Kumbakonam December 21, 2005
Shanmugha Arts, Science, Technology, Research Academy (Sastra)

INTERNATIONAL CONFERENCE
on
"NUMBER THEORY AND MATHEMATICAL PHYSICS"

On recent Diophantine results

Michel Waldschmidt

Abstract

Diophantus of Alexandria was a greek mathematician, around 200 AD, who studied mathematical problems, mostly geometrical ones, which he reduced to equations in rational integers or rational numbers. He was interested in producing at least one solution. Such equations are now called *Diophantine equations*. An example is $y^2 - x^3 = 1$, a solution of which is $(x = 2,\ y = 3)$. More generally, a Diophantine equation is an equation $f(x_1, \ldots, x_n) = 0$, where $f \in \mathbf{Z}[X_1, \ldots, X_n]$ is a given polynomial with rational integer coefficients, while the unknowns $x_1, \ldots, x_n$ are either rational integers or rational numbers. Hilbert's tenth problem is to give an algorithm answering the question of whether such an equation has a solution or not (it is known since 1970 that there is no such algorithm for integral solutions — see [12]).

One speaks of an *exponential Diophantine equation* when some of the exponents are unknown. A well known example is Fermat's equation $x^n + y^n = z^n$, where the unknowns are the positive rational integers x, y, z, n and $n \geq 2$ (see again [12]). Other examples are Catalan's equation $x^p - y^q = 1$, where the unknowns are the rational integers (x, y, p, q) with p and q both ≥ 2 and the more general Pillai's equation $x^p - y^q = k$, where $k \geq 1$ is fixed and the unknowns are again (x, y, p, q).

After Diophantus who was interested finding *at least one* solution, Pierre de Fermat considered the question of finding *all* solutions. Nowadays one of the most efficient tool for solving Diophantine equations is *Diophantine approximation theory*, which studies the approximation of real or complex

numbers by rational numbers or by algebraic numbers. Instead of speaking of solutions of polynomial equations, one may rather consider integer or rational points on algebraic varieties and use the language (and the powerful tools) of Diophantine geometry. The methods involved in Diophantine approximation are essentially those which yield irrationality or transcendence results. We consider these different aspects of Diophantine analysis.

1 Diophantine equations

A *perfect power* is a positive integer of the form a^b, where a and b are positive integers and $b \geq 2$. The set of perfect powers is the set of squares

$$1^2=1,\ 2^2=4,\ 3^2=9,\ 4^2=16,\ 5^2=25,\ 6^2=36,\ 7^2=49,\ 8^2=64,$$

$$9^2=81,\ 10^2=100,\ 11^2=121,\ 12^2=144,\ 13^2=169,\ 14^2=196,\ \dots$$

together with the cubes

$$1^3=1,\ 2^3=8,\ 3^3=27,\ 4^3=64,\ 5^3=125,\ 6^3=216,\ 7^3=343,\ \dots$$

the fifth power

$$1^5=1,\ 2^5=32,\ 3^5=243,\ 4^5=1\,024,\ 5^5=3\,125,\ 6^5=7\,776,\ \dots$$

and so on.

Hence the increasing sequence of perfect powers starts with

$$1,\ 4,\ 8,\ 9,\ 16,\ 25,\ 27,\ 32,\ 36,\ 49,\ 64,\ 81,\ 100,\ 121,\ 125,\ 128,\ 144,\ \dots \qquad (1)$$

In 1844 E. Catalan conjectured that $(8,9)$ is the only example of two consecutive number in this sequence. This question was studied by many a mathematician and was finally solved only in 2002 by P. Mihăilescu [16]; see [6, 15, 23].

The next conjecture was proposed by S.S. Pillai [17] (see also [25] and [2, 3, 5, 24]).

Conjecture 2 (S.S. Pillai) *Let k be a positive integer. The equation*

$$x^p - y^q = k,$$

where the unknowns x, y, p and q take integer values, all ≥ 2, has only finitely many solutions (x, y, p, q).

An equivalent statement is that in the increasing sequence (1) of perfect powers, the difference between two consecutive terms tends to infinity. It is not even known whether for, say, $k = 2$, Pillai's equation has only finitely many solutions. Only the case $k = 1$ is known: this result of R. Tijdeman (1976 — see [6, 15, 16, 23]) has been an important step towards the final solution by Mihăilescu of Catalan's Conjecture.

The original proof of Mihăilescu involved tools from transcendental number theory (measures of linear independence of logarithms of algebraic numbers) and from algebraic number theory (arithmetic of cyclotomic fields). Later Mihăilescu showed how to remove the transcendence arguments and to produce a proof using only arithmetic tools.

We briefly mention a few other questions related with perfect powers.

To solve the equation

$$x^p + y^q = z^r$$

is the same as to describe the set of perfect powers which can be written as a sum of two perfect powers. This exponential Diophantine equation has also a long history in relation with Fermat's last Theorem (see for instance [10, 26]). Up to obvious symmetries, only 10 solutions in positive integers (x, y, z, p, q, r) for which

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1,$$

and such that x, y, z are relatively prime, are known (F. Beukers, D. Zagier), namely

$$1 + 2^3 = 3^2, \qquad 2^5 + 7^2 = 3^4, \qquad 7^3 + 13^2 = 2^9, \qquad 2^7 + 17^3 = 71^2,$$

$$3^5 + 11^4 = 122^2, \qquad 17^7 + 76271^3 = 21063928^2, \qquad 1414^3 + 2213459^2 = 65^7,$$

$$9262^3 + 15312283^2 = 113^7, \quad 43^8 + 96222^3 = 30042907^2, \quad 33^8 + 1549034^2 = 15613^3.$$

For all known solutions, one of p, q, r is 2; *Beal's Conjecture* (also due to R. Tijdeman and D. Zagier) is that there is no solution with the further restriction that each of p, q and r is ≥ 3.

For the question of perfect powers with identical digits, we refer to the survey paper of T.N. Shorey [24] — we just quote the solution by Y. Bugeaud and M. Mignotte (1999) of a conjecture due to Inkeri: *there is no perfect power with identical digits in its decimal expansion.*

Several recent results on Diophantine equations combine the transcendence method of Gel'fond-Baker [25] with the so-called *modular method* (see for instance [13] and [10]) involving Frey curves and their associated Galois representations, which originates with the solution by A. Wiles of Fermat's last Theorem.

An example of such a result whose proof requires the combination of both strategies has been obtained in 2004 by Y. Bugeaud, M. Mignotte and Siksek [8]. It deals with the Fibonacci sequence

$$1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34,\ 55,\ 89,\ 144,\ \ldots \tag{3}$$

where $F_1 = F_2 = 1$, $F_n = F_{n-1} + F_{n-2}$ $(n \geq 3)$.

Theorem 4 (Bugeaud, Mignotte, Siksek) *The only perfect powers in the sequence of Fibonacci numbers are* 1*,* 8 *and* 144*.*

This means that the exponential Diophantine equation $F_n = x^k$, where the unknowns are the rational integers n, x, k with $n \geq 1$, $x \geq 1$ and $k \geq 2$, has only the solutions $(n = 1,\ x = 1,\ k \geq 2)$, $(n = 2,\ x = 1,\ k \geq 2)$, $(n = 6,\ x = 2,\ k = 3)$, $(n = 12,\ x = 12,\ k = 2)$.

A further result on this topic has been obtained by F. Luca and T.N. Shorey (2005, [14]) who shows that the product of 2 or more consecutive Fibonacci numbers other than $F_1F_2 = 1$ is never a perfect power.

We also refer to [4] where M. Bennett uses similar arguments and proves, among other results, that for positive integers n, D, with $n \geq 3$ and D non-square, the equation $x^2 - Dy^{2n} = 1$ has at most two solutions in positive integers x and y.

2 Diophantine approximation

Let us start with a nice example, due to Ramanujan [18], which was indicated to me by D.W. Masser: the algebraic number

$$\frac{63}{25}\left(\frac{17+15\sqrt{5}}{7+15\sqrt{5}}\right)=3.141\,592\,653\,805\ldots$$

is a root of $P(x)=168\,125\,x^2-792\,225x+829\,521$. The numbers

$$\pi=3.141\,592\,653\,589\ldots,$$

$$e^{\pi\sqrt{163}}=262\,537\,412\,640\,768\,743,999\,999\,999\,999\,250\,072\,5\ldots$$

and

$$e^{\pi\sqrt{427}}=7\,805\,727\,756\,261\,891\,959\,906\,304\,744{+}999\,421\,027\,517\,377\,348\,595\,712\,000\,\sqrt{61}{+}\epsilon$$

with $|\epsilon|<10^{-22}$ are transcendental.

Let ξ be a real number. Since $\mathbf{Q}$ is dense in $\mathbf{R}$, for any $\epsilon>0$ there exists $p/q\in\mathbf{Q}$ such that

$$\left|\xi-\frac{p}{q}\right|\le\epsilon.$$

For each $q\ge 1$ select the (or one of the) integer(s) p for which $|q\xi-p|$ is minimal. The corresponding value of $|q\xi-p|$ is nothing else than $\|q\xi\|$, where $\|\cdot\|$ denotes the distance to the nearest integer. The main question on the *rational approximation of* ξ is to investigate properties of the sequence

$$(\|q\xi\|)_{q\ge 1}=\{\|\xi\|,\|2\xi\|,\|3\xi\|,\ldots\}$$

The behaviour of this sequence is governed by the continued fraction expansion of ξ. The case where ξ is rational is easy. Otherwise a lower bound for $\|q\xi\|$ is an *irrationality measure* for ξ.

The question of simultaneous approximation of several numbers is not yet completely understood. Given two real numbers ξ, η, there are (at least) two natural ways of considering the question of simultaneous rational approximation: one may consider either the sequence

$$\bigl(\max\{\|q\xi\|,\|q\eta\|\}\bigr)_{q\ge 1}$$

or else the sequence

$$\bigl(\min\{\|p_1\xi + p_2\eta\| \; ; \; 0 < \max\{|p_1|, |p_2|\} \leq q\}\bigr)_{q\geq 1}.$$

Transference theorems ([22] § IV.5) show that the behaviours of these two sequences are closely connected.

We consider here a simple example of a simultaneous approximation question where recent progress has been achieved, namely the question of the simultaneous approximation of a number and its square.

Let ξ be an irrational real number. From Dirichlet's box principle it follows that for any real number $X \geq 1$, there exists $(x_0, x_1, x_2) \in \mathbf{Z}^3$ satisfying

$$0 < x_0 \leq X, \quad |x_0\xi - x_1| \leq \varphi(X) \;\text{ and }\; |x_0\xi^2 - x_2| \leq \varphi(X), \tag{5}$$

where $\varphi(X) = 1/[\sqrt{X}]$. If ξ is algebraic of degree 2, the same is true with $\varphi(X) = c/X$ where $c > 0$ depends only on ξ. For $\lambda > 1/2$, it is known that the set E_λ of ξ which are not quadratic over $\mathbf{Q}$ and for which these inequalities (5) have a solution for arbitrarily large values of X with $\varphi(X) = X^{-\lambda}$ has Lebesgue measure zero (by a metrical result of V.G. Sprindzuck — see [7]) and contains no algebraic number (by the subspace theorem of W.M. Schmidt [22, 11]). No element in this set was known and the general expectation was that this set should be empty. It was proved by H. Davenport and W.M. Schmidt that the set E_λ is empty for $\lambda > \lambda_0 = (-1+\sqrt{5})/2 = 0.618\ldots$; more precisely for any irrational ξ which is not quadratic over $\mathbf{Q}$ there is a constant $c(\xi)$ such that the above inequalities (5) have no solution when X is sufficiently large and $\varphi(X) = c(\xi)X^{-\lambda_0}$.

In [20, 21], D. Roy shows that, surprisingly, this result of Davenport and Schmidt is optimal: he produces explicit examples of transcendental numbers ξ for which the inequalities (5) have a solution for arbitrarily large values of X with $\varphi(X) = cX^{-\lambda_0}$ with a suitable constant c.

His example again involves the Fibonacci sequence (3). *Fibonacci word* on an alphabet with two letters $\{a,\; b\}$ is defined inductively, starting with $f_1 = b$ and $f_2 = a$, by $f_n = f_{n-1}f_{n-2}$: each word is obtained from the two previous ones by concatenation. Hence we have the sequence

$f_1 = b$
$f_2 = a$

$f_3 = ab$
$f_4 = aba$
$f_5 = abaab$
$f_6 = abaababa$
$f_7 = abaababaabaab$
$f_8 = abaababaabaababaababa$

Since each of these words, from f_2 on, starts with the same letters, one deduces an infinite word

$w = abaababaabaababaababaabaababaabaab\ldots$

Another equivalent definition of w is that it is the fixed point of the morphism

$a \mapsto ab,\ b \mapsto a,$

since, under this morphism, the image of f_n is f_{n+1}.

For $n \geq 2$ the word f_n is deduced from w by taking only the first F_n letters. This word w has minimal complexity among the non-periodic words. There are exactly three words of two letters which occur in the sequence, namely aa, ab and ba. In other terms bb does not occur. There are exactly 4 factors of length 3 (while the number of words of length 3 on the alphabet with two letters is 8), namely aab, aba, baa, bab. There are 5 words of 4 letters (among 16 possibilities) and more generally for each n the number $p(n)$ of factors of length n in w is $n+1$. It is easy to check that $p(n) = n+1$ is the minimum value of the complexity function p for a nonperiodic word (while for a periodic word the complexity function is ultimately constant): the word w is called *Sturmian*. On the alphabet $\{a,\ b\}$, a Sturmian word is characterized by the property that for each $n \geq 1$, there is exactly one factor v of u of length n such that both va and vb are factors of u of length $n+1$.

Theorem 6 (Roy) *Let A and B be two distinct positive integers. Let $\xi \in (0,1)$ be the real number whose continued fraction expansion is obtained from w by replacing the letters a and b by the two selected numerical values A and B respectively:*

$$[0; A, B, A, A, B, A, B, A, A, B, A, A, B, A, B, A, A, B, A, B, A, A, B\ldots]$$

Then there exists a constant c such that the inequalities (5) have a solution for arbitrarily large values of X with $\varphi(X) = cX^{-\lambda_0}$.

Further more recent results on this topic are due to D. Roy, M. Laurent, Y. Bugeaud…

3 Diophantine geometry

Mordell's Conjecture has been settled by G. Faltings (see [12]): *the set of rational points on a curve of genus* ≥ 2 *over a number field is finite.* The result is noneffective. Even for *integer* points on a curve of genus 2, there is no known algorithm so far. The main obstruction is that, in the proof, one needs to consider *large* solutions, which turn out not to exist. A typical example where a noneffective argument is required occurs in the proof of Thue-Siegel-Roth Theorem: in the earliest work of Thue who produced the first improvement on Liouville's estimate, he needs to consider a first good rational approximation p_1/q_1 to x, and then a second good approximation p_2/q_2 where q_2 is large in terms of q_1. E. Bombieri succeeded to reach an effective result using a similar strategy by producing (at least in some cases) a first sharp approximation p_1/q_1, but for the proof of Roth's Theorem a single sharp approximation does not suffice, several ones are required.

This type of argument does not suffice to get effective bounds for the solutions of the given Diophantine equation; but they may suffice to produce upper bounds for the *number* of solution.

In the case of Faltings' Theorem, an upper bound for the number of rational points over a number field on a curve of genus ≥ 2 has been achieved by G. Rémond [19] in 2000.

In a different direction, studying the analog of Hilbert's tenth problem for rational solution of a Diophantine equation, B. Mazur was led to suggest a statement dealing with the density (for the real topology) of rational points on an algebraic variety over the field of rational numbers. His conjecture was disproved in [9] by J-L. Colliot-Thélène, A.N. Skorobogatov and P. Swinnerton-Dyer in the general case. However, in the special case of Abelian varieties, Mazur's question reduces to an open problem, which amounts to solving a conjecture in transcendental number theory. We refer to [26] for further references on this topic, we only use this question as a transition towards the next section.

4 Irrationality and transcendence

Let $g \geq 2$ be a positive integer. The g-ary expansion of a real number x is

$$x = \sum_{k \geq 1} \frac{a_k}{g^k}$$

where $(a_k)_{k \geq 1}$ is a sequence of elements in $\{0, 1, \ldots, g-1\}$ (one omits the sequences which are ultimately constant equal to $g-1$).

It is well known (and easy to prove) that the g-ary expansion of a rational number is ultimately periodic. In 1950 É. Borel suggested that the expansion of an algebraic irrational number should satisfy certain laws which govern random numbers (see [7]). In this direction one can ask whether the g-ary expansion of an algebraic irrational number can be generated by a finite automaton. The solution of this problem (namely a negative answer) was claimed by J.H. Loxton and A.J. van der Poorten in 1988, using a transcendence method of K. Mahler. However their proof turned out to contain a gap. A correct answer has been obtained only in 2004 by B. Adamczewski and Y. Bugeaud [1]:

Theorem 7 (Adamczewski, Bugeaud) *The g-ary expansion of an algebraic irrational number cannot be generated by a finite automaton.*

The proof in [1] rests on the subspace Theorem of W.M. Schmidt and its ultrametric generalization by H.P.S. Schlickewei (see [22, 11]).

Recall (§ 2) the *complexity function* p of the sequence $(a_k)_{k \geq 1}$ (or of the g-ary expansion of x): for each integer $n \geq 1$, $p(n)$ is the number of words of length n which appear in the sequence $(a_1, a_2, \ldots)$. S. Ferenczy and C. Mauduit proved in 1997 (by means of a result from Diophantine approximation, namely the p-adic extension, due to Ridout, of the Thue-Siegel–Roth Theorem - which is now a special case of the Schmidt-Schlickewei subspace Theorem) that any x whose g-ary expansion is Sturmian is transcendental. One of the main theorems in [1] is that the complexity function p of a real irrational algebraic number x satisfies

$$\liminf_{n \to \infty} \frac{p(n)}{n} = +\infty.$$

Theorem 7 follows from this result, since automatic sequences have a complexity $p(n) = O(n)$ by a result of Cobham (1972).

References

[1] B. Adamczewski, Y. Bugeaud – "On the complexity of algebraic numbers I. Expansions in integer basis", *Annals of Math.*, to appear (18 p.). http://www.math.princeton.edu/menusa/index6.html

[2] M. A. Bennett – "On some exponential equations of S. S. Pillai", *Can. J. Math.* **53** (2001), no. 5, p. 897–922.

[3] — , "Pillai's conjecture revisited", *J. Number Theory* **98** (2003), no. 2, p. 228–235.

[4] — , "Powers in recurrence sequences: Pell equations", *Trans. Am. Math. Soc.* **357** (2005), no. 4, p. 1675–1691.

[5] M. A. Bennett & C. M. Skinner – "Ternary Diophantine equations via Galois representations and modular forms", *Can. J. Math.* **56** (2004), no. 1, p. 23–54.

[6] Y. F. Bilu – "Catalan's conjecture", in *Bourbaki seminar. Volume 2002/2003. Exposes 909-923* , Paris: Société Mathématique de France. Astérisque 294, 1-26 , 2004.

[7] Y. Bugeaud – *Approximation by algebraic numbers.*, Cambridge Tracts in Mathematics 160. Cambridge: Cambridge University Press. xv, 274 p., 2004.

[8] Y. Bugeaud, M. Mignotte & S. Siksek – "On Fibonacci numbers of the form $q^k y^k$", *C. R., Math., Acad. Sci. Paris* **339** (2004), no. 5, p. 327–330.

[9] J.-L. Colliot-Thélène, A. Skorobogatov & P. Swinnerton-Dyer – "Double fibres and double covers: Paucity of rational points", *Acta Arith.* **79** (1997), no. 2, p. 113–135.

[10] H. Darmon – “A fourteenth lecture on Fermat’s Last Theorem”, in *Kisilevsky, Hershy (ed.) et al., Number theory. Papers from the 7th conference of the Canadian Number Theory Association, University of Montreal, Montreal, QC, Canada, May 19-25, 2002.* , Providence, RI: American Mathematical Society (AMS). CRM Proceedings & Lecture Notes 36, 103-115 , 2004.

[11] N. I. Fel’dman & Y. V. Nesterenko – “Transcendental numbers”, in *Number theory, IV*, Encyclopaedia Math. Sci., vol. 44, Springer, Berlin, 1998, p. 1–345.

[12] M. Hindry & J. H. Silverman – *Diophantine geometry*, Graduate Texts in Mathematics, vol. 201, Springer-Verlag, New York, 2000, An introduction.

[13] A. Kraus – “On the equation $x^p + y^q = z^r$: a survey”, *Ramanujan J.* **3** (1999), no. 3, p. 315–333.

[14] F. Luca & T. Shorey – “Diophantine equations with products of consecutive terms in Lucas sequences”, *J. Number Theory* **114** (2005), p. 289–311.

[15] T. Metsänkylä – “Catalan’s Conjecture: Another old Diophantine problem solved”, *Bull. Am. Math. Soc., New Ser.* **41** (2004), no. 1, p. 43–57.

[16] P. Mihăilescu – “Primary cyclotomic units and a proof of Catalan’s conjecture”, *J. reine angew. Math.* **572** (2004), p. 167–195.

[17] S. Pillai – “On the equation $2^x - 3^y = 2^X + 3^Y$”, *Bull. Calcutta Math. Soc.* **37** (1945), p. 15–20.

[18] S. Ramanujan – *Collected papers. Edited by G. H. Hardy, P. V. Seshu Aiyar, B. M. Wilson*, XXXVI und 355 p. Cambridge, University Press, 1927.

[19] G. Rémond – “Inégalité de Vojta en dimension supérieure”, *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)* **29** (2000), no. 1, p. 101–151.

[20] D. Roy – "Approximation to real numbers by cubic algebraic integers. II", *Ann. of Math. (2)* **158** (2003), no. 3, p. 1081–1087.

[21] — , "Approximation to real numbers by cubic algebraic integers. I", *Proc. London Math. Soc. (3)* **88** (2004), no. 1, p. 42–62.

[22] W. M. Schmidt – *Diophantine approximation.*, Lecture Notes in Mathematics. 785. Berlin-Heidelberg-New York: Springer-Verlag. X, 299 p. DM 34.50; $ 20.40 , 1980.

[23] R. Schoof – "Mihăilescu's proof of Catalan's Conjecture", http://mat.uniroma2.it/∼schoof/catalan.pdf, (pdf 370K); see also http://www.mri.ernet.in/∼ntweb/N4.html#catalan.

[24] T. N. Shorey – "Diophantine approximations, diophantine equations, transcendence and applications", Indian Journal of Pure and Applied Mathematics., to appear, 2005.

[25] T. N. Shorey & R. Tijdeman – *Exponential Diophantine equations*, Cambridge Tracts in Mathematics, vol. 87, Cambridge University Press, Cambridge, 1986.

[26] M. Waldschmidt – "Open Diophantine problems", *Mosc. Math. J.* **4** (2004), no. 1, p. 245–305.

Michel WALDSCHMIDT
Université P. et M. Curie (Paris VI)
Institut de Mathématiques CNRS UMR 7586
Théorie des Nombres Case 247
175, rue du Chevaleret
F–75013 PARIS
e-mail: miw@math.jussieu.fr
URL: http://www.math.jussieu.fr/∼miw/