof. When $y \le 10$ one has $c > 10^y$ because $c > 4 \cdot 10^{10}$. For the same reason, $c > 2.2^y$ when y is between 14 and 30. It is much harder to obtain similar inequalities for higher values of y. We now prove that always $c > 2.1716^y$.

As seen above, v_1 has a prime divisor p. Recall that in Lagrange's formula given in Lemma 2.1 the coefficients for n odd are

$$c_{n,j} = \frac{(n-j-1)!\,n}{(n-2j)!\,j!},$$

where $0 \le j \le (n-1)/2$, and the quotient $(n-j-1)!/j!$ is an integer. It follows that

$$v_p(c_{n,j}) \ge v_p(n) - v_p((n-2j)!) > v_p(n) - \frac{n-2j}{p-1} \ge v_p(n) - \frac{n-2j}{2}.$$

As p divides v_1, it does not divide c, and therefore

$$
\begin{aligned}
v_p(c_{z,j}c(-4v_1^2)^{(z-1)/2-j}) &= v_p(c_{z,j}) + (z-1-2j)v_p(v_1) \\
&\ge v_p(z) - \tfrac{1}{2}(z-1-2j) + (z-1-2j)v_p(v_1) \\
&\ge v_p(z) + \tfrac{1}{2}(z-1-2j)v_p(v_1) > v_p(z)
\end{aligned}
$$

for $0 \le j < (z-1)/2$.

Corollary 2.4 yields

$$yv_p(b) = 2(v_p(z) + v_p(v_1)).$$

Having in mind the upper bounds for z given in Lemma 3.5, we see that for $y \ge 34$ we have $v_3(z) \le 5$, and $v_p(z) \le 3$ for $p \ge 5$. Consequently, for $p = 3$ one obtains

$$c > v_1^2 \ge 3^{y-10} \ge 3^{y(1-5/17)} > 2.1716^y.$$

For $p \ge 5$ one has $c > p^{y-6} \ge 5^{y-6} > 3^{y-10}$, so that the claim that $c > 2.1716^y$ is true for any solution of the system (3) satisfying (4).

Set provisionally $\mu = b^2/c^r$. Then $c^z > b^y$ implies that

$$\mu^{y/2} < c^{z-ry/2} \leq c^{-2} < 2.1716^{-2y}.$$

Hence,

$$a = b\sqrt{\mu^{-1} - 1} > b\sqrt{2.1716^4 - 1} > 4.608\, b.$$

Since $a^2 < c^{z-2}$ and $c > 10^{10}$ we have $b^y > (1 - 10^{-20})c^z$, and the inequality $c > 2.1716^y$ implies

$$b > 2.171^z.$$

The inequalities relating y and z are proved in three steps. First, we show that we always have $y \leq 2z + 12$. Next, we disprove the equalities $y = 2z + 8$ and $y = 2z + 12$ by combining information already available with some more computations. Similar arguments are employed to show that one cannot have $y = 2z + 4$ for $y \geq 34$, while $y \neq 2z$ follows from a result of Darmon and Merel mentioned in Remark 2 below. Here are the details.

The upper bound

$$y < z\left(2 + \frac{\log(1 + (r+1)^2/\pi^2)}{\log b}\right),$$

combined with the lower bound $b > 2.171^z$, leads to

$$y < 2z + \frac{\log(1 + (r+1)^2/\pi^2)}{\log 2.171}.$$

The bound $y \leq 2z + 12$ is trivially satisfied for $y \leq 22$, and for $y \geq 22$ we have seen that $r < 396$, so that

$$y < 2z + \frac{\log(1 + 396^2/\pi^2)}{\log 2.171} < 2z + 12.5,$$

which implies $y \leq 2z + 12$. To show that the equality in this relation never holds, one argues similarly to the case $y = 2z + 4$ for $y \geq 34$ detailed below. Then one repeats the reasoning to show that $y \neq 2z + 8$, so that we always have

$$y \leq 2z + 4.$$

Suppose that $y = 2z + 4$ for some $y \geq 34$. Chen's result recalled in the proof of Theorem 5.6 implies $y \geq 38$ and we verify by a computation with linear form estimates that

$$y \geq 38 \implies r \leq 239.$$

From the relation $b^y < c^z$, we get

$$y = 2z + 4 \implies b < c^{1/2 - 2/y}.$$

Moreover, we know that

$$b < c^{(r-1)/2} \implies u < (r+1)v/\pi \implies c < (1 + (r+1)^2/\pi^2)v^2.$$

Put $b = vb'$; then b' is a positive integer. The above facts imply

$$y = 2z + 4 \;\Rightarrow\; c < \left(\frac{1}{b'} \sqrt{1 + \frac{(r+1)^2}{\pi^2}} \right)^{y/2}.$$

Now we consider v_1. We have $v_1 > u_1 \pi / (2(z+1))$, thus

$$v_1^2 > \left(1 + \frac{4(z+1)^2}{\pi^2} \right)^{-1} c.$$

Moreover, we can write

$$v_1 = w_1^{y/2} / w_0, \quad \text{where} \quad w_0 \mid \gcd(z, v_1^2)$$

and $b = w_1 b''$, where b'' is a positive integer.

If $b' = 1$, a short computer verification shows that $w_1 < 9$ for $y \geq 38$. Since w_1 is an odd integer greater than 1, one has $w_1 \in \{3, 5, 7\}$. But we know that b is not a power of a prime, hence $b' \geq 3$, with $b' \geq 5$ when $w_1 = 3$. Using now $b' \geq 3$, another computer verification leads to $w_1 \in \{3, 5\}$ and $w_1 = 3$ for $y \geq 102$.

Now we apply again Laurent's result but with the much better lower bound $c > 3^{y-10}$ (better for $y \geq 34$ than $c > 4 \cdot 10^{10}$) and we get for example

$$y \geq 102 \;\Rightarrow\; r \leq 181 \text{ and } z \leq 373,$$
$$y \geq 302 \;\Rightarrow\; r \leq 157 \text{ and } z \leq 329,$$
$$y \geq 602 \;\Rightarrow\; r \leq 149 \text{ and } z \leq 319.$$

Comparing the previous estimates we conclude that we always have $y \leq 634$. ∎

COROLLARY 5.5. *Assume* (2) *holds and* $b > 0.218\,a$. *Then Conjecture* 1.1 *is true.*

It is very likely that actually there are no solutions to (3) under the conditions stated in (4). This is the case under the hypothesis of our last result.

THEOREM 5.6. *The system* (3) *has no solutions* (r, y, z) *subject to the restrictions* (4) *in which z is divisible by 3 and* $y \neq 6$, 10, 14, 18, 30, 42, 50, 54, 62, 70, 90, 98, 126, 150, 162, 186, 210, 250, 270, 294, 310, 350, 378, 434, 450, 486, 490, 558, 630.

Proof. I. Chen [7] very recently proved that for any prime satisfying the restrictions $7 < p < 10^7$ and $p \neq 31$ there are no coprime integers A, B, C satisfying

$$A^2 + B^{2p} = C^3.$$

This confirms Terai's conjecture in case z is a multiple of 3 and y has a prime divisor $p > 7$, $p \neq 31$. The only values of the y-component in a

solution of (3)–(4) not covered by Chen's result are listed in the statement, by taking into account Proposition 5.4. ∎

The following remarks are helpful when trying to further reduce the number of candidate pairs (y, z).

REMARK 1. When r divides z, we may remove the multiples of 3 from this list because Mignotte and Pethő [16] have proved that if there are points with both coordinates greater than 1 on the curve $X^m - X = Y^n - Y$, then $\gcd(m, n) = 1$.

REMARK 2. A deep result of Darmon and Merel [8], according to which the equation $X^n + Y^n = Z^2$ has no solutions in nonzero integers when $n \geq 4$, implies that $\gcd(y, z) \leq 3$ always holds.

References

[1]   M. Abouzaid, *Les nombres de Lucas et Lehmer sans diviseurs primitifs*, J. Théor. Nombres Bordeaux 18 (2006), 299–313.

[2]   J. M. Basilla, *On the solution of $x^2 + dy^2 = m$*, Proc. Japan Acad. Ser. A Math. Sci. 80 (2004), 40–41.

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

[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. L. Dong, *On the Terai–Jeśmanowicz conjecture*, Publ. Math. Debrecen 61 (2002), 253–265.

[6]   —, —, *An application of a lower bound for linear forms in two logarithms to the Terai–Jeśmanowicz conjecture*, Acta Arith. 110 (2003), 153–164.

[7]   I. Chen, *On the equation $s^2 + y^{2p} = \alpha^3$*, Math. Comput. 262 (2007), 1223–1227.

[8]   H. Darmon and L. Merel, *Winding quotients and some variants of Fermat's last theorem*, J. Reine Angew. Math. 490 (1997), 81–100.

[9]   H. Davenport, D. J. Lewis and A. Schinzel, *Equations of the form $f(x) = g(y)$*, Quart. J. Math. 12 (1961), 304–312.

[10] L. Jeśmanowicz, *Some remarks on Pythagorean numbers*, Wiadom. Mat. (2) 1 (1956), 196–202.

[11] M. Laurent, *Linear forms in two logarithms and interpolation determinants II*, Acta Arith. 133 (2008), 325–348.

[12] M. Laurent, M. Mignotte et Yu. Nesterenko, *Formes linéaires en deux logarithmes et déterminants d'interpolation*, J. Number Theory 55 (1995), 285–321.

[13]   M. H. Le, *A conjecture concerning the exponential diophantine equation $a^x + b^y = c^z$*, Acta Arith. 106 (2003), 345–353.
[14]   —, *A conjecture concerning the pure exponential equation $a^x + b^y = c^z$*, Acta Math. Sinica English Ser. 21 (2004), 943–948.
[15]   K. Mahler, *Zur Approximation algebraischer Zahlen I: Über den grössten Primteiler binären Formen*, Math. Ann. 107 (1933), 691–730.
[16]   M. Mignotte and A. Pethő, *On the Diophantine equation $x^p - x = y^q - y$*, Publ. Mat. 43 (1999), 207–216.
[17]   L. J. Mordell, *Diophantine Equations*, Academic Press, London, 1969.
[18]   A. Nitaj, *L'algorithme de Cornacchia*, Expo. Math. 13 (1995), 358–365.
[19]   C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abh. Akad. Wiss. Göttingen. Math.-Phys. Kl. 1 (1929), 70 pp.; reprinted in *Collected Works*, Springer, Berlin, 1966, 209–266.
[20]   W. Sierpiński, *On the equation $3^x + 4^y = 5^z$*, Wiadom. Mat. (2) 1 (1956), 194–195.
[21]   L. Stickelberger, *Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper*, in: Verhandlungen des ersten Internationalen Mathematiker-Kongresses, Zürich, 1897, 182–193.
[22]   R. G. Swan, *Factorization of polynomials over finite fields*, Pacific J. Math. 12 (1962), 1099–1106.
[23]   N. Terai, *The Diophantine equation $a^x + b^y = c^z$*, Proc. Japan Acad. Ser. A Math. Sci. 70 (1994), 22–26.
[24]   —, *The Diophantine equation $a^x + b^y = c^z$. III*, ibid. 72 (1996), 20–22.
[25]   —, *Applications of a lower bound for linear forms in two logarithms to exponential Diophantine equations*, Acta Arith. 90 (1999), 17–35.

Institute of Mathematics   U. F. R. de Mathématiques
Romanian Academy   Université Louis Pasteur
P.O. Box 1-764   7, rue René Descartes
RO-014700 Bucureşti, Romania   67084 Strasbourg Cedex, France
and   E-mail: mignotte@math.u-strasbg.fr
U. F. R. de Mathématiques
Université Louis Pasteur
7, rue René Descartes
67084 Strasbourg Cedex, France
E-mail: mihai.cipu@imar.ro