Journal de Théorie des Nombres
de Bordeaux **17** (2005), 69–85

Catalan without logarithmic forms
(after Bugeaud, Hanrot and Mihăilescu)

par Yuri F. BILU

Résumé. C'est un rapport sur le travail récent de Bugeaud, Hanrot et Mihăilescu, montrant qu'on peut démontrer l'hypothèse de Catalan sans utiliser les formes logarithmiques, ni le calcul avec un ordinateur.

Abstract. This is an exposition of the recent work of Bugeaud, Hanrot and Mihăilescu showing that Catalan's conjecture can be proved without using logarithmic forms and electronic computations.

To Rob Tijdeman

1. Introduction

Recently, Preda Mihăilescu [15, 1] resolved the long-standing Catalan's problem.

Theorem 1.1. (Mihăilescu) *The equation $x^p - y^q = 1$ has no solutions in non-zero integers x, y and odd prime numbers p, q.*

The original question of Catalan [4] was whether the equation $x^u - y^v = 1$ has no solutions in integers $x, y, u, v > 1$ other than the obvious $3^2 - 2^3 = 1$. Lebesgue [9] and Ko Chao [7] settled the case when one of the exponents u, v is 2, which reduced the problem to Theorem 1.1.

Mihăilescu's proof of Theorem 1.1 splits into two cases, treated in totally different ways:

the first case: $p \not\equiv 1 \bmod q$ and $q \not\equiv 1 \bmod p$;
the second case: either $p \equiv 1 \bmod q$ or $q \equiv 1 \bmod p$.

The argument in the first case is algebraic and relies on the theory of cyclotomic fields. However, the second case requires difficult analytic tools (Tijdeman's argument [18], logarithmic forms [10]) and electronic computations [11, 12, 13]. See [1, Section 4] for the details.

In 1999 Bugeaud and Hanrot [2] proved that for any solution (x, y, p, q) of Catalan's equation[1] with $q > p$, the exponent q divides the relative class

[1] that is, x, y are non-zero integers and p, q are odd prime numbers such that $x^p - y^q = 1$

number of the cyclotomic field $\mathbb{Q}(e^{2\pi i/p})$. Though this result wasn't used in Mihăilescu's proof of Catalan's conjecture, it strongly inspired his work.

Recently Mihăilescu [16] discovered that the argument of Bugeaud and Hanrot [2], properly modified, implies a new proof for the second case. This new proof does not use anything but the very basic facts about cyclotomic fields, including the Stickelberger theorem. Neither does this proof depend on any electronic computations. Thus, now we have similar algebraic proofs for both cases of Catalan's problem.

In the present paper we give a detailed exposition of this new proof for the second case, that is, of the following theorem.

Theorem 1.2. *Let (x,y,p,q) be a solution*[1] *of Catalan's equation. Then $q \not\equiv 1 \bmod p$ (and $p \not\equiv 1 \bmod q$ by symmetry, because $(-y,-x,q,p)$ is a solution as well).*

What Mihăilescu actually proves is the following theorem.

Theorem 1.3. *Let (x,y,p,q) be a solution of Catalan's equation. Then $q < 3(p-1)^2$.*

Due to a clever observation of Mignotte, Theorem 1.2 is an almost immediate consequence of Theorem 1.3 and Mihăilescu's "double Wieferich" criterion (Proposition 8.3). See Section 8 for the details.

The present note also includes the original result of Bugeaud and Hanrot, see Theorem 6.1. Though it is formally obsolete now (in particular, Theorem 1.2 can, in principle, be proved without any reference to Theorem 6.1, see Remark 8), we establish all techniques needed for this beautiful result, and it would be unreasonable to miss it. As a benefit, we can quickly dispose of the small exponents (see Corollary 6.2).

Plan of the paper In Sections 2 and 3 we recall basic notation and facts concerning cyclotomic fields and heights. Section 4 is crucial: we introduce the notion of Mihăilescu ideal and prove that it has few elements of small size and zero weight. This section is formally independent of Catalan's equation. In the remaining part of the paper we apply this to solutions of Catalan's equation. In Section 6 we prove the theorem of Bugeaud and Hanrot. In Section 8 we prove Theorems 1.3 and 1.2.

Acknowledgements I am pleased to thank Radan Kučera for useful explanations about the Stickelberger ideal. I also thank Yann Bugeaud, Gabi Hecke and Tauno Metsänkylä, who detected numerous inaccuracies in the original text.

2. The cyclotomic field

Unless the contrary is stated explicitly, everywhere in this paper p and q are distinct odd prime numbers, ζ is a primitive p-th root of unity, $K = \mathbb{Q}(\zeta)$

is the corresponding cyclotomic field, and $G = \mathrm{Gal}(K/\mathbb{Q})$ is the Galois group of K. We fix, once and for all, a complex embedding $K \hookrightarrow \mathbb{C}$.

For an integer $k \not\equiv 0 \bmod p$ we denote by σ_k the automorphism of K defined by $\zeta \mapsto \zeta^k$, so that

$$G = \{\sigma_1, \ldots, \sigma_{p-1}\}.$$

We also denote by ι the complex conjugation, so that $\iota = \sigma_{p-1}$.

We define two real-valued functions on the group ring $\mathbb{Q}[G]$, the *weight* w and the *size* $\|\cdot\|$, as follows. If

$$\Theta = \sum_{\sigma} m_\sigma \sigma \in \mathbb{Q}[G], \tag{1}$$

then

$$w(\Theta) = \sum_{\sigma} m_\sigma, \qquad \|\Theta\| = \sum_{\sigma} |m_\sigma|.$$

The weight function is additive and multiplicative; the size function satisfies the inequalities

$$\|\Theta_1\Theta_2\| \leq \|\Theta_1\| \cdot \|\Theta_2\|, \qquad \|\Theta_1 + \Theta_2\| \leq \|\Theta_1\| + \|\Theta_2\|.$$

We say that Θ is non-negative (notation: $\Theta \geq 0$) if $m_\sigma \geq 0$ for all $\sigma \in G$. In this case $\|\Theta\| = w(\Theta)$.

For a given Θ as in (1) put

$$\Theta^+ = \sum_{\sigma} \max\{m_\sigma, 0\}\,\sigma, \qquad \Theta^- = -\sum_{\sigma} \min\{m_\sigma, 0\}\,\sigma.$$

Then Θ^+, Θ^- are non-negative, $\Theta = \Theta^+ - \Theta^-$ and $\|\Theta\| = \|\Theta^+\| + \|\Theta^-\|$.

Let $\mathcal{I}$ be an ideal of the ring $R = \mathbb{Z}[G]$. We define the *augmented part of* $\mathcal{I}$ and the *the minus-part of* $\mathcal{I}$ by

$$\mathcal{I}^{\mathrm{aug}} = \{\Theta \in \mathcal{I} : w(\Theta) = 0\}, \qquad \mathcal{I}^- = (1 - \iota)\mathcal{I}.$$

Notice that $\mathcal{I}^- \subseteq \mathcal{I}^{\mathrm{aug}}$. Also, given a positive real number r, we define the r-ball of $\mathcal{I}$ by

$$\mathcal{I}(r) := \{\Theta \in \mathcal{I} : \|\Theta\| \leq r\}.$$

More specific notation will be introduced at the appropriate points of the paper.

3. Heights

In this subsection we recall basic facts about heights. Let α be an algebraic number. Fix a number field K (which is not necessarily the K from Section 2) containing α, and denote by M_K the set of all (non-equivalent) valuations of K normalized to extend the standard infinite or p-adic valuations of $\mathbb{Q}$. The (absolute logarithmic) height $h(\alpha)$ is defined by

$$h(\alpha)=\frac{1}{[K\colon\mathbb{Q}]}\sum_{v\in M_K}[K_v\colon\mathbb{Q}_v]\log\max\{|\alpha|_v,1\}. \tag{2}$$

One immediately verifies that the right-hand side is independent of the choice of K, and so we have a well-defined function $h:\bar{\mathbb{Q}}\to\mathbb{R}_{\geq 0}$. The definition implies that for any $\alpha,\alpha_1,\ldots,\alpha_n\in\bar{\mathbb{Q}}$ and $m\in\mathbb{Z}$ we have

$$h(\alpha_1+\cdots+\alpha_n)\leq h(\alpha_1)+\cdots+h(\alpha_n)+\log n, \tag{3}$$

$$h(\alpha_1\cdots\alpha_n)\leq h(\alpha_1)+\cdots+h(\alpha_n), \tag{4}$$

$$h(\alpha^m)=|m|h(\alpha). \tag{5}$$

If $\alpha\in\mathbb{Z}$ then $h(\alpha)=\log|\alpha|$. If α is a root of unity then $h(\alpha)=0$.

Let K be a number field. The product formula

$$\prod_{v\in M_K}|\alpha|_v^{[K_v\colon\mathbb{Q}_v]}=1\qquad(\alpha\in K^*)$$

implies that for any $V\subset M_K$ and $\alpha\in K^*$ one has the following "Liouville inequality":

$$\prod_{v\in V}|\alpha|_v^{[K_v\colon\mathbb{Q}_v]}\geq e^{-[K\colon\mathbb{Q}]h(\alpha)}.$$

In particular, if K is a subfield of $\mathbb{C}$, then any $\alpha\in K^*$ satisfies

$$|\alpha|^f\geq e^{-[K\colon\mathbb{Q}]h(\alpha)}, \tag{6}$$

where $f=1$ if $K\subset\mathbb{R}$, and $f=2$ otherwise.

Another consequence of the product formula is the identity

$$h(\alpha/\beta)=\frac{1}{[K\colon\mathbb{Q}]}\sum_{v\in M_K}[K_v\colon\mathbb{Q}_v]\log\max\{|\alpha|_v,|\beta|_v\} \tag{7}$$

for any $\alpha\in K$ and $\beta\in K^*$.

4. The Mihăilescu ideal

As the work of Mihăilescu suggests, the basic property of a solution (x,y,p,q) of Catalan's equation is that $(x-\zeta)^\Theta$ is a q-th power in K for "many" elements Θ of the group ring $R=\mathbb{Z}[G]$. (We use the notation from Section 2.) We find it useful to axiomatize this property.

In this section p and q are fixed distinct odd prime numbers, and x is a fixed integer. *We do not assume that they come from a solution of Catalan's equation.*

Definition. The *Mihăilescu ideal* $\mathcal{I}_M$ as the set of all $\Theta\in R$ such that $(x-\zeta)^\Theta\in(K^*)^q$.

It turns out that, when $|x|$ is sufficiently large, the augmented part $\mathcal{I}_M^{\mathrm{aug}}$ contains few elements of small size. More precisely, we have the following.

Theorem 4.1. (Mihăilescu) *Let ε be a real number satisfying $0 < \varepsilon \le 1$, and assume that*

$$|x| \ge \max\left\{\left(\frac{36 \cdot 2^{p-1}}{(p-1)^2}\right)^{1/\varepsilon}, \frac{4}{\pi}\frac{q}{p-1}+1\right\}. \tag{8}$$

Put

$$r = (2-\varepsilon)\frac{q}{p-1}.$$

Then $\left|\mathcal{I}_M^{\mathrm{aug}}(r)\right| \le q$.

Theorem 4.1 implies that $|\mathcal{I}_M^{\mathrm{aug}}(2)| \le q$ when $p \le (1-\varepsilon/2)q+1$ and when (8) is satisfied. This can be refined with (8) replaced by a slightly stronger assumption.

Theorem 4.2. (Bugeaud and Hanrot) *Assume that $p \le (2-\varepsilon)q+1$ where $0 < \varepsilon \le 1$. Assume further that*

$$|x| \ge \max\left\{\left(\frac{36 \cdot 2^{p-1}}{(p-1)^2}\right)^{1/\varepsilon}, 8\left(0.8q(p')^{1/(p-1)}\right)^q\right\}, \tag{9}$$

where $p' = 1$ if $x \equiv 1 \bmod p$ and $p' = p$ otherwise. Then $\mathcal{I}_M^{\mathrm{aug}}(2) = \{0\}$.

It is useful to formulate separately the particular case of this theorem, corresponding to $\varepsilon = 1$ and $x \equiv 1 \bmod p$.

Corollary 4.3. *Assume that $p < q$, that $x \equiv 1 \bmod p$ and that*

$$|x| \ge 8\,(0.8q)^q.$$

Then $\mathcal{I}_M^{\mathrm{aug}}(2) = \{0\}$.

To deduce the corollary from Theorem 4.2, observe that $0.8q > 2$ and $16 > 36/(p-1)^2$. Hence

$$8\,(0.8q)^q > 16 \cdot 2^{q-1} > \frac{36 \cdot 2^{p-1}}{(p-1)^2}$$

whenever $q > p$.

The proof of Theorems 4.1 and 4.2 occupies the rest of this section.

4.1. The algebraic number $(x-\zeta)^\Theta$. In this section, we investigate the number $(x-\zeta)^\Theta$. First of all, we have to estimate its height.

Proposition 4.4. *For any $x \in \mathbb{Z}$ and $\Theta \in R$ we have*

$$h\left((x-\zeta)^\Theta\right) \le \frac{\|\Theta\| + |w(\Theta)|}{2}\log(|x|+1).$$

Proof. Write $\Theta = \Theta^+ - \Theta^-$ as in Section 2. Using (7) with $\alpha = (x-\zeta)^{\Theta^+}$ and $\beta = (x-\zeta)^{\Theta^-}$, we obtain

$$h\left((x-\zeta)^\Theta\right) = \frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K}[K_v:\mathbb{Q}_v]\log X_v,$$

where

$$X_v = \max\left\{\left|(x-\zeta)^{\Theta^+}\right|_v, \left|(x-\zeta)^{\Theta^-}\right|_v\right\}.$$

We have trivially

$$X_v \le (|x|+1)^{\max\{\|\Theta^+\|,\|\Theta^-\|\}}$$

if v is archimedean, and $X_v \le 1$ if v is non-archimedean. This implies

$$h\left((x-\zeta)^\Theta\right) \le \left(\max\left\{\|\Theta^+\|, \|\Theta^-\|\right\}\right)\log(|x|+1).$$

Since

$$\max\left\{\|\Theta^+\|, \|\Theta^-\|\right\} = \frac{\|\Theta\| + |w(\Theta)|}{2},$$

the proposition follows. □

Next, we observe that $(x-\zeta)^\Theta$ is "very close" to 1 if $w(\Theta)=0$. Below log stands for the principal branch of the complex logarithm, that is

$$-\pi < \operatorname{Im}\log z \le \pi.$$

Proposition 4.5. *If* $|x|>1$ *and* $w(\Theta)=0$ *then* $\left|\log(x-\zeta)^\Theta\right| \le \frac{\|\Theta\|}{|x|-1}$.

Proof. For any complex z satisfying $|z|<1$ we have

$$|\log(1+z)| \le \frac{|z|}{1-|z|}.$$

In particular,

$$\left|\log\left(1-\frac{\zeta^\sigma}{x}\right)\right| \le \frac{1}{|x|-1}.$$

Since $(x-\zeta)^\Theta = (1-\zeta/x)^\Theta$ when $w(\Theta)=0$, the result follows. □

Finally, we show that $(x-\zeta)^\Theta$ is distinct from 1 under certain mild assumptions.

Proposition 4.6. *Let x be an integer satisfying $|x|\ge 2$, and, in addition, $x\ne -2$ for $p=3$. Then, for $\Theta\in R$, we have $(x-\zeta)^\Theta \ne 1$ unless $\Theta = 0$.*

Proof. Let $\mathfrak{p}$ be the prime ideal of K lying over p. Then $\mathfrak{p}^{p-1}=(p)$ and $\mathfrak{p} = (\zeta^\sigma - \zeta^\tau)$ for any distinct $\sigma,\tau\in G$. In particular, for distinct σ and τ we have

$$(x-\zeta^\sigma, x-\zeta^\tau)\,|\,\mathfrak{p}. \tag{10}$$

If $x-\zeta$ has no prime divisors other than $\mathfrak{p}$, then $(x-\zeta)=\mathfrak{p}^k$, and (10) implies that $k\le 1$. Taking the norms, we obtain $\Phi_p(x)\in\{\pm1,\pm p\}$, where

$$\Phi_p(x) = x^{p-1}+x^{p-2}+\cdots+1$$

is the cyclotomic polynomial.

On the other hand, in the case $p \geq 5$ and $|x| \geq 2$ we have

$$|\Phi_p(x)| \geq 2^{p-2} > p.$$

Similarly, we have $|\Phi_3(x)| > 3$ if $|x| \geq 3$ or $x = 2$. This shows that $x - \zeta$ has a prime divisor $\mathfrak{q}$ distinct from $\mathfrak{p}$.

Put $\ell = \operatorname{ord}_{\mathfrak{q}}(x - \zeta)$. Then (10) implies that

$$\operatorname{ord}_{\mathfrak{q}^\sigma}(x - \zeta^\tau) = \begin{cases} \ell, & \text{if } \sigma = \tau, \\ 0, & \text{if } \sigma \neq \tau. \end{cases}$$

Hence, writing Θ as in (1), we obtain

$$\operatorname{ord}_{\mathfrak{q}^\sigma}\left((x - \zeta)^\Theta\right) = \ell m_\sigma \quad (\sigma \in G).$$

Now, if $(x - \zeta)^\Theta = 1$ and $\ell \neq 0$, then $m_\sigma = 0$ for all σ. Hence $\Theta = 0$. □

4.2. The q-th root of $(x - \zeta)^\Theta$. By definition, for every $\Theta \in \mathcal{I}_M$ there exists a *unique* $\alpha = \alpha(\Theta) \in K^*$ such that $\alpha(\Theta)^q = (x - \zeta)^\Theta$. (Uniqueness follows from the fact that K does not contain q-th roots of unity other than 1.) Moreover, uniqueness implies that $\alpha(\Theta_1 + \Theta_2) = \alpha(\Theta_1)\alpha(\Theta_2)$ for $\Theta_1, \Theta_2 \in \mathcal{I}_M$; that is, **the map $\alpha : \mathcal{I}_M \to K^*$ is a group homomorphism.**

Proposition 4.7. *Assume that $|x| \geq 2$ and $x \neq -2$ if $p = 3$. Then for a non-zero $\Theta \in \mathcal{I}_M$ we have $\alpha(\Theta) \neq 1$. Also,*

$$h(\alpha(\Theta)) \leq \frac{\|\Theta\| + w(\Theta)}{2q} \log(|x| + 1).$$

Proof. The first statement follows from Proposition 4.6. For the second, notice that $qh(\alpha(\Theta)) = h\left((x - \zeta)^\Theta\right)$ by (5), and apply Proposition 4.4. □

It is crucial that, for $\Theta \in \mathcal{I}_M^{\mathrm{aug}}$, the number $\alpha(\Theta)$ is close (in the complex metric) to a q-th root of unity. More precisely, we have the following.

Proposition 4.8. *Assume that $|x| \geq 2$ and that*

$$r < \frac{\pi}{2}(|x| - 1). \tag{11}$$

Then for any $\Theta \in \mathcal{I}_M^{\mathrm{aug}}(2r)$ there exists a unique q-th root of unity $\xi = \xi(\Theta)$ such that

$$\left|\log\left(\alpha(\Theta)\xi(\Theta)^{-1}\right)\right| \leq \frac{\|\Theta\|}{q(|x| - 1)}.$$

Moreover, $\xi(-\Theta) = \xi(\Theta)^{-1}$. Further, for any $\Theta_1, \Theta_2 \in \mathcal{I}_M^{\mathrm{aug}}(r)$ we have $\xi(\Theta_1 + \Theta_2) = \xi(\Theta_1)\xi(\Theta_2)$; that is, the map $\xi : \mathcal{I}_M^{\mathrm{aug}}(r) \to \mu_q$ is a "local homomorphism".

(Here μ_q stands for the group of q-th roots of unity.)

Proof. Existence of $\xi(\Theta)$ follows from Proposition 4.5. Further, since

$$\|\Theta\| \le 2r < \pi(|x|-1),$$

we have

$$\left|\log\left(\alpha(\Theta)\xi(\Theta)^{-1}\right)\right| \le \frac{\|\Theta\|}{q(|x|-1)} < \frac{\pi}{q}. \tag{12}$$

On the other hand, $\left|\log \xi_1\xi_2^{-1}\right| \ge 2\pi/q$ for any two distinct q-th roots of unity ξ_1 and ξ_2. This implies the uniqueness of $\xi(\Theta)$. The "local homomorphism" property follows from the uniqueness. □

4.3. Proof of Theorem 4.1. We may assume that $q > p$, since otherwise the statement of the theorem is trivial. In particular, $q \ge 5$. Also, observe that in the set-up of Theorem 4.1 we have (11). Indeed, since

$$|x| \ge \frac{4}{\pi}\frac{q}{p-1} + 1,$$

we have

$$r < 2\frac{p}{q-1} \le \frac{\pi}{2}(|x|-1).$$

Hence for every $\Theta \in \mathcal{I}_M(2r)$ we have the well-defined $\xi(\Theta)$ as in Proposition 4.8.

Proposition 4.9. *Let $\Theta \in \mathcal{I}_M^{\mathrm{aug}}(2r)$ satisfy $\xi(\Theta) = 1$. Then $\Theta = 0$.*

Proof. Fix a non-zero $\Theta \in \mathcal{I}_M^{\mathrm{aug}}(2r)$ with $\xi(\Theta) = 1$ and put $\alpha = \alpha(\Theta)$. Using (3) together with the estimates from Subsection 4.2, we obtain

$$h(\alpha - 1) \le \frac{\|\Theta\|}{2q}\log(|x|+1) + \log 2$$

Also, (12) implies that

$$|\log\alpha| \le \frac{\|\Theta\|}{q(|x|-1)} < \frac{\pi}{q} \le \frac{\pi}{5},$$

because $q \ge 5$. The latter inequality implies that[2]

$$|\alpha - 1| \le 1.4|\log\alpha| \le 1.4\frac{\|\Theta\|}{q(|x|-1)}.$$

The Liouville inequality (6) for the algebraic number $\alpha - 1$ (which is distinct from 0 by Proposition 4.7) reads $|\alpha-1|^2 \ge e^{-(p-1)h(\alpha-1)}$. Combining

[2] One has $|e^z - 1| \le 1.4|z|$ for $z \in \mathbb{C}$ with $|z| \le \pi/5$. Indeed, if $|z| \le r$ then

$$|e^z - 1| = \left|z + \frac{z^2}{2!} + \frac{z^3}{3!} + \dots\right| \le r + \frac{r^2}{2!} + \frac{r^3}{3!} + \dots = e^r - 1.$$

The Schwarz lemma implies that

$$|e^z - 1| \le \frac{e^r - 1}{r}|z|.$$

Taking $r = \pi/5$, we obtain $|e^z - 1| \le 1.4|z|$.

this with the previously established estimates for $|\alpha-1|$ and $h(\alpha-1)$, we obtain

$$2\left(\log(|x|-1)-\log\frac{1.4\|\Theta\|}{q}\right)\le(p-1)\left(\frac{\|\Theta\|}{2q}\log(|x|+1)+\log 2\right),$$

which can be rewritten as

$$\begin{aligned}\left(2-\frac{p-1}{2q}\|\Theta\|\right)\log|x| \le{}& 2\log\frac{1.4\|\Theta\|}{q}+2\log\frac{|x|}{|x|-1}\\ &+\frac{p-1}{2q}\|\Theta\|\log\frac{|x|+1}{|x|}+(p-1)\log 2.\end{aligned}\tag{13}$$

By the assumption,

$$\frac{p-1}{2q}\|\Theta\|\le\frac{p-1}{2q}2r=2-\varepsilon<2.$$

Replacing $\frac{p-1}{2q}\|\Theta\|$ by $2-\varepsilon$ in the left-hand side of (13), and by 2 in the right-hand side, we obtain

$$\varepsilon\log|x|\le 2\log\frac{5.6}{p-1}+2\log\frac{|x|+1}{|x|-1}+(p-1)\log 2.$$

Now notice that $|x|\ge 36$ by (8). It follows that

$$\varepsilon\log|x|\le 2\log\frac{5.6}{p-1}+2\log\frac{37}{35}+(p-1)\log 2<\log 36\frac{2^{p-1}}{(p-1)^2},$$

which contradicts (8). □

Proof of Theorem 4.1. Let $\Theta_1,\Theta_2\in\mathcal{I}_M^{\mathrm{aug}}(r)$ satisfy $\xi(\Theta_1)=\xi(\Theta_2)$. Then $\xi(\Theta_1-\Theta_2)=1$ by Proposition 4.8, and Proposition 4.9 implies that $\Theta_1-\Theta_2=0$. We have shown that the map $\xi:\mathcal{I}_M^{\mathrm{aug}}(r)\to\mu_q$ is injective, which proves the theorem. □

4.4. Proof of Theorem 4.2. Assume that $\mathcal{I}_M^{\mathrm{aug}}\ni\Theta$ with $\|\Theta\|=2$. Put $\alpha=\alpha(\Theta)$. Proposition 4.9 implies that $\xi(\sigma\Theta)\ne 1$ for any $\sigma\in G$. Equivalently, $|\arg(\alpha^\sigma)|\ge\pi/q$ for any σ, which implies that $|\alpha^\sigma-1|>\sin(\pi/q)$ for any σ. In other words,

$$|\alpha-1|_v>\sin(\pi/q)>2.5/q$$

for any archimedean valuation v.

Write now $\Theta=\sigma_1-\sigma_2$, where σ_1 and σ_2 are distinct elements of G, and put $\zeta_i=\zeta^{\sigma_i}$. Assume that $|\alpha-1|_v<1$ for a non-archimedean v. Then $|\alpha^q-1|_v\le|\alpha-1|_v<1$. However,

$$\alpha^q-1=(x-\zeta)^\Theta-1=\frac{\zeta_2-\zeta_1}{x-\zeta_2}.$$

Notice that $\zeta_2-\zeta_1$ divides $x-\zeta_2$ if and only if $x\equiv 1 \bmod p$. We conclude that $|\alpha-1|_v\ge 1$ for all non-archimedean v if $x\equiv 1\bmod p$, and

$$|\alpha-1|_v\ge|\zeta_2-\zeta_1|_v=|p|_v^{1/(p-1)}$$

for all non-archimedean v if $x\not\equiv 1\bmod p$.

We have proved that

$$\left|(\alpha-1)^{-1}\right|_v<0.4q$$

if v is archimedean, and

$$\left|(\alpha-1)^{-1}\right|_v\le|p'|_v^{-1/(p-1)}$$

if v is non-archimedean. (Recall that $p'=1$ if $x\equiv 1\bmod p$ and $p'=p$ otherwise.) It follows that

$$h(\alpha-1)=h\left((\alpha-1)^{-1}\right)<\log 0.4q+\frac{\log p'}{p-1}=\log 0.4q(p')^{1/(p-1)}$$

and

$$h(\alpha)\le h(\alpha-1)+\log 2<\log 0.8q(p')^{1/(p-1)}.$$

Now we apply (3–5) to obtain

$$\begin{aligned}\log|x|=h(x)&=h\left(\frac{\zeta_2-\zeta_1}{\alpha^q-1}+\zeta_2\right)\\&\le qh(\alpha)+3\log 2<\log 8\left(0.8q(p')^{1/(p-1)}\right)^q,\end{aligned}$$

which contradicts (9). □

5. Solutions of Catalan's equation

In this section we summarize necessary properties of solutions. Everywhere in this section, (x,y,p,q) is a solution of Catalan's equation; that is, x,y are non-zero integers and p,q are odd prime numbers satisfying $x^p-y^q=1$. Recall the symmetrical property of solutions: if (x,y,p,q) is a solution, then $(-y,-x,q,p)$ is a solution as well.

We begin with the classical result of Cassels [3].

Proposition 5.1. **(Cassels)** *We have $q|x$ and $p|y$. Moreover, there exist non-zero integers a,b and positive integers u,v such that*

$$\begin{aligned}x-1&=p^{q-1}a^q,\quad y=pau,\quad \frac{x^p-1}{x-1}=pu^q,\\ y+1&=q^{p-1}b^p,\quad x=qbv,\quad \frac{y^q+1}{y+1}=qv^p.\end{aligned}$$

□

The following is an easy consequence of Proposition 5.1 (see [1, Corollary 2.2]).

Proposition 5.2. *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.* □

Another consequence of Cassels relations is lower bounds for $|x|$ and $|y|$ in terms of p and q. We need the following result of Hyyrö [5].

Proposition 5.3. *We have $|x| \geq p^{q-1}(q-1)^q + 1$.*

Proof. We shall use the following obvious fact: the four numbers x, y, a, b in Proposition 5.1 are either altogether positive (*the positive case*), or altogether negative (*the negative case*).

Since $q|x$, we have

$$p^{q-1}a^q = x - 1 \equiv -1 \bmod q.$$

Since $p^{q-1} \equiv 1 \bmod q$, this implies $a^q \equiv -1 \bmod q$, which is equivalent to $a \equiv -1 \bmod q$. Similarly, $b \equiv 1 \bmod p$. Now, in the positive case we have $a \geq q-1$ and $x \geq p^{q-1}(q-1)^q + 1$. In the negative case we have either $a \leq -q-1$, which implies that

$$|x| \geq p^{q-1}(q+1)^q - 1 > p^{q-1}(q-1)^q + 1,$$

or $a = -1$.

It remains to show that the last option is impossible. Thus, assume that $a = -1$, which implies $1 - x = 1 + |x| = p^{q-1}$. Since we are in the negative case, we have $b \leq 1 - p$, and

$$\begin{aligned} |y| = (|x|^p + 1)^{1/q} \leq (1 + |x|)^{p/q} < p^p < \\ < 2^{p-1}(p-1)^p < q^{p-1}|b|^p = |1 + y| < |y|, \end{aligned}$$

a contradiction. □

6. The relative class number

Warning. In this section h stands for the class number rather than for the height function.

As usual, let ζ be a primitive p-th root of unity and $K = \mathbb{Q}(\zeta)$. Denote by K^+ the totally real part of K, and by H and H^+ the class groups of K and K^+, respectively. It is well-known [19, Theorem 4.14] that H^+ naturally embeds into H. The index $[H\colon H^+]$ is called *the relative class number* and is denoted by $h^- = h^-(p)$.

In this section we prove the following theorem, due to Bugeaud and Hanrot [2].

Theorem 6.1. (Bugeaud and Hanrot) *Let (x, y, p, q) be a solution of Catalan's equation with $q > p$. Then $q|h^-(p)$.*

It is not difficult to calculate the relative class number, using the standard class-number formulas; see, for instance, [19, Theorem 4.17]. Already Kummer [8, pages 544, 907–918] calculated $h^-(p)$ for $p < 100$ (and even determined the structure of the group H/H^+). Tables of relative class numbers are widely available; see, for instance, [19, pages 412–420]. Using the tables, it is easy to verify that, for $p \le 41$, the number $h^-(p)$ has no prime divisors greater than p. We obtain the following consequence.

Corollary 6.2. *Let (x, y, p, q) be a solution of Catalan's equation. Then $p, q \ge 43$.* □

Proof of Theorem 6.1. We assume that q does not divide $h^-(p)$ and derive a contradiction. Put $\lambda := (x - \zeta)/(1 - \zeta)$. Proposition 5.2 implies that $(\lambda) = \mathfrak{a}^q$, where $\mathfrak{a}$ is an ideal of K. The class of $\mathfrak{a}$ belongs to the q-component of H. Since q does not divide $h^-(p) = [H\colon H^+]$, the q-component of H is contained in H^+. Thus, $\mathfrak{a} = \alpha\mathfrak{b}$, where $\alpha \in K^*$ and $\mathfrak{b}$ is an ideal of K^+. Write the principal ideal $\mathfrak{b}^q$ as (β), where $\beta \in K^+$. Then $\lambda = \alpha^q\beta$ times a unit of K.

Now recall that every unit of K is a real unit times a root of unity, the latter being a q-th power in K. Hence, redefining α and β, we obtain $\lambda = \alpha^q\beta$ with $\alpha \in K$ and $\beta \in K^+$.

Since $(1 - \zeta)/(1 - \bar{\zeta})$ is a root of unity, it is a q-th power in K. Hence

$$\frac{x - \zeta}{x - \bar{\zeta}} = \frac{1 - \zeta}{1 - \bar{\zeta}} \cdot \frac{\lambda}{\bar{\lambda}} = \frac{1 - \zeta}{1 - \bar{\zeta}} \left(\frac{\alpha}{\bar{\alpha}}\right)^q \in (K^*)^q .$$

In other words, $1 - \iota \in \mathcal{I}_M$, where ι is the complex conjugation and $\mathcal{I}_M$ the Mihăilescu ideal, defined in Section 4.

On the other hand, $x \equiv 1 \bmod p$ by Proposition 5.1, and

$$|x| \ge p^{q-1}(q-1)^q + 1 > 8\,(0.8q)^q$$

by Proposition 5.3. We are in a position to apply Corollary 4.3, which forbids $\mathcal{I}_M$ to have elements of weight 0 and size 2. Since $1 - \iota$ is such an element, we obtain a contradiction. □

7. The Stickelberger ideal

The *Stickelberger ideal* $\mathcal{I}_S$ of the group ring $R = \mathbb{Z}[G]$ is defined by $\mathcal{I}_S = R\theta \cap R$, where

$$\theta = \frac{1}{p}\sum_{a=1}^{p-1} a\sigma_a^{-1}$$

is the *Stickelberger element.* In this section we establish some properties of the ideal $(1 - \iota)\mathcal{I}_S$, where ι, as above, stands for the complex conjugation. First of all, we recall the notion of the "minus-part".

By definition, the minus-part of R is $R^- = (1-\iota)R$. Further, for any ideal $\mathcal{I}$ of R the minus part of $\mathcal{I}$ is defined by $\mathcal{I}^- = \mathcal{I} \cap R$. We have

$$\mathcal{I}^- \supseteq (1-\iota)\mathcal{I} \supseteq 2\mathcal{I}^-. \tag{14}$$

Here the first inclusion is obvious. To prove the second, observe that $(1-\iota)^2 = 2(1-\iota)$, which implies the identity $(1-\iota)\Theta = 2\Theta$ for every $\Theta \in R^-$. Hence

$$(1-\iota)\mathcal{I} \supset (1-\iota)\mathcal{I}^- = 2\mathcal{I}^-,$$

which proves the second inclusion in (14).

Relation (14) implies, in particular, that the ideals $\mathcal{I}^-$ and $1-\iota)\mathcal{I}$ are of the same $\mathbb{Z}$-rank.

After this deviation, we return to the Stickelberger ideal.

Proposition 7.1. *There is a* $\mathbb{Z}$*-basis* $\theta_1, \ldots, \theta_{(p-1)/2}$ *of* $(1-\iota)\mathcal{I}_S$ *satisfying*

$$\|\theta_k\| \le p-1 \qquad (k = 1, \ldots, (p-1)/2).$$

Proof. First of all, observe that the $\mathbb{Z}$-rank of $(1-\iota)\mathcal{I}_S$ is $(p-1)/2$. Indeed, the $\mathbb{Z}$-rank of R^- is $(p-1)/2$, because it has the $\mathbb{Z}$-basis

$$\sigma_k - \sigma_{p-k} \qquad (k = 1, \ldots, (p-1)/2).$$

Further, it is well-known that the index $[R^- : \mathcal{I}_S^-]$ is finite (and equal to the relative class number); see, for instance, [19, Theorem 6.19]. This implies that the rank of $\mathcal{I}_S^-$ is also $(p-1)/2$, and so is the rank of $(1-\iota)\mathcal{I}_S$, because, as we have observed above, the two ranks are equal.

Now, given an integer k not divisible by p, put

$$\Theta_k = (k - \sigma_k)\theta$$

Then $\mathcal{I}_S$ is generated (over $\mathbb{Z}$) by all the Θ_k (see [19, Lemma 6.9][3]). Since $\Theta_{k+p} = \Theta_k + p\theta$, the ideal $\mathcal{I}_S$ is generated by $\Theta_1 = 0, \Theta_2, \ldots, \Theta_{p-1}$ and $p\theta$. Since

$$\Theta_k(1-\iota) + \Theta_{p-k}(1-\iota) = p\theta(1-\iota),$$

the ideal $(1-\iota)\mathcal{I}_S$ is generated by the set

$$\{\Theta_k(1-\iota) : k = 1, \ldots, (p+1)/2\}.$$

Since $\Theta_1 = 0$, it is also generated by $\theta_1, \ldots, \theta_{(p-1)/2}$, where

$$\theta_k = (\Theta_{k+1} - \Theta_k)(1-\iota).$$

Since the $\mathbb{Z}$-rank of $(1-\iota)\mathcal{I}_S$ is $(p-1)/2$, the elements $\theta_1, \ldots, \theta_{(p-1)/2}$ form a $\mathbb{Z}$-basis of $\mathcal{I}_S^-$. It remains to estimate the size of θ_k.

An easy calculation shows that $w(\theta) = (p-1)/2$. Hence

$$w(\Theta_k) = (k-1)\frac{p-1}{2},$$

[3] In the statement of the lemma Washington writes "generated" without specifying "over $\mathbb{Z}$", but he proves exactly what we need.

and

$$w\left(\Theta_{k+1}-\Theta_k\right)=\frac{p-1}{2}.$$

On the other hand, we have $\Theta_k=\sum_{a=1}^{p-1}\lfloor ak/p\rfloor\,\sigma_a^{-1}$ which implies that $\Theta_{k+1}-\Theta_k\geq 0$, and

$$\|\Theta_{k+1}-\Theta_k\|=w\left(\Theta_{k+1}-\Theta_k\right)=\frac{p-1}{2}.$$

It follows that $\|\theta_k\|\leq\|1-\iota\|\cdot\|\Theta_{k+1}-\Theta_k\|=p-1$, as wanted. □

For a positive integer n and a positive real r denote by $S(n,r)$ the number of points $(x_1,\dots,x_n)\in\mathbb{Z}^n$ satisfying $|x_1|+\cdots+|x_n|\leq r$. The following is an immediate consequence of Proposition 7.1.

Corollary 7.2. *Let r be a positive integer. Then the ideal $(1-\iota)\mathcal{I}_S$ contains at least $S\left((p-1)/2,r/(p-1)\right)$ elements of size not exceeding r.* □

8. Proof of Theorems 1.3 and 1.2

Mihăilescu proved the following (see [1, Proposition 3.1.1]).

Proposition 8.1. *Let (x,y,p,q) be a solution of Catalan's equation. Then $\mathcal{I}_M\supseteq(1-\iota)\mathcal{I}_S$.* □

Since the elements of $(1-\iota)\mathcal{I}_S$ are of weight 0, the ideal $(1-\iota)\mathcal{I}_S$ is contained in the augmented part of $\mathcal{I}_M$. Combining this with Corollary 7.2, we obtain the lower bound

$$\mathcal{I}_m^{\mathrm{aug}}(r)\geq S\left(\frac{p-1}{2},\frac{r}{p-1}\right)\tag{15}$$

for any $r>0$.

On the other hand, in Section 4, we obtained an upper bound for $\mathcal{I}_m^{\mathrm{aug}}(r)$. We are going to show that the two bounds are contradictory.

To adapt (15) for our purposes, we need a simple lemma.

Lemma 8.2. *Let n and r be integers satisfying $n\geq 11$ and $r\geq 3$. Then*

$$S(n,r)>4n^2(r+1).\tag{16}$$

Proof. When r is an integer, we have

$$S(n,r)=\sum_{k=0}^{n}2^k\binom{n}{k}\binom{r}{k}$$

(see [6, Lemma 2.3]). If $n \ge 11$ and $r \ge 3$ then

$$\begin{aligned} 8\binom{n}{3}\binom{r}{3} &= \frac{2}{9}n(n-1)(n-2)r(r-1)(r-2) \\ &\ge \frac{2}{9}\cdot\frac{10}{11}\cdot n^2\cdot 9\cdot\frac{3}{4}\cdot(r+1)\cdot 2\cdot 1 \\ &= \frac{30}{11}n^2(r+1), \\ 4\binom{n}{2}\binom{r}{2} &= n(n-1)r(r-1) \\ &\ge \frac{10}{11}\cdot n^2\cdot\frac{3}{4}\cdot(r+1)\cdot 2 \\ &= \frac{15}{11}n^2(r+1). \end{aligned}$$

It follows that

$$S(n,r) \ge 4\binom{n}{2}\binom{r}{2} + 8\binom{n}{3}\binom{r}{3} \ge \frac{45}{11}n^2(r+1) > 4n^2(r+1). \qquad \square$$

Proof of Theorem 1.3. Assume that $q \ge 3(p-1)^2$ and put

$$r = \left\lfloor \frac{q}{(p-1)^2} \right\rfloor, \qquad n = \frac{p-1}{2}.$$

Then $r \ge 3$ by the assumption and $n \ge 21$ by Corollary 6.2. Further, Proposition 5.3 implies that

$$|x| \ge p^{q-1}(q-1)^q + 1 \ge \frac{36\cdot 2^{p-1}}{(p-1)^2}.$$

Now using subsequently Theorem 4.1 with $\varepsilon = 1$, inequality (15) and Lemma 8.2, we obtain

$$q \ge \left|\mathcal{I}_M^{\mathrm{aug}}((p-1)r)\right| \ge S\left(n,r\right) > 4n^2(r+1) > 4\left(\frac{p-1}{2}\right)^2\frac{q}{(p-1)^2} = q,$$

a contradiction. □

Theorem 1.2 is a consequence of Theorem 1.3 and Mihăilescu's "double Wieferich criterion" [14] (see also [1, Theorem 3.2]).

Proposition 8.3. (Mihăilescu [14]**)** *Let (x,y,p,q) be a solution of Catalan's equation. Then*

$$q^{p-1} \equiv 1 \bmod p^2, \qquad p^{q-1} \equiv 1 \bmod q^2. \qquad \square$$

Proof of Theorem 1.2. Assume that $q \equiv 1 \bmod p$. Since $q^{p-1} \equiv 1 \bmod p^2$ by Proposition 8.3, we have $q \equiv 1 \bmod p^2$. Since q is odd, it cannot be equal to p^2+1 or $3p^2+1$. Also, notice that $p \ne 3$ by Corollary 6.2. It follows that

$q \neq 2p^2+1$, because the latter number is divisible by 3 (this observation is due to Mignotte). Thus, $q \geq 4p^2+1$, which contradicts Theorem 1.3. □

Remark. It is worth mentioning that, for $p \geq 5$, one can prove Theorem 1.2 without any reference to Corollary 6.2. Indeed, the same argument as in Lemma 8.2 shows that (16) holds for $n \geq 5$ and $r \geq 4$. This implies that that $q \leq 4(p-1)^2$ for $p \geq 11$, which is sufficient to conclude that Theorem 1.2 is true for $p \geq 11$.

Further, (16) is true for $n=3$ and $r \geq 5$, as well as for $n=2$ and $r \geq 9$. This implies that $q \leq 5(p-1)^2 = 180$ for $p=7$, and $q \leq 9(p-1)^2 = 144$ for $p=5$. Hence Theorem 1.2 is true for $p=7$ and $p=5$, except perhaps the case $(p,q)=(5,101)$. The latter can be ruled out by verifying that $5^{100} \not\equiv 1 \bmod 101^2$ (which can be done on a pocket calculator) and applying Proposition 8.3.

Finally, recall that the case $p=3$ has been solved long ago by Nagell [17].

References

[1] YU.F. BILU, *Catalan's conjecture (after Mihăilescu).* Séminaire Bourbaki, Exposé 909, 55ème année (2002-2003); Astrisque **294** (2004), 1–26.

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

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

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

[5] S. HYYRÖ, *Über das Catalansche Problem.* Ann. Univ. Turku Ser. AI **79** (1964), 3–10.

[6] P. KIRSCHENHOFER, A. PETHŐ, R.F. TICHY, *On analytical and Diophantine properties of a family of counting polynomials.* Acta Sci. Math. (Szeged), **65** (1999), no. 1-2, 47–59.

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

[8] E. KUMMER *Collected papers.* Springer, 1975.

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

[10] M. LAURENT, M. MIGNOTTE, YU. NESTERENKO, *Formes linéaires en deux logarithmes et déterminants d'interpolation.* J. Number Theory **55** (1995), 285–321.

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

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

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

[14] P. MIHĂILESCU, *A class number free criterion for Catalan's conjecture.* J. Number Theory **99** (2003), 225–231.

[15] P. MIHĂILESCU, *Primary cyclotomic units and a proof of Catalan's conjecture.* J. reine angew. Math., to appear.

[16] P. MIHĂILESCU, On the class groups of cyclotomic extensions in the presence of a solution to Catalan's equation. A manuscript.

[17] T. NAGELL, *Des équations indéterminées* $x^2+x+1=y^n$ *and* $x^2+x+1=3y^n$. Norsk Matem. Forenings Skrifter I, **2** (1921), 14 pp. (See also: *Collected papers of Trygve Nagell,* ed. P. Ribenboim, Queens Papers in Pure and Applied Mathematics **121**, Kingston, 2002; Vol.1, pp. 79–94.)

[18] R. TIJDEMAN, *On the equation of Catalan.* Acta Arith. **29** (1976), 197–209.

[19] L. Washington, *Introduction to Cyclotomic Fields.* Second edition, Graduate Texts in Math. **83**, Springer, New York, 1997.

Yuri F. Bilu
A2X, Université Bordeaux 1
351 cours de la Libération
33405 Talence France
E-mail : yuri@math.u-bordeaux1.fr