Séminaire Bourbaki Novembre 2002
55ème année, 2002-2003, n° 909

CATALAN'S CONJECTURE
[after Mihăilescu]

by **Yuri F. BILU**

Table of contents

To E.W.

1. INTRODUCTION

In 1844 Crelle's journal published the following note [9].

> **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'admèt 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 [29] and Mignotte's survey [22].

Seven years after Catalan note appeared, Lebesgue [17] proved that equation $x^m - y^2 = 1$ has no solutions in positive integers x, y, m with $m > 1$. In 1965 Ko Chao [14] 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 [8] 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 [32] 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 [3] 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 [12, 13] and others obtained algebraic criteria of solubility of (1) in terms of the exponents p and q. In 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.* [6] and O'Neil [27]). By 2000, it was proved that p and q lie between 10^7 and 10^{18}. See [25] for more precise results and a survey of this period.

In 1999 Preda Mihăilescu enters the scene. In his first paper [25] he drastically refined Inkeri's criterion. And quite recently, after several unsuccessful attempts, he finally settled [26] 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 [8] 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 integers 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

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

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

and this can be refined without much effort.

Hyyrö [11] obtained an estimate of a different kind: $|x| \geq q(2p+1)(2q^{p-1}+1)$ (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 $q^{p-2} | (u-1)$.*

Proof Rewriting (6) as

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

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 $|x| \geq q^{p-1}$.*

Proof If $p|(q-1)$ then $p < q$ and the result follows from (7). If p does not divide $q-1$ then $q^{p-2} | (u-1)$, and, since u is positive, this implies $u \geq q^{p-2}+1$. Since $x = qub$, we have $|x| \geq qu \geq q^{p-1} + q$, 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 [26, Appendix A] obtained a much sharper estimate $|x| \geq (q^{2p-2}/2)^4$.

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 [12, 13]:

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 [20], Schwarz [30] and others; see [22] for a survey of these results. I would especially mention the paper of Bugeaud and Hanrot [7], 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 [25] 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 [19, 28] 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*. It main property is *Stickelberger theorem*: any $\Theta \in \mathcal{I}$ annihilates the class group of K. That is, for any ideal $\mathfrak{a}$ of K and any $\Theta \in \mathcal{I}$, the ideal $\mathfrak{a}^\Theta$ is principal. See [34, Section 6.2] for the details.

Let $\iota = \sigma_{p-1}$ be the complex conjugation. Mihăilescu proves the following assertion.

PROPOSITION 3.1.1. — *For any $\Theta \in (1-\iota)\mathcal{I}$, the element $(x-\zeta)^\Theta$ is a q-th power in K.*

Proof Write $\Theta = (1-\iota)\Theta'$, where $\Theta' \in \mathcal{I}$. Put $\lambda := (x-\zeta)/(1-\zeta)$. By Corollary 2.2 the principal ideal (λ) is a q-th power: $(\lambda) = \mathfrak{a}^q$. By the Stickelberger theorem $\mathfrak{a}^{\Theta'}$ is a principal ideal, say, (α). It follows that $\left(\lambda^{\Theta'}\right) = (\alpha)^q$, or $\lambda^{\Theta'} = \eta\alpha^q$, where η is a unit of K. We obtain

$$(x-\zeta)^\Theta = \left(\frac{1-\zeta}{1-\bar{\zeta}}\right)^{\Theta'} \frac{\eta}{\bar{\eta}} \left(\frac{\alpha}{\bar{\alpha}}\right)^q. \tag{10}$$

Since η is a unit, $\eta/\bar{\eta}$ is a root of unity[1] . The quotient $(1-\zeta)/(1-\bar{\zeta})$ is a root of unity as well. Thus, $(x-\zeta)^\Theta$ is a q-th power times a root of unity. Since any root of unity in K is a q-th power, so is $(x-\zeta)^\Theta$. □

Proof of $q^2|x$ Since $(1-\zeta x)^\Theta$ is equal to $(x-\zeta)^\Theta$ times a root of unity, it is a q-th power as well. On the other hand, $q|x$ implies that $(1-\zeta x)^\Theta \equiv 1 \bmod q$. Since q is unramified in K, this implies that $(1-\zeta x)^\Theta \equiv 1 \bmod q^2$ (cf. Proposition 5.3.1 below).

However, if $\Theta = \sum_{\sigma\in G} n_\sigma \sigma$, then a quick calculation shows that

$$(1-\zeta x)^\Theta \equiv 1 - x\sum_{\sigma\in G} n_\sigma \zeta^\sigma \bmod q^2.$$

It follows that either $q^2|x$ or $q|\sum_{\sigma\in G} n_\sigma\zeta^\sigma$. In the latter case $q|n_\sigma$ for any $\sigma \in G$. However, this is not true if, for instance,

$$\Theta = (1-\iota)\Theta_2 = -\sigma_1^{-1} - \cdots - \sigma_{(p-1)/2}^{-1} + \sigma_{(p+1)/2}^{-1} + \cdots + \sigma_{p-1}^{-1}.$$

Thus, $q^2|x$. □.

Proof of (9) This is just an elementary exercise. Since $q^2|x$, the first equality in (3) implies that

$$p^{q-1}a^q \equiv -1 \bmod q^2. \tag{11}$$

Since $p^{q-1} \equiv 1 \bmod q$, we have $a^q \equiv -1 \bmod q$, which implies $a^q \equiv -1 \bmod q^2$, which, together with (11), implies (9). □

[1] It is an algebraic integer, and for any $\sigma \in G$ we have $|(\eta/\bar{\eta})^\sigma| = 1$

4. LOGARITHMIC FORMS, TIJDEMAN'S ARGUMENT AND THE RELATION $p \not\equiv 1 \bmod q$

As I mentioned in the introduction, Tijdeman [32] applied Baker's theory of logarithmic form to establish an effective upper bound for the solutions, reducing the problem to a finite computation. In this section we use Tijdeman's argument and electronic computations due to Mignotte and Roy to prove the following important theorem.

THEOREM 4.1. — *Let (x, y, p, q) be a solution of (2). Then $p \not\equiv 1 \bmod q$.*

The relation $p \not\equiv 1 \bmod q$ is indispensable for Mihăilescu's proof. It is repeatedly used in Section 6 and in the proof of Theorem 6.3.2. A reader ready to take Theorem 4.1 for granted may skip the rest of this section.

When writing this section, I profited a lot from helpful explanations and suggestions of Maurice Mignotte and Andrew Glass.

4.1. Logarithmic forms

In this subsection we recall Baker's lower bound for logarithmic forms

$$\Lambda = b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n.$$

Here $b_1, \ldots, b_n$ are non-zero integers and $\alpha_1, \ldots, \alpha_n$ are usually algebraic numbers. To avoid unnecessary technicalities, we shall assume that $\alpha_1, \ldots, \alpha_n$ are **positive rational numbers, distinct from** 1. This is totally sufficient for applications in Catalan's problem.

Define the height of a rational number $\alpha = \mu/\nu$ (where μ and ν are relatively prime integers) by $h(\alpha) = \log \max\{|\mu|, |\nu|\}$. Assume that $\Lambda \neq 0$. Then it is rather easy to bound $|\Lambda|$ from below. Indeed, $e^{\Lambda} - 1$ is a non-zero rational number with denominator bounded by $e^{(h(\alpha_1)+\cdots+h(\alpha_n))B}$, where

$$B = \max\{|b_1|, \ldots, |b_n|\}.$$

It follows that

$$|\Lambda| \gg e^{-(h(\alpha_1)+\cdots+h(\alpha_n))B}, \tag{12}$$

where here and below in this subsection the positive constants implied by $O(\cdot)$, $\ll$ and $\gg$ are absolute and effective.

However, (12) is too weak for applications: one needs $o(B)$ in the exponent. Such an estimate was obtained by Gelfond [10] for $n = 2$ and by Baker [2] in the general case. Baker's inequality belongs to the top arithmetical results of twentieth century.

The modern estimate [4, 18, 33] is of the form

$$|\Lambda| \geq e^{-c(n)h(\alpha_1)\cdots h(\alpha_n)\log B} \tag{13}$$

(provided $\Lambda \neq 0$.) See the recent volume [35] for the history of the subject and the present state of art.

When one wants to be explicit, the numerical value of the constant $c(n)$ becomes vital. For growing n, the best result is due to Matveev [18], who showed that one may take $c(n) = c^n$ with an explicit absolute constant c.

However, in Catalan's problem one uses (13) only with $n = 2$ and $n = 3$. Therefore it is practical to have special bounds for these two cases, which are numerically sharper than the general bound (13). Such bounds were obtained by Laurent, Mignotte and Nesterenko [16] for binary forms and by Bennett *et al.* [5] for ternary forms. Here is a simplified form of the Laurent-Mignotte-Nesterenko result (see Corollary 2 from [16, Section 2]), to be used in Subsection 4.3 below.

PROPOSITION 4.1.1. — *Let α_1, α_2 be multiplicatively independent positive rational numbers and b_1, b_2 positive integers. Let A_1, A_2 be real numbers satisfying $A_i \geq \max\{h(\alpha_i), 1\}$ for $i = 1, 2$. Put $B = b_1/A_2 + b_2/A_1$ and $\Lambda = b_1 \log \alpha_1 - b_2 \log \alpha_2$. Then*

$$\log |\Lambda| \geq -24.34 \left(\max\left\{\log B + 0.14,\, 21\right\}\right)^2 A_1 A_2. \tag{14}$$

This is asymptotically weaker than (13) when B grows (because $\log B$ is replaced by $(\log B)^2$), but for small B inequality (14) is very sharp numerically.

I do not formulate the result of [5], because it is very involved and will not be used here.

4.2. **An informal introduction to Tijdeman's argument**

In this subsection we assume that $p > q$.

In Catalan's problem, the most obvious logarithmic form to try is $\Lambda = p \log |x| - q \log |y|$. The upper estimate is obvious: $|\Lambda| \leq |x|^{-p}$. The lower estimate coming from (13) is $|\Lambda| \geq e^{-O(p \log |x| \log |y|)}$, and comparing the two estimates does not yield any interesting consequence.

Tijdeman's [32] brilliant idea was to use $\Lambda = q \log |y + 1| - p \log |x|$. Upper bound is now slightly worse: $\Lambda| \ll q|y|^{-1}$. For the lower bound, we use Cassels' relations (6) to obtain $\Lambda = p \log \alpha - q \log q$, where $\alpha = (q|b|)^{q-1} u^{-1}$ (recall that $u > 0$). It is easy to show (see Subsection 4.3) that $h(\alpha) = \log |u| + O(1) \leq (q/p) \log |y| + O(1)$. Now (13) implies that $|\Lambda| \geq e^{-O((q/p) \log |y| \log q \log p)}$, which, compared with the lower estimate, implies that

$$p \ll q \log q \log p. \tag{15}$$

If (14) is used instead of (13), then one obtains the slightly weaker inequality

$$p \ll q \log q (\log p)^2. \tag{16}$$

Similarly, using

$$\Lambda = q \log |y + 1| - p \log |x - 1| = pq \log \beta - q \log q + p \log p$$

with $\beta = bq/ap$, one obtains the estimate

$$q \ll (\log p)^2 \log q. \tag{17}$$

Together with (15) this implies an effective upper bound for p, as wanted.

As I already mentioned in Subsection 4.1, Tijdeman's argument does not require the full strength of Baker's inequality. One needs a lower bound for binary logarithmic forms to obtain (15) and a lower bound for ternary logarithmic form to obtain (17).

Langevin [15] made Tijdeman' work explicit by proving that $p, q \leq 10^{110}$. This bound has been refined several times until O'Neil [27] (see also [6]) proved that $p \leq 3.2 \cdot 10^{17}$ and $q \leq 2.6 \cdot 10^{12}$, and Mignotte [25] announced that $p \leq 7.8 \cdot 10^{16}$ and $q \leq 7.2 \cdot 10^{11}$. Mignotte used the already mentioned bounds for binary and ternary logarithmic forms from [16] and [5], respectively.

4.3. **Explicit Tijdeman's inequality**

In this subsection we apply Proposition 4.1.1 to obtain an explicit analogue of (16).

PROPOSITION 4.3.1. — *For any solution of (2) we have*

$$p \leq 24.34q \left(\max \left\{ \log \frac{p+1}{\log q} + 0.14,\ 21 \right\} \right)^2 \log q. \tag{18}$$

Inequality (18) will be used in Subsection 4.5. It is less sharp than the corresponding results from [23] and [6], but easier to prove and sufficient for our purposes.

Proof of Proposition 4.3.1 We may assume that

$$p \geq 10000q \log q, \tag{19}$$

and, in particular, $p > q$, since otherwise (18) holds trivially.

As indicated in Subsection 4.2, we will compare upper and lower estimates for the quantity

$$\Lambda = q \log |y+1| - p \log |x| = p \log \alpha - q \log q,$$

with $\alpha = (q|b|)^{q-1} u^{-1}$, where $b \in \mathbb{Z}$ and $u \in \mathbb{Z}_{>0}$ are defined in Proposition 2.1.

The upper estimate is trivial. Rewriting Catalan's equation (2) as

$$p \log |x| = q \log |y| + \log(1 + y^{-q}),$$

we obtain

$$\Lambda = q \log \left(1 + y^{-1}\right) - \log \left(1 + y^{-q}\right). \tag{20}$$

Since $|\log(1+t)| \leq 2|t|$ for $|t| \leq 1/2$, this implies that

$$|\Lambda| \leq 2|y|^{-q} + 2q|y|^{-1} \leq 3q|y|^{-1}, \tag{21}$$

and $|\Lambda| < 1$ by (8). Equality (20) implies also that $\Lambda \neq 0$: the first term always dominates over the second one.

For the lower bound, let us estimate $h(\alpha)$. Since

$$\log\left((q|b|)^{q-1}\right) = \log u + (\Lambda + q\log q)/p \le \log u + 1,$$

we have $h(\alpha) \le \log u + 1$. Also, q and α are multiplicatively independent: otherwise, Λ would have been a multiple of $\log q$, contradicting the previously established inequality $0 < |\Lambda| < 1$.

Thus, we are in a position to use Proposition 4.1.1. We obtain

$$\log|\Lambda| \ge -24.34\left(\max\{\log B + 0.14, 21\}\right)^2(\log u + 1)\log q \tag{22}$$

with $B = p/\log q + q/(\log u + 1)$. Proposition 2.3 and (19) imply that

$$u \ge q^{p-2} \ge e^{9000q(\log q)^2}. \tag{23}$$

Hence $B \le (p+1)/\log q$. Substituting this into (22) and combining the resulting inequality with (21), we obtain

$$\frac{\log|y|}{\log u} \le 24.34\left(\max\left\{\log\frac{p+1}{\log q} + 0.14, 21\right\}\right)^2 \log q\left(1 + \frac{1}{\log u}\right) + \frac{\log(3q)}{\log u}. \tag{24}$$

Further, (6) implies that $q|y|^{q-1} \ge qu^p$, whence

$$p \le (q-1)\frac{\log|y|}{\log u} \le 24.34(q-1)\left(\max\left\{\log\frac{p+1}{\log q} + 0.14,\ 21\right\}\right)^2 \log q\left(1 + \frac{1}{\log u}\right) + \frac{(q-1)\log(3q)}{\log u}. \tag{25}$$

Using (19) and (23), one easily shows that the right-hand side of (25) does not exceed the right-hand side of (18). The proposition is proved. □

4.4. **Lower bounds for p and q**

One can bound exponents p and q from below, using algebraic criteria (see Section 3) and electronic computations. This has been realized by Mignotte and Roy [23, 24, 25]. To show that $q \ge Q_0$, one has to verify an algebraic criterion (Inkeri's or other), for all pairs (p, q) satisfying $q \le Q_0$, $p > q$ and (18). Actually, Mignotte and Roy used sharper, than (18), inequalities.

With Inkeri-type criteria, Mignotte and Roy managed to prove that

$$\min\{p, q\} \ge 10^5, \tag{26}$$

using several months of computations. With Mihăilescu's criterion (Theorem 3.2) this required only a few hours of computations, and with one month of computations they managed to prove that $\min\{p, q\} \ge 10^7$. I am aware about the computations of Grantham and Wheeler showing that $\min\{p, q\} \ge 3.2 \cdot 10^8$ but I have never seen this result announced in print.

Inequality (26) will be used in Subsection 4.5.

4.5. **Proof of Theorem 4.1**

First of all, we deduce from Proposition 4.3.1 the following consequence.

PROPOSITION 4.5.1. — *If $q \geq 28000$ then $p \leq 4q^2$.*

Proof Assume first that

$$\log \frac{p+1}{\log q} + 0.14 \leq 21.$$

Then (18) reads $p \leq 10734q \log q$, and $p \geq 4q^2$ would imply $q \leq 2683.5 \log q$, which is wrong for $q \geq 28000$.

Now assume that

$$\log \frac{p+1}{\log q} + 0.14 \geq 21.$$

Then (18) reads

$$p \leq 24.34q \left(\log \frac{p+1}{\log q} + 0.14 \right)^2 \log q.$$

Since $0.14 - \log\log q \leq 0.14 - \log\log 28000 \leq -2.18$, this implies that

$$\frac{p}{(\log(p+1) - 2.18)^2} \leq 24.34q \log q. \tag{27}$$

It is easy to show, calculating the derivative, that the left hand-side of (27), viewed as a function in p, increases when $p \geq 67$. Hence, assuming that $p \geq 4q^2$, we may replace in (27) p by $4q^2$, which would result in the inequality $q \leq 6.085 \left(\log\left(4q^2+1\right) - 2.18\right)^2 \log q$. Since $\log\left(4q^2+1\right) - 2.27 \leq \log q^2$, we obtain the inequality $q \leq 24.34(\log q)^3$, which is contradictory for $q \geq 28000$. □

Proof of Theorem 4.1 Assume that $p \equiv 1 \bmod q$. Wieferich's relation (9) implies that $p \equiv 1 \bmod q^2$. Since p is odd, it cannot be equal to q^2+1 or $3q^2+1$. Also, $p \neq 2q^2+1$, because the latter number is divisible by 3. (This simple, but important observation is due to Mignotte.) Thus, $p \geq 4q^2+1$. On the other hand (26) and Proposition 4.5.1 imply that $p \leq 4q^2$, a contradiction.

REMARK 4.2. — Inequality (26) is the only result, used by Mihăilescu, that depends on electronic computations. One can avoid using it, showing instead that

there exist no pairs (p,q) satisfying $q < 28000$,

$$1 + 4q^2 \leq p \leq 24.34q \left(\max\left\{ \log \frac{p+1}{\log q} + 0.14,\ 21 \right\} \right)^2 \log q,$$

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

The running time of the corresponding PARI-script (written by Preda Mihăilescu at my request) is about 1 minute on a modern computer.

Still, it would be very interesting to find a purely algebraic proof of $p \not\equiv 1 \bmod q$, or, at least, a proof independent of electronic computations. Recently Mihăilescu announced that he has such a proof.

5. GENERALITIES

In this section we recall some simple results about modules over commutative rings and several other facts to be used in the proof. They are certainly well-known, but it was easier for me to supply direct proofs than to look for suitable references.

All rings in this section are **commutative and with unity**. An ideal $\mathfrak{a}$ of a ring R is *radical* if $R/\mathfrak{a}$ has no non-zero nilpotent elements.

5.1. Rings and modules

Let R be a ring and M an R-module. Given a subset $S \subseteq M$, we denote by $\mathrm{ann}_R(S)$ the ideal of annihilators of S in R. When no confusion is possible, we omit the index and write $\mathrm{ann}(S)$. In this subsection *isomorphic* means R-isomorphic. For instance, a cyclic R-module M is (non-canonically) isomorphic to $R/\mathrm{ann}(M)$.

The following property of cyclic modules is immediate.

PROPOSITION 5.1.1. — *Let M be a cyclic R-module. Then any quotient of M is cyclic. If R is a principal ideal ring, then any submodule of R is cyclic as well.* □

PROPOSITION 5.1.2. — *Let R be a ring and M a finitely generated R-module. Let $\mathfrak{b}$ be an ideal of R such that $\mathfrak{b} + \mathrm{ann}_R(M)$ is a radical ideal of R. Then $\mathrm{ann}_{R/\mathfrak{b}}(M/\mathfrak{b}M)$ is the image of $\mathrm{ann}_R(M)$ in $R/\mathfrak{b}$.*

Proof We have to prove that for any $\alpha \in R$ one has

$$\alpha M \subseteq \mathfrak{b}M \Longleftrightarrow \alpha \in \mathfrak{b} + \mathrm{ann}_R(M).$$

Implication "$\Leftarrow$" is obvious, so we are left with "$\Rightarrow$". Let φ be an endomorphism of M such that $\varphi(M) \subseteq \mathfrak{b}M$. Then, according to [1, Proposition 2.4], there exist a positive integer n and $\beta_1, \ldots, \beta_n \in \mathfrak{b}$ such that $\varphi^n + \beta_1\varphi^{n-1} + \cdots + \beta_n = 0$. For φ equal to multiplication by α this means that $\alpha^n + \beta_1\alpha^{n-1} + \cdots + \beta_n \in \mathrm{ann}(M)$. Thus, $\alpha^n \in \mathfrak{b} + \mathrm{ann}(M)$. Since the latter ideal is radical, we obtain $\alpha \in \mathfrak{b} + \mathrm{ann}(M)$, which proves "$\Rightarrow$". □

PROPOSITION 5.1.3. — *Let R be a direct product of finitely many fields: $R = \prod_{\alpha\in \mathrm{A}} K_\alpha$, where each K_α is a field. Then we have the following.*

(1) *If $\mathrm{B} \subseteq \mathrm{A}$ then the set $\mathcal{I}(\mathrm{B}) := \{(x_\alpha)_{\alpha\in\mathrm{A}} : x_\alpha = 0 \text{ for } \alpha \in \mathrm{B}\}$ is an ideal of R, and all ideals are of this form. In particular, any quotient of R is itself a direct product of fields.*
(2) *For any ideals $\mathcal{I}, \mathcal{I}' \trianglelefteq R$ one has $\mathcal{I}\mathcal{I}' = \mathcal{I} \cap \mathcal{I}'$. Moreover, for any $b \in \mathcal{I}\mathcal{I}'$ there exist $a \in \mathcal{I}$ and $a' \in \mathcal{I}'$ such that $b = aa'$. In particular, $\mathcal{I}^2 = \mathcal{I}$, and for any $a \in \mathcal{I}$ there exist $a_1, a_2 \in \mathcal{I}$ such that $a = a_1a_2$.*
(3) *For any ideal $\mathcal{I} \trianglelefteq R$ there is a uniquely defined ideal $\mathcal{I}^\perp \trianglelefteq R$ such that $\mathcal{I}\mathcal{I}^\perp = (0)$ and $\mathcal{I} + \mathcal{I}^\perp = R$.*

(4) *For any ideals* $\mathcal{I}, \mathcal{I}' \trianglelefteq R$ *one has*

$$(\mathcal{I}\mathcal{I}')^{\perp} = \mathcal{I}^{\perp} + \mathcal{I}'^{\perp}, \quad (\mathcal{I} + \mathcal{I}')^{\perp} = \mathcal{I}^{\perp}\mathcal{I}'^{\perp}. \tag{28}$$

Also, $\mathcal{I}\mathcal{I}' = (0)$ *if and only if* $\mathcal{I}' \subseteq \mathcal{I}^{\perp}$.

(5) *Let* M *a cyclic* R*-module and* M' *is a submodule* M*. Then*

$$\operatorname{ann}(M') + \operatorname{ann}(M/M') = R \quad \textit{and} \quad \operatorname{ann}(M')\operatorname{ann}(M/M') = \operatorname{ann}(M).$$

(6) *Let* M *be an* R*-module. Then there exists* $a \in M$ *such that* $\operatorname{ann}(a) = \operatorname{ann}(M)$*. In other words,* M *has a submodule isomorphic to* $R/\operatorname{ann}(M)$*. In particular, if* R *is finite then* $|M| \geq |R/\operatorname{ann}(M)|$*, with equality if and only if* M *is cyclic.*

Proof **Part 1** is obvious, and **parts 2–5** are its immediate consequences.

In the sequel we write $\mathcal{I}(\alpha)$ for $\mathcal{I}(\{\alpha\})$. For $\beta \in \mathrm{A}$ denote by $\mathbf{1}_\beta$ the element $(x_\alpha)_{\alpha\in\mathrm{A}} \in R$ such that $x_\beta = 1$ and $x_\alpha = 0$ for $\alpha \neq \beta$. For any $x \in R \setminus \mathcal{I}(\beta)$ there exists $y \in R$ such that $yx = \mathbf{1}_\beta$.

After this preparation we are ready to prove **part 6**. Let $\mathrm{B} \subseteq \mathrm{A}$ be such that $\operatorname{ann}(M) = \mathcal{I}(\mathrm{B})$. I claim that for any $\beta \in \mathrm{B}$ there exists $b_\beta \in M$ such that $\operatorname{ann}(b_\beta) \subseteq \mathcal{I}(\beta)$. Indeed, assume that for any $b \in M$ there exists $x \in R \setminus \mathcal{I}(\beta)$ such that $xb = 0$. Then, as follows from the previous paragraph, $\mathbf{1}_\beta b = 0$ for any $b \in M$, which is a contradiction because $\mathbf{1}_\beta \notin \operatorname{ann}(M)$.

Now put $a = \sum_{\beta\in\mathrm{B}} \mathbf{1}_\beta b_\beta$. If $x = (x_\alpha)_{\alpha\in\mathrm{A}} \in \operatorname{ann}(a)$, then for any $\beta \in \mathrm{B}$ one has $0 = \mathbf{1}_\beta x a = \mathbf{1}_\beta x b_\beta$. Hence $\mathbf{1}_\beta x \in \mathcal{I}(\beta)$ by the choice of b_β, or, in other words, $x_\beta = 0$.

Thus, $x_\beta = 0$ for any $\beta \in \mathrm{B}$. Hence $x \in \mathcal{I}(\mathrm{B})$, which proves part 6. □

5.2. **Group rings**

Let A be a commutative ring and G a finite abelian group. Consider the group ring $A[G]$. Define the *weight* of $\Theta = \sum_{g\in G} n_g g \in A[G]$ by $w(\Theta) = \sum_{g\in G} n_g \in A$. The weight function is additive and multiplicative, defining thereby a ring homomorphism $A[G] \xrightarrow{w} A$. The kernel of this homomorphism is called *the augmentation ideal* of the group ring $A[G]$. It is generated over A by the elements of the form $\sigma - \tau$, where $\sigma, \tau \in G$.

The following proposition is true for any finite abelian groups, but we formulate it only for cyclic groups, which is sufficient for our purposes.

Proposition 5.2.1. — *Let* G *be a finite cyclic group of order* n*. Then we have the following.*

(1) *Let* K *be a field of characteristic not dividing* n*. Then the group ring* $K[G]$ *is a direct product of finitely many fields.*

(2) *An ideal of the ring* $\mathbb{Z}[G]$ *containing a prime number not dividing* n *is a radical ideal of* $\mathbb{Z}[G]$.

Proof **Part 1** follows by observing that $K[G] = K[x]/(x^n - 1)$. Since the characteristic does not divide n, the polynomial $x^n - 1$ is separable over K, which means that $K[x]/(x^n - 1)$ is a direct product of several finite extensions of K.

To prove **part 2**, let $\mathfrak{a}$ be an ideal of $\mathbb{Z}[G]$ containing a prime number q not dividing n. Then $Z[G]/\mathfrak{a} = \mathbb{F}_q[G]/\mathfrak{a}'$, where $\mathbb{F}_q$ is the field of q elements and $\mathfrak{a}'$ is the image of $\mathfrak{a}$ in $\mathbb{F}_q[G]$. Part 1 implies that $\mathbb{F}_q[G]$ is a direct product of fields, and hence so is $\mathbb{F}_q[G]/\mathfrak{a}'$ (see Proposition 5.1.3:1). Thus, $Z[G]/\mathfrak{a}$ has no non-zero nilpotents, as wanted. □

5.3. **Miscellaneous**

PROPOSITION 5.3.1. — *Let R be a ring and q a prime number such that the principal ideal (q) is radical. (In particular, the assumption is satisfied if K is a number field, q a prime number unramified in K and $R = S^{-1}\mathcal{O}_K$, where $S \subset \mathcal{O}_K$ consists of elements co-prime with q.) Let $\alpha, \beta \in R$ satisfy $\alpha^q \equiv \beta^q \bmod q$. Then $\alpha^q \equiv \beta^q \bmod q^2$.*

Proof We have $(\alpha - \beta)^q \equiv \alpha^q - \beta^q \equiv 0 \bmod q$. Since (q) is radical, this implies $\alpha \equiv \beta \bmod q$, which, in turn, yields $\alpha^q \equiv \beta^q \bmod q^2$. □

PROPOSITION 5.3.2. — *Let R be an integral domain and K its quotient field. Let*

$$\sum_{k=0}^{\infty} \frac{a_k}{k!} T^k, \quad \sum_{k=0}^{\infty} \frac{b_k}{k!} T^k \in K[[T]]$$

be formal power series with the following properties:

$$a_k, b_k \in R, \qquad a_k \equiv a^k \bmod \mathfrak{a}, \quad b_k \equiv b^k \bmod \mathfrak{a} \qquad (k = 0, 1, \ldots)$$

for some $a, b \in R$ and an ideal $\mathfrak{a} \trianglelefteq R$. Then

$$\left(\sum_{k=0}^{\infty} \frac{a_k}{k!} T^k\right)\left(\sum_{k=0}^{\infty} \frac{b_k}{k!} T^k\right) = \sum_{k=0}^{\infty} \frac{c_k}{k!} T^k$$

with $c_k \in R$ satisfying $c_k \equiv (a + b)^k \bmod \mathfrak{a}$.

Proof We have $c_k = \sum_{i=0}^{k} \binom{k}{i} a_i b_{k-i} \equiv \sum_{i=0}^{k} \binom{k}{i} a^i b^{k-i} = (a + b)^k$, as wanted. □

PROPOSITION 5.3.3. — *Let m be a non-negative integer and α a rational number with denominator b. Then for a sufficiently large positive integer N one has $b^N \binom{\alpha}{m} \in \mathbb{Z}$.*

Proof Write $\alpha = a/b$. For any prime number p not dividing b we have

$$\operatorname{ord}_p\big(a(a-b)\cdots(a-(m-1)b)\big) \geq \lfloor m/p \rfloor + \lfloor m/p^2 \rfloor + \cdots = \operatorname{ord}_p(m!),$$

whence the result. □

6. **OVERVIEW OF THE PROOF**

In this section I give a general overview of the proof of Theorem 1.3 and show how it reduces to three more technical statements.

6.1. **Three steps**

The structure of the proof of Theorem 1.3 resembles that of the proof of the statement $q^2|x$ in Theorem 3.2. Recall that the latter argument consisted of three steps.

(1) Find "many" $\Theta \in \mathbb{Z}[G]$ such that $(x-\zeta)^\Theta$ is a q-th power.
(2) Show that $(x-\zeta)^\Theta$ is a q-th power only if either $q|\Theta$ or $q^2|x$.
(3) Show that not all Θ from step (1) are divisible by q.

The proof of Theorem 1.3 has steps (1) and (3), but step (2) has to be replaced by the following much more difficult task:

(2*) Show that $(x-\zeta)^\Theta$ is a q-th power only if $q|\Theta$.

Unfortunately, we are able to verify step (2*) only if Θ is even, that is, $(1+\iota)|\Theta$, where $\iota \in G$ is the complex conjugation. This creates several serious problems.

First of all, there are too few even elements in the Stickelberger ideal (see [34, Example (a) after Theorem 6.10]). Hence we cannot use Stickelberger's theorem anymore, and have to find a substitute. Fortunately, such a substitute is available: it is the famous theorem of Thaine [31], who gave a (partial) analogue of Stickelberger's theorem for real abelian fields.

Second, now we have $\Theta = (1+\iota)\Theta'$ rather than $\Theta = (1-\iota)\Theta'$. Hence instead of $\big((1-\bar\zeta)/(1-\zeta)\big)^{\Theta'}(\eta/\bar\eta)$, as in (10), which is a root of unity, we have $\big((1-\bar\zeta)(1-\zeta)\big)^{\Theta'}\eta\bar\eta$, which is usually not a root of unity and *a priori* has no reasons to be a q-th power.

In Subsection 6.3 we reduce Theorem 2 to three statements, corresponding to steps (1), (2*) and (3) above. But before, we need some preparations. It will be more convenient to work $\bmod q$. In the next subsection we introduce certain modules over the ring $\mathbb{F}_q[G]$ which will play vital role in the sequel.

6.2. **The ring $R = \mathbb{F}_q[G]$ and some R-modules**

In this subsection p and q are distinct odd prime numbers satisfying

$$p \not\equiv 1 \bmod q. \tag{29}$$

As usual, ζ is a primitive p-th root of unity, $K = \mathbb{Q}(\zeta)$ and $G = \mathrm{Gal}(K/\mathbb{Q})$.

Consider the group ring $R = \mathbb{F}_q[G]$. Relation (29) and Proposition 5.2.1:1 imply that R is a direct product of fields, and, in particular, **Proposition 5.1.3 applies to this ring**. This will be repeatedly used in the sequel.

By Proposition 5.1.3, for any ideal $\mathcal{I} \trianglelefteq R$ there is a uniquely defined $\mathcal{I}^\perp \trianglelefteq R$ such that $\mathcal{I}+\mathcal{I}^\perp = R$ and $\mathcal{I}\mathcal{I}^\perp = 0$. For instance, $(1+\iota)^\perp = (1-\iota)$, where $\iota \in G$ is the complex conjugation, and $(\mathcal{N})^\perp$ is the augmentation ideal (see Subsection 5.2), where

$$\mathcal{N} = \sum_{\sigma\in G} \sigma \in R$$

is the "norm" element.

PROPOSITION 6.2.1. — *Let E be the group of units of K. Then E/E^q is a cyclic R-module, and, in the notation of Subsection 5.1, we have*

$$\operatorname{ann}(E/E^q) = (\mathcal{N}, 1-\iota). \tag{30}$$

Proof Let Ω the group of roots of unity from K and put $\bar{E} = E/\Omega$. Since the roots of unity in K are q-th powers, E/E^q is G-isomorphic to $\bar{E}/\bar{E}^q$.

In every pair of complex conjugate elements of G pick a representative. Denote by $\widetilde{\mathcal{N}}'$ the sum of chosen representatives in $\mathbb{Z}[G]$ and by $\mathcal{N}'$ its image in $R = \mathbb{F}_q[G]$, so that $\mathcal{N} = \mathcal{N}'(1+\iota)$. Then the annihilator of the $\mathbb{Z}[G]$-module $\bar{E}$ is $(\widetilde{\mathcal{N}}', 1-\iota)$. Proposition 5.2.1:2 implies that $(\widetilde{\mathcal{N}}', 1-\iota, q)$ is a radical ideal of $\mathbb{Z}[G]$, and Proposition 5.1.2 implies that $\operatorname{ann}_{\mathbb{F}_q[G]}\left(\bar{E}/\bar{E}^q\right) = (\mathcal{N}', 1-\iota)$. Since

$$\mathcal{N}' = \frac{1}{2}\left(\mathcal{N} + (1-\iota)\mathcal{N}'\right) \in (\mathcal{N}, 1-\iota),$$

we have $(\mathcal{N}', 1-\iota) = (\mathcal{N}, 1-\iota)$, which proves (30).

Further, since $1-\iota$ belongs to the augmentation ideal $(\mathcal{N})^{\perp}$, we have $\mathcal{N} \cap (1-\iota) = \mathcal{N}(1-\iota) = (0)$, which implies that

$$|(\mathcal{N}, 1-\iota)| = |(\mathcal{N})| \cdot |(1-\iota)| = q \cdot q^{(p-1)/2} = q^{(p+1)/2}.$$

We obtain $|R/(\mathcal{N}, 1-\iota)| = q^{(p-3)/2} = \left|\bar{E}/\bar{E}^q\right|$, and the R-module $\bar{E}/\bar{E}^q$ is cyclic by Proposition 5.1.3:6. □

DEFINITION 6.1. — We say that $\beta \in \mathcal{O}_K$ is *q-primary* if there exists $\gamma \in \mathcal{O}_K$ such that $\beta \equiv \gamma^q \bmod q^2$.

Denote by C and C_q the groups of cyclotomic units and of q-primary cyclotomic units of K, respectively. Recall C is, by definition, the group generated by $-\zeta$ and units of the form $(1-\zeta^k)/(1-\zeta)$. It is a full rank subgroup of E.

The R-modules E/CE^q, C/C_q and $C_q/(C_q \cap E^q)$ and there annihilators play central role in Mihăilescu's work. Since $C/C_q \cong CE^q/C_qE^q$ and $C_q/(C_q \cap E^q) \cong C_qE^q/E^q$, all three are cyclic R-modules by Proposition 5.1.1. Moreover, Proposition 5.1.3:5 and equality (30) imply the following.

PROPOSITION 6.2.2. — *The three ideals*

$$\mathcal{I}_1 = \operatorname{ann}(E/CE^q), \quad \mathcal{I}_2 = \operatorname{ann}(C/C_q), \quad \mathcal{I}_3 = \operatorname{ann}(C_q/(C_q \cap E^q) \tag{31}$$

are pairwise coprime and satisfy

$$\mathcal{I}_1\mathcal{I}_2\mathcal{I}_3 = (\mathcal{N}, 1-\iota). \tag{32}$$

□

6.3. **The three main theorems**

In this subsection we reduce Theorem 1.3 to three statements, corresponding to steps (1), (2*) and (3) from Subsection 6.1. We use the notation of Subsection 6.2.

REMARK 6.3.1. — In the sequel, for $\gamma \in K^*$ and $\Theta \in R$ we define γ^Θ as $\gamma^{\widetilde{\Theta}}$, where $\widetilde{\Theta}$ is a lifting of Θ to $\mathbb{Z}[G]$. Of course, γ^Θ is well-defined only up to multiplication by a q-th power. This, however, will never be confusing, since any statement involving terms like γ^Θ will include the q-th power of an (unspecified) element of K^*.

In the first two theorems, x, y, p, q is a solution of the Catalan equation (2). In particular, (29) is satisfied, as follows from Theorem 4.1.

THEOREM 6.3.2. — *For any $\Theta \in (\mathcal{N})^\perp(1+\iota)\mathcal{I}_1\mathcal{I}_3$ we have $(x-\zeta)^\Theta \in (K^*)^q$.*

THEOREM 6.3.3. — *Assume that $q \geq 7$. If for $\Theta \in (\mathcal{N})^\perp(1+\iota)$ we have $(x-\zeta)^\Theta \in (K^*)^q$, then $\Theta = 0$.*

The third theorem is a general fact, independent of Catalan's condition; in fact, even (29) is not required.

THEOREM 6.3.4. — *If $p > q$ then $C_q \neq C$.*

Proof of Theorem 1.3 (assuming Theorems 6.3.2, 6.3.3 and 6.3.4) Let (x, y, p, q) be a solution. Replacing it, if necessary, by $(-y, -x, q, p)$, we may assume that $p > q$. We may also assume that $q \geq 7$ by (26). Thus, the assumptions of Theorems 6.3.2–6.3.4 are verified.

Theorems 6.3.2 and 6.3.3 imply that $(1+\iota)(\mathcal{N})^\perp\mathcal{I}_1\mathcal{I}_3 = (0)$, which, by Proposition 5.1.3:4 and (32), implies that

$$\mathcal{I}_1\mathcal{I}_3 \subseteq \big((1+\iota)(\mathcal{N})^\perp\big)^\perp = (1+\iota)^\perp + (\mathcal{N}) = (1-\iota) + (\mathcal{N}) = \mathcal{I}_1\mathcal{I}_2\mathcal{I}_3.$$

On the other hand $\mathcal{I}_2$ and $\mathcal{I}_1\mathcal{I}_3$ are co-prime by Proposition 6.2.2. Hence

$$1 \in \mathcal{I}_2 + \mathcal{I}_1\mathcal{I}_3 \subseteq \mathcal{I}_2 + \mathcal{I}_1\mathcal{I}_2\mathcal{I}_3 = \mathcal{I}_2,$$

that is, $\mathcal{I}_2 = (1)$. Since $\mathcal{I}_2 = \mathrm{ann}(C/C_q)$, this means that $C = C_q$, contradicting Theorem 6.3.4. □

Theorems 6.3.2, 6.3.3 and 6.3.4 are proved in the next three sections. Theorem 6.3.2 is purely algebraic and relies on the already mentioned result of Thaine about cyclotomic fields. The proof of Theorem 6.3.3 is a beautiful Runge-type diophantine argument, while that of Theorem 6.3.4 is short and elementary.

7. PROOF OF THEOREM 6.3.2

Thus, let (x, y, p, q) be a solution of Catalan's equation (2). Theorem 4.1 implies that $p \not\equiv 1 \bmod q$. In particular, Proposition 5.1.3 applies to the group ring $R = \mathbb{F}_q[G]$, to be repeatedly used in the sequel.

Let H be the class group of the number field $K = \mathbb{Q}(\zeta)$ and H^+ the "plus-part" of H (it consists of the classes stable with respect to the complex conjugation). Recall that $\Theta \in \mathbb{Z}[G]$ is called *even* if it is divisible by $1 + \iota$. The following is a particular case of [34, Theorem 15.2].

THEOREM 7.1 (Thaine). — *Let an even $\Theta \in \mathbb{Z}[G]$ annihilate the q-part of the group E/C. Then Θ annihilates the q-part of H^+ as well.*

(By the *q-part* we mean the q-Sylow subgroup.)

REMARK 7.2. — Thaine's result is more general. Let L be a real abelian field, and denote by E_L, C_L, H_L and G_L, the groups of units, of cyclotomic units, the class group and the Galois group of L, respectively. Let q be an odd prime number not dividing $[L\colon \mathbb{Q}]$. Then any $\Theta \in \mathbb{Z}[G_L]$, annihilating the q-part of the group E_L/C_L, annihilates the q-part of H_L as well. For $q = 2$ a slightly weaker statement holds.

In our case $L = \mathbb{Q}(\zeta + \bar{\zeta})$ and the condition "q does not divide $[L\colon \mathbb{Q}]$" is ensured by $p \not\equiv 1 \bmod q$.

We shall use the following consequence of Theorem 7.1.

PROPOSITION 7.3. — *Any $\Theta \in (1 + \iota)\mathcal{I}_1$ has a lifting $\widetilde{\Theta} \in \mathbb{Z}[G]$ annihilating the q-part of H.*

Proof Let q^m be the order of the q-part of E/C. By Proposition 5.1.3:2, there exist $\Theta_1, \dots, \Theta_m \in \mathcal{I}_1$ such that $\Theta = (1 + \iota)^2\Theta_1 \cdots \Theta_m$. Pick liftings $\widetilde{\Theta}_1, \dots, \widetilde{\Theta}_m$ for $\Theta_1, \dots, \Theta_m$, respectively, and put $\widetilde{\Theta}' = (1 + \iota)\widetilde{\Theta}_1 \cdots \widetilde{\Theta}_m$ and $\widetilde{\Theta} = (1 + \iota)\widetilde{\Theta}'$. Since every Θ_i annihilates E/CE^q, we have $E^{\widetilde{\Theta}_i} \subseteq CE^q$, which implies $E^{\widetilde{\Theta}'} \subseteq CE^{q^m}$. By the definition of m this means that $\widetilde{\Theta}'$ annihilates the q-part of E/C. By Thaine's theorem, it annihilates the q-part of H^+ as well. Since $H^{1+\iota} \subseteq H^+$, the q-part of H is annihilated by $\widetilde{\Theta} = (1 + \iota)\widetilde{\Theta}'$. □

PROPOSITION 7.4. — *For any $\Theta \in (1 + \iota)(\mathcal{N})^\perp\mathcal{I}_1$ we have $(x - \zeta)^\Theta \in E(K^*)^q$.*

Proof Put $\lambda = (x - \zeta)/(1 - \zeta)$. By Corollary 2.2, there exists an ideal $\mathfrak{a}$ of K such that $(\lambda) = \mathfrak{a}^q$. The class of the ideal $\mathfrak{a}$ belongs to the q-part of the class group of K. Since the statement of the proposition does not depend on the choice of the lifting $\widetilde{\Theta}$ used to define (cf. Remark 6.3.1) $(x - \zeta)^\Theta$, we may select $\widetilde{\Theta}$ in the most suitable way. Thus, let $\widetilde{\Theta}$ be a lifting which annihilates the q-part of the class group, which exists by Proposition 7.3.

Then $\mathfrak{a}^{\widetilde{\Theta}}$ is a principal ideal. Thus, the principal ideal $\left(\lambda^{\Theta}\right)$ is a q-th power of another principal ideal, that is, $\lambda^{\Theta} \in E(K^*)^q$.

On the other hand, since Θ belongs to the augmentation ideal $(\mathcal{N})^{\perp}$, we have $(1-\zeta)^{\Theta} \in C(K^*)^q \subseteq E(K^*)^q$. (Indeed, the augmentation ideal is generated by the elements of the form $\sigma - \tau$, where $\sigma, \tau \in G$; and $(1-\zeta)^{\sigma-\tau}$ is a cyclotomic unit.) Thus, $(x-\zeta)^{\Theta} = \lambda^{\Theta}(1-\zeta)^{\Theta} \in E(K^*)^q$, as wanted. □

Next, we use Mihăilescu's Theorem 3.2 to refine Proposition 7.4. Recall that C_q stands for the group of q-primary cyclotomic units.

PROPOSITION 7.5. — *For any $\Theta \in (1+\iota)(\mathcal{N})^{\perp}\mathcal{I}_1$ we have $(x-\zeta)^{\Theta} \in C_q(K^*)^q$.*

Proof By Proposition 5.1.3:2 we have $\Theta = \Theta_1\Theta_2$ with $\Theta_1 \in (1+\iota)(\mathcal{N})^{\perp}\mathcal{I}_1$ and $\Theta_2 \in \mathcal{I}_1$. Proposition 7.4 implies that $(x-\zeta)^{\Theta_1} \in E(K^*)^q$. Since $\Theta_2 \in \mathcal{I}_1 = \mathrm{ann}(E/CE^q)$, we have

$$(x-\zeta)^{\Theta} = (x-\zeta)^{\Theta_1\Theta_2} \in E^{\Theta_2}(K^*)^q \subseteq C(K^*)^q.$$

Write $(x-\zeta)^{\Theta} = \eta\alpha^q$ with $\eta \in C$ and $\alpha \in K^*$. Since $q^2|x$ by Theorem 3.2, we have $\eta\alpha^q \equiv (-\zeta)^{\Theta} \bmod q^2$. Since $-\zeta$ is a q-th power, η is q-primary, and the proposition follows. □

We are ready to prove Theorem 6.3.2. Let $\Theta \in (1+\iota)(\mathcal{N})^{\perp}\mathcal{I}_1\mathcal{I}_3$. By Proposition 5.1.3:2 we have $\Theta = \Theta_1\Theta_2$ with $\Theta_1 \in (1+\iota)(\mathcal{N})^{\perp}\mathcal{I}_1$ and $\Theta_2 \in \mathcal{I}_3 = \mathrm{ann}\,(C_q/(C_q \cap E^q))$. Now

$$(x-\zeta)^{\Theta} = (x-\zeta)^{\Theta_1\Theta_2} \in C_q^{\Theta_2}(K^*)^q \subseteq (K^*)^q.$$

Theorem 6.3.2 is proved. □

8. PROOF OF THEOREM 6.3.3

8.1. A reformulation

In the proof of Theorem 6.3.3 it is more practical to work in the ring $\mathbb{Z}[G]$ rather than $\mathbb{F}_q[G]$. Thus, we have to find a suitable lifting of $\Theta \in \mathbb{F}_q[G]$ to $\mathbb{Z}[G]$. Since $(x-\zeta)^{\Theta}$ is a q-th power if and only if $(x-\zeta)^{-\Theta}$ is, we may choose between lifting Θ or $-\Theta$.

Recall that an element Θ of $\mathbb{F}_q[G]$ or $\mathbb{Z}[G]$ is *even* if it is divisible by $1+\iota$. Equivalently, $\Theta = \sum_{\sigma\in G} n_\sigma\sigma$ is even if for any $\sigma \in G$ we have $n_\sigma = n_{\bar\sigma}$, where $\bar\sigma = \iota\sigma$ is the complex conjugate of σ.

We say that $\Theta = \sum_{\sigma\in G} n_\sigma\sigma \in \mathbb{Z}[G]$ is *non-negative* if $n_\sigma \geq 0$ for any $\sigma \in G$. We say that $\Theta \in \mathbb{Z}[G]$ is *positive* if it is non-negative and distinct from 0.

PROPOSITION 8.1.1. — *Let $\Theta \in \mathbb{F}_q[G]$. Then either Θ or $-\Theta$ has a non-negative lifting $\widetilde{\Theta} \in \mathbb{Z}[G]$ such that $w(\widetilde{\Theta}) \leq q(p-1)/2$. If Θ belongs to the augmentation ideal of $\mathbb{F}_q[G]$ then $q|w(\widetilde{\Theta})$. If Θ is even then so is $\widetilde{\Theta}$.*

Proof Let $\widetilde{\Theta}_1$ be the smallest non-negative lifting of Θ. That is, $\widetilde{\Theta}_1 = \sum_{\sigma\in G} \widetilde{n}_\sigma \sigma$ with $\widetilde{n}_\sigma \in \{0, 1, \dots, q-1\}$. Further, put $\widetilde{\Theta}_2 = q\sum_{\sigma\in G}\sigma - \widetilde{\Theta}_1$, so that $\widetilde{\Theta}_2$ is a non-negative lifting of $-\Theta$. Obviously, both $\widetilde{\Theta}_1$ and $\widetilde{\Theta}_2$ are even if Θ is, and both the weights $w(\widetilde{\Theta}_1)$ and $w(\widetilde{\Theta}_2)$ are divisible by q if Θ is belongs to the augmentation ideal.

Since $w(\widetilde{\Theta}_1) + w(\widetilde{\Theta}_2) = q(p-1)$, one of the weights $w(\widetilde{\Theta}_1)$ and $w(\widetilde{\Theta}_2)$ does not exceed $q(p-1)/2$. The proposition is proved. □

By this proposition, Theorems 6.3.3 is equivalent to the following statement.

Theorem 6.3.3′. *Let x, y, p, q be a solution of the Catalan equation with $q \geq 7$. Let Θ be an even positive element of $\mathbb{Z}[G]$ satisfying $q|w(\Theta)$ and $w(\Theta) \leq q(p-1)/2$. Assume that $(x-\zeta)^\Theta$ is a q-th power in K. Then $q|\Theta$.*

This theorem will be proved in Subsection 8.3, after some preparations in Subsection 8.2.

8.2. **The power series** $(1-\zeta T)^{\Theta/q}$

In this section we investigate the properties of a special power series introduced by Mihăilescu. Everywhere below capital T stands for an independent variable, while small letters t, z etc. denote complex numbers. For instance, $(1+T)^r$ denotes the binomial series $\sum_{k=0}^\infty \binom{r}{k} T^k$, while, for $|t| < 1$, the expression $(1+t)^r$ is the complex number, equal to the sum of the binomial series at $T = t$. In particular, $(1+t)^r$ is a positive real number if $r \in \mathbb{R}$ and $t \in (-1, 1)$.

Fix a $\Theta = \sum_{\sigma\in G} n_\sigma \sigma \in \mathbb{Z}[G]$. The series we are interested in is

$$(1-\zeta T)^{\Theta/q} = \prod_{\sigma\in G} (1-\zeta^\sigma T)^{n_\sigma/q}. \tag{33}$$

Its convergence radius is 1. Let us estimate its remainder term. Write

$$(1-\zeta T)^{\Theta/q} = \sum_{k=0}^\infty \alpha_k(\Theta) T^k, \tag{34}$$

and denote by $S_m(T) = \sum_{k=0}^m \alpha_k(\Theta) T^k$ the m-th partial sum.

Proposition 8.2.1. — *Let $\Theta \in \mathbb{Z}[G]$ be non-negative. Then for $|z| < 1$ one has*

$$\left|(1-\zeta z)^{\Theta/q} - S_m(z)\right| \leq \binom{w(\Theta)/q + m}{m+1} (1-|z|)^{-w(\Theta)/q - m - 1} |z|^{m+1}. \tag{35}$$

Proof A power series $\sum_{k=0}^\infty a_k T^k$ with complex coefficients is *dominated* by the series $\sum_{k=0}^\infty b_k T^k$ with non-negative real coefficients if $|a_k| \leq b_k$ for $k = 0, 1, \dots$. The relation of dominance is preserved by addition and multiplication of power series.

Let $r > 0$ be a positive real number, and χ a complex number satisfying $|\chi| \leq 1$. Then the binomial series $(1+\chi T)^r = \sum_{k=0}^\infty \binom{r}{k} \chi^k T^k$ is dominated by $(1-T)^{-r} = \sum_{k=0}^\infty (-1)^k \binom{-r}{k} T^k$. Indeed, the coefficients of the latter series are positive and $\left|\binom{r}{k}\right| \leq \left|\binom{-r}{k}\right|$.

It follows that $(1-\zeta T)^{\Theta/q}$ is dominated by $(1-T)^{-\nu}$, where $\nu = w(\Theta)/q$. Denoting by $\bar{S}_m(T)$ the m-th partial sum of the series $(1-T)^{-\nu}$, we obtain the following:

$$\begin{aligned}\left|(1-\zeta z)^{\Theta/q} - S_m(z)\right| &\le \left|(1-|z|)^{-\nu} - \bar{S}_m(|z|)\right| \\ &\le \sup_{0\le\xi\le|z|}\left|\left(\frac{d^{m+1}(1-T)^{-\nu}}{dT^{m+1}}\Big|_{T=\xi}\right)\right| \frac{|z|^{m+1}}{(m+1)!} \\ &= \binom{\nu+m}{m+1}(1-|z|)^{-\nu-m-1}|z|^{m+1},\end{aligned}$$

as wanted. □

Next, we investigate the arithmetic of the coefficients of Mihăilescu's series. Say that $\alpha \in K$ is a *q-integer* if $q^N\alpha \in \mathbb{Z}[\zeta]$ for a sufficiently large positive integer N.

Proposition 8.2.2. — *The coefficients $\alpha_0(\Theta), \alpha_1(\Theta), \ldots$ of Mihăilescu's series $(1-\zeta T)^{\Theta/q}$ are q-integers. Write*

$$(1-\zeta T)^{\Theta/q} = \sum_{k=0}^{\infty} \frac{a_k(\Theta)}{q^k k!} T^k, \tag{36}$$

(so that $\alpha_k(\Theta) = a_k(\Theta)/q^k k!$). Then

$$a_k(\Theta) \in \mathbb{Z}(\zeta) \quad \text{and} \quad a_k(\Theta) \equiv \left(-\sum_{\sigma\in G} n_\sigma \zeta^\sigma\right)^k \bmod q \qquad (k = 0, 1, \ldots). \tag{37}$$

Proof As follows from Proposition 5.3.3, for every $n \in \mathbb{Z}$ the coefficients of the series $(1-\zeta T)^{n/q}$ are q-integers. Hence so are the coefficients of $(1-\zeta T)^{\Theta/q}$.

Further, $(1-\zeta q T)^{n/q} = \sum_{k=0}^{\infty}(b_k/k!)T^k$ with

$$b_k = n(n-q)\cdots(n-(k-1)q)(-\zeta)^k \equiv (-n\zeta)^k \bmod q.$$

Now, applying Proposition 5.3.2 to the equality

$$\sum_{k=0}^{\infty} \frac{a_k(\Theta)}{k!} T^k = \prod_{\sigma\in G} (1-\zeta^\sigma q T)^{n_\sigma/q},$$

we obtain (37). □

We arrived to the most delicate part of Mihăilescu's argument. The G-action extends to the ring of power series $K[T]$ by $\left(\sum_{k=0}^{\infty} a_k T^k\right)^\sigma = \sum_{k=0}^{\infty} a_k^\sigma T^k$, and we have the "compatibility relation"

$$\left((1-\zeta T)^{\Theta/q}\right)^\sigma = (1-\zeta T)^{\sigma\Theta/q}. \tag{38}$$

However, since the Galois action is not continuous in the complex topology, this relation **does not**, in general, extend to the *values* of power series, even if the convergence is

ensured. For instance, if $t \in \mathbb{Q}$ satisfies $|t| < 1$ then we need not have

$$\left((1-\zeta t)^{\Theta/q}\right)^{\sigma} = (1-\zeta t)^{\sigma\Theta/q}. \tag{39}$$

In fact, the left-hand side is even not well-defined, because $(1-\zeta t)^{\Theta/q}$ need not belong to the field K.

Nevertheless, under some additional assumptions (39) may hold.

PROPOSITION 8.2.3. — *Assume that Θ is even. Let $t \in \mathbb{Q}$ satisfy $|t| < 1$, and assume that $(1-\zeta t)^{\Theta/q} \in K$. Then (39) is true for any $\sigma \in G$.*

Proof Since Θ is even, the series $(1-\zeta T)^{\Theta/q}$ has real coefficients. It follows that

$$\alpha := (1-\zeta t)^{\Theta/q} \in \mathbb{R}.$$

Thus, α belongs to the real cyclotomic field $\mathbb{Q}(\zeta+\bar{\zeta})$, which implies that $\alpha^{\sigma} \in \mathbb{R}$ for any $\sigma \in G$.

Now fix $\sigma \in G$. Then $\sigma\Theta$ is also even, which implies that $\beta := (1-\zeta t)^{\sigma\Theta/q} \in \mathbb{R}$ as well.

On the other hand, $(\alpha^{\sigma})^q = (\alpha^q)^{\sigma} = \left((1-\zeta t)^{\Theta}\right)^{\sigma} = (1-\zeta t)^{\sigma\Theta}$. Hence α^{σ} is equal to the real q-th root of $(1-\zeta t)^{\sigma\Theta}$, which is β. The proposition is proved. □

8.3. **Proof of Theorem 6.3.3′**

8.3.1. *The number $(1-\zeta/x)^{\Theta/q}$.* By the assumption, $(x-\zeta)^{\Theta}$ has a q-th root in the field K. Moreover, it has exactly one q-th root in K, because this field does not contain q-th roots of unity (other than 1).

Since Θ is even, $(x-\zeta)^{\Theta}$ is a positive real number. It follows that the real q-th root of $(x-\zeta)^{\Theta}$ belongs to K. This real root is equal to $|x|^{w(\Theta)/q}\,(1-\zeta/x)^{\Theta/q}$, where $(1-\zeta/x)^{\Theta/q}$ is defined as the sum of Mihăilescu series

$$(1-\zeta T)^{\Theta/q} = \sum_{k=0}^{\infty} \alpha_k(\Theta) T^k \tag{40}$$

at $T = 1/x$.

So far, everything was true for any even Θ. Now recall the assumption $q|w(\Theta)$, that is, $w(\Theta) = mq$ with $m \in 2\mathbb{Z}$. We have just proved that $x^m\,(1-\zeta/x)^{\Theta/q} \in K$. Hence $(1-\zeta/x)^{\Theta/q} \in K$, and proposition 8.2.3 implies that

$$\left((1-\zeta/x)^{\Theta/q}\right)^{\sigma} = (1-\zeta/x)^{\sigma\Theta/q} \qquad (\sigma \in G). \tag{41}$$

8.3.2. *The polynomial $P(T)$.* For $k = 1, 2, \ldots$ put $E(k) = k + \mathrm{ord}_q(k!)$. Then

$$E(k+1) \geq E(k) + 1, \tag{42}$$

$$E(k) \leq kq/(q-1). \tag{43}$$

Since Θ is positive, we have $m > 0$. Consider the polynomial

$$P(T) = q^{E(m)}\left(\alpha_0(\Theta)T^m + \alpha_1(\Theta)T^{m-1} + \cdots + \alpha_m(\Theta)\right), \tag{44}$$

where $\alpha_k(\Theta)$ are the coefficients of the Mihăilescu series (40). Proposition 8.2.2 implies that $q^{E(k)}\alpha_k(\Theta) \in \mathbb{Z}[\zeta]$. It follows that $P(T) \in \mathbb{Z}[\zeta][T]$, and (42) implies that

$$P(T) \in q^{E(m)}\alpha_m(\Theta) + q\mathbb{Z}[\zeta][T]. \tag{45}$$

Also, (38) implies that for $\sigma \in G$

$$P^\sigma(T) = q^{E(m)}\left(\alpha_0(\sigma\Theta)T^m + \alpha_1(\sigma\Theta)T^{m-1} + \cdots + \alpha_m(\sigma\Theta)\right). \tag{46}$$

8.3.3. *The number β and its conjugates.* Since Θ is non-negative, the number $(x-\zeta)^\Theta$ is an algebraic integer. Therefore its q-th root $x^m\,(1-\zeta/x)^{\Theta/q}$ is an algebraic integer as well. Hence so is

$$\beta := q^{E(m)}x^m\,(1-\zeta/x)^{\Theta/q} - P(x).$$

Relations (41) and (46) imply that

$$\beta^\sigma = q^{E(m)}x^m\left((1-\zeta/x)^{\sigma\Theta/q} - \sum_{k=0}^{m}\alpha_k(\sigma\Theta)x^{-k}\right) \qquad (\sigma \in G). \tag{47}$$

Now estimate $|\beta^\sigma|$ using Proposition 8.2.1 (with $\sigma\Theta$ instead of Θ). We obtain

$$|\beta^\sigma| \le q^{E(m)}\binom{2m}{m+1}\left(1-|x|^{-1}\right)^{-2m-1}|x|^{-1} = A|x|^{-1}. \tag{48}$$

Now recall that $|x| \ge q^{p-1}$ by Corollary 2.4, and, in particular, $|x| \ge 49$ because $q \ge 7$. Using (43), estimating $\binom{2m}{m+1} \le 2^{2m}$ and using that $|x| \ge 49$, we obtain $A < q^{mq/(q-1)}2.05^{2m}$.

Further, the assumption $w(\Theta) \le q(p-1)/2$ implies that $m \le (p-1)/2$, and we obtain $A < \left(2.05q^{7/12}\right)^{p-1} < q^{p-1}$ (we again use the assumption $q \ge 7$). Thus, $A < |x|$, which implies that $|\beta^\sigma| < 1$ for all $\sigma \in G$. Since β is an algebraic integer, this is only possible if $\beta = 0$.

8.3.4. *Finishing the proof.* Thus, $P(x) = q^{E(m)}x^m\,(1-\zeta/x)^{\Theta/q}$. Since $x^m\,(1-\zeta/x)^{\Theta/q}$ is an algebraic integer, (45) implies that

$$q^{E(m)}\alpha_m(\Theta) \equiv 0 \bmod q.$$

By Proposition 8.2.2, this is possible only if $q|\left(\sum_{\sigma\in G} n_\sigma\zeta^\sigma\right)^m$. Since q is unramified in K, this implies that $q|\sum_{\sigma\in G} n_\sigma\zeta^\sigma$, that is, $q|n_\sigma$ for all $\sigma \in G$. Thus, $q|\Theta$, and this completes the proof of Theorem 6.3.3′.

9. **PROOF OF THEOREM 6.3.4**

To begin with, introduce the polynomial

$$f(T) = \left((1+T)^q - 1 - T^q\right)/q \in \mathbb{Z}[T]. \tag{49}$$

It is a non-zero monic polynomial of degree $q-1$.

Now assume that all cyclotomic units of K are q-primary. In particular, so is $1+\zeta^q = (1-\zeta^{2q})/(1-\zeta^q)$. Thus, there exists $\nu \in \mathbb{Z}[\zeta]$ such that $1+\zeta^q \equiv \nu^q \bmod q^2$. Then $(1+\zeta)^q \equiv 1+\zeta^q \equiv \nu^q \bmod q$. Proposition 5.3.1 implies that $(1+\zeta)^q \equiv \nu^q \bmod q^2$.

Thus, $(1+\zeta)^q \equiv 1+\zeta^q \bmod q^2$ This can be rewritten as $f(\zeta) \equiv 0 \bmod q$, where $f(T)$ is the polynomial defined in (49).

Applying the Galois conjugation, we obtain $f(\zeta^\sigma) \equiv 0 \bmod q$ for any $\sigma \in G$. Let now $\mathfrak{q}$ be a prime ideal of K dividing q. Then we have $p-1$ congruences

$$f(\zeta^\sigma) \equiv 0 \bmod \mathfrak{q} \qquad (\sigma \in G). \tag{50}$$

Since $\zeta^\sigma \not\equiv \zeta^\tau \bmod \mathfrak{q}$ for distinct $\sigma, \tau \in G$, congruences (50) imply that $p-1 \le \deg f = q-1$, which contradicts our assumption $p > q$. The theorem is proved.

REFERENCES

[1] M.F. Atiyah, I.G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, 1969.

[2] A. Baker, Linear forms in the logarithms of algebraic numbers I–IV *Mathematika* **13** (1966), 204–216; **14** (1967), 102–107; 220–224; IV, *ibid.* **15** (1968), 204–216.

[3] A. Baker, Bounds for solutions of hyperelliptic equations, *Proc. Cambridge Phil. Soc.* **65** (1969), 439–444.

[4] A. Baker, G. Wüstholz, Logarithmic forms and group varieties, *J. reine angew. Math.* **442** (1993), 19–62.

[5] C.D. Bennett, J. Blass, A.M.W. Glass, D.B. Meronk, R.P. Steiner, Linear forms in the logarithms of three positive rational numbers, *J. Th. Nombres Bordeaux* **9** (1997), 97–136.

[6] J. Blass, A.M.W. Glass, T.W. O'Neil, Catalan's conjecture and linear forms in logarithms, *Ulam Q. J.*, accepted, but never appeared in print.

[7] Y. Bugeaud G. Hanrot, Un nouveau critère pour l'équation de Catalan, *Mathematika* **47** (2000), 63–73.

[8] J. W. S. Cassels, On the equation $a^x - b^y = 1$, II, *Proc. Cambridge Society* **56** (1960), 97–103.

[9] E. Catalan, Note extraite d'une lettre adressée à l'éditeur, *J. reine angew. Math.* **27** (1844), 192.

[10] A.O. Gelfond, *Transcendent and Algebraic Numbers* (Russian), Moscow 1952; English trans.: New York, Dover, 1960.

[11] S. Hyyrö, Über das Catalan'sche Problem, *Ann. Univ. Turku Ser. AI* **79** (1964), 3–10.

[12] K. Inkeri, On Catalan's problem, *Acta Arith.* **9** (1964), 285–290.

[13] K. Inkeri, On Catalan's conjecture, *J. Number Th.* **34** (1990), 142–152.

[14] Ko Chao, On the diophantine equation $x^2 = y^n + 1$, $xy \neq 0$, *Sci. Sinica* **14** (1965), 457–460.

[15] M. Langevin, Quelques applications de nouveaux résultats de Van der Poorten, *Sém. Delange-Pisot-Poitou* **17** (1975/76), Paris, 1977.

[16] M. Laurent, M. Mignotte, Y. Nesterenko, Formes linéaires en deux logarithmes et déterminants d'interpolation, *J. Number Theory* **55** (1995), 285–321.

[17] V.A. Lebesgue, Sur l'impossibilité en nombres entiers de l'équation $x^m = y^2 + 1$, *Nouv. Ann. Math.* **9** (1850), 178–181.

[18] E. Matveev, An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers I,II (Russian), I *Izv. Ross. Akad. Nauk Ser. Mat.* **62** (1998), 81–136; **64** (2000), 125–180; English trans.: *Izv. Math.* **62** (1998), 723–772; **64** (2000), 1217–1269.

[19] T. Metsänkylä, Catalan's equation with a quadratic exponent, *C. R. Math. Acad. Sci. Soc. R. Can.* **23** (2001), 28–32.

[20] M. Mignotte, Un critère élémentaire pour l'équation de Catalan, *C. R. Math. Rep. Acad. Sci. Canada*, **15** (1993), 199–200.

[21] M. Mignotte, A criterion on Catalan's equation, *J. Number Th.* **52** (1995), , 280–284.

[22] M. Mignotte, Catalan's equation just before 2000, *Number theory (Turku, 1999)*, de Gruyter, Berlin, 2001, pp. 247–254.

[23] M. Mignotte, Y. Roy, Catalan's equation has no new solutions with either exponent less than 10651, *Experimental Math.* **4** (1995), 259–268.

[24] M. Mignotte, Y. Roy, Minorations pour l'équation de Catalan, *C. R. Acad. Sci. Paris* **324** (1997), 377–380.

[25] P. Mihăilescu, A class number free criterion for Catalan's conjecture, *J. Number Th.*, to appear.

[26] P. Mihăilescu, Primary cyclotomic units and a proof of Catalan's conjecture, submitted.

[27] T.W. O'Neil, Improved upper bounds on the exponents in Catalan's equation, a manuscript (1995).
[28] J.-C. Puchta, On a criterion for Catalan's conjecture, *Ramanujan J.* **5** (2001), 405–407.
[29] P. Ribenboim, *Catalan's Conjecture*, Acad. Press, Boston, 1994.
[30] W. Schwarz, A note on Catalan's equation, *Acta Arith.* **72** (1995), 277–279.
[31] F. Thaine, On the ideal class groups of real abelian number fields, *Ann. of Math.* **128** (1988), 1–18.
[32] R. Tijdeman, On the equation of Catalan, *Acta Arith.* **29** (1976), 197–209.
[33] M. Waldschmidt, Minorations de combinaisons linéaires de logarithmes de nombres algébriques, *Canadian J. Math.* **45** (1993), 176–224.
[34] L. Washington, *Introduction to cyclotomic fields*, second edition, Graduate Texts in Math. **83**, Springer, New York, 1997.
[35] G. Wüstholz (ed.), *A Panorama of Number Theory or The View from Bakers Garden*, Cambridge University Press 2002.

Yuri F. BILU

A2X, Université Bordeaux 1
351, cours de la Libération,
F–33405 TALENCE Cedex
E-mail : yuri@math.u-bordeaux.fr