Bulletin of the *Transilvania* University of Braşov
Series III: Mathematics and Computer Science, Vol. 5(67), No. 1 - 2025, 161-172
https://doi.org/10.31926/but.mif.2025.5.67.1.12

AN ALTERNATIVE PROOF OF THE CATALAN CONJECTURE

Chang LIU [1] **and Preda MIHĂILESCU**[*,2]

Abstract

The original proof [5] of Catalan's conjecture uses real binomial power series expansions and annihilation of real class groups, based on a Theorem of Thaine. In this paper we provide a simplified approach to this proof, which uses Stickelberger annihilation of the minus part of the class group, and thus does not require the Theorem of Thaine. The approach is based on proving the existence of a character connecting *Galois exponents* of roots of unity.

2020 Mathematics Subject Classification: 11D61, 11R18, 11R27, 11D41
Key words: proof of celebrated Catalan's equation; cyclotomic units

1 Introduction

Catalan's equation is

$$X^m - Y^n = 1; \quad X, Y \in \mathbb{N}; m, n \geq 2, \tag{1}$$

and it was proved to have no solutions except for $(X, Y, m, n) = (3, 2, 2, 3)$, [5]. We recommend the reader interested in more historical details about the progress towards the proof of this fact, to read the books like [9], [1] or [8] written on the subject.

The purpose of the present paper is to provide a new proof of the above fact, based on a simplification brought to the arguments in [5]. First, we shall consider integer solutions $X, Y \in \mathbb{Z}$, and due to early results – see [8] – we may assume that $m, n > 3$ in (1). It will thus suffice to show that the equation

$$x^p - y^q = 1; \quad \text{with primes } p, q > 3 \text{ and integers } x, y \in \mathbb{Z} \setminus \{0, \pm 1\} \tag{2}$$

[1]Mathematisches Institut der Universität Göttingen, e-mail: chang.liu@mathematik.uni-goettingen.de
[2*] *Corresponding author*, Mathematisches Institut der Universität Göttingen, e-mail: Preda@uni-math.gwdg.de

has no solutions. Allowing integers solutions has the advantage that if $(x, y; p, q)$ is a solution to (2), then so is $(-y, -x, q, p)$: if there is a solution to the pair (p, q) of exponents, there is one also for the exponents in switched order, (q, p). This remark allows us to impose the condition $q > p$, without restriction of generality.

The work of Cassels [2] allows one to assume that if there are solutions to (2), then the following necessary conditions hold, among others:

$$\frac{x^p - 1}{x - 1} = pz^q; \quad x - 1 = p^{q-1}b^q \quad y = pbz. \tag{3}$$

We shall show that (3) has no solutions with $x \in \mathbb{Z} \setminus \{0, \pm 1\}$, and odd primes $p, q > 3$. With this, we prove:

Theorem 1. *The equation (3) has non non-trivial solutions with $q > p > 3$.*

By the above, this implies the truth of the Catalan Conjecture, thus offering a new proof of the same.

1.1 Notations and overview of the approach

Let $\mathbb{K} = \mathbb{Q}[\zeta_p] = \mathbb{Q}[\zeta] = \mathbb{Q}[X]/(\Phi_p(X))$ be the $p-$th cyclotomic extension with, $\Phi_p(X) = \frac{X^p-1}{X-1}$, the $p-$th cyclotomic polynomial and ζ, a root thereof. Denote by $G = \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ the Galois group of $\mathbb{K}/\mathbb{Q}$ and let the automorphisms $\sigma_c \in G : \zeta \mapsto \zeta^c$, for $c \in P := \{1, 2, 3, \ldots, p-1\}$. We write, in multiplicative notation, $a^\sigma = \sigma(a)$ for all $a \in \mathbb{K}$ and $\sigma \in G$. We let $\jmath \in G$ be the complex conjugation and $\lambda = (1 - \zeta)$ which is an algebraic integer generating the unique ramified prime ideal above p in $\mathbb{K}$. Denote by $\boldsymbol{\mu_n} = \{z \in \mathbb{C} \mid z^n = 1\}$ the group of $n-$th root of unity.

The fractional and principal ideals of $\mathbb{K}$ are $\mathcal{F}(\mathbb{K}), \mathcal{P}(\mathbb{K})$, respectively and the class group is $\mathcal{C}(\mathbb{K}) = \mathcal{F}/\mathcal{P}$. The Stickelberger Ideal $I \subset \mathbb{Z}[G]$ annihilates the class group. Assuming x, z is a non trivial solution to (3), we show that the G-orbit of $\alpha := \frac{x-1}{1-\zeta} \in \mathbb{Z}[\zeta]$ is built of mutually coprime algebraic integers and the ideal $\mathfrak{A} = (\alpha, z)$ has order dividing q. By applying some $\theta \in I$ to $\mathfrak{A}$ we obtain identities of the type

$$(\beta/\overline{\beta})^q = \left(\frac{1 - \zeta/x}{1 - \bar{\zeta}/x}\right)^\theta,$$

with $\beta \in \mathbb{Z}[\zeta]$ being an integral element that depends on x and θ. If $G_\theta \in \mathbb{K}[[T]]$ is the formal binomial series $G_\theta(T) = (1 + \zeta T)^{\theta/q}$, it is absolutely convergent for $|T| < 1$, in particular at $T = -1/x$. Fixing some primitive $q-$th root of unity $\xi \in \mathbb{C}$, there is thus a *Galois exponent* $\kappa(\theta) \in \mathbb{Z}/(q \cdot \mathbb{Z})$, such that

$$\beta/\overline{\beta} = \xi^{\kappa(\theta)} G_{\theta(1-\jmath)}(-1/x).$$

The key result of this paper is the following

Proposition 1. *Notations being like above, for each $\theta \in I$, either $\kappa(\sigma\theta) = 0$ for all $\sigma \in G$, or else there is a character $\chi = \chi_\theta : G \to \mathbb{F}_q^\times$ such that*

$$\kappa(\sigma\theta) = \chi(\sigma) \cdot \kappa(\theta), \quad \forall \sigma \in G. \tag{4}$$

Using this result, we may produce some simple $\theta \in I$ such that $\kappa(\sigma\theta) = 0$ for all $\sigma \in G$. Some simple, non vanishing linear combinations of conjugates of $\beta(\theta)$ can be defined, which have vanishing leading terms in their power series developments. This leads to the strong upper bound on $|x| < 2$, that confirm the Theorem 1.

2 Cyclotomy, classical and elementary facts.

We assume in the sequel that (x, z) is a solution to equation (3), for the prime exponents $p < q$. We note the following relation between x and z:

Lemma 1. *Let (x, y, p, q) be a solution to equation (2) with $p < q$, $a(p-1) = q-1$ where $a > 1$ is a positive real number and z is defined as in equation (3). Then $|x| > |z|^a$.*

Proof. Consider equation (3),

$$pz^{q-1} < p|z|^q = |\frac{x^p - 1}{x - 1}| = |x^{p-1} + x^{p-2} + \cdots + 1| < px^{p-1},$$

therefore, $|z^a| < |x|$. □

2.1 Characteristic numbers and characteristic ideals

Lemma 2. *Let $\alpha = \frac{x-\zeta}{1-\zeta}$ and $\mathfrak{A} = (\alpha, z)$: the* characteristic number and ideal*, respectively.*

1. *Then $\alpha \in \mathbb{Z}[\zeta]; \alpha \equiv 1 \bmod \lambda^2$.*
2. *The conjugates of the characteristic number are mutually coprime:*

$$(\sigma_c(\alpha), \sigma_d(\alpha)) = (1), \quad \textit{for } 1 \leq c < d \leq p-1$$

3. *The conjugates of the* characteristic ideal $\mathfrak{A}$ *are mutually coprime and*

$$\mathfrak{A}^q \;=\; (\alpha), \quad \textit{and } \mathbf{N}_{\mathbb{K}/\mathbb{Q}}(\mathfrak{A}) = (z). \tag{5}$$

Proof. For point 1: since $p = \prod_{i=1}^{p-1}(1 - \zeta^i)$ and $p|(x-1)$, $(1-\zeta)|(x-1+1-\zeta)$, so $\alpha = 1 + \frac{x-1}{1-\zeta} \equiv 1 \bmod \lambda^2$ is integral and verifies the claimed congruence.

For point 2, let $I(c,d) = (\sigma_c(\alpha), \sigma_d(\alpha)) = (\frac{x-\zeta^c}{1-\zeta^c}, \frac{x-\zeta^d}{1-\zeta^d})$. We note that for any integers k and j not divisible by p, the number $\frac{1-\zeta^k}{1-\zeta^j}$ is a cyclotomic unit of the field $\mathbb{K}$ – e.g. [10], Proposition 8.1. Therefore, $\frac{x-\zeta^c}{1-\zeta^c} \cdot \frac{1-\zeta^c}{1-\zeta^d} = \frac{x-\zeta^c}{1-\zeta^d} \in I(c,d)$. Then $\frac{\zeta^c-\zeta^d}{1-\zeta^d} \in I(c,d)$. The ideal $I(c,d)$ thus contains a unit and it must be $I = (1)$.

For point 3, $z^q = \prod_{c\in P} \sigma_c(\alpha)$ by equation (3), so $\alpha | z^q$, and $z^q/\alpha = \prod_{c\in P, \sigma_c \neq \sigma_{id}} \sigma_c(\alpha)$. Hence, by point 2, we know $(\alpha, z^q/\alpha) = (1)$. For the characteristic ideal, this implies:

$$\mathfrak{A}^q = \big(\alpha^q, \alpha^{q-1}z, \ldots, \alpha z^{q-1}, \alpha \cdot (z^q/\alpha)\big) = (\alpha) \cdot (\alpha^{q-1}, \ldots, z^{q-1}, z^q/\alpha) = (\alpha),$$

hence $\mathfrak{A}^q = (\alpha)$ which means that the characteristic ideal is either principal or has order q. $\mathbf{N}(\mathfrak{A}) = \prod_{c\in P}(\alpha^{\sigma_c}, z) = (\mathbf{N}(\alpha), z, z^2, \ldots, z^{p-1})$ by point 2. Since $\mathbf{N}(\alpha) = z^q$, we get the relation $\mathbf{N}(\mathfrak{A}) = (z)$. □

2.2 The Stickelberger's ideal

As mentioned above, the Stickelberger ideal is a subideal of the group ring $\mathbb{Z}[G]$ with the property of annihilating the class group. It is defined as the intersection of a fractional, principal ideal, with $\mathbb{Z}[G]$, as follows:

Definition 1. *The* Stickelberger element *is defined by*

$$\vartheta = \frac{1}{p}\sum_{c=1}^{p-1} c\sigma_c^{-1} \in \frac{1}{p}\mathbb{Z}[G] \tag{6}$$

and Stickelberger's ideal is defined as

$$I = \vartheta\mathbb{Z}[G] \cap \mathbb{Z}[G]. \tag{7}$$

We note that $\mathbf{N} = \mathbf{N}_{\mathbb{K}/\mathbb{Q}} \in I$ *and* $I \subset (1-\jmath)\mathbb{Z}[G] \oplus (\mathbf{N})$. *There exists a base for* $I^- = (1-\jmath)I$ *made of* $(p-1)/2$ *elements, called* Fueter elements, *e.g. [6], which are*

$$\psi_n = \vartheta(1+\sigma_n - \sigma_{n+1}) = \sum_{c\in S_n} n_c\sigma_c^{-1} \in \mathbb{Z}_{\geq 0}[G], \text{for } n \in \left\{1, 2, \ldots, \frac{p-1}{2}\right\} \tag{8}$$

$$\text{with} \quad n_c = \left(\left[\frac{(n+1)c}{p}\right] - \left[\frac{nc}{p}\right]\right)$$

$$\text{and} \quad n_c + n_{p-c} = 1, \tag{9}$$

From $n_c + n_{p-c} = 1$ *and* $n_c \geq 0$, *we note* $n_c = 0$ *or* $n_c = 1$, *and* $(1+\jmath)\cdot\psi_n = \mathbf{N}_{\mathbb{K}/\mathbb{Q}}$, *which means for every ideal* $\mathfrak{P} \subset \mathbb{Z}[\zeta]$, $\mathfrak{P}^{(1+\jmath)\cdot\psi_n} = \mathbf{N}(\mathfrak{P})$.

We define $I^+ := \vartheta\mathbb{Z}[G] \cap \mathbb{Z}_+[G]$. *Combining the property of Stickelberger's ideal and the property of Fueter elements, we note that for every ideal* $\mathfrak{P} \subset \mathbb{Z}[\zeta]$ *and each* $\theta \in I^+$, *the ideal* $\mathfrak{P}^\theta \subset \mathbb{Z}[\zeta]$ *is generated by some* $\gamma \in \mathbb{Z}[\zeta]$, *which satisfies* $\gamma\cdot\overline{\gamma} = \mathbf{N}(\mathfrak{P})^{\varsigma_\theta}$, *for an integer* $\varsigma_\theta \in \mathbb{Z}$, *which we call the* relative weight *of* θ. *Note that the relative weight of each Fueter element is* 1. *Furthermore, we denote by* the absolute weight *of* $\theta = \sum_{c\in P^*} n_c\sigma_c^{-1} \in \mathbb{Z}[G]$ *the sum* $w(\theta) = \sum_c |n_c|$.

We define the Fermat quotient map $\phi : \mathbb{Z}[G] \to \mathbb{F}_p$ *such that* $\zeta^\theta = \zeta^{\phi(\theta)}$. *Explicitly,*

$$\phi\left(\sum_{c\in P^*} n_c\sigma_c^{-1}\right) = \sum_{c\in P^*} n_c/c \in \mathbb{F}_p. \tag{10}$$

We identify the value $\phi(\theta) \in \mathbb{F}_p$ *with its natural lift to* $\mathbb{N}$, *under the least non-negative remainder representation of* $\mathbb{F}_p$. *The* Fermat ideal *is* $I_0 = I \cap Ker\,(\phi)$: *this is the module of all Stickelberger elements* θ *such that* $\zeta^\theta = 1$.

We note the following useful property of the action of I on λ:

Lemma 3. *Let $M_\mu := (1-\zeta)^\mu$, for some $\mu \in I$, then $M_\mu = \pi^{\varsigma(\mu)} \cdot (\zeta)^{\phi(\mu)/2}$, where $\mathbb{Q}(\pi) \in \mathbb{K}$ is the quadratic subfield of $\mathbb{K}$ and $\pi^2 = p \cdot \left(\frac{-1}{p}\right)$.*[3] *Moreover, $M_\mu^{\sigma-1} = \pm\zeta^{(\sigma-1)\phi(\mu)/2} \in \mu_{2p}$, for $\sigma \in G$.*

Proof. Since $\mathbf{N}_{\mathbb{K}/\mathbb{Q}}(1-\zeta) = p$, then $M_\mu \cdot \overline{M_\mu} = (1-\zeta)^{\mu(1+\jmath)} = p^{\varsigma(\mu)}$. Furthermore, $M_\mu/\overline{M_\mu} = (\frac{1-\zeta}{1-\zeta})^\mu = (-\zeta)^\mu$ and from the definition of the Fermat quotient map ϕ, $\zeta^\theta = \zeta^{\phi(\theta)}$, then it is equal to $\left(\frac{-1}{p}\right)^{\varsigma(\mu)} \zeta^{\phi(\mu)}$, so $M_\mu^2 = p^{\varsigma(\mu)} \cdot \left(\frac{-1}{p}\right)^{\varsigma(\mu)} \cdot \zeta^{\phi(\mu)}$. Hence, $M_\mu = \pi^{\varsigma(\mu)} \cdot \zeta^{\phi(\mu)/2}$. The last statement follows from $\sigma_c(\pi) = \left(\frac{c}{p}\right)\pi$. □

2.2.1 The β_0-map

Stickelberger's theorem implies that for $\theta \in I$, there is a principal ideal $\mathfrak{a}(\theta) = \mathfrak{A}^\theta$, and the principal ideal arising from the action of the elements from Stickelberger ideal is generated by Jacobi numbers, which are products of Jacobi sums[6]. The product of Jacobi numbers by their complex conjugates are rational integers, which are equal to the norm of $\mathfrak{A}$ raised to the relative weight of θ , i.e. $|\mathbb{Z}[\zeta]/\mathfrak{A}|^{\varsigma_\theta} = |z|^{\varsigma_\theta}$.

Iwasawa proved in [4] that every Jacobi number $\mathbf{J}$ verifies

$$\mathbf{J} \equiv 1 \bmod (1-\zeta)^2, \tag{11}$$

Let $\beta_0 \in \mathfrak{J}(\theta)$ be the Jacobi number that generates the ideal. By the identity $(\alpha^\theta) = \mathfrak{A}^{q\theta} = \mathfrak{P}^q$, we obtain

$$\alpha^\theta = \eta \cdot \beta_0^q, \tag{12}$$

where η is a unit in $\mathbb{Z}[\zeta]$. Multiplying their complex conjugates on both sides of equation (12) and since

$$\alpha^{\theta(1+\jmath)} = \mathbf{N}_{\mathbb{K}/\mathbb{Q}}(\alpha)^{\varsigma_\theta} = z^{q\varsigma_\theta} = \beta_0^{q(1+\jmath)}$$

we get $\eta \cdot \bar{\eta} = 1$. It follows from Kronecker's Unit Theorem, that $\eta \in \mu_{2p}$. Combined with the congruence in Point 1. of Lemma 2 and (11), we obtain that in fact $\eta = 1$. Hence $\alpha^\theta = \beta_0^q$. We herewith define the maps $\beta_0 : I^+ \to \mathbb{Z}[\zeta]$ and $\gamma : I \to \mathbb{K}$ as follows. For $\theta \in I^+$, we let $\beta_0(\theta)$ be the unique Jacobi number defined above by the identity $\alpha^\theta = \beta_0^q$. Then $\gamma_0(\theta) := \frac{\beta_0(\theta)}{\beta_0(\jmath\theta)}$, for $\theta \in I$.

2.3 Formal binomial power series

This section basically follows the original paper proving the Catalan conjecture in Part 4.1 [5] except the subscripts are slightly different. Therefore, some proofs will be omitted in this context.

[3] Here $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol modulo p.

2.3.1 Definition

The identity $\alpha^\theta = \beta(\theta)^q$ leads to a binomial series expansion which converges absolutely. In this section we consider this series in detail.

For $\mu = \sum_{c\in P^*} n_c\sigma_c^{-1} \in \mathbb{Z}[G]$, we let $G_\mu(T), G_{\mu(1-J)}(T) \in \mathbb{K}[[T]]$ be the formal binomial power series

$$\begin{aligned} G_\mu(T) &= (1+\zeta T)^{\mu/q} = \prod_{c\in P^*}(1+\sigma_{1/c}(\zeta)T)^{n_c/q} \\ &= \prod_{c\in P^*}\left(1+\sum_{n\geq 1}\binom{n_c/q}{n}(\sigma_{1/c}(\zeta)T)^n\right) =: 1+\sum_{n\geq 1} c_n(\mu)T^n, \quad (13) \end{aligned}$$

and the coefficients $c_n(\mu)$ arise from the multiplication and rearrangement of the terms in the product in (13). In particular, denoting $\eta_\mu := q\cdot c_1 = \sum_{c\in P} n_c\zeta^{\sigma_{1/c}}$, we obtain

$$G_\mu(T) = 1+\eta_\mu T/q + \sum_{n\geq 2} c_n(\mu)T^n. \quad (14)$$

2.3.2 Coefficients

We investigate some properties of these coefficients on base of the coefficients in binomial series. Note that $\left((1+\zeta T)^{\mu/q}\right)^\sigma = (1+\zeta T)^{\mu\sigma/q}$, by definition, as formal power series. In addition, the common domain of convergence in $\mathbb{C}$ is $D = \{|T|<1\} \subset \mathbb{C}$, so the evaluations of the two power series are equal in this domain.

Lemma 4. *The coefficients $c_n(\mu) \in \mathbb{Z}[\zeta, 1/q]$ are q-integers, which means $a'_n := c_n\cdot q^k \in \mathbb{Z}[\zeta]$ for some k. More precisely, $k \geq E(n) = n + v_q(n!)$. In particular, $E(n) = n + v_q(n!) < n\cdot\frac{q}{q-1}$.*

It is an easy consequence of the following statement.

Lemma 5. *Let $b_n(\mu) = n!q^n\cdot a_n$, a'_n be same as previous definition, $C(\mu) = \sum_{c\in P} n_c\zeta^c$. Then, for all $n>0$ and $\mu\in\mathbb{Z}[G]$, there is a $v\in\mathbb{Z}, (v,q)=1$ such that $b_n = va'_n$, and*

$$b_n(\mu) \equiv C(\mu)^n \bmod q\mathbb{Z}[\zeta]. \quad (15)$$

Proof. It can be found in the proof of the Catalan Conjecture [5]. □

Now, we investigate upper bounds for the coefficients. A power series $f(T) = \sum_{k=0}^\infty a_kT^k$ with complex coefficients is *dominated* by the series $g(T) = \sum_{k=0}^\infty A_kT^k$ with non-negative real coefficients if $|a_k| \leq A_k$ holds for $k = 0, 1, \ldots$; if this is the case, we write $g \gg f$. The relation of dominance is preserved by addition and multiplication of power series.

Let r be a real number and s a complex number satisfying $|s| \leq 1$. Then for the binomial series we have

$$(1+sT)^r = \sum_{k=0}^{\infty} \binom{r}{k} s^k T^k$$
$$(1-T)^{-|r|} = \sum_{k=0}^{\infty} (-1)^k \binom{-|r|}{k} T^k.$$

The coefficients of the latter series are positive and $\left|\binom{r}{k}\right| \leq \left|\binom{-|r|}{k}\right|$. Combining with $|\zeta| = 1$, it follows that $G_{\mu(1-\jmath)}(T) \ll (1-T)^{-h/q}$ where h is the absolute weight of $\mu(1-\jmath)$. Combining with the previous result, we obtain the following bounds:

Lemma 6. *Let $a'_n = q^{E(n)} a_n$, where a_n is the coefficients of $G_{\mu(1-\jmath)}(T)$ and $E(n) = n + v_q(n!)$, h is the absolute weight of $\mu(1-\jmath)$, $h' = \lceil h/q \rceil$ Then*

$$|a_n| \leq (-1)^k \binom{-h/q}{n} < \binom{h'+n-1}{n},$$

$$|a'_n| \leq q^{E(n)} (-1)^k \binom{-h/q}{n} < \binom{h'+n-1}{n} q^{E(n)},$$

Finally, we consider the convergence of these binomial power series.

Lemma 7. *The series $G_\mu(t)$ are absolutely convergent in $\mathbb{C}$ when $|t| \leq 1$.*

Proof. It follows that $G_\mu(t)$ is dominated by $(1-T)^{-h/q}$. For every non-negative integer m, we define the m -th partial sum by

$$G_\mu(t)|_m = 1 + \sum_{n=1}^{m} a_n(\mu) t^n.$$

Using the common remainder estimates for Taylor series, the remainder $|R_{m+1}|$ is given by $|G_\mu(t) - G_\mu(t)|_m| \leq \binom{h'+m}{m+1} \cdot \frac{|t|^{m+1}}{(1-|t|)^{h'+m+1}}$ as a consequence of Lemma 6 . □

3 Proof of Proposition 1 and the main result

We have seen that $\eta = 1$ in (12), so

$$\beta_0(\theta)^q = \alpha^\theta = \left(\frac{x-\zeta}{1-\zeta}\right)^\theta. \tag{16}$$

Dividing by the complex conjugate, we get

$$\gamma_0(\theta)^q = \left(\frac{1-\zeta/x}{1-\bar{\zeta}/x}\right)^\theta \cdot (1-\zeta)^{\theta(\jmath-1)} = \left(G_{\theta(1-\jmath)}(-1/x) \cdot (-\overline{\zeta^{1/q}})^\theta\right)^q. \tag{17}$$

Likewise, for $\sigma \in G \setminus \{\sigma_1\}$, in view of Lemma 3,

$$\begin{aligned} \left(\frac{\beta_0(\theta)}{\beta_0(\sigma\theta)}\right)^q &= \left(\frac{1-\zeta/x}{1-\zeta^\sigma/x}\right)^\theta (1-\zeta)^{\theta(\sigma-1)} \\ &= \left(G_{\theta(1-\sigma)}(-1/x)\cdot\left(\left(\frac{-1}{p}\right)\varsigma(\theta)\cdot\zeta^{\phi(\theta)/2q}\right)^{(\sigma-1)}\right)^q. \end{aligned} \tag{18}$$

We fix $\xi \in \mathbb{C}$, a primitive $q-$th root of unity, and give the formal definition of the *Galois exponent map* $\kappa : I \to \mathbb{Z}/(q\mathbb{Z})$ used in the formulation of Proposition 1:

$$\gamma_0(\theta) = G_{\theta(1-\jmath)}(-1/x)\cdot\xi^{\kappa(\theta)}\cdot\left((-1)^\theta\cdot\zeta^{-\phi(\theta)/q}\right), \tag{19}$$

We denote for simplicity, the $2p-$th root of unity above by $\nu(\theta) = (-1)^\theta\cdot\zeta^{-\phi(\theta)/q}$.

In order to investigate the behavior of $\kappa(\theta)$ under the action of G, we introduce the module

$$B = \left\{b(\theta) = \left(\gamma_0(\theta), G_{\theta(1-\jmath)}(-1/x)\cdot\nu(\theta)\right) \ : \ \theta \in I\right\}.$$

The set B is endowed with an action of $\mathbb{Z}[G]$ as follows: $z \in \mathbb{Z}$ acts on b via

$$\left(\gamma_0(\theta), \nu(\theta)\cdot G_{\theta(1-\jmath)}(-1/x)\right)^z = \left(\gamma_0(\theta)^z, \left(\nu(\theta)\cdot G_{\theta(1-\jmath)}(-1/x)\right)^z\right),$$

while $\sigma \in G$ acts naturally on the first components of $b(\theta)$. It acts on $\nu(\theta)\cdot G_{\theta(1-\jmath)}(-1/x)$ by acting on the coefficients of the power series and acting naturally on the root of unity. Extending these actions by multiplicativity turns B into a $\mathbb{Z}[G]$-module. We denote the components of elements of B by $b(\theta) = (b_1(\theta), b_2(\theta))$. The relation to the κ-map is obvious, being given by

$$\xi^{\kappa(\theta)} = \frac{b_1(\theta)}{b_2(\theta)}. \tag{20}$$

This induces an equivalence relation on B given by

$$b \sim_k b' \ \Leftrightarrow \ b_1/b_2 = b_1'/b_2'.$$

The equivalence classes of $\sim_k$ are represented by the q powers of ξ. We now prove the Proposition 1:

Proof. Fix some $\theta \in I$ and let $k = \kappa(\theta) \in \mathbb{Z}/(q\cdot\mathbb{Z})$. We investigate the relations between elements of the orbit $K(\theta) = \{\kappa(\sigma\theta) \ : \ \sigma \in G\}$. Let $\sigma \in G$ be a generator of the group. Since $\jmath = \sigma^{(p-1)/2}$ acts continuously on complex power series, we have $\kappa(\jmath\theta) = -k$.

Assume first that $k \neq 0$; then $\kappa(\sigma\theta) = c\cdot k$ for some $c \in \mathbb{Z}$ which is uniquely defined modulo q. In the module B we then have $\sigma\left(b(\theta)\right) \sim_k b(\theta)^c$. We let σ act on the above congruence and find

$$b(\sigma^2(\theta)) = \sigma^2(b(\theta)) \sim_k \sigma(b^c(\theta)) \sim_k \sigma(b(\theta))^c \sim_k b(\theta)^{c^2}.$$

By recursion, we deduce that for $e \in P^*$ we have $b(\sigma^e\theta)) = b(\theta)^{c^e}$. Since $\sigma^{p-1} = 1$, it follows that $c^{p-1} \equiv 1 \bmod q$. We may thus define a character

$$\chi_\theta : G \to \mathbb{F}_q; \quad \chi(\sigma^e) = c^e.$$

Note that $\chi(\jmath) = -1$, so χ is an odd character. We had to assume that $k \neq 0$ and deduce, by means of the character χ, that then κ is non vanishing on all the orbit $K(\theta)$. Conversely, if κ vanishes for some element in $G\theta$, then the orbit $K(\theta) = \{0\}$. This completes the proof of the Proposition. □

Remark 1. *One verifies now that the implicit* $q-$th *root of unity in (18) is*

$$\xi^{\kappa'(\theta,\sigma)} = \frac{\beta_0((1-\sigma)\theta)}{G_{(1-\sigma)\theta}\nu((1-\sigma)\theta)} = \xi^{((1-\chi_\theta(\sigma))\kappa(\theta))/2}.$$

In particular, $\kappa'(\theta,\sigma)$ *vanishes if either* $\kappa(\theta) = 0$ *of* $\chi_\theta(\sigma) = 1$.

Suppose that $\chi_\theta : G \to \mathbb{F}_q^\times$ is injective; then necessarily $(p-1)|(q-1)$, since the map $\mathbb{F}_p^\times \to \mathbb{F}_q^\times$ is an embedding. Conversely, if $(p-1) \nmid (q-1)$, there is some $\sigma \neq \sigma_1 \in \mathrm{Ker}\,(\chi_\theta)$, such that $\chi_\theta(\sigma) = 1$. In this case, we choose ψ to be a Fueter element and let $\sigma \neq \sigma_1 \in \mathrm{Ker}\,(\chi_\psi)$. Then $\theta = \psi + \jmath\sigma\psi$ has by construction weight 2 and vanishing Galois exponent κ. We can compute $\beta_0(\theta) = \beta_0((1+\jmath\sigma)\psi)$ as follows:

$$\begin{aligned}\beta_0((1+\jmath\sigma)\psi) &= \beta_0(\psi)\beta_0(\jmath\sigma\psi) = \beta_0(\psi)\overline{\beta_0(\sigma\psi)} = \beta_0(\psi)\overline{\beta_0(\sigma\psi)} \cdot \frac{\beta_0(\sigma\psi)}{\beta_0(\sigma\psi)} \\ &= z \cdot \frac{\beta_0(\psi)}{\beta_0(\sigma\psi)}.\end{aligned}$$

We now define $\beta(\theta) = \nu((1-\sigma)\theta/2)\beta_0(\theta)$, which verifies $|\beta(\theta)| = |\beta_0(\theta)| = z^{\varsigma(\theta)}$. It follows from the choice of σ that

$$\beta(\theta) = z \cdot G_{\psi(1-\sigma)}. \tag{21}$$

Let $G_{\psi(1-\sigma)} = 1 - \frac{a_1'}{qx} + R_2$, where R_2 is the remainder $\sum_{n\geq 2} a_n(-1/x)^n$. From Lemma 6, $|a_2| \leq (-1)^2\binom{-h/q}{2}$ with h the absolute weight of $\psi(1-\sigma)$ which is less than or equal to $p-1$. Since we assumed $p < q$, we get $|a_2| < 1$. By the same calculation, $|a_n| < 1$ for $n \geq 2$. Hence, $|R_2| < \sum_{n\geq 2} |1/x^n| < 2/x^2$ by Lemma 7.

On the other hand, writing $\psi = \sum_{c\in P} n_c\sigma_c^{-1}$ and $\sigma\psi = \sum_{c\in P} m_c\sigma_c^{-1}$, and $\eta_\psi = a_1'(\psi) = \sum_c n_c\zeta^{1/c}$, we find

$$\eta_\psi = \sum_{c\in P} n_c\sigma_c^{-1}(\zeta) \quad \text{and} \quad \eta_{\sigma\psi} = \sum_{c\in P} m_c\sigma_c^{-1}(\zeta).$$

Since $\bar\psi = \sum_{c\in P} n_{p-c}\sigma_c^{-1}$ and by the property of Fueter elements, $n_c + n_{p-c} = 1$ for every $c \in P$, it follows that $\eta_\psi + \overline{\eta_\psi} = \sum_{c\in P}\sigma_c^{-1}(\zeta) = -1$. Similarly, $\eta_\sigma\psi + \overline{\eta_\sigma\psi} = \sum_{c\in P}\sigma_c^{-1}(\zeta) = -1$. Hence, $a_1' + \overline{a_1'} = \eta_\theta + \overline{\eta_\theta} = \eta_\psi - \eta_{\sigma\psi} + \overline{\eta_\psi} - \overline{\eta_{\sigma\psi}} = 0$. Denote

$$\delta := \beta(\theta) + \overline{\beta(\theta)} - 2z = z\left(R_2 + \bar R_2\right) < z(4/x^2).$$

Since the right hand side is Galois invariant, it follows that for all $\sigma \in G$ we have

$$|\sigma(\delta)| < |z|(4/x^2). \tag{22}$$

Note that $\delta = \left(\sqrt{\beta(\theta)} - \sqrt{\overline{\beta(\theta)}}\right)^2$; consequently, if $\delta = 0$, it follows that $\beta(\theta) = \overline{\beta(\theta)}$, which means $(\beta_0(\theta)) = (\overline{\beta_0(\theta)})$ and thus $(\alpha^\theta) = (\alpha^{\jmath\theta)})$, in contradiction with the fact that the conjugates of α are pairwise coprime, as shown in Lemma 2. We thus proved that $\delta \neq 0$. Since δ is an algebraic integer and Lemma 1, we conclude from (22) and $|z| < |x|$

$$1 \leq \mathbf{N}_{\mathbb{K}/\mathbb{Q}}(\delta) < \left(4|z|/x^2\right)^{p-1} \quad \Rightarrow \quad |x| < 2. \tag{23}$$

Since z is totally split in $\mathbb{Z}[\zeta]$, we have $|x| > |z| \geq 2p + 1 \geq 11$, and reached thus a contradiction. The Catalan conjecture follows for all but possibly some cases when $(p-1)|(q-1)$.

If $(p-1)|(q-1)$ – so in particular $q \geq 2p-1$, we assume that χ_ψ is injective for all Fueter elements $\psi \in I$; otherwise we can use the argument above and complete the proof. We have thus to assume that χ_ψ is injective for all Fueter elements; we shall have in this case to extend the range of elements in I to take into consideration, for obtaining a combination with vanishing Galois exponent.

Lemma 8. *There are at least two elements $\theta_1, \theta_2 \in I^+$ with relative weight 2 such that $\kappa(\theta_1) = \kappa(\theta_2)$.*

Proof. There are at most $q-1$ possible values for $\kappa(\theta)$, since $\kappa(\theta) \in \mathbb{F}_q^\times$ for every $\theta \in I$. On the other hand, the second author proves in [7] that $q < (p-1)^2$. Thus, showing that $I_2 = \{t \in I^+ \ : \ \varsigma(t) = 2\}$ has cardinality $N_2 := |I_2| \geq (p-1)^2 > q$ will imply the claim.

Consider the elements

$$J := \{\psi(a,b) = \vartheta(\sigma_a + \sigma_b - \sigma_{a+b}) \ : \ a, b \in \mathbb{F}_p^\times; ab(a+b) \not\equiv 0 \bmod p\} \subset I.$$

These have all relative weight 1 and $|J| = \binom{p}{2} - (p-1) = \binom{p-1}{2}$; here, the first term stands for the combinations of 2 elements of $\mathbb{F}_p^\times$ with possible repetitions, while the correction terms removes the combinations in which $a + b \equiv 0 \bmod p$. Note that $\psi(p-a, p-b) = \jmath\psi(a,b)$. The number of sums of two elements in J in which one element can be repeated, but the sum is different from the norm, is obtained in a similar way and it equals

$$N_2 = \binom{|J|}{2} - |J| = \binom{|J|-1}{2} = \left(\frac{(p-1)(p-2)}{2} - 1\right) \cdot \left(\frac{(p-1)(p-2)}{2} - 2\right).$$

We have proved that $\theta \in I_2$ can be chosen in $N_2 > q$ ways, so by the pigeon hole principle, there are $\theta_i \in I_2; i = 1, 2$ with $\kappa(\theta_1) = \kappa(\theta_2)$. By the above, setting $\theta = \theta_1 + \jmath\theta_2$ we have

$$\varsigma(\theta) = 4 \quad \text{and} \quad \kappa(\theta) = 0.$$

Note that the constants involved even show that there is a variety of possible choices for θ, but we shall not need this fact. Moreover, if the positive element θ has a norm as term, say $\theta = \mathbf{N} + \theta'$, then $\kappa(\theta) = \kappa(\theta')$, from the definition of κ, so this case reduced to the one of θ' of relative weight 2. This completes the proof. □

We choose thus a combination $\theta' = \theta_1 + \jmath\theta_2$, with $\varsigma(\theta_i) = 2; i = 1, 2$ and such that $\kappa(\theta') = 0$. Like in the previous case, we have

$$\beta(\theta') = z^2 \frac{\beta(\theta_1)}{\beta(\theta_2)} = z^2 \cdot G_{\theta_1 - \theta_2}(-1/x)$$

Also be analogy to the previous case, and noticing that this time $|\beta(\theta')| = z^2$, we define

$$\delta = (\beta(\theta') + \overline{\beta}(\theta') - 2z^2) = \left(\sqrt{\beta(\theta')} - \sqrt{\overline{\beta(\theta')}}\right)^2,$$

and the argument used before implies that in this case too, $\delta \neq 0$, while $|\delta| < \frac{4z^2}{x^2}$. While z occurs this time at a power, we can use the assumption $(p-1)|(q-1)$ and let $q - 1 = a(p-1)$ with $a \geq 2$. From the defining equation (3), we have

$$|z|^q = \Big|\frac{x^p - 1}{p(x-1)}\Big| < |x|^p, \quad \text{hence} \quad |z|^2 \leq |z|^{q/p} < |x|.$$

By inserting this bound for $|z|$ in the one for δ and taking norms, we find in this case too:

$$1 \leq \mathbf{N}_{\mathbb{K}/\mathbb{Q}}(\delta) < \left(4z^2/x^2\right)^{p-1} \quad \Rightarrow \quad |x| < 4.$$

We reach the same contradiction as in the case $(p-1) \nmid (q-1)$. This completes the proof.

Remark 2. *The character revealed in Proposition 1 can be used for the investigation of the Nagell-Ljunggren equation*

$$\frac{x^p - 1}{x - 1} = p^e z^q \quad x, y \in \mathbb{Z} \setminus \{0, \pm 1\}; \quad e = \begin{cases} 0 & \text{if } x \not\equiv 1 \bmod p \text{ and} \\ 1 & \text{for } x \equiv 1 \bmod p. \end{cases} \tag{24}$$

The proof above readily settles the case $q > p$ and $e = 1$, while the case $e = 0$ is similar. We shall treat in subsequent papers the cases $q = p$ and $q < p$.

References

[1] Y. Bilu, Y., Bugeaud, Y. and Mignotte, M.,: *The Problem of Catalan*, Springer, 2014.

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

[3] Fueter, R., *Kummer's Kriterien zum letzten Theorem von Fermat*, Mathematische Annalen **85** (1922), 11-20.

[4] Iwasawa, K., *A note on Jacobi sums*, AMS Proceedings of Symposia in Pure Mathematics **15** (1975), 447-459.

[5] Mihăilescu, P., *Primary cyclotomic units and a proof of Catalan's conjecture*, J. Reine Angew. Math. (Journal für die Reine und Angewandte Mathematik) **572** (2004), 167-195.

[6] Mihăilescu, P., *Class number conditions for the diagonal case of the equation of Nagell and Ljunggren*, In *Festschrift to the 70-th Birthday of Wolfgang Schmidt*, Eds. Schlickewei et. al, Springer 2008, 243-274.

[7] Mihăilescu, P., *New bounds and conditions for the equation of Nagell-Ljunggren*, Journal of Number Theory, **124** (207), no. 2, 380-395.

[8] Ribenboim, P., *Catalan's conjecture*, Séminaire de Philosophie et Mathématiques **6** (1994), 1-11.

[9] Schoof, R., *Catalan's Conjecture*, Universitext, Springer, 2008.

[10] Washington, L., *Introduction to cyclotomic fields*, 2nd edition, Graduate Texts in Mathematics, Springer, 1997.