Séminaire BOURBAKI Novembre 2002
55e année, 2002-2003, nO 909, p. 1 à 26

CATALAN'S CONJECTURE
[after Mihăilescu]

by **Yuri F. BILU**

To E.W.

1. INTRODUCTION

In 1844 Crelle's journal published the following note [13].

> **Note**
>
> extraite d'une lettre adressée à l'éditeur par Mr. *E. Catalan*, Répétiteur à l'école polytechnique de Paris.
>
> Je vous prie, Monsieur, de vouloir bien énoncer, dans votre recueil, le théorème suivant, que je crois vrai, bien que je n'aie pas encore réussi à le démontrer complètement : d'autres seront peut-être plus heureux :
>
> Deux nombres entiers consécutifs, autres que 8 et 9, ne peuvent être des puissances exactes ; autrement dit : l'équation $x^m - y^n = 1$, dans laquelle les inconnues sont entières et positives, n'admet qu'une seule solution.

Thus, we have the following conjecture.

Conjecture 1.1 (Catalan). — *Equation $x^u - y^v = 1$ has no solutions in integers $x, y, u, v > 1$ other than $3^2 - 2^3 = 1$.*

Now, 158 years after, the conjecture is completely proved. Let us briefly review the most important events which lead to the solution of this celebrated problem. This is *not* a comprehensive historical account of Catalan's problem; the latter can be found in Ribenboim's book [34] and Mignotte's survey [26].

Seven years after Catalan's note appeared, Lebesgue [21] proved that equation $x^m - y^2 = 1$ has no solutions in positive integers x, y, m with $m > 1$. In 1965 Ko Chao [18] showed that equation $x^2 - y^n = 1$ has no solutions in positive integers x, y, n with $n > 1$ other than $3^2 - 2^3 = 1$. These two results reduce Catalan's conjecture to the following assertion.

Conjecture 1.2. — *Equation*

$$x^p - y^q = 1 \tag{1}$$

has no solutions in non-zero integers x, y and odd primes p, q.

Notice that we no longer assume x and y positive. It is convenient, because now the problem is symmetric: if (x, y, p, q) is a solution, then so is $(-y, -x, q, p)$. This will be repeatedly used in the sequel.

From now on Conjecture 1.2 will be referred to as *Catalan's conjecture* and (1) as Catalan's equation.

Cassels [12] discovered important arithmetical properties of solutions of Catalan's equation. His results (see Proposition 2.1) are indispensable in most of the subsequent works on Catalan's equation.

In 1976 Tijdeman [37] made a breakthrough. Using Baker's theory, he proved that the exponents p and q are bounded by an explicit absolute constant. Together with the classical result of Baker [6] this implies that $|x|$ and $|y|$ are bounded by an explicit absolute constant as well, and Catalan's problem is thereby decidable.

In a different direction, Inkeri [16, 17] and others obtained algebraic criteria of solubility of (1) in terms of the exponents p and q. In the nineties, Mignotte and Roy used Inkeri-type criteria, Tijdeman's argument and electronic computations to obtain tight lower and upper bounds for p and q. (Upper bounds were also obtained by Blass *et al.* [10] and O'Neil [32].) By 2000, it was proved that p and q lie between 10^7 and 10^{18}. See [29] for more precise results and a survey of this period.

In 1999 Preda Mihăilescu enters the scene. In his first paper [29] he drastically refined Inkeri's criterion. And quite recently, after several unsuccessful attempts, he finally settled [30] Catalan's conjecture:

Theorem 1.3 (Mihăilescu). — *Conjecture 1.2 is true.*

The present paper contains a reasonably self-contained proof of this result.

Plan of the paper. — In Section 2 we recall Cassels' relations and derive their immediate consequence, in particular, Hyyrö's lower bounds for $|x|$ and $|y|$. In Section 3 we very briefly review algebraic criteria for Catalan's equation in terms of p and q, and prove Mihăilescu's "double Wieferich" criterion. In Section 4 we use binary logarithmic forms, Tijdeman's argument, and computations by Mignotte and Roy to show that $p \not\equiv 1 \bmod q$. Section 5 contains general lemmas. In Section 6 Theorem 1.3 is reduced to three more technical statements, which are proved in the three final section.

Acknowledgements. — My deepest gratitude goes to Hendrik W. Lenstra and Yann Bugeaud, who carefully read the manuscript and suggested numerous corrections and improvements. I am indebted to Yann Bugeaud, Andrew Glass, Guillaume Hanrot, Maurice Mignotte and Preda Mihăilescu for explaining to me various results from Sections 2 and 4 and other useful discussions. I also thank Bruno Anglès, John Coates, Gabi Hecke, Shanta Laishram, Hendrik W. Lenstra, Tauno Metsänkylä and Gisbert Wüstholz, who detected inaccuracies in previous versions of this note. Finally, I thank Denis Benois and Leonid Positselski for a tutorial in commutative algebra.

1.1. Notation

In the sequel we assume, unless the contrary is indicated explicitly, that x, y are non-zero integers and p, q are odd prime numbers satisfying

$$x^p - y^q = 1. \tag{2}$$

As we had already noticed, (2) implies that $(-y)^q - (-x)^p = 1$, and all the statements below remain true with x, y, p, q replaced by $-y, -x, q, p$.

We denote by ζ a primitive p-th root of unity and put

$$K = \mathbb{Q}(\zeta), \quad G = \mathrm{Gal}(K/\mathbb{Q}).$$

The principal ideal $(1-\zeta)$ will be denoted by $\mathfrak{p}$. Recall that it is a prime ideal of K and that $(p) = \mathfrak{p}^{p-1}$.

More specific notation will be introduced at the appropriate places.

2. CASSELS' RELATIONS AND LOWER ESTIMATES FOR $|x|$ AND $|y|$

Cassels [12] proved that $q|x$ and $p|y$. More precisely, he established the following relations.

Proposition 2.1 (Cassels). — *There exist a non-zero integer a and a positive integer v such that*

$$x - 1 = p^{q-1}a^q, \quad y = pav, \tag{3}$$

$$\frac{x^p - 1}{x - 1} = pv^q, \tag{4}$$

and, symmetrically, there exist a non-zero integer b and a positive integer u such that

$$y + 1 = q^{p-1}b^p, \quad x = qub, \tag{5}$$

$$\frac{y^q + 1}{y + 1} = qu^p. \tag{6}$$

□

The following consequence is crucial.

Corollary 2.2. — *The number* $\lambda := (x-\zeta)/(1-\zeta)$ *is an algebraic integer. The principal ideal* (λ) *is a* q*-th power of an ideal of the field* K.

Proof. — Since $p|(x-1)$ by (3), the prime ideal $\mathfrak{p}=(1-\zeta)$ divides $x-\zeta$, but $\mathfrak{p}^2$ does not. Hence λ is an algebraic integer, not divisible by $\mathfrak{p}$, and the same is true for its conjugates λ^σ, where $\sigma \in G$. Identity $(1-\zeta^\sigma)\lambda^\sigma - (1-\zeta^\tau)\lambda^\tau = \zeta^\tau - \zeta^\sigma$ implies that for distinct $\sigma, \tau \in G$, the greatest common divisor of λ^σ and λ^τ divides $(\zeta^\tau - \zeta^\sigma) = \mathfrak{p}$. Hence the numbers λ^σ are pairwise co-prime.

Now rewrite (4) as $\prod_{\sigma\in G}\lambda^\sigma = v^q$. Since the factors are pairwise co-prime, each principal ideal (λ^σ) is a q-th power of an ideal. ☐

Cassels' relations imply various lower estimates for the variables x and y in terms of p and q. For instance, (3) and (5) immediately yield

$$|x| \geqslant p^{q-1} - 1, \tag{7}$$

$$|y| \geqslant q^{p-1} - 1, \tag{8}$$

and this can be refined without much effort.

Hyyrö [15] obtained an estimate of a different kind: $|x| \geqslant q(2p+1)(2q^{p-1}+1)$ (and similarly for $|y|$). Since Hyyrö's paper is not easily available, I prove below a slightly weaker estimate, which is totally sufficient for our purposes. It is an easy consequence of the following proposition.

Proposition 2.3. — *If* p *does not divide* $q-1$ *then* $q^{p-2}\,\big|\,(u-1)$.

Proof. — Rewriting (6) as

$$\big((-y)^{q-1}-1\big) + \big((-y)^{q-2}-1\big) + \cdots + (-y-1) = q\,(u^p-1)\,,$$

we deduce that $(y+1)\,|(q\,(u^p-1))$. Now (5) implies that $u^p \equiv 1 \bmod q^{p-2}$. Since p does not divide the order $q^{p-3}(q-1)$ of the multiplicative group $\bmod q^{p-2}$, this implies that $u \equiv 1 \bmod q^{p-2}$. ☐

Corollary 2.4. — *We have* $|x| \geqslant q^{p-1}$.

Proof. — If $p|(q-1)$ then $p<q$ and the result follows from (7). If p does not divide $q-1$ then $q^{p-2}\,\big|\,(u-1)$, and, since u is positive, this implies $u \geqslant q^{p-2}+1$. Since $x = qub$, we have $|x| \geqslant qu \geqslant q^{p-1}+q$, better than wanted. ☐

Remark 2.5. — This version of Hyyrö's argument is due to Mignotte and Bugeaud. It was kindly communicated to me by Yann Bugeaud. Using more advanced tools, Mihăilescu [30, Appendix A] obtained a much sharper estimate $|x| \geqslant \big(q^{2p-2}/2\big)^4$.

3. ALGEBRAIC CRITERIA

Using Cassels' relations and some algebraic number theory, one may get various algebraic criteria of solvability of Catalan's equation with given exponents p and q. The most famous criterion is due to Inkeri [16, 17]:

THEOREM 3.1 (Inkeri). — *With the notation of Subsection 1.1, put* $K_p = \mathbb{Q}(\sqrt{-p})$ *if* $p \equiv 3 \bmod 4$ *and* $K_p = K$ *if* $p \equiv 1 \bmod 4$. *Then either* $p^{q-1} \equiv 1 \bmod q^2$ *or* q *divides the class number of the field* K_p. □

It will be explained in Subsection 4.4 how algebraic criteria of this kind, together with electronic computations, allow one to obtain lower bounds for p and q.

Refinements of and supplements for Inkeri's criterion were suggested by Mignotte [25], Schwarz [35] and others; see [26] for a survey of these results. I would especially mention the paper by Bugeaud and Hanrot [11], which strongly influenced Mihăilescu's work.

Verification of Inkeri's criterion for a given pair (p, q) requires computing certain class numbers, which seriously affects its computational efficiency. Mihăilescu [29] made a major step forward, showing that the class number condition can be omitted.

THEOREM 3.2 (Mihăilescu). — *For any solution of* (x, y, p, q) *of (2) we have* $q^2|x$ *and*

$$p^{q-1} \equiv 1 \bmod q^2. \tag{9}$$

Congruence (9) (called *Wieferich's relation*) will be used in Section 4 to prove that $p \not\equiv 1 \bmod q$. Relation $q^2|x$ is crucial in the proof of Theorem 6.3.2.

By symmetry, one has $q^{p-1} \equiv 1 \bmod p^2$. Pairs (p, q), satisfying this and (9) are called *double Wieferich pairs*. Only six such pairs are currently known:

$$(2, 1093), (3, 1006003), (5, 1645333507), (83, 4871), (911, 318917), (2903, 18787).$$

I sketch the proof of Theorem 3.2, because it is very instructive and can serve as a good model of the much more involved proof of Theorem 1.3. See [24, 33] for different proofs.

3.1. Proof of Theorem 3.2

For $a \in \{1, 2, \ldots, p-1\}$ let σ_a be the element of $G = \mathrm{Gal}(K/\mathbb{Q})$ be defined by $\zeta \mapsto \zeta^a$. In the group ring $\mathbb{Z}[G]$ consider elements

$$\Theta_c = \sum_{a=1}^{p-1} \lfloor ac/p \rfloor \sigma_a^{-1} \qquad (c = 1, 2, \ldots, p-1).$$

In particular, $\Theta_1 = 0$ and $\Theta_2 = \sigma_{(p+1)/2} + \cdots + \sigma_{p-1}$. Ideal $\mathcal{I} = (\Theta_1, \Theta_2, \ldots, \Theta_{p-1})$ of $\mathbb{Z}[G]$ is called the *Stickelberger ideal*. Its main property is the *Stickelberger theorem*: