Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Robert Tijdeman

# Some applications of Baker's sharpened bounds to diophantine equations

*Séminaire Delange-Pisot-Poitou. Théorie des nombres*, tome 16, n° 2 (1974-1975), exp. n° 24, p. 1-7

<http://www.numdam.org/item?id=SDPP_1974-1975__16_2_A3_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
16e année, 1974/75, n° 24, 7 p.

26 mai 1975

# SOME APPLICATIONS OF BAKER'S SHARPENED BOUNDS TO DIOPHANTINE EQUATIONS

by Robert TIJDEMAN [Leiden]

1. In 1966-1968, BAKER [1] published four papers entitled "Linear forms in the logarithms of algebraic numbers". His results were improved by himself and others. Some very important improvements can be found in a serie of three papers of BAKER [4] named "A sharpening of the bounds for linear forms in logarithms", which were published in 1972-1975. I shall discuss some consequences of the first of these papers to the following diophantine equations.

$$ax^n - by^n = k \ , \qquad a\ , b\ , x\ , y\ , k \in \underset{\sim}{A} \cap \underset{\sim}{R}\ , \qquad n \in \underset{\sim}{N}\ , \tag{1}$$

$$y^m = P(x)\ , \qquad m\ , x\ , y \in \underset{\sim}{N}\ , \quad P \in \underset{\sim}{Q}[z]\ , \tag{2}$$

$$x^m - y^n = 1\ , \qquad m\ , n\ , x\ , y \in \underset{\sim}{N}\ . \tag{3}$$

As usual $\underset{\sim}{N}$ , $\underset{\sim}{Q}$ , $\underset{\sim}{A}$ , $\underset{\sim}{R}$ stand for positive rational integers, rational numbers, algebraic numbers and real numbers.

2. Let us first assume that $a$ , $b$ , $k$ and $n$ in equation (1) are fixed positive rational integers with $n \geqslant 3$ . It was proved by THUE [18], around 1908, that (1) has only finitely many integer solutions $x$ , $y$ . In fact, THUE proved his result for the class of equations $f(x\ , y) = k$ , where $k$ is a non-zero integer, and $f$ is an irreducible binary form with integer coefficients of degree $n \geqslant 3$ . He derived this result from his theorem on the approximation of algebraic numbers by rationals. This last theorem was subsequently improved by SIEGEL, and ROTH [10]. The well known theorem of Thue-Siegel-Roth states that for any algebraic number $\alpha$ and for any $\varepsilon > 0$ there exists a constant $c_1 = c_1(\alpha\ , \varepsilon) > 0$ such that

$$|\alpha - \frac{x}{y}| > \frac{c_1}{y^{2+\varepsilon}} \quad \text{for all} \quad x\ , y \in \underset{\sim}{Z} \quad \text{with} \quad \alpha \neq \frac{x}{y}\ . \tag{4}$$

We now assume that $a$ , $b$ and $k$ are positive algebraic numbers. We apply inequality (4) with $\alpha = \sqrt[n]{b/a}$ . Hence, there exists a constant $c_2 = c_2(a, b, n, \varepsilon) > 0$ such that

$$|\sqrt[n]{\frac{b}{a}} - \frac{x}{y}| > \frac{c_2}{y^{2+\varepsilon}}\ . \tag{5}$$

On the other hand, by the mean value theorem, there exists a $\xi$ with $\sqrt[n]{b/a} < \xi < x/y$ such that

$$0 < (\frac{x}{y})^n - \frac{b}{a} = (\frac{x}{y} - \sqrt[n]{\frac{b}{a}})n\xi^{n-1}\ .$$

So we obtain

$$(6) \qquad 0 < \frac{x}{y} - \sqrt[n]{\frac{b}{a}} = \frac{1}{n\xi^{n-1}} \cdot \frac{k}{ay^n} \leqslant c_3 \frac{k}{y^n}$$

for some $c_3 = c_3(a , b , n) > 0$ . The combination of (5) and (6) yields a constant $c_4 = c_4(a , b , n , \varepsilon) > 0$ such that

$$(7) \qquad k > c_4\, y^{n-2-\varepsilon} \, .$$

In particular, if $a$ and $b$ are fixed algebraic numbers, $n \geq 3$ is a fixed positive integer, and $k$ is bounded, then there exist only finitely many rational integers $(x , y)$ satisfying (1).

Roth's theorem has been generalized by W. M. SCHMIDT [12]. Let $\alpha$ be an algebraic integer, $d$ a positive (rational) integer, and $\varepsilon > 0$ . Schmidt's theorem implies the existence of a constant $c_5 = c_5(\alpha , d , \varepsilon) > 0$ such that

$$|\alpha - \beta| > \frac{c_5}{H^{d+1+\varepsilon}}$$

for every algebraic number $\beta \neq \alpha$ of degree at most $d$ and with height at most $H$ $(\geq 2)$ . One can deduce as above that if $x/y$ is an algebraic number of degree at most $d$ and height at most $H$ such that (1) holds, then there exists a constant $c_6 = c_6(a , b , n , d , \varepsilon) > 0$ such that

$$(8) \qquad k > c_6 \frac{y^n}{H^{d+1+\varepsilon}} \, .$$

$\underset{\sim}{3}$. Several authors have given upper bounds for the number of solutions $x , y , k \in \underset{\sim}{N}$ of equation (1) for fixed rational integers $a$ , $b$ (See for example SIEGEL [16], HYYRÖ [7]). However, all theorems which I have mentioned up to now in $\underset{\sim}{2}$ and $\underset{\sim}{3}$ have the disadvantage that their proofs are ineffective. This implies that the constants $c_4$ and $c_6$ cannot be calculated from the proofs. The first effective proof of Thue's result on $f(x , y) = k$ was given by BAKER [2] in 1968. This was one of the first applications of Baker's method on linear forms in the logarithms of algebraic numbers. Baker's sharpened bounds were recently used by SPRINDZUK [17] to derive a generalization to norm forms.

In order to illustrate the applicability of Baker's sharpened bounds to equation (1), we assume that $a , b , k , x , y$ are positive algebraic numbers of degree at most $d$ . It follows from (1) that

$$\frac{a}{b} \left(\frac{x}{y}\right)^n - 1 = \frac{k}{by^n} > 0 \, .$$

Hence,

$$(9) \qquad 0 < \log \frac{a}{b} + n \log \frac{x}{y} < \frac{k}{by^n} \, .$$

This is a linear form in the logarithms of algebraic numbers. Baker's "sharpened" theorem ([4], I) reads as follows. (By $\log x$ , we mean the principal value of $\log x$ .)

THEOREM 1. - *Let* $\alpha_1 , \dots , \alpha_n$ *be non-zero algebraic numbers with degrees at most* $d$ , *and let the heights of* $\alpha_1 , \dots , \alpha_{n-1}$ *and* $\alpha_n$ *be at most* $A'$ $(\geq 2)$ *and* $A$ $(\geq 2)$ *respectively. Then there exists on effectively computable constant* $C = C(d , n , A')$ *such that the inequalities*

$$0 < |b_1 \log \alpha_1 + \dots + b_n \log \alpha_n| < \exp( - C \log A \log B)$$

*have no solutions in rational integers* $b_1 , \dots , b_n$ *with absolute values at most* $B$ $(\geq 2)$ .

Hence there exists a constant $c_7 = c_7(a , b , d) > 0$ such that

$$(10) \qquad |\log \frac{a}{b} + n \log \frac{x}{y}| > \exp( - c_7 \log H \log n) ,$$

where $H$ $(\geq 2)$ is an upper bound for the height of $x/y$ .

On combining (9) and (10), we obtain

$$(11) \qquad k > \frac{by^n}{H^{c_7 \log n}} .$$

The bound for $k$ is comparable with (8), but the constant $c_7$ is effectively computable. It follows from [19] (Theorem 2] that there are positive constants $c_8 = c_8(d)$ and $c_9$ such that $c_7 = c_8(\log h)^{c_9}$ , where $h$ $(\geq 2)$ is the height of $a/b$ .

A very remarkable feature of (11) is the fact that $c_7$ dies not depend on $n$ . Let us assume that $a , b , k , x$ and $y$ are positive rational integers, $y \geq 2$ . Then $H \leq \max(x , y) \leq c_{10}(a , b , k)y$ in view of (1). It follows from (11) that for $n > c_7 \log n$

$$kc_{10}^{c_7 \log n} > by^{n-c_7 \log n} \geq b.2^{n-c_7 \log n} .$$

Hence, $n \leq c_{11}(a , b , k)$ . BAKER's effective proof of Thue's theorem [2], implies that for every integer $n \geq 3$ there exist effective upper bounds for $x$ and $y$ . So we have deduced as a simple consequence of a much more general result.

THEOREM 2. - *Let* $a$ , $b$ *and* $k$ *be fixed positive rational integers. Then the number of solutions in integers* $n \geq 3$ , $x \geq 2$ , $y \geq 2$ *of the inequality* $ax^n - by^n = k$ *is finite. There are effectively computable upper bounds for* $n$ , $x$ *and* $y$ .

4. We turn our attention to the equation $y^m = P(x)$ , where $P \in \mathbb{Z}[z]$ and $m$ is an integer, $m \geq 2$ . There are some trivial cases in which there might be infinitely many integer solutions $x , y$ . For example, if $m = 2$ and the degree of $P$ equals 2 (Pellian equation) or if $P$ has only one distinct root. On the other hand, it follows from a much more general result of SIEGEL ([14], [15]) that (2) has only finitely many integer solutions $x$ , $y$ if

(a) $P$ has at least two distinct simple roots and $m \geq 3$ or

(b) $P$ has at least three distinct simple roots and $m = 2$ .

Siegel's proof is ineffective, and the first effective proofs of (a) and (b) were given by BAKER [3]. These results imply that under very general conditions a polynomial with integer coefficients assumes at most finitely many squares, finitely many cubes, and so on, at integer points.

One may ask whether it can occur at all that a polynomial assumes infinitely many perfect powers at integer points. Of course this might happen if $P$ has only one distinct root. The following theorem shows that in all other cases only finitely many different kinds of powers can be attained at integer points.

THEOREM 3 (SCHINZEL and TIJDEMAN [11]). - *If a polynomial* $P(x)$ *with rational coefficients has at least two distinct zeros, then the equation*

$$y^m = P(x)$$

*in integers* $x$ , $y$ *with* $|y| > 1$ *implies* $m < c(P)$ , *where* $c(P)$ *is an effectively computable constant.*

The following reasoning shows the relation between the equations (1) and (2).

Let $K$ be the splitting field of $P$ , and let

$$(12) \qquad y^m = P(x) = a \prod_{i=1}^{n} (x - \alpha_i)^{r_i} .$$

For our convenience we assume $a = r_1 = r_2 = 1$ . Since for every integer $x$ ,

$$(x - \alpha_i \, , \, x - \alpha_j) | (\alpha_i - \alpha_j)$$

the highest common divisor of any two factors on the right hand side of (12) is composed exclusively of prime ideals of $K$ dividing $\Delta = \prod_{i<j} (\alpha_i - \alpha_j)$ . Hence, for $i = 1 , 2$ , we have

$$x - \alpha_i = \mathfrak{b}_i \, \mathfrak{c}_i^m$$

for some ideals $\mathfrak{b}_i$ and $\mathfrak{c}_i$ such that $\mathfrak{b}_i$ is composed exclusively of prime factors of $\Delta$ and $(\mathfrak{c}_i , \Delta) = 1$ . Denote by $\mathfrak{b}_i'$ and $\mathfrak{c}_i'$ ideals of $K$ inverse to $\mathfrak{b}_i$ and $\mathfrak{c}_i$ , respectively. Then

$$\mathfrak{b}_i' \, \mathfrak{c}_i'^m (x - \alpha_i) = (\mathfrak{b}_i \, \mathfrak{b}_i')(\mathfrak{c}_i \, \mathfrak{c}_i')^m .$$

So we find algebraic integers $\xi_i$ and $\eta_i$ such that

$$x - \alpha_i = \xi_i \, \eta_i^m \qquad i = 1 , 2 .$$

Hence,

$$\xi_1 \, \eta_1^m - \xi_2 \, \eta_2^m = (x - \alpha_1) - (x - \alpha_2) = \alpha_2 - \alpha_1 .$$

This equation is just of the form (1).

The complete proof of theorem 3 is considerably more complicated than the proof of theorem 2, but apart from some classical algebraic number theory only results obtained by Baker's method are used. One of these results is Baker's sharpened bound ([4], I), the other one is a result due to SCHINZEL, KEATES, SPRINDŽUK and KOTOV (see [8]) that the greatest prime factor of $P(x)$ exceeds $c_{12} \log\log |x|$, where $c_{12} = c_{12}(P) > 0$. In fact, it would have sufficed to use an older result of COATES [5], also proved by p-adic methods. A different proof, not using any p-adic methods, has been given by SHOREY. See [13]. This paper also contains some generalizations of the result of KOTOV et.al.

5. Finally, we turn to Catalan's equation (3). One might try to prove the analogue of theorem 2 for the more general equation in positive integer variables $m, n, x, y$

$$(13) \qquad ax^m - by^n = k , \qquad m > 1 , \quad n > 1 , \quad mn \geq 6 , \quad x > 1 , \quad y > 1 ,$$

where $a$, $b$ and $k$ are fixed positive integers. It is easy to derive a corresponding linear form $\log a/b + m \log x - n \log y$, but the application of Baker's theorem 1 does not provide the desired result, since both $x$ and $y$ are not constant. If $m$ or $n$ is fixed, then we can apply theorem 3 to $ax^m - k$ or $by^n + k$ respectively. We can then conclude that there are only finitely many solutions in the three remaining variables. It has not been proved yet in general that for fixed integers $a$, $b$ and $k$ there exist only finitely many solutions $m, n, x, y$ satisfying (13). However, for very special values of $a$, $b$ and $k$ there are such results. The first result of this kind concerned Catalan's case $a = b = k = 1$.

CATALAN conjectured, in 1844, that the only solution of the equation $x^m - y^n = 1$, $m > 1$, $n > 1$, $x > 1$, $y > 1$, is given by $3^2 - 2^3 = 1$. By using a refinement of theorem 1 one can prove

THEOREM 4 [19]. - The equation $x^m - y^n = 1$, in integers $m > 1$, $n > 1$, $x > 1$, $y > 1$ has only finitely many solutions. Effective bounds for the solutions can be given.

The proof is based on a double application of the factorization argument in the previous section. It is no loss of generality to assume that $m$ and $n$ are primes. Since LEBESGUE [9] proved that $n \neq 2$, it follows that $n$ is odd. Hence we have the factorizations

$$y^n = x^m - 1 = (x - 1)(x^{m-1} + x^{m-2} + \dots + 1)$$

and

$$x^m = y^n + 1 = (y + 1)(y^{n-1} - y^{n-2} + \dots + 1) .$$

It is easy to see that the greatest common divisor of the two factors on the right-hand sides divide $m$ and $n$ respectively. So we obtain integers $d_1$, $d_2$, $c_1$ and $c_2$ such that

$$x - 1 = d_1 c_1^n , \quad y + 1 = d_2 c_2^m .$$

Here $d_1$ is a power of $m$ and $d_2$ is a power of $n$. On substituting this in

(3), we find

$$(d_1 c_1^n + 1)^m - (d_2 c_2^m - 1)^n = 1 .$$

It follows that the difference $d_1^m c_1^{mn} - d_2^n c_2^{mn}$ is small. This leads to a linear form $m \log d_1 - n \log d_2 + mn \log c_1/c_2$ . Although $m$ , $n$ , $d_1$ and $d_2$ are not really constants, they are relatively small. It is possible to deduce theorem 4 from a refinement of theorem 1, namely with $C(d , n , A')$ replaced by $C(d , n)(\log A')^{c(n)}$ , to find upper bounds for $m$ and $n$ , and then to apply Baker's results mentioned in the beginning of 4.

It is clear from the proof that more complicated arguments are needed for generalizations of (3). Certain generalizations have been announced by ČUDNOVSKIJ (see [6], §6) and by VAN DER POORTEN.

I hope that your conclusion of this paper will be that Baker's sharpened bounds provide an essentially new tool to obtain information on variables in the exponents of diophantine equations.

## REFERENCES

[1] BAKER (A.). - Linear forms in the logarithms of algebraic numbers, I, II, III, IV, Mathematika, London, t. 13, 1966, p. 204-216 ; t. 14, 1967, p. 102-107, 220-228 ; t. 15, 1968, p. 204-216.

[2] BAKER (A.). - Contributions to the theory of diophantine equations, I : On the representation of integers by binary forms, Phil. Trans. Roy. Soc. London, Series A, t. 263, 1968, p. 173-191.

[3] BAKER (A.). - Bounds for the solutions of the hyperelliptic equation, Proc. Camb. phil. Soc., t. 65, 1969, p. 439-444.

[4] BAKER (A.). - A sharpening of the bounds for linear forms in logarithms, I, II, III, Acta Arith., Warszawa, t. 21, 1972, p. 117-129 ; t. 24, 1973, p. 33-36 ; t. 27, 1975, p. 247-252.

[5] COATES (J.). - An effective p-adic analogue of a theorem of Thue, II : The greatest prime factor of a binary form, Acta Arith., Warszawa, t. 16, 1970, p. 399-412.

[6] ČUDNOVSKIJ (G. V.). - Some analytic methods in the theory of diophantine approximations [in Russian], Preprint 74-9, Math. Institute Acad. Sc. Ukrainian S.S.R., Kiev, 1974.

[7] HYYRÖ (S.). - Über die Gleichung $ax^n - by^n = z$ und das Catalansche Problem, Ann. Acad. Sc. Fenn., Ser. A, 1964, n° 355.

[8] KOTOV (S. V.). - Greatest prime factor of a polynomial, Math. Notes, t. 13, 1973, p. 313-317 ; [in Russian], Mat. Zametki, t. 13, 1973, p. 515-522.

[9] LEBESGUE (V. A.). - Sur l'impossibilité en nombres entiers de l'équation $x^m = y^2 + 1$ , Nouv. Ann. Math., t. 9, 1850, p. 178-181.

[10] ROTH (K. F.). - Rational approximations to algebraic numbers, Mathematika, London, t. 2, 1955, p. 1-20 ; Corrigendum, ibid., p. 168.

[11] SCHINZEL (A.) and TIJDEMAN (R.). - On the equation $y^m = P(x)$ , Acta Arith., Warszawa (to appear).

[12] SCHMIDT (W. M.). - Simultaneous approximation to algebraic numbers by rationals, Acta Math., Uppsala, t. 125, 1970, p. 189-201.

[13] SHOREY (T. N.) and TIJDEMAN (R.). - On the greatest prime factor of a polynomial at integer points (to appear).

[14] SIEGEL (C. L.). - The integer solutions of the equation $y^2 = ax^n+bx^{n-1}+...+k$, J. London math. Soc., t. 1, 1926, p. 66-68 (under the pseudonym X.).

[15] SIEGEL (C. L.). - Über einige Anwendungen diophantischer Approximationen, Abh. Preuss. Akad. Wiss., 1929, n° 1, 70 p.

[16] SIEGEL (C. L.). - Die Gleichung $ax^n - by^n = c$, Math. Annalen, t. 114, 1937, p. 57-68.

[17] SPRINDŽUK (V. G.). - Representation of numbers by the norm forms with two dominating variables, J. Number Theory, t. 6, 1974, p. 481-486.

[18] THUE (A.). - Über Annäherungswerte algebraïscher Zahlen, J. für reine angew. Math., t. 135, 1909, p. 284-305.

[19] TIJDEMAN (R.). - On the equation of Catalan, Acta Arith., Warszawa (to appear).

(Texte reçu le 20 juin 1975)

Robert TIJDEMAN<br>
Mathematische Instituut<br>
der Rijkuniversiteit<br>
Postbox 2160<br>
LEIDEN<br>
(Pays-Bas)