Bulletin de la Société Royale des Sciences de Liège, Vol. 84, 2015, p. 97 - 101

Exponential Diophantine equations

BUGEAUD Yann[1]

Mathématiques, Université de Strasbourg, 7 rue René Descartes
F-67084 STRASBOURG (France)

The notion of variable, or unknown, appeared in the works of the Greek mathematician Diophantus, who lived (probably) during the third century *a.d.* He was particularly interested in the following question: does a given polynomial equation with integral (or rational) coefficients have a solution in integers (or in rational numbers)? Among the most classical examples is the equation $x^2 + y^2 = z^2$, whose integral solutions give us the lengths of the sides of Pythagorean triangles. At that time (and, most probably, even since a few centuries before that time), all these solutions were perfectly known.

Nowadays, we call Diophantine equation any polynomial equation with integer coefficients and whose unknowns are supposed to be rational integers. This definition is often extended to any type of equations involving integers and where the unknown are also integers. An emblematic example is Fermat's equation $x^n + y^n = z^n$, where x, y, z and $n > 3$ are unknown positive integers. We often use the terminology “exponential Diophantine equation” when one or more exponents are unknown.

The natural question is the following: an equation being given, determine the complete set of its integral solutions. Sometimes, this is quite easy, in particular when one can use congruences modulo a suitable integer. Let us for example consider the equation $3^m - 2^n = 1$, which was solved by Levi ben Gershon (1288-1344), answering a question of the French composer Philippe de Vitry. Assume that there are integers m, n with $n > 2$ and $3m - 2n = 1$. Then, 4 divides $3m - 1$, whence m must be even. Writing $m = 2k$ we obtain $(3^k - 1)(3^k + 1) = 2n$, which implies that both $3^k - 1$ and $3^k + 1$ are powers of 2. But the only powers of 2 which differ by 2 are 2 and 4. Hence $k = 1$ and we have proved that $3^2 - 2^3 = 1$ is the only solution to $3^m - 2^n = 1$ with $n > 2$.

However, in most of the cases, to determine the complete set of integral solutions of a Diophantine equation remains an unsolved problem, and often it is even very difficult to prove whether this set is finite or not. When it is infinite, the next step is to give a complete description of all the integral solutions of the equation. For instance, the positive solutions of the equation

$$5x^2 - y^2 = \pm 4$$

are precisely given by the integer pairs (F_n, L_n), where $(F_n)_{n\geq 1}$ and $(L_n)_{n\geq 1}$ are the Fibonacci and the Lucas sequences defined by $F_1 = F_2 = 1$, $L_1 = 1$, $L_2 = 3$, and satisfying $F_{n+2} = F_{n+1} + F_n$ and $L_{n+2} = L_{n+1} + L_n$, for $n > 1$.

[1] e-mail : bugeaud@math.unistra.fr

In the case of finiteness of the number of solutions, the second natural step is to try to compute an upper bound for their absolute values (or, equivalently, for the number of their digits), or at least to compute an upper bound for the number of the solutions. This is not always possible. Indeed, if we manage to show that the number of digits of the largest solution does not exceed ten times the number of digits of the smallest, this information immediately implies the finiteness of the number of solutions, but it does not allow us to deduce an upper bound for the number of solutions (except, of course, if we already know one solution).

Furthermore, if we can prove that an equation has at most, say, ten solutions, nothing ensures us that it has exactly ten solutions and while we have not found ten solutions we cannot be sure that we have completely solved the equation. However, if we manage to prove that all the solutions have at most, say, ten billions of digits, then, by enumerating all the possible solutions, we can, at least in principle (!), solve completely our equation. In the latter case, we know when we can stop our enumeration process, which is not the case when our informations only deal with the number of solutions.

In 1970, building on earlier works by Robinson, Davis and Putnam, Yuri Matiyasevich showed that there does not exist an algorithm which, given any polynomial Diophantine equation with integer coefficients, can decide whether this equation has zero or at least one integer solution. This solves Hilbert's tenth problem.

A few years before Matiyasevich's achievement, Alan Baker developed the theory of linear forms in the logarithms of algebraic numbers and applied it to several classical families of Diophantine equations. He gave explicit (albeit huge) upper bounds for the absolute values of the solutions to Thue's equation

$$F(x,y) = b, \tag{1}$$

where $F(X, Y)$ is an homogeneous, irreducible, integral polynomial of degree at least 3, and b is a given non-zero integer. Of course, the bounds obtained depend on $F(X, Y)$ and b. Baker also computed upper bounds for the absolute values of the solutions to the superelliptic equations

$$f(x) = y^m, \tag{2}$$

where $f(X)$ is an irreducible, integral polynomial of degree at least 2 and $m > 3$ is an integer. These results show that, at least in principle, equations (1) and (2) can be completely solved. Note that it was known long before Baker that (1) and (2) have only finitely many solutions. These results were established by Thue in 1909 and by Siegel in 1929, but the methods they used do not provide us with upper bounds for the absolute values of the solutions.

Apart from this aspect, the theory of linear forms in logarithms appears to be, in many aspects, much more powerful than the techniques developed by Thue and Siegel. Indeed, it also applies to certain families of exponential Diophantine equations (recall

that this terminology means that one or several exponents are unknown), like for instance

$$f(x) = y^q, \tag{3}$$

where $f(X)$ is a given irreducible, integral polynomial of degree at least 3 and x, y and $q > 2$ are unknown integers with $|y| \geq 2$. Baker's theory enables us to compute an explicit upper bound for the size of the largest solution of (3), while Thue-Siegel's method appears to be useless.

In my opinion, the most spectacular application of Baker's theory to Diophantine equations was found by Tijdeman in 1976. He proved that Catalan's equation

$$x^m - y^n = 1, \tag{4}$$

in integers x, y, m and n at least equal to 2, has only finitely many solutions, whose size can be explicitely bounded. Following Tijdeman's proof and using the estimates for linear forms in logarithms available at that time, Langevin has computed that every solution (x, y, m, n) of (4) satisfies

$$x^m < \exp\exp\exp\exp 730.$$

Very roughly speaking, the situation thirty years ago was the following: we were able to compute explicit upper bounds for many equations or classes of equations, but these were far too huge in order to solve completely the equations considered.

Since then, numerous spectacular results have been proved, which a little while ago seemed to be out of reach. There are three main explanations. A first one is a theoretical improvement concerning estimates for linear forms in logarithms. A second one is the de-velopment of the algorithmic and computational number theory, a now very active branch of mathematics. A third one is the influence of the deep works of Wiles and Taylor and Wiles.

For instance, we have now at our disposal efficient algorithms which enable us to solve quickly any Thue equation of small degree, say of degree less than thirteen, and with small coefficients.

Let me end with several recent achievements.

Theorem (Wiles, Taylor and Wiles, 1995). *Let $n > 3$ be an integer. All the integer solutions x, y, z to*

$$x^n + y^n = z^n$$

satisfy $xyz = 0$.

The next result deals with an infinite family of Thue equations.

Theorem (Bennett, 2001). *Let $a > b \geq 1$ and $n > 3$ be integers. Then the Diophantine equation*

$$|ax^n - by^n| = 1 \tag{5}$$

has at most one solution in positive integers x and y.

The proof of Bennett's theorem involves Baker's theory and several other methods from Diophantine approximation. Observe that, for $a = b + 1$, the equation (5) has the solution given by $x = y = 1$ and the theorem asserts that it has no other solution with positive x and y.

The longstanding Catalan's equation was finally completely solved in 2002.

Theorem (Mihăilescu, 2002). *Catalan's equation*

$$x^m - y^n = 1$$

has only the solution $3^2 * 2^3$ *in integers x, y, m, n greater than or equal* to 2.

The first proof of this theorem involved at one step Baker's theory and some (not heavy) computer calculations. However, Mihăilescu found a few years later an alternative approach for this part of the proof, allowing him to remove the appeal to estimates for logarithmic forms and to computer calculations.

Recall that the Fibonacci sequence $(F_n)_{n>1}$ is defined by $F_1 = F_2 = 1$ and the recursion $F_{n+2} = F_{n+1} + F_n$ for $n > 1$. It starts with

1,1,2,3,5,8,13,21,34,55,89,144,233, 377,610,987, ...

A positive integer n is a perfect power if it can be written as $n = m^q$, where m and q are integers with $q > 2$.

Theorem (Bugeaud, Mignotte, Siksek, 2006). *The only perfect powers in the Fibonacci sequence are* 1, 8 *and* 144.

The proof of the above theorem combines Baker's theory with a modulai- approach based on some of the ideas of the proof of Fermat's Last Theorem.

Short bibliography

The books listed below are accessible to (post)graduate students. Baker's theory of linear forms in logarithms is discussed in details in [6]. Many applications to Diophantine equations are given in [5]. Various other methods to investigate Diophantine equations are presented in [2, 3]. More specifically, Mihăilescu's theorem is the main object of the monographs [1, 4] and is also proved in [3].

[1] Yu. Bilu, Y. Bugeaud and M. Mignotte, The Problem of Catalan. Springer, 2014.

[2] H. Cohen, Number theory. Vol. I. Tools and Diophantine equations. Graduate Texts in Mathematics, 239. Springer, New York, 2007.

[3] H. Cohen, Number theory. Vol. II. Analytic and modern tools. Graduate Texts in Mathematics, 240. Springer, New York, 2007.

[4] R. Schoof, Catalan's conjecture. Universitext. Springer-Verlag London, Ltd., London, 2008.

[5] T. N. Shorey and R. Tijdeman, Exponential Diophantine equations. Cambridge Tracts in Mathematics, 87. Cambridge University Press, Cambridge, 1986.

[6] M. Waldschmidt, Diophantine approximation on linear algebraic groups. Tran-scendence properties of the exponential function in several variables. Grundlehren der Mathematischen Wissenschaften, 326. Springer-Verlag, Berlin, 2000.