

## Exponential Diophantine equations

*Yann Bugeaud*

### 1. Introduction

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 considered polynomial equations with integral or rational coefficients, and was searching for an integral or rational solution. One of the most popular examples is the equation  $x^2 + y^2 = z^2$ , whose integral solutions give us the lengths of the sides of Pythagorean triangles. At the time of Diophantus (and most probably since ever a few centuries), these 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 exponential equations, like Fermat's equation  $x^n + y^n = z^n$ , where  $x, y, z$  and  $n \geq 3$  are unknown; however, when (at least) one exponent is unknown, we use sometimes the terminology of exponential Diophantine equations.

We are concerned with the following problem:

*A Diophantine equation being given, determine the set of its integral solutions.*

In most of the cases, this is far from being easy, and it is often even quite difficult to determine whether this set is finite or not.

If we can prove the finiteness of the number of solutions, then the second natural step is to try to bound this number. We point out that this is not always possible. Indeed, if one is able to prove that, for a given equation, the number of digits of its 'largest' solution is less than twice the number of digits of its 'smallest' solution, then this shows that the number of solutions is finite, but without giving any further information on this number!

A third step is to compute an upper bound for the absolute values of the solutions. Note that if we know that an equation has at most ten solutions, nothing ensures us that it has exactly ten solutions, and unless we have found ten solutions we cannot be sure that we have completely solved the equation. However, if we manage to prove that all the solutions are less than, say,  $10^{100}$ , then, by checking every possible values of the unknowns between 1 and  $10^{100}$ , we can, at least in principle (!), solve completely our equation. Thus, we know when we can stop our enumeration process, which is not the case when we only have a bound for the number of solutions.

We give in the present informal notes a short (and far from being complete) overview of some achievements in the theory of Diophantine equations appeared during the twentieth century.

## 2. Two elementary observations

First of all, we mention a simple example of a Diophantine equation in two unknowns having infinitely many solutions, namely the Diophantine equation

$$x^2 - 2y^2 = 1. \quad (1)$$

Indeed,  $x = 3, y = 2$  is clearly a solution to (1) and, if the positive integers  $a$  and  $b$  satisfy  $a^2 - 2b^2 = 1$ , then

$$(3a + 4b)^2 - 2(2a + 3b)^2 = (9 - 8)a^2 + (16 - 18)b^2 = a^2 - 2b^2 = 1,$$

thus  $x = 3a + 4b, y = 2a + 3b$  is another solution to the Pellian equation (1).

From now on, all the equations that we consider have only finitely many solutions.

A useful, and very elementary, method to solve Diophantine equations is to use congruences modulo a suitably chosen prime number. Consider for instance the equation

$$x^5 - 2y^5 = 4.$$

It has no integer solutions. To see this, look at it modulo 11. A fifth power is congruent to 0 or  $\pm 1$  modulo 11. Consequently,  $x^5 - 2y^5$  is congruent to 0,  $\pm 1$ ,  $\pm 2$  or  $\pm 3$  modulo 11, and  $x^5 - 2y^5$  cannot be equal to 4.

A necessary condition for the congruence method to work is that the equation has no solutions. The equation  $x^5 - 2y^5 = 3$  admits the solution  $x = 1, y = -1$ , and the congruence method is useless to prove that there are no other solutions. Whatever the prime  $p$ , we do not get a contradiction by looking at the equation modulo  $p$ .

Most often, it is easier to prove that an equation has no solutions than to prove that it has exactly one solution.

## 3. Ineffective methods

Apart from a result of Runge dealing with a restricted family of Diophantine equations of the shape  $F(x, y) = 0$ , where  $F \in \mathbf{Z}[X, Y]$  is a polynomial, we knew at the beginning of the twentieth century no general statement on the resolution of Diophantine equations. In 1909, exactly one century ago, the Norwegian mathematician Axel Thue succeeded in proving that, for any homogeneous, irreducible polynomial  $F \in \mathbf{Z}[X, Y]$  of degree at least 3, the equation (now called Thue equation)

$$F(x, y) = b, \quad (2)$$

where  $b$  is a given non-zero integer, has only finitely many solutions  $x, y$  in  $\mathbf{Z}^2$ . The method of the proof allows us to compute an explicit bound for the number of solutions, but unfortunately not for their size. We say that Thue's result is *ineffective*, which means that its proof does not yield an effectively computable upper bound for the absolute values of the solutions.

Another general result, established by Siegel in 1929, asserts that the superelliptic equation

$$f(x) = y^m, \quad (3)$$

where  $f$  in  $\mathbf{Z}[X]$  is an irreducible polynomial of degree at least 2 and  $m \geq 3$  is an integer, has only finitely many solutions  $x, y$  in  $\mathbf{Z}^2$ . Like Thue's theorem, Siegel's result is ineffective. And all the extensions of their works suffer from the same inconvenience: the finiteness results are proved by ineffective methods... And we had to wait until the end of the sixties to see the development of a new and very powerful theory.

#### 4. Baker's theory

In the forties, Gelfond has obtained non-trivial explicit lower bounds for non-zero expressions of the shape

$$\Lambda = |b_1 \log a_1 + b_2 \log a_2|,$$

where  $a_1, a_2, b_1$  and  $b_2$  are non-zero algebraic numbers. These lower estimates can be used to get explicit upper bounds for the solutions of certain Thue equations of degree 3. Gelfond also pointed out that a generalization of his result to linear forms in  $n \geq 3$  logarithms of algebraic numbers would yield an effective upper bound for the size of the solutions of any Thue equation of arbitrarily large degree.

Such a generalization was proved by Alan Baker in 1966 and refined in several subsequent works. This enabled Baker to compute, for the first time, explicit (albeit huge) upper bounds for the size of the solutions to (2) and (3).

Apart from this aspect, the theory of linear forms in logarithms appears to be much more powerful than the methods 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

$$f(x) = y^z, \quad (4)$$

where  $f \in \mathbf{Z}[X]$  is a given irreducible polynomial of degree at least 3 and  $x, y$  and  $z \geq 2$  are unknown integers with  $|y| \geq 2$ . Baker's theory enables us to compute an explicit upper bound for the size of the solutions to (4), while, at present, we are unable to derive the finiteness of the number of solutions to (4) from the Thue-Siegel method.

In my opinion, the most spectacular application of Baker's theory to Diophantine equations is the proof, by Tijdeman in 1976, that Catalan's equation

$$x^m - y^n = 1 \quad (5)$$

has only finitely many solutions in integers  $x, y, m$  and  $n$  at least equal to 2. Following Tijdeman's proof, Langevin has computed in 1976 that any solution  $(x, y, m, n)$  to (5) satisfies

$$\max\{x, y, m, n\} \leq \exp \exp \exp \exp 730.$$

Ten years ago, it was known that if (5) has a solution  $(x, y, m, n)$  with  $m$  and  $n$  prime numbers, then  $m$  and  $n$  have between 7 and 15 decimal digits. But this was not sufficient to complete the resolution of (5), even with the help of rapid computers.

Finally, Mihăilescu established in 2003 that the only solution to (5) is given by  $3^2 - 2^3 = 1$ . His proof mainly uses the theory of cyclotomic fields and does not require Baker's theory.

Many applications of the theory of linear forms in logarithms to Diophantine equations were published in the 70's and in the 80's. New families of (exponential) Diophantine equations have been shown to have only finitely many solutions. Mathematicians were able to compute explicit upper bounds for the solutions, but these bounds were, in most cases, far too huge in order to solve completely the equations considered.

We content ourselves to quote only one result. Let  $(F_n)_{n \geq 0}$  denote the Fibonacci sequence defined by  $F_0 = 0$ ,  $F_1 = 1$  and the recursion

$$F_{n+2} = F_{n+1} + F_n, \quad \text{for } n \geq 0.$$

The first few terms of the Fibonacci sequence are

$$0 \ 1 \ 1 \ 2 \ 3 \ 5 \ 8 \ 13 \ 21 \ 34 \ 55 \ 89 \ 144 \ 233 \ 377 \ 610 \ 987,$$

among which 1, 8 and 144 are the only perfect powers. At the beginning of the 80's, Stewart and Shorey and, independently, Pethő, established that there are only finitely many powers in the Fibonacci sequence. In other words, the Diophantine equation

$$F_n = y^p$$

has only finitely many solutions  $(n, y, p)$  with  $y \geq 2$  and  $p \geq 2$ .

## 5. A result from arithmetic geometry

A common feature of all the results mentioned above is that they belong to the area usually called 'Diophantine approximation'. Motivated in part by Fermat's conjecture, another branch of mathematics, namely arithmetic geometry, appeared in the middle of the twentieth century. Many mathematicians have contributed to its development, and one of their main achievements is Wiles' theorem that there is no solution in positive integers  $x$ ,  $y$ ,  $z$  and  $n \geq 3$  to the Fermat equation

$$x^n + y^n = z^n. \quad (6)$$

The proof is very difficult and extremely ingenious. Very roughly, it can be summarized as follows. One associates to every putative solution to (6) an elliptic curve (the so-called Frey curve). Since every elliptic curve is modular (this was the difficult step!), this curve is attached to a newform of a certain level, of level 2 in the present case. But there are no newforms at level 2, so there are no solutions to Fermat's equation.

Later, similar ideas have been used to solve completely several (families of) Fermat-type equations of the form  $ax^p + by^q = cz^r$ . One of the difficulties is that there are newforms at all levels  $> 60$ , so one cannot hope to always reach a contradiction, as in the case of (6). Nevertheless, even when newforms exist, some other arguments may be employed to conclude that there are no solutions.

## 6. Two further recent results

Unlike at the end of the 80's, we are now, and since about twenty years, able to solve completely some 'classical' Diophantine equations (and not only to say that these have only finitely many solutions). There are two main explanations. The first one concerns a theoretical improvement: the size of the numerical constants appearing in the estimates for linear forms in logarithms has been substantially reduced and is now (at least in the case of two logarithms) rather satisfactory. The second one is the development of algorithmic number theory.

For instance, we have now at our disposal efficient algorithms which enable us to solve any Thue equation of small degree, say of degree less than twelve, and with small coefficients. Further, there are examples of Thue equations of high degree which are completely solved.

Among the results I like very much is the following spectacular theorem proved by Bennett in 2001. If  $a$  and  $n \geq 3$  are positive integers, then the Thue equation

$$(a + 1)x^n - ay^n = 1,$$

in positive integers  $x, y$ , has only the solution given by  $x = y = 1$ .

I conclude with an overview of the proof that 1, 8 and 144 are the only Fibonacci powers, a result established in 2003 by Mignotte, Siksek and myself.

Using elementary arguments, Ljunggren proved in 1951 that 1 and 144 are the only Fibonacci squares, while London and Finkelstein showed in 1969 that 8 is the only Fibonacci cube. Consequently, we are concerned with the equation

$$F_n = y^p, \quad n > 2, \quad p > 3. \quad (7)$$

Taking into account that elementary arguments show that for each solution  $(n, y, p)$  to (7) we have  $n \equiv \pm 1$  modulo 6, the five main steps to solve (7) are the following (we simplify a little):

Step 1. Using lower bounds for linear forms in three logarithms one gets an upper bound on the (prime) exponent  $p$ , namely

$$p < 2 \times 10^8;$$

Step 2. The modular method is used for all  $p < 2 \times 10^8$  to prove the congruence

$$n \equiv \pm 1 \pmod{p},$$

(the computer time was around 50 hours);

Step 3. The previous condition allows us to view the initial linear form in three logarithms as a linear form in two logarithms, which leads to the important progress

$$p \leq 733;$$

Step 4. A detailed study of the family of associated Thue equations corresponding to the range  $5 \leq p \leq 733$  leads to the condition

$$n < 10^{9000},$$

(recall that  $n$  is an index!);

Step 5. Using once more the modular method one proves that there are no further solutions for  $5 \leq p \leq 733$  (the computer time was less than 100 hours).

Let us add a few comments.

Firstly, observe that at Step 2 we cannot hope for a better conclusion. Indeed, if we use the recursion to define the Fibonacci sequence backwards, we see that  $F_{-1} = 1$ , thus  $F_{-1}$  and  $F_1$  are  $p$ -th powers for every  $p > 3$ .

Secondly, recall that the Lucas sequence  $(L_n)_{n \geq 0}$ , defined by  $L_0 = 2$ ,  $L_1 = 1$  and the recursion

$$L_{n+2} = L_{n+1} + L_n, \quad \text{for } n \geq 0,$$

is closely related to the Fibonacci sequence, namely by

$$L_n^2 + 4 = 5F_n^2, \quad \text{for } n \geq 1 \text{ odd.} \quad (8)$$

To prove that (7) has no solution, it is thus sufficient to solve the Diophantine equation

$$x^2 + 4 = 5y^p. \quad (9)$$

Unfortunately, current techniques do not allow us to solve (9) completely. Nevertheless, we know how to derive from (9) a Thue equation of degree  $p$ , thus, we can bound the solutions  $x, y$  to (9) in terms of  $p$ . By (8), we then get a bound for  $n$  in terms of  $p$  for every putative solution  $(n, y, p)$  to (7). This is precisely what we are doing at Step 4.

Thirdly, at Steps 2 and 5, Equation (9) is viewed as a particular case of the Fermat-type equation  $5y^p - 4z^p = x^2$ . For a fixed prime exponent  $p$  and a good prime  $\ell$  (all primes are good, except finitely many), the method allows us to get congruence conditions on  $x, y, z$  modulo  $\ell$ , hence on  $n$  modulo  $\ell - 1$ . At Step 2, we do this with several primes  $\ell$  of the form  $hp + 1$  and we get that  $n$  must be  $\pm 1$  modulo  $p$ . We have to do this for every  $p$  between 5 and  $2 \times 10^8$ .

We conclude by two challenging open problems.

*To solve the equation  $x^2 - 2 = y^p$ .*

Current techniques allow us to bound  $p$  from above by one thousand.

*To solve the equation  $x^m - y^n = 2$ .*

This equation has conjecturally only finitely many solutions in integers  $x, y, m, n$  all at least 2, but this remains unproved!

Yann Bugeaud, Université de Strasbourg, France.

e-mail : [bugeaud@math.u-strasbg.fr](mailto:bugeaud@math.u-strasbg.fr)