Bull. Math. Soc. Sci. Math. Roumanie
Tome 53(101) No. 3, 2010, 231–237

Bounds for counterexamples to Terai's conjecture

by
Mihai Cipu and Maurice Mignotte

Dedicated to the memory of Laurenţiu Panaitopol (1940-2008) on the occasion of his 70th anniversary

Abstract

We give strong bounds for putative counterexamples to a conjecture of Terai (1994) asserting that if a, b, c are fixed coprime integers with $\min(a,b,c) > 1$ such that $a^2 + b^2 = c^r$ for a certain odd integer $r > 1$, then the equation $a^x + b^y = c^z$ has only one solution in positive integers with $\min(x,y,z) > 1$. Moreover, we confirm the conjecture in case z is multiple of 3.

Key Words: Simultaneous exponential equations, linear forms in logarithms.
2010 Mathematics Subject Classification: Primary 11D09; Secondary 11D45, 11J20, 11J86.

1 The results

The statement that for any coprime integers a, b, c with $\min(a,b,c) > 1$ there exists at most one solution (x,y,z) in integers greater than 1 to the equation

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

is nowadays referred to as Terai's conjecture. It is still open in full generality, only particular instances have been confirmed (see, e.g., [14]). Recent results have been established in the case

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

In this case it is known that $(2,2,r)$ is the only solution to the equation (1) if a single one of the following additional conditions holds:

(α) (Cao [2]) c is a prime power,

(β) (Le [11]) $c > 3 \cdot 10^{27}$ and $r > 7200$,

(γ) (Cipu-Mignotte [5]) a or b is a prime power.

These papers contain references to the work of other authors who have pointed out conditions under which the conjecture can be proved.

Bounds for the size of solutions can be derived from Yu's work on linear forms in p-adic logarithms. Hirata-Kohno [8] gives the following answer to the question: *How big can be the components of a solution to Eq.* (1)?

Theorem 1.1. *Suppose that c is odd and has the prime decomposition $c = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$. Assume moreover that there exists an integer $g \geq 2$ coprime with c such that*

$$v_{p_i}(a^g - 1) \geq e_i \quad \textit{and} \quad v_{p_i}(b^g - 1) \geq 1, \; i = 1, 2, \ldots, s.$$

Then we have

$$\max\{|x|, |y|, |z|\} \leq 2^{288} \sqrt{abc} \left(\log(abc)\right)^3.$$

The main result of [5] is that there are at most finitely many values (c, r) as above for which Terai's conjecture can be refuted.

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

In order to prove this result, the authors study the positive solutions (r, y, z) to the system of Diophantine equations

$$a^2 + b^2 = c^r, \qquad a^2 + b^y = c^z, \tag{3}$$

where

$$r, z > 1 \text{ are odd}, \; a \equiv 2 \pmod 4, \; b \equiv 3 \pmod 4, \; \text{and } \gcd(a, b) = 1. \tag{4}$$

It can be shown that it necessarily holds $y \equiv 2 \pmod 4$, so that $y \geq 6$. Combining the study of arithmetical properties of hypothetic solutions with extensive computations, in [5] it is established that the existence of at least one solution to the system (3) entails the following bounds:

$$c > 4 \cdot 10^{10}, \; y \leq 634, \; r \leq 769, \; z \leq 983.$$

The aim of this note is to improve this by pointing out stronger necessary conditions that must be satisfied by hypothetic solutions of the system under investigation.

Theorem 1.3. *If the system* (3) *has solutions subject to restrictions from* (4) *then:*

a) $c > 10^{24000}$, $a > 10^{77.668}\, b$, $b > 10^{38.83\, z}$,

b) $y \le 2z - 4$, $y \le 618$,

c) *for* $y = y_0$ *one has* $r \le r_0$, *with* y_0, r_0 *given as in Table 1, and*

d) *for* $r \le r_0$ *one has* $z \le z_0$, *where* r_0 *and* z_0 *are given in Table 2.*

y_0	6	10	14	18	22	30	50	70	310
r_0	387	259	219	197	185	173	159	153	141

Table 1: Bounds for r

r_0	3	5	7	9	11	21	31	167
z_0	147	157	167	175	185	197	205	375

Table 2: Bounds for z

In a different vein, we can confirm Terai's conjecture under an extra mild assumption.

Theorem 1.4. *The system* (3) *has no solutions subject to restrictions from* (4) *in which* z *is divisible by 3.*

It is possible to prove further necessary conditions for hypothetical solutions. For instance, the next result helps to shrink the search space for any instance of the system of interest.

Theorem 1.5. *Let* (x, y, z) *be a solution to* (3) *satisfying the hypotheses from Eq.* (4). *If* y *has a prime factor greater than 17 which is congruent to 1 modulo 4 then* z *is not divisible by 5.*

In the next section we will describe the method used to establish such results. We largely follow [5] and therefore do not write down here all the details. However, we strive to provide enough explanations, so that the reader understand and possibly replicate what we have done.

2 The approach

As is well-known, the equation

$$a^2 + b^2 = c^r \tag{5}$$

implies that c is a sum of two squares, which are coprime if a and b are supposed so. All such decompositions for a given value of c can be obtained by using Cornacchia's algorithm (see, for instance, [1]). Knowing the structure of integer solutions to (5) (cf. [12, pp.122–123]), we then obtain the values of a and b corresponding to each decomposition $c = u^2 + v^2$, with u even, v odd and $\gcd(u, v) = 1$. The pairwise comparison of y, r, z is possible thanks to the next result, proved in [5, Lemma 3.4].

Lemma 2.1. *Assume all conditions* (3)–(4) *are fulfilled. 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* $\mu_1 > 0$, $\mu_2 > 0$ *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.*

Another key ingredient of our procedure is a very recent version of Laurent [9] for the main theorem of Laurent-Mignotte-Nesterenko [10]. The novelty is the appearance of an extra parameter on which the lower bound for a linear form in logarithms

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

depends. Here, α_1 and α_2 are nonzero algebraic numbers, both different from 1, and b_1 and b_2 are positive integers. By carefully exploiting the additional degree of liberty thus gained, it is possible to provide improved lower bounds for $|\Lambda|$. These in turn imply inequalities of the type taken care of by part *c*) of Lemma 2.1. In this way one can bound from above r. A similar technique, combining Laurent's theorem with part *a*) of Lemma 2.1, allows us to derive bounds for z.

Essentially the same arguments have been employed in [5, Prop. 5.5] to prove that one always has $y \leq 2z + 4$ and even better $y \leq 2z - 4$ for $y \geq 34$. Therefore, an upper bound on z readily yields an upper bound on y.

In the proofs of results from our previous work [5], we have applied Cornacchia's algorithm for all $c < 4 \cdot 10^{10}$. To obtain the upper bounds for y, r and z reported in this paper we extended the computations for $c < 10^{11}$. Going beyond this threshold is extremely time consuming in the computational environment we have access to. In order to improve the value of c for which the system (3) is solvable under the conditions stated in (4), we have made extensive use of Laurent's theorem. Namely, we made further computations using the already obtained bounds on r and z and studied suitable linear forms in the logarithms of algebraic numbers numerically. After about one week (and in several steps) we could verify that the conditions (3)–(4) do not simultaneously hold if $c < 10^{24000}$.

We resume our computations by incorporating the piece of information just gained $c > 10^{24000}$. Since we already know that $y \leq 634$, it readily follows

$$c > 10^{24000\, y/634} > 10^{37.854\, y}. \tag{6}$$

Put $\mu = b^2/c^r$. As $c^z > b^y$, we have

$$\mu^{y/2} < c^{z-ry/2} \leq c^{-2} < 10^{-75.708\, y},$$

and therefore

$$a = b\sqrt{\mu^{-1} - 1} > b\sqrt{10^{151.416} - 1} > 10^{75.7}\, b. \tag{7}$$

Since $a^2 < c^{z-2}$ and $c > 10^{24000}$, we have $b^y > (1 - 10^{-48000})c^z$, and the inequality (6) yields

$$b > 10^{37.85\, z}. \tag{8}$$

This together with $r < 770$ and the upper bound

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

obtained in the proof of Lemma 3.7 from [5] give at once

$$y < 2z + \frac{\log\left(1 + 770^2/\pi^2\right)}{37.85 \log 10} < 2z + 1,$$

so that $y \leq 2z$. The equality can not hold in this relation because Darmon and Merel [7] have proved that the equation $X^n + Y^n = Z^2$ has no solutions in nonzero integers when $n \geq 4$. We thus obtained the first inequality stated in part *b*) of Theorem 1.3. In order to prove the second inequality in part *b*) and the remaining claims, we apply again Laurent's result and get $z \leq 311$ as soon as $y \geq 602$.

The stronger lower bounds for a and b stated in part *a*) are derived by iterating the above reasoning, after replacing (6) by

$$c > 10^{24000\, y/618} > 10^{38.834\, y}.$$

Now we come to the proof of Theorem 1.4. In [5, Prop. 5.4] the assertion is established provided that y has a prime divisor $p > 7$, $p \neq 31$, by using a theorem of Chen [3]. This hypothesis can be removed thanks to results brought to our attention by M.A. Bennett. In [6], Dahmen shows that $A^2 + B^{62} = C^3$ and $A^2 + B^{10} = C^3$ have no solutions in coprime nonzero integers. In the case when 7 divides y, the conclusion of our theorem follows from [13]. Since it is known that $1^6 + 2^3 = 3^2$ and permutations thereof are the only equations of the type $A^2 + B^6 = C^3$ solvable in coprime nonzero integers, the proof is complete.

Theorem 1.5 follows similarly from a difficult result of Chen [4] concerning the Diophantine equation $A^2 + B^{2p} = C^5$.

Acknowledgements

We are grateful to M.A. Bennett for help with the proof of Theorem 1.4. The first author has been partially supported by the CEEX Program of the Romanian Ministry of Education, Research and Youth, Grant 2-CEx06-11-20/2006.

References

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

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

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

[4] I. Chen, On the equation $a^2 + b^{2p} = c^5$, submitted.

[5] M. Cipu and M. Mignotte, On a conjecture on exponential Diophantine equations, Acta Arith., **140**(2009), 251–270.

[6] S.R. Dahmen, A refined modular approach to the Diophantine equation $x^2 + y^{2n} = z^3$, arXiv:1002.0020

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

[8] N. Hirata-Kohno, S-unit equations and integer solutions to exponential Diophantine equations, in *Analytic Number Theory and surrounding Areas 2006*, Kyoto RIMS Kokyuroku, 2006, 92–97. (see http://hdl.handle.net/2433/58606)

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

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

[11] M.H. Le, A conjecture concerning the pure exponential equation $a^x + b^y = c^z$, Acta Math. Sinica, English Series, **21**(2004), 943–948.

[12] L.J. Mordell, *Diophantine Equations*, Academic Press, London, 1969.

[13] B. Poonen, E.F. Schaeffer and M. Stoll, Twists of $X(7)$ and primitive solutions to $x^2 + y^3 = z^7$, Duke Math. J. **137**(2007), 103–158.

[14] N. Terai, The diophantine equation $a^x + b^y = c^z$, Proc. Japan Acad. Ser. A Math. Sci., **70**(1994), 22–26.

Received: 20.04.2010.

Institute of Mathematics
of the Romanian Academy,
P.O Box 1–764,
RO-014700 Bucharest,
Romania,
E-mail: `mihai.cipu@imar.ro`

Université de Strasbourg,
U. F. R. de Mathématiques,
7, rue René Descartes,
67084 Strasbourg Cedex,
France
E-mail: `maurice.mignotte@math.unistra.fr`