Catalan's conjecture (after Mihăilescu)

Yuri F. Bilu

May 7, 2002

Abstract

It is an exposition of Mihăilescu's recent proof of Catalan's conjecture.

1 Introduction

In this note we prove the following theorem, recently established by Mihăilescu [13].

Theorem 1.1 (Mihăilescu) *The equation*

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

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

Together with the results of Lebesgue [8] and Ko Chao [6] this implies the celebrated conjecture of Catalan (1843):

The the only solution to $x^u - y^v = 1$ in integers $x, y > 0$ and $u, v > 1$ is $3^2 - 2^3 = 1$.

Plan of the paper In Section 2 we remind previous results on the Catalan equation, to be used in the proof. Section 3 contains general lemmata. In Section 4 Theorem 1.1 is reduced to three more technical statements, which are proved in the three final section.

Acknowledgements I am pleased to thank Yann Bugeaud, Andrew Glass, Guillaume Hanrot and Preda Mihăilescu for explaining me various results from Section 2 and other useful discussions.

2 Prerequisites

In this section we collect previously known results on the Catalan equation, to be used in the proof. It is **not** a historical account of Catalan's problem; the latter can be found in Ribenboim's book [14] and Mignotte's survey [9].

In the sequel we assume the equality

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

with non-zero integers x, y and odd primes p, q. Since (2) implies $(-y)^q - (-x)^p = 1$, all the statements below remain true with x, y, p, q replaced by $-y, -x, q, p$.

We start with the following result of Cassels [2].

Proposition 2.1 (Cassels) *There exist non-zero integers a and v such that*

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

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

Cassels' relations imply various lower estimates for the variables x and y in terms of p and q. For instance, (3) immediately yields $|x| \geq p^{q-1} - 1$, and this can be refined without much effort.

Hyyrö [3] obtained an estimate of a different kind: $|x| \geq q(2p+1)(2q^{p-1}+1)$. Since Hyyroö's paper is not easily available, I include below a slightly weaker statement, which is totally sufficient for our purposes.

Proposition 2.2 *If* $p \not\equiv 1 \mod q$ *then* $|x| \geq q^{p-1} - q$.

Proof Applying Proposition 2.1 to the equation $(-y)^q - (-x)^p = 1$, we find integers u and b such that

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

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

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 $(y+1) \,|\, q\left(u^p - 1\right)$. Now (5) implies that $q^{p-2} \,\big|\, \left(u^p - 1\right)$, and in particular $u^p \equiv 1 \mod q$. Since $p \not\equiv 1 \mod q$, this implies that $u \equiv 1 \mod q$.

Now, since $\gcd\left(u - 1, \left(u^p - 1\right)/(u - 1)\right)$ divides p, the prime q cannot simultaneously divide both $u - 1$ amd $\left(u^p - 1\right)/(u - 1)$. Thus, $q^{p-2} \,\big|\, (u - 1)$, and $|u| \geq q^{p-2} - 1$.

Finally, since $x = qub$, we have $|x| \geq q|u| \geq q^{p-1} - q$, as wanted. ■

Remark 2.3 This version of Hyyrö's argument is due to Mignotte and Bugeaud. It was kindly communicated to me by Yann Bugeaud. Using slightly more advanced tools, Mihăilescu [13, Lemma 2] obtained the much sharper estimate $|x| \geq \left(q^{2p-2}/2\right)^4$.

Tijdeman [16] used the theory of logarithmic form to establish explicit upper bounds for the exponents p, q, reducing the problem to a finite computation. Mignotte and Roy [10, Relation 2.14] refined Tijdeman's estimate, using the very sharp lower bound for the binary logarithmic forms from [7].

Proposition 2.4 (Mignotte-Roy) *If* $p > q > 3000$ *then*

$$p < 2.77q\left(\log(p/\log q) + 2.333\right)^2 \log q \tag{7}$$

(Warning: Mignotte and Roy assume that $q > p$.)

Further refinement are due to Bennett *et al.* [1]. However, we shall only need the following weaker inequality.

Corollary 2.5 *If* $q \geq 10^5$ *then* $p < q^2$.

Proof This is just a stupid calculation. If $q \geq 10^5$ then $\log\log q > 2.44$ which implies

$$\left(\log(p/\log q) + 2.333\right)^2 \leq (\log p)^2. \tag{8}$$

Combining the inequality $\log p \leq (22/e)p^{1/22}$ with (7) and (8), we obtain

$$p \leq \left(2.77 \cdot (22/e)^2 q \log q\right)^{1.1}. \tag{9}$$

Now, since the function $f(q) = q^{-0.8}\log q$ is decreasing for $q \geq 6$, we have $f(q) \leq f(10^5)$, or $\log q \leq 10^{-4}\log(10^5)q^{0.8}$. Substituting this into (9), we obtain

$$p \leq \left(2.77 \cdot (22/e)^2 \cdot 10^{-4}\log(10^5)\right)^{1.1} q^{1.98} < 0.4q^{1.98},$$

better than wanted. ■

Using an algebraic criterion of Inkeri [4, 5] together with electronic computations, Mignote and Roy [11] proved that

$$\min\{p, q\} \geq 10^5. \tag{10}$$

Recently Mihăilescu [12] drastically refined Inkeri's criterion by proving that

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

Another important result, established in [12], is

$$q^2 | x. \tag{12}$$

(see [12, end of Section 3]).

Congruence (11), together with the results of Mignotte and Roy, implies that

$$p \not\equiv 1 \mod q. \tag{13}$$

Indeed, if, $p \equiv 1 \mod q$ then $p \equiv 1 \mod q^2$ because of (11). Then $p > q^2$. On the other hand, $q \geq 10^5$ by (10), which implies that $p < q^2$ by Corollary 2.5, a contradiction.

Remark 2.6 Inequality (10) is the only result, used by Mihăilescu, that depends on electronic computations. As Mignotte indicated in [9], if one uses (11) instead of Inkeri's criterion, the proof of (10) requires just a few seconds of processor time.

3 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.

Proposition 3.1 *Let $\mathfrak{a}$ and $\mathfrak{b}$ be co-prime ideals of a commutative ring R satisfying $\mathfrak{ab} = \mathfrak{a}$. Then $\mathfrak{b} = (1)$.*

Proof Since $\mathfrak{a}$ and $\mathfrak{b}$ are coprime, there are $\alpha \in \mathfrak{a}$ and $\beta \in \mathfrak{b}$ such that $\alpha + \beta = 1$. Since $\mathfrak{ab} = \mathfrak{a}$, we have $\mathfrak{a} \subseteq \mathfrak{b}$, in particular $\alpha \in \mathfrak{b}$. Then $1 \in \mathfrak{b}$, as wanted. ■

Let R be a commutative ring and M an R-module. Denote by $\mathrm{ann}(M)$ the ideal of annihilators of M in R. If M is a cyclic R-module, then it is (non-canonically) isomorphic[1] to $R/\mathrm{ann}(M)$.

Proposition 3.2 *Let R be a principal ideal commutative ring and M a finitely generated R-module.*

1. *The module M has a submodule isomorphic to $R/\mathrm{ann}(M)$.*
2. *If R is finite and $|M| = |R/\mathrm{ann}(M)|$ then $M \cong R/\mathrm{ann}(M)$.*

[1] Everywhere in this section *isomorphic* means R-isomorphic.

Proof Since R is a principal ideal ring and the module M finitely generated, we have $M \cong \bigoplus_{i=1}^m R/\mathfrak{a}_i$, where $\mathfrak{a}_1, \ldots, \mathfrak{a}_m$ are ideals of R, and $\operatorname{ann}(M) = \bigcap_{i=1}^m \mathfrak{a}_i$. Consider the diagonal embedding

$$R \to \bigoplus_{i=1}^m R/\mathfrak{a}_i, \qquad x \mapsto (x \bmod \mathfrak{a}_1, \ldots, x \bmod \mathfrak{a}_m).$$

Its kernel is $\bigcap_{i=1}^m \mathfrak{a}_i$, which is equal to $\operatorname{ann}(M)$, as we had just seen. Thus, $R/\operatorname{ann}(M)$ faithfully embeds into $\bigoplus_{i=1}^m R/\mathfrak{a}_i$, which proves part 1. Part 2 is an immediate consequence of part 1. ■

Proposition 3.3 *Let R be a direct sum of fields. The we have the following.*

1. *For any ideals $\mathfrak{a}, \mathfrak{b} \trianglelefteq R$ one has $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$. Moreover, for any $c \in \mathfrak{ab}$ there exist $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ such that $c = ab$.*

   In particular, $\mathfrak{a}^2 = \mathfrak{a}$, and for any $a \in \mathfrak{a}$ there exist $a_1, a_2 \in \mathfrak{a}$ such that $a = a_1 a_2$.

2. *Let M a cyclic R-module and M' is a submodule M. Then the ideals $\operatorname{ann}(M')$ and $\operatorname{ann}(M/M')$ are coprime and $\operatorname{ann}(M) = \operatorname{ann}(M')\operatorname{ann}(M/M')$.*

Proof Write $R = \bigoplus_{\alpha \in \mathrm{A}} K_\alpha$, where each K_α is a field. If $\mathrm{A}' \subseteq \mathrm{A}$ then the set

$$\mathcal{I}(\mathrm{A}) := \{(x_\alpha)_{\alpha \in \mathrm{A}} : x_\alpha = 0 \text{ for } \alpha \in \mathrm{A}'\}$$

is an ideal of R, and all ideals are of this form. This implies part 1.

To prove part 2, define $\mathrm{B} \subseteq \mathrm{A}$ from $\operatorname{ann}(M) = \mathcal{I}(\mathrm{B})$. Then $\operatorname{ann}(M') = \mathcal{I}(\mathrm{B}')$, where $\mathrm{B}' \subseteq \mathrm{B}$. Since M is cyclic, we have $M \cong R/\mathcal{I}(\mathrm{B}) \cong \mathcal{I}(\mathrm{A} \setminus \mathrm{B})$, the image of M' in $\mathcal{I}(\mathrm{A} \setminus \mathrm{B})$ being $\mathcal{I}(\mathrm{A} \setminus \mathrm{B}')$. It follows that $\operatorname{ann}(M/M') = \mathcal{I}(\mathrm{B}'')$, where $\mathrm{B}'' = \mathrm{B} \setminus \mathrm{B}'$.

Now, since $\mathrm{B}' \cap \mathrm{B}'' = \varnothing$ and $\mathrm{B}' \cup \mathrm{B}'' = \mathrm{B}$, part 2 follows. ■

Remark 3.4 Let K be a field and G a finite cyclic group of order n, not divisible by the characteristic of K. Then the group ring $K[G]$ is isomorphic to $K[x]/(x^n - 1)$, which is a direct sum of several finite extensions of K. Hence Proposition 3.3 applies to $R = K[G]$.

Proposition 3.5 *Let K be a number field and q a odd prime number unramified in K. Let $\alpha, \beta \in \mathcal{O}_K$ satisfy $\alpha^q \equiv \beta^q \mod q$. Then $\alpha^q \equiv \beta^q \mod q^2$.*

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

Proposition 3.6 *Let R be an integral domain of characteristic 0 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:

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

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 $c_k \equiv (a+b)^k \mod \mathfrak{a}$.

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 3.7 *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

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

whence the result. ■

We conclude this section with one more definition.

Definition 3.8 Let R be a commutative ring and G a finite group. Define the *weight* of $\Theta = \sum_{\sigma \in G} n_\sigma \sigma \in R[G]$ by $w(\Theta) = \sum_{\sigma \in G} n_\sigma$.

The weight function is additive and multiplicative, defining thereby a ring homomorphism $R[G] \stackrel{w}{\to} R$.

4 Overview of the proof

In this section I give a general overview of the proof of Theorem 1.1. Let p and q be distinct odd prime numbers and ζ a primitive p-th root of unity. Put

$$G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}), \qquad K = \mathbb{Q}\left(\zeta + \zeta^{-1}\right), \qquad G^+ = \mathrm{Gal}(K/\mathbb{Q}).$$

Since we mainly deal with multiplicative structures, we write the Galois action exponentially. Say, for $\lambda \in K$ and $\sigma \in G^+$, the σ-image of λ is denoted by λ^σ.

The proof will employ the group ring $\mathbb{F}_q[G^+]$ and various $\mathbb{F}_q[G^+]$-modules. Let

$$\mathcal{N} = \sum_{\sigma \in G^+} \sigma$$

be the "norm" element of $\mathbb{F}_q[G^+]$.

Proposition 4.1 *Let E be the groups of positive units of K. Then E/E^q is a cyclic $\mathbb{F}_q[G^+]$-module, and, in the notation of Section 3, we have*

$$\mathrm{ann}\,(E/E^q) = (\mathcal{N}). \tag{14}$$

Proof Relation (14) is obvious. Further, since $|E/E^q| = |\mathbb{F}_q[G^+]/(\mathcal{N})| = q^{(p-3)/2}$, the $\mathbb{F}_q[G^+]$-module E/E^q cyclic by Proposition 3.2.2. ■

Definition 4.2 We say that $\beta \in \mathcal{O}_K$ is *q-primary* if there exists $\gamma \in \mathcal{O}_K$ such that $\beta \equiv \gamma^q \mod q^2$.

Denote by C and C_q the groups of positive cyclotomic units and of q-primary cyclotomic units of K, respectively. We have three more cyclic $\mathbb{F}_q[G^+]$-modules E/CE^q, C/C_q and $C_q/(C_q \cap E^q)$.

Proposition 4.3 *Assume that*

$$p \not\equiv 1 \mod q. \tag{15}$$

Then the three ideals

$$\mathfrak{a}_1 = \mathrm{ann}\,(E/CE^q), \quad \mathfrak{a}_2 = \mathrm{ann}\,(C/C_q), \quad \mathfrak{a}_3 = \mathrm{ann}\,(C_q/(C_q \cap E^q) \tag{16}$$

are pairwise coprime and satisfy

$$\mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3 = (\mathcal{N}). \tag{17}$$

Proof Notice that $C/C_q \cong CE^q/C_qE^q$ and $C_q/(C_q \cap E^q) \cong C_qE^q/E^q$ as $\mathbb{F}_q[G^+]$-modules. By (15) and Remark 3.4, Proposition 3.3, applies to the group ring $\mathbb{F}_q[G^+]$. Thus, the three annihilators $\operatorname{ann}(E/CE^q)$, $\operatorname{ann}(CE^q/C_qE^q)$ and $\operatorname{ann}(C_qE^q/E^q)$ are pairwise coprime, and

$$\operatorname{ann}(E/CE^q)\operatorname{ann}(CE^q/C_qE^q)\operatorname{ann}(C_qE^q/E^q) = \operatorname{ann}(E/E^q) = (\mathcal{N}),$$

as wanted. ■

Definition 4.4 For $\gamma \in K^*$ and $\Theta \in \mathbb{F}_q[G^+]$ 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^*. The same convention applies to γ^Θ with $\gamma \in \mathbb{Q}(\zeta)^*$ and $\Theta \in \mathbb{F}_q[G]$.

Call $\Theta \in \mathbb{F}_q[G^+]$ *balanced* if $w(\Theta) = 0$ (see Definition 3.8). Mihăilescu proves the following three theorems.

Theorem 4.5 *Let x, y, p, q be a solution of the Catalan equation (1). Then for any balanced $\Theta \in \mathfrak{a}_1\mathfrak{a}_3$ we have*

$$\big((x-\zeta)(x-\bar{\zeta})\big)^\Theta \in (K^*)^q\,. \tag{18}$$

Theorem 4.6 *Let x, y, p, q be a solution of the Catalan equation with $q \geq 7$. If for a balanced $\Theta \in \mathbb{F}_q[G^+]$ we have $\big((x-\zeta)(x-\bar{\zeta})\big)^\Theta \in (K^*)^q$, then $\Theta = 0$.*

Theorem 4.7 *If $p > q$ then $C_q \neq C$.*

Proof of Theorem 1.1 (assuming Theorems 4.5, 4.6 and 4.7) 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 (10). Thus, the asumptions of Theorems 4.5–4.7 are verified.

Theorems 4.5 and 4.6 together imply that the product $\mathfrak{a}_1\mathfrak{a}_3$ contains no non-zero balanced elements. It follows that

$$\mathfrak{a}_1\mathfrak{a}_3 = (\mathcal{N}). \tag{19}$$

Indeed, fix $\Theta \in \mathfrak{a}_1\mathfrak{a}_3$. Since $(p-1, q) = 1$ by (13), we may find $r \in \mathbb{F}_q$ such that $r(p-1)/2 = w(\Theta)$. Then $\Theta - r\mathcal{N}$ is balanced, which implies that $\Theta = r\mathcal{N}$, proving (19).

Now (17), (19) and Proposition 3.1 imply that $\mathfrak{a}_2 = (1)$, that is, $C = C_q$. This is, however, impossible by Theorem 4.7. ■

Theorems 4.5, 4.6 and 4.7 are proved in the next three sections.

5 Proof of Theorem 4.5

Thus, let (x, y, p, q) be a solution of (1). Recall that

$$p \not\equiv 1 \mod q \tag{20}$$

by (13). Our starting point is the following fundamental theorem of Thaine [15]. (See also [17, Theorem 15.2].) Denote by H the ideal class group of the field K.

Theorem 5.1 (Thaine) *Let $\widetilde{\Theta} \in \mathbb{Z}[G^+]$ annihilate the q-part[2] of the group E/C. Then Θ annihilates the q-part of H as well.*

Thaine's result is more general and holds for any real abelian field K, provided q does not divide the degree $[K\colon \mathbb{Q}]$. In our case $[K\colon \mathbb{Q}] = (p-1)/2$, and the required condition is ensured by (20).

We apply Thaine's theorem in the following weaker form.

Proposition 5.2 *Any $\Theta \in \mathfrak{a}_1$ 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 3.3.1, there exist $\Theta_1, \ldots, \Theta_m \in \mathfrak{a}_1$ such that $\Theta_1 \cdots \Theta_m = \Theta$.

Pick liftings $\widetilde{\Theta}_1, \ldots, \widetilde{\Theta}_m$ for $\Theta_1, \ldots, \Theta_m$ and put $\widetilde{\Theta} = \widetilde{\Theta}_1 \cdots \widetilde{\Theta}_m$. 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. ■

Proposition 5.3 *For any $\Theta \in \mathfrak{a}_1$ we have*

$$\left(\frac{(x-\zeta)\,(x-\bar{\zeta})}{(1-\zeta)\,(1-\bar{\zeta})} \right)^{\Theta} \in E \cdot (K^*)^q\,. \tag{21}$$

Proof Relation (4) can be rewritten as

$$\prod_{k=1}^{(p-1)/2} \frac{(x-\zeta^k)\,(x-\bar{\zeta}^k)}{(1-\zeta^k)\,(1-\bar{\zeta}^k)} = v^q. \tag{22}$$

Since $(x,p) = 1$ by (3), the factors in the left-hand side of (22) are co-prime. It follows that the corresponding principal ideals are q-th powers of ideals of K. In particular, there exists an ideal $\mathfrak{A}$ of K such that

$$\left(\frac{(x-\zeta)\,(x-\bar{\zeta})}{(1-\zeta)\,(1-\bar{\zeta})} \right) = \mathfrak{A}^q. \tag{23}$$

The class of the ideal $\mathfrak{A}$ belongs to the q-part of the class group.

Since the statement of the proposition does not depend on the choice of the lifting $\widetilde{\Theta}$ used to define[3] the left-hand side of (21), 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. Such a lifting exists by Proposition 5.2. Then $\mathfrak{A}^{\widetilde{\Theta}}$ is a principal ideal; write $\mathfrak{A}^{\widetilde{\Theta}} = (\alpha)$. We obtain the equality

$$\left(\left(\frac{(x-\zeta)\,(x-\bar{\zeta})}{(1-\zeta)\,(1-\bar{\zeta})} \right)^{\widetilde{\Theta}} \right) = (\alpha)^q,$$

of principal ideals, whence the result. ■

Denote by $\mathfrak{b}$ the ideal of balanced elements of $\mathbb{F}_q[G^+]$:

$$\mathfrak{b} = \left\{ \Theta \in \mathbb{F}_q[G^+] : w(\Theta) = 0 \right\}. \tag{24}$$

Recall that C_q is the group of q-primary cyclotomic units (cf. Definition 4.2).

Proposition 5.4 *For any $\Theta \in \mathfrak{a}_1 \cap \mathfrak{b}$ we have $\left((x-\zeta)\,(x-\bar{\zeta})\right)^{\Theta} \in C_q \cdot (K^*)^q$.*

[2] that is, the q-Sylow subgroup

[3] cf. Definition 4.4

Proof By Proposition 3.3.1 we have $\Theta = \Theta_1\Theta_2$ with $\Theta_1, \Theta_2 \in \mathfrak{a}_1 \cap \mathfrak{b}$. Proposition 5.3 implies that

$$\left(\frac{(x-\zeta)\left(x-\bar{\zeta}\right)}{(1-\zeta)\left(1-\bar{\zeta}\right)}\right)^{\Theta_1} \in E \cdot (K^*)^q\,. \tag{25}$$

Since $\Theta_1 \in \mathfrak{b}$, we have

$$\left((1-\zeta)\left(1-\bar{\zeta}\right)\right)^{\Theta_1} \in E \cdot (K^*)^q\,. \tag{26}$$

(In fact, we even have $\left((1-\zeta)\left(1-\bar{\zeta}\right)\right)^{\Theta_1} \in C \cdot (K^*)^q$, but we do not need this more precise statement.) Combining (25) and (26), we obtain $\left((x-\zeta)\left(x-\bar{\zeta}\right)\right)^{\Theta_1} \in E \cdot (K^*)^q$.

Now, since $\Theta_2 \in \mathfrak{a}_1 = \mathrm{ann}(E/CE^q)$, we have

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

Write

$$\left((x-\zeta)\left(x-\bar{\zeta}\right)\right)^{\Theta} = \eta\alpha^q \tag{27}$$

with $\eta \in C$ and $\alpha \in K^*$. The left-hand side of (27) is congruent to 1 mod q^2, as follows from (12). Hence η is q-primary, and the proposition follows. ■

We are ready to prove Theorem 4.5. Let $\Theta \in (\mathfrak{a}_1\mathfrak{a}_3) \cap \mathfrak{b}$. By Proposition 3.3.1 we have $\Theta = \Theta_1\Theta_2$ with $\Theta_1 \in \mathfrak{a}_1 \cap \mathfrak{b}$ and $\Theta_2 \in \mathfrak{a}_3$. Now $\left((x-\zeta)\left(x-\bar{\zeta}\right)\right)^{\Theta_1} \in C_q \cdot (K^*)^q$ by Proposition 5.4, and ${C_q}^{\Theta_2} \subset (K^*)^q$ because $\Theta_2 \in \mathfrak{a}_3 = \mathrm{ann}\,(C_q/(C_q \cap E^q))$. Theorem 4.5 is proved.

6 Proof of Theorem 4.6

6.1 A reformulation

In this subsection we slightly reformulate Theorem 4.6 to make more convenient to deal with. First of all, it is more practical to work with the field $\mathbb{Q}(\zeta)$ and the group G.

Definition 6.1.1 An element $\Theta = \sum_{\sigma\in G} n_\sigma \sigma$ of $\mathbb{F}_q[G]$ or of $\mathbb{Z}[G]$ is called *even* if for any $\sigma \in G$ we have $n_\sigma = n_{\bar{\sigma}}$, where $\bar{\sigma}$ denotes the complex conjugation of σ.

Equivalently, Θ is even if it is divisible by $1+\iota$, where ι is the complex conjugation. If Θ is even, then so is $\sigma\Theta$ for any $\sigma \in G$.

Theorem 4.6 is plainly equivalent to the following statement.

Theorem 4.6′ *Let x, y, p, q be a solution of the Catalan equation with $q \geq 7$. Let Θ be a balanced even element of $\mathbb{F}_q[G]$ such that $(x-\zeta)^\Theta$ is a q-th power in $\mathbb{Q}(\zeta)$. Then $\Theta = 0$.*

Next, we have to select the most suitable lifting of Θ to $\mathbb{Z}[G]$. Since $(x-\zeta)^{-\Theta}$ is a q-th power as soon as $(x-\zeta)^\Theta$ is, we may choose between lifting Θ and $-\Theta$. Beforehand, one more definition.

Definition 6.1.2 We say that $\Theta = \sum_{\sigma\in G} n_\sigma\sigma \in \mathbb{Z}[G]$ is *positive* if $n_\sigma \geq 0$ for any $\sigma \in G$.

Notice that, with this definition, 0 is a positive element of $\mathbb{Z}[G]$.

Proposition 6.1.3 *Assume that λ^Θ is a q-th power for some $\lambda \in \mathbb{Q}[\zeta]$ and a non-zero $\Theta \in \mathbb{F}_q[G]$. Then there exists a non-zero positive $\widetilde{\Theta} \in \mathbb{Z}[G]$ such that $\lambda^{\widetilde{\Theta}}$ is a q-th power and $w(\widetilde{\Theta}) \leq q(p-1)/2$. If Θ is balanced then $q|w(\widetilde{\Theta})$. If Θ is even then so is $\widetilde{\Theta}$.*

Proof Let $\widetilde{\Theta}_1$ be the smallest positive lifting of Θ. That is, $\widetilde{\Theta}_1 = \sum_{\sigma\in G} \widetilde{n}_\sigma \sigma$ with $\widetilde{n}_\sigma \in \{0, 1, \dots, q-1\}$. Let $\widetilde{\Theta}_2$ be the similar lifting of $-\Theta$, so that $\widetilde{\Theta}_1 + \widetilde{\Theta}_2 = q\sum_{\sigma\in G}\sigma$. 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 balanced.

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 4.6 and 4.6′ are equivalent to the following statement.

Theorem 4.6″ *Let x, y, p, q be a solution of the Catalan equation with $q \geq 7$. Let Θ be a 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 $\mathbb{Q}(\zeta)$. Then $q|\Theta$.*

This theorem will be proved in Subsection 6.3, after some preparations in Subsection 6.2.

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

In this section we investigate the properties of a special power series introduced by Mihăilescu. Everywere 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 a 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

$$(1-\zeta T)^{\Theta/q} = \prod_{\sigma\in G} (1-\zeta^\sigma T)^{n_\sigma/q}. \tag{28}$$

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

$$(1-\zeta T)^{\Theta/q} = \sum_{k=0}^\infty \alpha_k(\Theta) T^k, \tag{29}$$

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

Proposition 6.2.1 *Let $\Theta \in \mathbb{Z}[G]$ be positive. Then for $|z|<1$ one has*

$$\left|(1-\zeta z)^{\Theta/q} - S_m(z)\right| \leq \binom{w(\Theta)/q+m+1}{m+1} (1-|z|)^{-w(\Theta)/q-m-1}|z|^{m+1}. \tag{30}$$

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:

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

as wanted. ■

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

Proposition 6.2.2 *The coefficients $\alpha_0(\Theta), \alpha_1(\Theta), \ldots$ of Mihăilescu's series $(1-\zeta T)^{\Theta/q}$ are q-integers. Write*

$$(1-\zeta T)^{\Theta/q} = \sum_{k=0}^{\infty} \frac{a_k(\Theta)}{q^k k!} T^k, \tag{31}$$

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

$$a_k(\Theta) \in \mathbb{Z}(\zeta) \quad \textit{and} \quad a_k(\Theta) \equiv \left(-\sum_{\sigma \in G} n_\sigma \zeta^\sigma \right)^k \mod q \qquad (k = 0, 1, \ldots). \tag{32}$$

Proof As follows from Proposition 3.7, 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 $(1-\zeta T)^{\Theta/q}$.

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

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

Now, applying Proposition 3.6 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 (32). ■

We arrived to the most delicate part of Mihăilescu's argument. The G-action extends to the ring of power series $\mathbb{Q}(\zeta)[T]$ 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"

$$\left((1-\zeta T)^{\Theta/q}\right)^\sigma = (1-\zeta T)^{\sigma\Theta/q}. \tag{33}$$

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

$$\left((1-\zeta t)^{\Theta/q}\right)^\sigma = (1-\zeta t)^{\sigma\Theta/q}. \tag{34}$$

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

Nevertheless, under some additional assumptions (34) may hold.

Proposition 6.2.3 *Assume that Θ is even (See Definition 6.1.1). Let $t \in \mathbb{Q}$ sarisfy $|t| < 1$, and assume that $(1-\zeta t)^{\Theta/q} \in \mathbb{Q}(\zeta)$. Then (34) 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 $\mathbb{Q}(\zeta + \zeta^{-1})$, which implies that $\alpha^\sigma \in \mathbb{R}$ for any $\sigma \in G$.

Now fix $\sigma \in G$. As we have seen after Definition 6.1.1, $\sigma\Theta$ 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. ■

6.3 Proof of Theorem 4.6″

6.3.1 The number $(1-\zeta/x)^{\Theta/q}$

By the assumption, $w(\Theta) = mq$, where $m \in \mathbb{Z}$ satisfies

$$0 \le m \le (p-1)/2. \tag{35}$$

Since $(x-\zeta)^{\Theta}$ is a q-th power in $\mathbb{Q}(\zeta)$, so is $x^{-mq}(x-\zeta)^{\Theta} = (1-\zeta/x)^{\Theta}$. (It is here where the assumtion $q|w(\Theta)$ is used!) It follows that

$$(1-\zeta/x)^{\Theta/q} \in \mathbb{Q}(\zeta),$$

where $(1-\zeta/x)^{\Theta/q}$ is defined as the sum of Mihăilescu series

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

at $T = 1/x$. Proposition 6.2.3 implies that

$$\left((1-\zeta/x)^{\Theta/q}\right)^{\sigma} = (1-\zeta/x)^{\sigma\Theta/q} \qquad (\sigma \in G). \tag{36}$$

6.3.2 The polynomial $P(T)$

For $k = 1, 2, \ldots$ put $E(k) = k + \mathrm{ord}_q(k!)$. Then

$$E(k+1) \ge E(k) + 1, \tag{37}$$

$$E(k) \le kq/(q-1). \tag{38}$$

Consider the polynomial

$$P(T) = q^{E(m)} \left(\alpha_0(\Theta) T^m + \alpha_1(\Theta) T^{m-1} + \cdots + \alpha_m(\Theta)\right). \tag{39}$$

Proposition 6.2.2 implies that the coefficients of the Mihăilescu series satisfy $q^{E(k)}\alpha_k(\Theta) \in \mathbb{Z}[\zeta]$. It follows that $P(T) \in \mathbb{Z}[\zeta][T]$, and (37) implies that

$$P(T) \in q^{E(m)}\alpha_m(\Theta) + q\mathbb{Z}[\zeta][T]. \tag{40}$$

Also, (33) implies that for $\sigma \in G$

$$P^{\sigma}(T) = q^{E(m)} \left(\alpha_0(\sigma\Theta) T^m + \alpha_1(\sigma\Theta) T^{m-1} + \cdots + \alpha_m(\sigma\Theta)\right). \tag{41}$$

6.3.3 The number β and its conjugates

Since Θ is positive, the number $x^m (1-\zeta/x)^{\Theta/q}$ is an algebraic integer. Hence so is

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

Relations (36) and (41) imply that

$$\beta^{\sigma} = q^{E(m)} x^m \left((1-\zeta/x)^{\sigma\Theta/q} - \sum_{k=0}^{m} \alpha_k(\sigma\Theta) x^{-k}\right) \qquad (\sigma \in G). \tag{42}$$

Now estimate $|\beta^{\sigma}|$ using Proposition 6.2.1 (with $\sigma\Theta$ instead of Θ). We obtain

$$|\beta^{\sigma}| \le q^{E(m)} \binom{2m+1}{m+1} \left(1 - |x|^{-1}\right)^{-2m-1} |x|^{-1} = A|x|^{-1}. \tag{43}$$

Next, we are going to apply Proposition 2.2. The assumption $p \not\equiv 1 \mod q$ is satisfied by (13), and so we have $|x| \geq q^{p-1} - q \geq 42$ (recall that $q \geq 7$).

Now, using (38), estimating $\binom{2m+1}{m+1} \leq 2^{2m+1}$ and using that $|x| \geq 42$, we obtain $A < q^{mq/(q-1)} 2.05^{2m+1}$. Further, $m \leq (p-1)/2$ by (35), and we obtain

$$A < \left(2.05 q^{7/12}\right)^{p-1} < q^{p-1} - q$$

(we again use the assumption $q \geq 7$). 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 $\beta = 0$.

6.3.4 Finishing the proof

Thus, $P(x) = q^{E(m)} x^m \left(1 - \zeta/x\right)^{\Theta/q}$. Since $x^m \left(1 - \zeta/x\right)^{\Theta/q}$ is an algebraic integer, (40) implies that

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

By Proposition 6.2.2, this is possible only if $q \left| \left(\sum_{\sigma \in G} n_\sigma \zeta^\sigma\right)^m \right.$. Since q is unramified in $\mathbb{Q}(\zeta)$, this implies that $q \left| \sum_{\sigma \in G} n_\sigma \zeta^\sigma \right.$, that is, $q | n_\sigma$ for all $\sigma \in G$. Thus, $q | \Theta$, and this completes the proof of Theorem 4.6″.

7 Proof of Theorem 4.7

To begin with, introduce the polynomial

$$f(T) = \left((1+T)^q - 1 - T^q\right)/q \in \mathbb{Z}[T]. \tag{44}$$

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

Let $\widetilde{C}$ be the group of all cyclotomic units of the field $\mathbb{Q}(\zeta)$, that is, the group generated by ± 1 and the units of the form $(1-\zeta^k)/(1-\zeta)$. It is a product of the group C of positive cyclotomic units and the finite group generated by $-\zeta$.

Assume now that all elements of C are q-primary. Since $-\zeta$ is a q-th power in $\mathbb{Z}[\zeta]$, all elements of $\widetilde{C}$ are q-primary in the ring $\mathbb{Z}[\zeta]$.

In particular, so is $1 + \zeta^q = (1-\zeta^{2q})/(1-\zeta^q)$. Thus, there exists $\nu \in \mathbb{Z}[\zeta]$ such that $1 + \zeta^q \equiv \nu^q \mod q^2$. Then $(1+\zeta)^q \equiv 1 + \zeta^q \equiv \nu^q \mod q$. Proposition 3.5 implies that $(1+\zeta)^q \equiv \nu^q \mod q^2$.

Thus, $(1+\zeta)^q \equiv 1 + \zeta^q \mod q^2$ This can be rewritten as $f(\zeta) \equiv 0 \mod q$, where $f(T)$ is the polynomial defined in (44).

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

$$f\left(\zeta^\sigma\right) \equiv 0 \mod \mathfrak{q} \qquad (\sigma \in G). \tag{45}$$

Since $\zeta^\sigma \not\equiv \zeta^\tau \mod \mathfrak{q}$ for distinct $\sigma, \tau \in G$, congruences (45) imply that

$$p - 1 \leq \deg f = q - 1,$$

which contradicts our assumption $p > q$. The theorem is proved.

References

[1] 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.

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

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

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

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

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

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

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

[9] M. Mignotte Catalan's equation just before 2000, *Proceedings Inkeri Colloqium, Turku (2000)*, Eds. Jutila and Metsänkylä, to appear.

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

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

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

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

[14] P. Ribenboim, *Catalan's Conjecture*, Acad. Press, Boston, 1994.

[15] F. Thaine, On the ideal class groups of real abelian number fields, *Ann. of Math.* **128** (1988), 1–18.

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

[17] L. Wasington, *Introduction to cyclotomic fields*, second addition, Graduate Texts in Math. **83**, Springer, New York, 1997.