Transnational Journal of Mathematical Analysis and Applications
Vol. 10, Issue 2, 2022, Pages 145-167
ISSN 2347-9086
Published Online on January 20, 2023

http://jyotiacademicpress.org

A NOTE ON THE DIOPHANTINE EQUATION $X^P - 1 = BZ^Q$

BENJAMIN DUPUY

Laboratoire de Mathematiques Mathmax
Lycée Max Linder
33505 Libourne
France
e-mail: benjamin.dupuy1@ac-bordeaux.fr

Abstract

In this paper, we consider the Diophantine equation $X^p - 1 = BZ^q$ which generalize the Catalan equation and which has not been studied so far. For the first time, we prove that this equation has no non-trivial solution under certain simple conditions on p, q and B.

1. Introduction

Let p and q be distinct odd prime numbers and B be a non-zero integer. In this paper, we consider the Diophantine equation

$$X^p - 1 = BZ^q, \tag{1}$$

2020 Mathematics Subject Classification: 11D72, 11R18, 11R27, 11R29, 11R32.
Keywords and phrases: Nagell-Ljunggren, Mihailescu ideal, class number, Stickelberger ideal, Jacobi integers.
Communicated by Francisco Bulnes.
Received December 30, 2022

where X and Z are the unknown integers. A solution $(X; Z)$ of this equation with $|X| \leqslant 1$ is called *trivial solution*. A such equation generalize the Catalan equation $X^p - 1 = Z^q$ and has not been studied so far. In this paper, we prove, for the first time, that this Diophantine equation has no non trivial solution under some conditions on p, q and B.

The Catalan equation has been successfully solved by Mihailescu (see [1]). In his work (see [1] or [7]), Mihailescu proved that if Catalan's equation has a non-trivial solution then $q | h_p^-$ (so, by symmetry, $p | h_q^-$), where h_p^- is the p-th relative class number. A quite natural question is to know if this class number criterion can be extended to the Diophantine equation (1). In other words, can we claim that if $q \nmid h_p^-$ then the Diophantine equation (1) has no non-trivial solution ? There exists no paper where this question is studied. In this article, we propose to prove that this claim holds under certain simple conditions on p, q and B.

From now, we assume, once and for all, that if ℓ is a prime number dividing B, then $\ell \neq 1 \mod p$. In this paper, we first prove the following beautiful theorem which is a simple consequence of the principal result of [3]:

Theorem 1. *Assume that* $p > 3$, $p | B$ *and* $q \nmid h_p^-$. *Thus, the only solution of the Diophantine equation* (1) *is* $X = 1$, $Z = 0$.

Then, by using methods which go back to [5], [7] and by using a new method based on the use of a recent result on a circulant matrix (see [4]), we prove the following beautiful theorem:

Theorem 2. *Assume that* $7 \leqslant p < q$, $q \nmid h_p^-$ *and that the* q*-adic valuation of* B *is equal to* 1. *Furthermore, we assume that* $p \equiv 3 \mod 4$ *if* $p \leqslant 191$. *Thus, the only solution of the Diophantine equation* (1) *is* $X = 1$, $Z = 0$.

Example 1. Assume that $p \equiv 3 \mod 4$, $7 \leqslant p \leqslant 31$ and that the q-adic valuation of B is equal to 1. If $p < q$, then the only solution of the Diophantine equation (1) is $X = 1$, $Z = 0$. Namely, for such p, h_p^- has no prime factor q such that $q > p$.

2. The Stickelberger Ideal

In this section, we give some useful results on the Stickelberger ideal. We refer the reader to [1], [2], [7] or [9] for more details.

2.1. Prerequisites and notations

We put $\zeta = e^{\frac{2i\pi}{p}}$ and $P = \{1; 2; \cdots; p-1\}$. For $c \in P$, we denote by σ_c the $\mathbb{Q}$-automorphism of $\mathbb{Q}(\zeta)$ defined by $\zeta^{\sigma_c} = \zeta^c$. The extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ is a Galois extension whose Galois group G is given by $G = \{\sigma_c : c \in P\}$. If $n \in \mathbb{Z}$ is congruent to $c \in P$ modulo p, we put $\sigma_n = \sigma_c$. Particularly, σ_{-1} is the complex conjugation.

Definition 1. (1) The Stickelberger element $\theta \in \mathbb{Q}[G]$ is defined by

$$\theta = \frac{1}{p}\sum_{c \in P} c\sigma_c^{-1}.$$

(2) The Stickelberger ideal $\mathcal{I}_{\mathcal{S}}$ is the ideal of $\mathbb{Z}[G]$ defined by

$$\mathcal{I}_{\mathcal{S}} = \mathbb{Z}[G] \cap \theta\mathbb{Z}[G].$$

In other words, $\mathcal{I}_{\mathcal{S}}$ is the set of $\mathbb{Z}[G]$-multiples of θ which have integral coefficients.

An element $\sum_{c \in P} n_c\sigma_c$ of $\mathcal{I}_{\mathcal{S}}$ is said to be positive if and only if

$$\forall c \in P,\ n_c \geqslant 0.$$

In this paper, the set of positive elements of $\mathcal{I}_{\mathcal{S}}$ is denoted by $\mathcal{I}_{\mathcal{S}}^+$. In other words

$$\mathcal{I}_{\mathcal{S}}^+ = \left\{\sum_{c \in P} n_c\sigma_c \in \mathcal{I}_{\mathcal{S}} : \forall c \in P,\ n_c \geqslant 0\right\}.$$

2.2. Particular elements of $\mathcal{I}_{\mathcal{S}}$

Let n be an integer such that $(n, p) = 1$. Recall that σ_n is the element of G defined by $\zeta^{\sigma_n} = \zeta^n$. By abuse of notation, the element $n\sigma_1$ is denoted by n. Using this notation, we put

$$\Theta_n = (n - \sigma_n)\theta \in \theta\mathbb{Z}[G].$$

For a real number x, we denote by $[x]$ the integer part of $x : [x] = \max \{a \in \mathbb{Z} : a \leqslant x\}$. We have (see [1], Proposition 7.2)

$$\Theta_n = \sum_{c \in P} \left[\frac{nc}{p}\right] \sigma_c^{-1}.$$

So, $\Theta_n \in \mathcal{I}_{\mathcal{S}}^+$. In particular

$$\Theta_2 = \sum_{c=\frac{p+1}{2}}^{p-1} \sigma_c^{-1} \in \mathcal{I}_{\mathcal{S}}^+.$$

From the above, we can deduce that

$$(1 + \sigma_{-1})\Theta_2 = \mathrm{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}, \tag{2}$$

where $\mathbf{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}$ is the norm relative to the extension $\mathbb{Q}(\zeta)/\mathbb{Q}$. Namely,

$$(1 + \sigma_{-1})\Theta_2 = \sum_{c=\frac{p+1}{2}}^{p-1} (1 + \sigma_{-1})\sigma_c^{-1} = \sum_{c=\frac{p+1}{2}}^{p-1} \sigma_c^{-1} + \sum_{c=\frac{p+1}{2}}^{p-1} \sigma_{-1}\sigma_c^{-1}$$

$$= \sum_{c=\frac{p+1}{2}}^{p-1} \sigma_c^{-1} + \sum_{c=\frac{p+1}{2}}^{p-1} \sigma_{p-c}^{-1} = \sum_{c=1}^{p-1} \sigma_c^{-1}$$

$$= \sum_{c=1}^{p-1} \sigma_c = \mathrm{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}.$$

2.3. A property of Θ_2 for $p \equiv 3 \bmod 4$

In this subsection, we assume that $p \equiv 3 \bmod 4$. Let $\mathbb{F}_p$ be the field of p elements. We fix, once and for all, a primitive element of $\mathbb{F}_p^{\times}$ which is denoted by g. Let $\sigma \in G$ defined by $\zeta^{\sigma} = \zeta^{g^2}$. -1 is not a square modulo p since $p \equiv 3 \bmod 4$. Consequently, for all $k \in \{0; \cdots; \frac{p-3}{2}\}$ there exist integers $a_k, b_k \in \{0; 1\}$, such that

$$\Theta_2 = \sum_{k=0}^{\frac{p-3}{2}} a_k \sigma_{g^{2k}} + b_k \sigma_{-g^{2k}} = \sum_{k=0}^{\frac{p-3}{2}} a_k \sigma^k + b_k \sigma_{-1} \sigma^k. \tag{3}$$

We have the following lemma:

Lemma 1. *There exists at least an integer* $k \in \{0; \cdots; \frac{p-3}{2}\}$ *such that* $a_k - b_k = \pm 1$.

Proof. There exists at least an integer $k \in \{0; \cdots; \frac{p-3}{2}\}$ such that $a_k - b_k = \pm 1$. Otherwise

$$\forall k \in \left\{0; \cdots; \frac{p-3}{2}\right\}, \; a_k = b_k,$$

since $\forall k \in \left\{0; \cdots; \frac{p-3}{2}\right\}$, $a_k, b_k \in \{0; 1\}$. Consequently, we obtain

$$\Theta_2 = \sum_{k=0}^{\frac{p-3}{2}} a_k \sigma^k + b_k \sigma_{-1} \sigma^k = \sum_{k=0}^{\frac{p-3}{2}} a_k \sigma^k + b_k \sigma_{-1} \sigma^k$$

$$= \sum_{k=0}^{\frac{p-3}{2}} a_k \sigma^k (1 + \sigma_{-1}),$$

so that

$$(1-\sigma_{-1})\Theta_2 = \sum_{k=0}^{\frac{p-3}{2}} a_k\sigma^k(1-\sigma_{-1})(1+\sigma_{-1})$$

$$= \sum_{k=0}^{\frac{p-3}{2}} a_k\sigma^k(1-\sigma_{-1}^2),$$

that is

$$\Theta_2 - \sigma_{-1}\Theta_2 = 0. \tag{4}$$

Equality (2) implies that

$$\Theta_2 - (\mathrm{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}} - \Theta_2) = 0, \tag{5}$$

that is

$$2\Theta_2 = \mathrm{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}. \tag{6}$$

Finally, we obtain

$$\sum_{c=\frac{p+1}{2}}^{p-1} 2\sigma_c^{-1} = \mathrm{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}, \tag{7}$$

which is false. □

2.4. The Stickelberger theorem

In the following, by (*fractional*) ideal we mean (fractional) ideal of $\mathbb{Z}[\zeta]$.

From Stickelberger's theorem, we know that Stickelberger's ideal $\mathcal{I}_{\mathcal{S}}$ annihilates the class group of $\mathbb{Q}(\zeta)$. In other words, if $\mathfrak{a}$ is a fractional ideal and if $\Theta \in \mathcal{I}_{\mathcal{S}}$, then $\mathfrak{a}^{\Theta}$ is principal. We can have a more precise result (see [7], page 4):

Theorem 3. *Let* $\mathfrak{a}$ *be an ideal. Suppose that* $\boldsymbol{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\mathfrak{a}) = t$, *where* t *is a product of powers of prime numbers* ℓ, $\ell \equiv 1 \bmod p$. *Then, for all* $\Theta \in \mathcal{I}_{st}^{+}$, *there exists a Jacobi integer* $j \in \mathbb{Z}[\zeta]$ *such that*

$$\mathfrak{a}^{\Theta} = (j). \tag{8}$$

3. The Mihailescu Ideal

3.1. The augmented part of an ideal of $\mathbb{Z}[G]$

The weight homomorphism $w : \mathbb{Z}[G] \longrightarrow \mathbb{Z}$ is defined by

$$w\left(\sum_{c \in P} n_c \sigma_c\right) = \sum_{c \in P} n_c.$$

By definition, its kernel consists of elements of weight 0. It is called the *augmentation ideal* of $\mathbb{Z}[G]$. If $\mathcal{I}$ is an ideal of $\mathbb{Z}[G]$, then the *augmented part* of $\mathcal{I}$ is the ideal of $\mathbb{Z}[G]$ defined by

$$\mathcal{I}^{aug} = \{\Theta \in \mathcal{I} : w(\Theta) = 0\}.$$

3.2. The r-ball of an ideal of $\mathbb{Z}[G]$

The size function $\|\cdot\|$ is defined from $\mathbb{Z}[G] \longrightarrow \mathbb{N}$ by

$$\left\|\sum_{c \in P} n_c \sigma_c\right\| = \sum_{c \in P} |n_c|.$$

Let $\mathcal{I}$ be an ideal of $\mathbb{Z}[G]$. The r-ball of $\mathcal{I}$ is defined by

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

3.3. A theorem on Mihailescu's ideal

In this subsection, we fix a non-zero integer x. Recall that q is an odd prime number distinct from p. Mihailescu's ideal $\mathcal{I}_M$ is the ideal of $\mathbb{Z}[G]$ consisting of $\Theta \in \mathbb{Z}[G]$ such that $(x - \zeta)^{\Theta} \in (\mathbb{Q}(\zeta)^{\times})^{q}$. We have the following result (see Theorem 8.5 of [1]):

Theorem 4. *Assume that* $p < q$. *If* $|x| \geqslant 8q^q$, *then* $\mathcal{I}_M^{aug}(2) = \{0\}$.

4. A Circulant Matrix

Recall that g is a primitive element of $\mathbb{F}_p^\times$ and that $\sigma \in G$ is defined by $\zeta^\sigma = \zeta^{g^2}$. We put $Z = \frac{1}{1-\zeta} - \frac{1}{1-\overline{\zeta}}$. We denote by $\mathcal{M}$ the circulant matrix whose first line is given by

$$Z\, Z^\sigma \cdots Z^{\sigma^{\frac{p-3}{2}}}.$$

This matrix plays an important role in the proof of the Theorem 2. We have the following lemma:

Lemma 2. *The coefficients of the matrix* $\mathcal{M}$ *are elements of the ring* $\mathbb{Z}\left[\zeta, \frac{1}{1-\zeta}\right]$.

Proof. Let $k \in \left\{0; \dots; \frac{p-3}{2}\right\}$. It is not difficult to see that

$$Z^{\sigma^k} = \frac{1+\zeta^{\sigma^k}}{1-\zeta^{\sigma^k}} = \frac{1-\zeta}{1-\zeta^{\sigma^k}} \cdot \frac{1+\zeta^{\sigma^k}}{1-\zeta}.$$

The algebraic number $\frac{1-\zeta}{1-\zeta^{\sigma^k}}$ is a unit of $\mathbb{Z}[\zeta]$ (called *cyclotomic* or *circular* unit). Consequently,

$$Z^{\sigma^k} = \frac{1-\zeta}{1-\zeta^{\sigma^k}} \cdot \frac{1+\zeta^{\sigma^k}}{1-\zeta} \in \mathbb{Z}\left[\zeta, \frac{1}{1-\zeta}\right].$$

□

Furthermore, if $p \equiv 3 \bmod 4$ then the determinant of $\mathcal{M}$ does not depend on the choice of the value of g and it is given by (see [4])

$$\det(\mathcal{M}) = (-1)^{\frac{p-3}{4}} \times 2^{\frac{p-3}{2}} \times p^{\frac{p-7}{4}} \times h_p^- \times \sqrt{-p}.$$

5. Some Useful Lemmas to Prove the Theorems 1 and 2

Lemma 3 (see [8], P1.2 page 11). *Let $x \neq 0$ and $y \neq 0$ be distinct co-prime integers. We have the following results*:

(1) *The quotient $\frac{x^p - y^p}{x - y}$ is a non-zero positive integer. Furthermore, we have $\frac{x^p - y^p}{x - y} = 1$ if and only if $x = 1$ and $y = -1$ or $x = -1$ and $y = 1$.*

(2) *p divides $\frac{x^p - y^p}{x - y}$ if and only if p divides $x - y$. Furthermore, the p-adic valuation of $\frac{x^p - y^p}{x - y}$ is equal to* 0 *or* 1.

(3) *We have* $\left(\frac{x^p - y^p}{x - y}, x - y\right) = (x - y, p)$.

Lemma 4. *Let x and y be distinct co-prime integers. We assume that there exist integers $n \geqslant 2$ and $z > 1$ such that*

$$\frac{x^p - y^p}{x - y} = z^n. \tag{9}$$

We have the following results:

(1) *The ideals $(x - \zeta^c y)$, $c \in P = \{1, 2, \cdots, p-1\}$ are pairwise co-prime.*

(2) *There exists an ideal $\mathfrak{a}$ such that $(x - \zeta y) = \mathfrak{a}^n$.*

(3) *For all prime number* ℓ *dividing* z, *we have* $\ell \equiv 1 \bmod p$. *Particularly,* $\boldsymbol{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\mathfrak{a}) = z$ *is a product of powers of prime numbers* ℓ *such that* $\ell \equiv 1 \bmod p$.

Proof. (1) The ideals $(x - \zeta^c y)$, $c \in P$ are pairwise co-prime. Otherwise, there exist $a, b \in P$ distinct integers and a prime ideal $\mathfrak{p}$ such that

$$x - \zeta^a y \in \mathfrak{p} \text{ and } x - \zeta^b y \in \mathfrak{p}, \tag{10}$$

so that $y(\zeta^b - \zeta^a) = x - \zeta^a y - (x - \zeta^b y) \in \mathfrak{p}$, that is, $y \in \mathfrak{p}$ or $\zeta^b - \zeta^a \in \mathfrak{p}$.

Suppose that $y \in \mathfrak{p}$. In this case, $x = x - \zeta^a y + \zeta^a y \in \mathfrak{p}$ in contradiction with the fact that *x* and *y* are co-prime integers.

Suppose that $\zeta^b - \zeta^a \in \mathfrak{p}$. Recall that p is totally ramified in the extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ and that $\zeta^b - \zeta^a$ is a generator of the only prime ideal of $\mathbb{Z}[\zeta]$ above *p* since $a \neq b \bmod p$. The ideal $(\zeta^b - \zeta^a)$ is even a maximal ideal of $\mathbb{Z}[\zeta]$ since $\mathbb{Z}[\zeta]$ is a Dedekind ring. From $\zeta^b - \zeta^a \in \mathfrak{p}$, we deduce that $\mathfrak{p} = (\zeta^b - \zeta^a)$, so that $x - \zeta^a y \in (\zeta^b - \zeta^a)$ since $x - \zeta^a y \in \mathfrak{p}$. The Equation (9) can be rewritten as

$$\prod_{c \in P} (x - \zeta^c y) = z^n. \tag{11}$$

Since $x - \zeta^a y \in (\zeta^b - \zeta^a)$, we have $p | z^n$. Particularly, the p-adic valuation of $\dfrac{x^p - y^p}{x - y}$ is greater than or equal to $n > 1$, in contradiction with the second assertion of Lemma 3.

(2) The ideals $(x - \zeta^c y)$, $c \in P$, being pairwise co-prime, we deduce from (11) that there exists an ideal $\mathfrak{a}$ such that $(x - \zeta y) = \mathfrak{a}^n$.

(3) Let $\mathcal{L}$ be a prime ideal above ℓ. From the equality (11), we deduce that there exists $k \in P$ such that $\mathcal{L} | (x - \zeta^k y)$. The ideals $(x - \zeta^c y)$, $c \in P$, being pairwise co-prime, we can claim that the prime ideals $\mathcal{L}^{\sigma}$, $\sigma \in G$ are pairwise distinct, so that the ideal $\mathcal{L}$ is totally split in the extension $\mathbb{Q}(\zeta)/\mathbb{Q}$. So, the decomposition group of ℓ in this extension is trivial. This group being generated by $\ell \bmod p$, so we have $\ell \equiv 1 \bmod p$. The last assertion is clear since

$$\begin{aligned} \mathbf{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\mathfrak{a})^n = \mathbf{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\mathfrak{a}^n) &= \left|\mathbf{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(x - \zeta y)\right| \\ &= \left|\prod_{c \in P} (x - \zeta^c y)\right| \\ &= z^n. \end{aligned}$$

□

Lemma 5 (see [2], Lemma 3.5.19)**.** *Let* $\alpha \in \mathbb{Q}(\zeta)$ *be such that* $\frac{\overline{\alpha}}{\alpha} \in \mathbb{Z}[\zeta]$. *Then* $\frac{\overline{\alpha}}{\alpha}$ *is a root of unity of* $\mathbb{Z}[\zeta]$, *that is a* $2p$*-th root of unity.*

Lemma 6. *Suppose* $p < q$ *and there exists integers* $x \neq 1$ *and* $z > 1$ *such that*

$$\frac{x^p - 1}{x - 1} = z^q.$$

If $q \nmid h_p^-$ *then* $|x| < 8q^q$.

Proof. From the second assertion of Lemma 4, there exists an ideal $\mathfrak{a}$ such that

$$(x - \zeta) = \mathfrak{a}^q. \tag{12}$$

As $q \nmid h_p^-$, the class of $\mathfrak{a}$ belongs to the real part of the class group of $\mathbb{Q}(\zeta)$. In other words, we have $\mathfrak{a} = \mathfrak{b}(\gamma)$ where $\gamma \in \mathbb{Q}(\zeta)^\times$ and $\mathfrak{b}$ is a "real" fractional ideal of $\mathbb{Z}[\zeta]$ (that is, $\mathfrak{b} = \bar{\mathfrak{b}}$). Furthermore, $\mathfrak{b}^q$ is a principal real ideal; in other words, $\mathfrak{b}^q = (\beta)$ where $\beta \in \mathbb{Q}(\zeta)$ and $\bar{\mathfrak{b}}^q = \mathfrak{b}^q$ that is $(\bar{\beta}) = (\beta)$. Particularly, there exists a unit u of $\mathbb{Z}[\zeta]$ such that $\bar{\beta} = \beta u$. In fact, by Lemma 5 u is a $2p$-th root of unity since $u = \frac{\bar{\beta}}{\beta} \in \mathbb{Z}[\zeta]$. From the equality (12), we deduce that

$$x - \zeta = \beta\gamma^q\eta,$$

where η is a unit of $\mathbb{Z}[\zeta]$. Particularly

$$\frac{x - \bar{\zeta}}{x - \zeta} = \frac{\bar{\eta}}{\eta} u \left(\frac{\bar{\gamma}}{\gamma}\right)^q. \tag{13}$$

We have $\frac{\bar{\eta}}{\eta} \in \mathbb{Z}[\zeta]$ since η is a unit of $\mathbb{Z}[\zeta]$. By lemma 5, $\frac{\bar{\eta}}{\eta}$ as u is a $2p$-th root of unity. Particularly, $\frac{\bar{\eta}}{\eta} u$ is the q-th power of a $2p$-th root of unity since $(2p, q) = 1$. From (13), we deduce that there exists $\mu \in \mathbb{Q}(\zeta)^\times$ such that $\frac{x - \bar{\zeta}}{x - \zeta} = \mu^q$, that is

$$(x - \zeta)^{\sigma_{-1} - 1} \in (\mathbb{Q}(\zeta)^\times)^q. \tag{14}$$

We have $w(\sigma_{-1} - 1) = 0$ and $\|\sigma_{-1} - 1\| = 2$. (14) implies that $\sigma_{-1} - 1 \in \mathcal{I}_M^{\mathrm{aug}}(2)$. Particularly, $\mathcal{I}_M^{\mathrm{aug}}(2) \neq \{0\}$. From Theorem 4 of the Subsection 3.3, we deduce that $|x| < 8q^q$. □

Lemma 7 (See [7], Lemma 1)**.** *Let* $\alpha \in \mathbb{Z}[\zeta]$ *such that* $\alpha \cdot \overline{\alpha} \in \mathbb{Z}$. *Suppose there exists a Jacobi integer j such that the ideal* (α) *is generated by j. Then*

$$\alpha = \pm\zeta^n \cdot j, \; n \in \mathbb{Z}.$$

Lemma 8 (See [5], Lemma 1)**.** *Let* $\mathfrak{q}$ *be a prime ideal of the ring of integers* $\mathcal{O}_K$ *of a number field* K. *Let q be the prime number below* $\mathfrak{q}$. *If* $\alpha, \beta \in \mathcal{O}_K$ *with* $\alpha^q \equiv \beta^q \bmod \mathfrak{q}$, *then* $\alpha^q \equiv \beta^q \bmod \mathfrak{q}^2$.

The following lemma is a nice application of the Theorem 1 of [4]:

Lemma 9. *Recall that p and q are distinct odd prime numbers. We assume that* $p \equiv 3 \bmod 4$ *and that there exists integers* x, y *and z such that*

$$\frac{x^p - y^p}{x - y} = z^q, \quad z > 1, \quad (x, y) = 1, \quad \nu_q(x - y) = 1,$$

where ν_q *is the q-adic valuation. Then we have* $q | h_p^-$.

Proof. By Lemma 4, there exists an ideal $\mathfrak{a}$ such that

$$(x - \zeta y) = \mathfrak{a}^q, \tag{15}$$

and $\mathbf{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\mathfrak{a}) = z$ is a product of powers of prime numbers ℓ such that $\ell \equiv 1 \bmod p$. Let Θ_2 be one of the positive elements of Stickelberger's ideal (see Subsection 2.2). By Theorem 3 of the Subsection 2.4, there exists a Jacobi integer $j \in \mathbb{Z}[\zeta]$ such that $\mathfrak{a}^{\Theta_2} = (j)$. From (15), we deduce that

$$((x - \zeta y)^{\Theta_2}) = (j^q). \tag{16}$$

By (2), we know that $(1+\sigma_{-1})\Theta_2 = \mathbf{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}$, so that

$$(x-\zeta y)^{\Theta_2} \cdot \overline{(x-\zeta y)^{\Theta_2}} = (x-\zeta y)^{(1+\sigma_{-1})\Theta_2} = (x-\zeta y)^{\mathbf{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}}$$

$$= \mathbf{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(x-\zeta y) = \left|\mathbf{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(x-\zeta y)\right|$$

$$= \mathbf{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\mathfrak{a}^q) = z^q \in \mathbb{Z}.$$

Furthermore, j^q is a Jacobi integer since j is one. By (16) and Lemma 7, there exist $n \in \mathbb{Z}$ and $\epsilon = \pm 1$ such that

$$(x-\zeta y)^{\Theta_2} = \epsilon \zeta^n j^q.$$

We have $(2p, q) = 1$ so that $\epsilon\zeta^n$ is the q-th power of a $2p$-th root of unity. So, we can suppose that $\epsilon\zeta^n = 1$. In other words, we can suppose that

$$(x-\zeta y)^{\Theta_2} = j^q, \tag{17}$$

with $j \in \mathbb{Z}[\zeta]$. Note that j is no longer necessarily a Jacobi integer but the fact that $j \in \mathbb{Z}[\zeta]$ is sufficient for our purpose.

From (17) we deduce that

$$(y(1-\zeta))^{\Theta_2}\left(1+\frac{x-y}{y(1-\zeta)}\right)^{\Theta_2} = j^q \Rightarrow \left(1+\frac{x-y}{y(1-\zeta)}\right)^{\Theta_2} = \frac{j^q}{y^{\frac{p-1}{2}}(1-\zeta)^{\Theta_2}}. \tag{18}$$

Recall that we have (see (3))

$$\Theta_2 = \sum_{k=0}^{\frac{p-3}{2}} a_k\sigma^k + b_k\sigma_{-1}\sigma^k,$$

with $a_k, b_k \in \{0; 1\}$, for all $k \in \{0; \cdots; \frac{p-3}{2}\}$, so that

$$\left(1+\frac{x-y}{y(1-\zeta)}\right)^{\Theta_2} = \prod_{k=0}^{\frac{p-3}{2}}\left(1+\frac{x-y}{y(1-\zeta^{\sigma^k})}\right)^{a_k} \times \prod_{k=0}^{\frac{p-3}{2}}\left(1+\frac{x-y}{y(1-\overline{\zeta}^{\sigma^k})}\right)^{b_k},$$

that is

$$\left(1+\frac{x-y}{y(1-\zeta)}\right)^{\Theta_2} = \prod_{k=0}^{\frac{p-3}{2}}\left(1+\frac{a_k(x-y)}{y(1-\zeta^{\sigma^k})}\right) \times \prod_{k=0}^{\frac{p-3}{2}}\left(1+\frac{b_k(x-y)}{y(1-\overline{\zeta}^{\sigma^k})}\right). \tag{19}$$

Let $\mathfrak{q}$ be a prime ideal above q, $s \geqslant 1$ an integer and $\alpha, \beta \in \mathbb{Q}(\zeta)$. In the rest of this paper, we adopt the following notation:

$$\alpha \equiv \beta \bmod \mathfrak{q}^s,$$

if and only if there exists $\gamma \in \mathbb{Q}(\zeta)$ such that

$$\alpha = \beta + \gamma,\ \nu_{\mathfrak{q}}(\gamma) \geqslant s,$$

where $\nu_{\mathfrak{q}}$ is the $\mathfrak{q}$-adic valuation.

Let $k \in \{0; \cdots; \frac{p-3}{2}\}$. Recall that $q | x - y$. Furthermore $1 - \zeta^{\sigma^k}$ is a generator of the only prime ideal of $\mathbb{Z}[\zeta]$ above p and $q \nmid y$ since $q | x - y$ and $(x, y) = 1$. Consequently, we have

$$\frac{x-y}{y(1-\zeta^{\sigma^k})} \equiv 0 \bmod \mathfrak{q} \text{ and } \frac{x-y}{y(1-\overline{\zeta}^{\sigma^k})} \equiv \bmod \mathfrak{q}.$$

From (19) we deduce that

$$\left(1+\frac{x-y}{y(1-\zeta)}\right)^{\Theta_2} \equiv 1 + \frac{x-y}{y}\sum_{k=0}^{\frac{p-3}{2}}\frac{a_k}{1-\zeta^{\sigma^k}} + \frac{b_k}{1-\overline{\zeta}^{\sigma^k}} \bmod \mathfrak{q}^2.$$

Using (18) we obtain

$$\frac{j^q}{y^{\frac{p-1}{2}}(1-\zeta)^{\Theta_2}} \equiv 1 + \frac{x-y}{y}\sum_{k=0}^{\frac{p-3}{2}} \frac{a_k}{1-\zeta^{\sigma^k}} + \frac{b_k}{1-\overline{\zeta}^{\sigma^k}} \bmod \mathfrak{q}^2. \tag{20}$$

By a similar reasoning to the above, we have

$$\frac{j^q}{y^{\frac{p-1}{2}}(1-\zeta)^{\Theta_2}} \equiv 1 + \frac{x-y}{y}\sum_{k=0}^{\frac{p-3}{2}} \frac{a_k}{1-\zeta^{\sigma k}} + \frac{b_k}{1-\overline{\zeta}^{\sigma^k}} \bmod \overline{\mathfrak{q}}^2,$$

so that

$$\frac{\overline{j}^q}{y^{\frac{p-1}{2}}(1-\overline{\zeta})^{\Theta_2}} \equiv 1 + \frac{x-y}{y}\sum_{k=0}^{\frac{p-3}{2}} \frac{a_k}{1-\overline{\zeta}^{\sigma^k}} + \frac{b_k}{1-\zeta^{\sigma k}} \bmod \mathfrak{q}^2. \tag{21}$$

Equations (20) and (21) imply that

$$\frac{j^q}{y^{\frac{p-1}{2}}(1-\zeta)^{\Theta_2}} - \frac{\overline{j}^q}{y^{\frac{p-1}{2}}(1-\overline{\zeta})^{\Theta_2}} \equiv \frac{x-y}{y}\sum_{k=0}^{\frac{p-3}{2}} (a_k - b_k) \times \left(\frac{1}{1-\zeta^{\sigma^k}} - \frac{1}{1-\overline{\zeta}^{\sigma^k}}\right) \bmod \mathfrak{q}^2,$$

that is,

$$\frac{1}{y^{\frac{p-1}{2}}(1-\zeta)^{\Theta_2}}\left(j^q - \frac{\overline{j}^q(1-\zeta)^{\Theta_2}}{(1-\overline{\zeta})^{\Theta_2}}\right) \equiv \frac{x-y}{y}\sum_{k=0}^{\frac{p-3}{2}} (a_k - b_k) \times \left(\frac{1}{1-\zeta^{\sigma^k}} - \frac{1}{1-\overline{\zeta}^{\sigma^k}}\right) \bmod \mathfrak{q}^2.$$

In other words

$$j^q - \bar{j}^q \frac{(1-\zeta)^{\Theta_2}}{(1-\bar{\zeta})^{\Theta_2}} \equiv y^{\frac{p-3}{2}}(1-\zeta)^{\Theta_2}(x-y)\sum_{k=0}^{\frac{p-3}{2}}(a_k - b_k)$$

$$\times \left(\frac{1}{1-\zeta^{\sigma^k}} - \frac{1}{1-\bar{\zeta}^{\sigma^k}}\right) \bmod \mathfrak{q}^2. \quad (22)$$

We have

$$\frac{(1-\zeta)^{\Theta_2}}{(1-\bar{\zeta})^{\Theta_2}} = (-\zeta)^{\Theta_2},$$

where $-\zeta$ is the q-th power of a $2p$-th root of unity since $(2p, q) = 1$. Particularly, there exists a $2p$-th root of unity denoted by r such that

$$(-\zeta)^{\Theta_2} = r^q.$$

We put $j_1 = r\bar{j} \in \mathbb{Z}[\zeta]$. Equation (22) implies that

$$j^q - j_1^q \equiv y^{\frac{p-3}{2}}(1-\zeta)^{\Theta_2}(x-y)\sum_{k=0}^{\frac{p-3}{2}}(a_k - b_k)\left(\frac{1}{1-\zeta^{\sigma^k}} - \frac{1}{1-\bar{\zeta}^{\sigma^k}}\right) \bmod \mathfrak{q}^2.$$

(23)

Recall that $q | x - y$ and for all $k \in \{0; \cdots; \frac{p-3}{2}\}$, $\nu_{\mathfrak{q}}(1-\zeta^{\sigma^k}) = 0$. Thus (23) implies that

$$j^q - j_1^q \equiv 0 \bmod \mathfrak{q}^2.$$

Therefore, by Lemma 8, we have

$$j^q - j_1^q \equiv 0 \bmod \mathfrak{q}^2. \quad (24)$$

Since $\nu_{\mathfrak{q}}\left(y^{\frac{p-3}{2}}(1-\zeta)^{\Theta_2}\right) = 0$, Equations (23) and (24) imply that

$$(x-y)\sum_{k=0}^{\frac{p-3}{2}}(a_k - b_k)\left(\frac{1}{1-\zeta^{\sigma^k}} - \frac{1}{1-\overline{\zeta}^{\sigma^k}}\right) \equiv 0 \bmod \mathfrak{q}^2. \tag{25}$$

By hypothesis $\nu_q(x-y) = 1$ and we know that q is unramified in the extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ since $q \neq p$, so that $\nu_{\mathfrak{q}}(x-y) = 1$. Thus, we deduce from (25) that

$$\sum_{k=0}^{\frac{p-3}{2}}(a_k - b_k)\left(\frac{1}{1-\zeta^{\sigma^k}} - \frac{1}{1-\overline{\zeta}^{\sigma^k}}\right) \equiv 0 \bmod \mathfrak{q}. \tag{26}$$

We put $Z = \frac{1}{1-\zeta} - \frac{1}{1-\overline{\zeta}}$ as noted in the Section 4. Equation (26) implies that

$$\sum_{k=0}^{\frac{p-3}{2}}(a_k - b_k)Z^{\sigma^k} \equiv 0 \bmod \mathfrak{q}. \tag{27}$$

Let $i \in \{1; \cdots; \frac{p-1}{2}\}$. By a similar reasoning to the above, we obtain

$$\sum_{k=0}^{\frac{p-3}{2}}(a_k - b_k)Z^{\sigma^k} \equiv 0 \bmod \mathfrak{q}^{\sigma^{i-1}},$$

that is

$$\sum_{k=0}^{\frac{p-3}{2}}(a_k - b_k)Z^{\sigma^{k-i+1}} \equiv 0 \bmod \mathfrak{q}. \tag{28}$$

As noted in the Section 4, let $\mathcal{M}$ be the circulant matrix whose first line is given by

$$Z\, Z^{\sigma} \cdots Z^{\sigma^{\frac{p-3}{2}}}.$$

Note that the coefficient of $\mathcal{M}$ on the i-th row and j-th column is given by

$$[\mathcal{M}]_{ij} = Z^{\sigma^{j-i}}.$$

Let $\mathcal{X}$ be the column matrix defined by

$$\mathcal{X} = \begin{pmatrix} a_0 - b_0 \\ \vdots \\ a_{\frac{p-3}{2}} - b_{\frac{p-3}{2}} \end{pmatrix}.$$

Let $i \in \{1; \cdots; \frac{p-1}{2}\}$ be an integer. We have

$$[\mathcal{M}\mathcal{X}]_{i1} = \sum_{k=1}^{\frac{p-1}{2}} [\mathcal{M}]_{ik}[\mathcal{X}]_{k1} = \sum_{k=1}^{\frac{p-1}{2}} Z^{\sigma^{k-i}}(a_{k-1} - b_{k-1}) = \sum_{k=0}^{\frac{p-3}{2}} Z^{\sigma^{k-i+1}}(a_k - b_k).$$

From (28), we deduce that

$$[\mathcal{M}\mathcal{X}]_{i1} \equiv 0 \bmod \mathfrak{q}.$$

i being an arbitrary element of $\{1; \cdots; \frac{p-1}{2}\}$, we have

$$\forall i \in \left\{1; \cdots; \tfrac{p-1}{2}\right\}, [\mathcal{M}\mathcal{X}]_{i1} \equiv 0 \bmod \mathfrak{q}. \qquad (29)$$

Let $\mathcal{A}$ be the adjugate of the matrix $\mathcal{M}$. It follows from Lemma 2 of the Section 4 that the coefficients of $\mathcal{A}$ are elements of the ring $\mathbb{Z}\left[\zeta, \frac{1}{1-\zeta}\right]$. Particularly

$$\forall i, k \in \left\{1; \cdots; \tfrac{p-1}{2}\right\}, \nu_{\mathfrak{q}}([\mathcal{A}]_{ik}) \geqslant 0.$$

From (29) we deduce that

$$\forall i \in \left\{1; \cdots; \tfrac{p-1}{2}\right\}, [\mathcal{AMX}]_{i1} = \sum_{k=1}^{\frac{p-1}{2}} [\mathcal{A}]_{ik}[\mathcal{MX}]_{k1} \equiv 0 \bmod \mathfrak{q}. \tag{30}$$

By a well-known result $\mathcal{AMX} = \det(\mathcal{M})\mathcal{X}$.

Since $p \equiv 3 \bmod 4$, by Theorem 1 of [4]

$$\det(\mathcal{M}) = (-1)^{\frac{p-3}{4}} \times 2^{\frac{p-3}{2}} \times p^{\frac{p-7}{4}} \times h_p^- \times \sqrt{-p}.$$

Particularly

$$\mathcal{AMX} = (-1)^{\frac{p-3}{4}} \times 2^{\frac{p-3}{2}} \times p^{\frac{p-7}{4}} \times h_p^- \times \sqrt{-p}\mathcal{X}.$$

From (30), we deduce that $\forall i \in \{1; \cdots; \frac{p-1}{2}\}$,

$$2^{\frac{p-3}{2}} \times p^{\frac{p-7}{4}} \times h_p^- \times \sqrt{-p}[\mathcal{X}]_{i1} \equiv 0 \bmod \mathfrak{q},$$

that is

$$\forall i \in \left\{0; \cdots; \tfrac{p-3}{2}\right\}, 2^{\frac{p-3}{2}} \times p^{\frac{p-7}{4}} \times h_p^- \times \sqrt{-p}(a_i - b_i) \equiv 0 \bmod \mathfrak{q}. \tag{31}$$

By Lemma 1 of the Subsection 2.3, there exists $i_0 \in \{0; \cdots; \frac{p-3}{2}\}$ such that $a_{i_0} - b_{i_0} = \pm 1$. From (31) we deduce that

$$2^{\frac{p-3}{2}} \times p^{\frac{p-7}{4}} \times h_p^- \times \sqrt{-p} \equiv 0 \bmod \mathfrak{q},$$

that is $q | h_p^-$. The lemma is proved. □

6. Proof of the Theorem 1

Suppose that the Diophantine equation (1) has a solution $(X; Z)$ with $X \neq 1$. Since $X \neq 1$, this equation can be rewritten as

$$(X-1)\frac{X^p - 1}{X - 1} = BZ^q. \tag{32}$$

Recall that $p|B$. Write

$$B = p^{\nu_p(B)}B_1,\ Z = p^{\nu_p(Z)}Z_1,\ (p,\ B_1Z_1) = 1,$$

where ν_p is the p-adic valuation. We have

$$(X-1)\frac{X^p-1}{X-1} = p^{\nu_p(B)+q\nu_p(Z)} \cdot B_1 \cdot Z_1^q. \tag{33}$$

Since $\nu_p(B)+q\nu_p(Z) > 0$, by assertion 2 and 3 of Lemma 3, we have

$$\left(X-1,\ \frac{X^p-1}{X-1}\right) = p \text{ and } \nu_p\left(\frac{X^p-1}{X-1}\right) = 1. \tag{34}$$

Recall that if ℓ is a prime number dividing B, then $l \not\equiv 1 \bmod p$. By Proposition 2.10 of [9], if $\ell \neq p$ is a prime number dividing $\frac{X^p-1}{X-1}$ then $l \equiv 1 \bmod p$. Furthermore, if ℓ is a prime number dividing B_1 then $\ell \neq p$ and $\ell \not\equiv 1 \bmod p$ since $B_1|B$. Consequently B_1 is a divisor of $X-1$. So, from (33) and (34), we deduce that there exists integers Z_2 and Z_3 such that

$$X-1 = p^{\nu_p(B)+q\nu_p(Z)-1} \cdot B_1 \cdot Z_2^q,\ \frac{X^p-1}{X-1} = p \cdot Z_3^q,\ Z_1 = Z_2 \cdot Z_3.$$

By Theorem 1.1 of [3], $q|h_p^-$ in contradiction with the hypothesis $q \nmid h_p^-$. The theorem is proved. □

7. Proof of the Theorem 2

Suppose that the Diophantine equation (1) has a solution $(X;\ Z)$ with $X \neq 1$. If $p|BZ$, reasoning as before, we can prove that $q|h_p^-$ in contradiction with the hypothesis $q \nmid h_p^-$. So, we can suppose in the following that BZ is co-prime to p.

By a similar reasoning, as one used in the previous proof, there exists integers Z_1 and Z_2 such that

$$X - 1 = BZ_1^q, \frac{X^p - 1}{X - 1} = Z_2^q, Z = Z_1 Z_2. \tag{35}$$

Note that $Z_2 > 1$. Namely, by Lemma 3, $\frac{X^p - 1}{X - 1} = Z_2^q$ is a non-zero positive integer. Consequently, if $Z_2 \leqslant 1$ then $Z_2 = 1$. By Lemma 3 (note that $X \neq 0$), we obtain $X = -1$. Equation (35) implies that

$$1 + BZ_1^q = -1 \Rightarrow q = 2 (\text{since } q | B),$$

which is false. Consequently, we have

$$X - 1 = BZ_1^q, \frac{X^p - 1}{X - 1} = Z_2^q, Z_2 > 1. \tag{36}$$

Particularly

$$q | X - 1, \frac{X^p - 1}{X - 1} = Z_2^q, Z_2 > 1. \tag{37}$$

• Assume that $7 \leqslant p \leqslant 191$. Thus, by hypothesis $p \equiv 3 \bmod 4$. From (37) we know that $q | X - 1$. By Lemma 9, $q^2 | X - 1$ since $q \nmid h_p^-$. From (36), we deduce that

$$q^2 | BZ_1^q \Rightarrow q | Z_1,$$

since the q-adic valuation of B is equal to 1. The fact that q is a divisor of Z_1 implies that

$$|X| = |1 + BZ_1^q| \geqslant |B| q^q - 1.$$

By hypothesis, $7 \leqslant p < q$ and $q | B$. Particularly $8 < q \leqslant |B|$, so that

$$|X| \geqslant |B| q^q - 1 \Rightarrow |X| > 8q^q - 1 \Rightarrow |X| \geqslant 8q^q.$$

Nevertheless, (36) and Lemma 6 imply that $|X| < 8q^q$ in contradiction with the previous result. Consequently, $X = 1$ and $Z = 0$ is the only solution of the Diophantine equation (1) if $7 \leqslant p \leqslant 191$, $p \equiv 3 \bmod 4$.

- Assume that $p > 191$. From (37) we know that $q | X - 1$. By Theorem 1 of [6], $q^2 | X - 1$ since $q \nmid h_p^-$. Then, reasoning as before, we can prove that $|X| \geqslant 8q^q$ and $|X| < 8q^q$ which give us a contradiction. The theorem is proved. □

References

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

DOI: https://doi.org/10.1007/978-3-319-10094-4

[2] H. Cohen, Number Theory, Springer, New York, 2007.

[3] B. Dupuy, A class number criterion for the equation $(x^p - 1)/(x - 1) = py^q$, Acta Arithmetica 127(4) (2007), 391-401.

DOI: https://doi.org/10.4064/aa127-4-5

[4] B. Dupuy, Note on a determinant, Integers 20 (2020); Article 48.

[5] P. Mihailescu, A class number free criterion for Catalan's conjecture, Journal of Number Theory 99(2) (2003), 225-231.

DOI: https://doi.org/10.1016/S0022-314X(02)00101-4

[6] P. Mihailescu, New bounds and conditions for the equation of Nagell-Ljunggren, Journal of Number Theory 124(2) (2007), 380-395.

DOI: https://doi.org/10.1016/j.jnt.2006.10.010

[7] P. Mihailescu, On the class groups of cyclotomic extensions in presence of a solution to Catalan's equation, Journal of Number Theory 118(1) (2006), 123-144.

DOI: https://doi.org/10.1016/j.jnt.2005.08.011

[8] P. Ribenboim, Catalan's Conjecture, Academic, Boston, 1994.

[9] L. Washington, Introduction to Cyclotomic Fields, Springer, Berlin, Second Edition, 1997.

■