ON THE EQUATION $X^n - 1 = BZ^n$

B. BARTOLOMÉ AND P. MIHĂILESCU

Abstract. We consider the Diophantine equation $X^n - 1 = BZ^n$, where $B \in \mathbb{Z}$ is understood as a parameter. We prove that if the equation has a solution, then either the Euler totient of the radical, $\varphi(\text{rad} (B))$, has a common divisor with the exponent $n$, or the exponent is a prime and the solution stems from a solution to the diagonal case of the Nagell–Ljunggren equation: $\frac{X^n - 1}{X - 1} = n^e Y^n$, $e \in \{0, 1\}$. This allows us to apply recent results on this equation to the binary Thue equation in question. In particular, we can then display parametrized families for which the Thue equation has no solution. The first such family was proved by Bennett in his seminal paper on binary Thue equations [BE].

1. Introduction

Let $B, n \in \mathbb{N}_{>1}$ be such that

$\varphi^*(B) := \varphi(\text{rad} (B))$ and $(n, \varphi^*(B)) = 1$.

Here rad $(B)$ is the radical of $B$ and the condition implies that $B$ has no prime factors $t \equiv 1 \mod n$. In particular, none of its prime factors split completely in the $n$-th cyclotomic field.

More generally, for fixed $B \in \mathbb{N}_{>1}$ we let

$\mathcal{N}(B) = \{n \in \mathbb{N}_{>1} \mid \exists k > 0$ such that $n | \varphi^*(B)^k \}$.

If $p$ is an odd prime, we shall denote by CF the combined condition requiring that

(i) The Vandiver Conjecture holds for $p$, so the class number $h^+_p$ of the maximal real subfield of the cyclotomic field is not divisible by $p$.

(ii) The index of irregularity of $p$ is large, namely $i(r) > \sqrt{p} - 1$, so there are $i(r)$ odd integers $k < p$ such that the Bernoulli number $B_k \equiv 0 \mod p$.

It is known from recent computations of Buhler and Harvey [BH] that the condition CF is satisfied by primes up to $163 \cdot 10^6$.

We consider the binary Thue equation

$X^n - 1 = B \cdot Z^n$,

where solutions with $Z \in \{-1, 0, 1\}$ are considered to be trivial. It is a special case of the general Pillai conjecture (Conjecture 13.17 of [BBM]). This equation is encountered as a particular case of binary Thue equations of the type

$aX^n - bY^n = c$,

see [BGMP]. In a seminal paper [BE], Michael Bennett proves that in the case of $c = \pm 1$ there is at most one solution for fixed $(a, b; n)$ and deduces that the

Date: December 19, 2014.
parametric family \((a + 1, a; n)\) has the only solution \((1, 1)\) for all \(n\). The equation (3) inserts naturally in the family of equations (4), with \(a = c = \pm 1\).

Current results on (3) are restricted to values of \(B\) which are built up from small primes \(p \leq 13\) [4]. If expecting that the equation has no solutions, – possibly with the exception of some isolated examples – it is natural to consider the case when the exponent \(n\) is a prime. Of course, the existence of solutions \((X, Z; B)\) for composite \(n\) imply the existence of some solutions with \(n\) prime, by raising \(X, Z\) to a power. In this vein, we prove the following:

**Theorem 1.** Let \(n\) be a prime and \(B > 1\) an integer with \((\varphi^*(B), n) = 1\). Suppose that the equation (3) has a non trivial integer solution different from \(n = 3\) and \((X, Z; B) = (18, 7; 17)\). Let \(X \equiv u \pmod{n}, 0 \leq u < n\) and \(e = 1\) if \(u = 1\) and \(e = 0\) otherwise. Then:

- (A) \(n > 163 \cdot 10^6\).
- (B) \(X - 1 = \pm B/n^e\) and \(B < n^e\).
- (C) If \(u \neq \pm 1\) then and condition CF (i) holds for \(n\) and

\[
\begin{align*}
2^n & \equiv 3^n \equiv 1 \pmod{n^2}, \\
r^{n-1} & \equiv 1 \pmod{n^2} \text{ for all } r | X(X^2 - 1).
\end{align*}
\]

If \(u = \pm 1\), then Condition CF (ii) holds for \(n\).

The particular solution \(n = 3\) and \((X, Z; B) = (18, 7; 17)\) is reminiscent of a solution of the diagonal Nagell solution; it is commonly accepted that the existence of non trivial solutions tends to render equations more difficult to solve. Based on Theorem 1 we prove nevertheless:

**Theorem 2.** If the equation (3) has a solution for fixed \(B\), then either \(n \in \mathcal{N}(B)\) or there is a prime \(p\) coprime to \(\varphi^*(B)\) and a \(m \in \mathcal{N}(B)\) such that \(n = p \cdot m\). Moreover \(X^m, Y^m\) are a solution of (3) for the prime exponent \(p\) and thus verify the conditions in Theorem 1.

2. Preliminary results

The proof of this Theorem is based on results from [4]. It has been pointed out that the proof of Theorem 3 in [4] may require some more detailed explanation in the case of a singular system of equations in the proof of Lemma 15 of [4]. We provide here a comprehensive proof which confirms the indications given in [4]; this will be done in form of an elementary lemma, in the next section.

2.1. Clarification on the singular case of Theorem 3 in [4]. Let \(m \in \mathbb{Z}_{>0}\) be a positive integer, \(K\) a field, \(V = K^m\) as a \(K\)-vector space and let \(f\) be an homomorphism from \(V\) into \(V\), of rank \(m - r\), with \(r \leq m\). Let \(L = \text{Ker } (f) \subset V\) be the kernel; so \(r = \dim_K(L)\). In a complex-vector space in finite dimension, we choose the standard Hermitian inner-product \(<x, y> = \sum_k x_k \bar{y}_k\). Fix an orthonormal basis \(E_L = (e_1, e_2, \ldots, e_r)\) of \(L\), which we complete to an orthonormal basis of \(V\), \(E = (e_1, e_2, \ldots, e_r, e_{r+1}, \ldots, e_m)\), and assume that there exists at least one vector \(w_1 \in L\) which is free of 0-entries over the base \(\mathcal{E}\). For \((x, y) \in V^2\), the Hadamard product is defined by \([x, y] = \text{Diag}(x) \cdot y \in V\), where \(\text{Diag}(x)\) is the diagonal matrix built from the vector \(x\). For any subspace \(W \subset V\) we define the \(W\)-bouquet of \(L\) by

\[
L_W = \{ [w, x] : w \in W, x \in L \}_K.
\]
the \( \mathbb{K} \)-span of all the Hadamard products of elements in \( W \) by vectors from \( L \).

**Lemma 1.** Let \( A_2 = \{\{a_1, a_2\}\} \) a set of two linear independent vectors which are free of \( 0 \)-entries over \( e \), such that the components of each \( a_i \) (\( 1 < i \leq l \)) are pairwise distinct over \( \mathcal{E} \) and such that \( a_1 = (1, 1, \ldots, 1) \) over \( e \). Let \( L_{A_2} \) be the resulting \( A_2 \)-bouquet. Then \( \dim(L_{A_2}) > \dim(L) \).

**Proof.** Obviously, \( L \subset L_{A_2} \) (as \( a_1 \in A \)). We would like to show that \( L_{A_2} \neq L \). We know that the system \((w_1, [w_1, a_2], [w_1, a_2^2], \ldots, [w_1, a_2^{m-1}])\) (the notion of power of a vector here is to be understood as an "Hadamard power") is free (as it induces a Vandermonde matrix over \( \mathcal{E} \), neither \( w_1 \) nor \( a_2 \) have any zero among their components and all components of \( a_2 \) are pairwise distinct). We know that \( w_1 \in L \), let us assume that \([w_1, a_2^i] \in L \) for \( i \leq j \) (we know that \( j \leq r \leq m \)). Then, \([w_1, a_2^i] \in L \) and \([w_1, a_2^{i+1}] \notin L \). However, the Hadamard product of \([w_1, a_2^i] \in L \) by \( a_2 \), that is \([w_1, a_2^{i+1}] \), belongs to \( L_{A_2} \). Thus, \( \dim L_{A_2} > \dim L \). \( \square \)

2.2. Application of Lemma [1] to the proof of the singular case in Lemma 15 of [M1]. We apply here the lemma in the first case (that is \( x \not\equiv s \) mod \( p \), where \( s \in \{-1, 0, 1\} \)), the application to the second case being identical.

Let all notations be like in Lemma 15 in [M1]. As in [M1], we will assume that \( A = (\zeta^{-\kappa_{ac} \cdot \theta} \cdot a_{a, c = 1}^{(p-1)/2}) \) (where \( \kappa_{ac} \) are the Galois exponents) is singular. Let \( m = (p-1)/2 \), \( \mathbb{K} = \mathbb{Q}(\zeta_p) \) and \( r = \) rank \( (A) < (p-1)/2 \). Without loss of generality, we assume that a regular \( r \)-submatrix of \( A \) is built with the first \( r \) rows and the first \( r \) columns. Therefore, the first \( r \) rows of \( A \) are independent, and we denote by \( W \) the sub-space of \( V = \mathbb{K}^m \) generated by the first \( r \) row vectors \( w_1, \ldots, w_r \) of \( A \). For \( a_1 = (1, 1, \ldots, 1) \), we let \( a_2 \) be the vector of \( V \) whose components are \((\eta(\sigma, \theta))^{(p-1)/2} \) and \( A_2 = \{a_1, a_2\} \). Then, according to Lemma [1] there exists at least one vector \( \bar{v} \in L_{A_2} \) which is independent on the first \( r \) vectors of \( A \).

Let \( S \) be the \((r+1) \times (r+1)\) submatrix of \( A \) comprising the first \( r \) rows and \( r+1 \) columns of \( A \), to which we have added an additional row: the first \( r+1 \) terms of \( \bar{v} \). Let \( \bar{X}' \) be the vector solution of \( A \bar{X}' = \bar{d}' \), where \( \bar{d}' = (\delta_{c, r+1})_{c=1}^{r+1} \). We know that \( \bar{X}' \neq 0 \), as \( S \) is regular and \( \bar{d}' \) is not the null vector. For \( 1 \leq c \leq r+1 \), by Cramer’s rule, \( \lambda_c = \frac{S_c}{\bar{d}} \), where \( S_c \) are the determinants of some minors of \( S \) obtained by replacing the \( c \)-column by \( \bar{d}' \), and \( S = \det S \).

Let \( \bar{X} \in V \) be a vector whose first \( r+1 \) coordinates are those of \( \bar{X}' \) and the others are 0. Let \((\delta_{c, r+1})_{c=1}^{r+1} \). Then, \( \bar{X} \) verifies: \( A \bar{X} = \bar{d} \).

Let \( \delta = \sum_{c=1}^{r+1} (\lambda_c \cdot \beta_c + \lambda_c \cdot \beta_c) \). Using Hadamard’s inequality, we bound \( |S_c| \leq (\frac{p+1}{p-1})^{p+1} = D_1 \) and \( |S| \leq (\frac{p+1}{p-1})^{3p+2} = D_0 \). Then, using the fact that the choice of \( \lambda_c \) eliminates the first term in the expansion of \( f_c \), we find that \( |S| \cdot |\delta| \leq 2x^{(p-1)/2} \cdot \sum_{c=1}^{r+1} |S_c||R_{c, 0}(x)| \), where \( R_{c, 0}(x) = f_c(x) - x^{(p-1)/2} \). With the same arguments as in [M1], we deduce:

\[
|S| < 2(p-1)D_1 \cdot \frac{1}{|x|^{(p-1)/2} + \frac{1}{|x|^{(p-1)(p+1)} \cdot 4^p}}.
\]

This inequality holds for all conjugates \( \sigma_c(\delta) \), thus leading to:

\[
|N(S)\delta| < (2(p-1)D_1)^{(p-1)/2} \cdot \frac{1}{|x|^{(p-1)(p+1)} \cdot 4^p}.
\]
If $\delta \neq 0$, then $|N(S\delta)| \geq 1$ and thus $|x| \leq 2^{5-p} \left(\frac{p}{2}\right)^{\frac{3}{2}}$. If $\delta = 0$, then $0 = S\delta = S \cdot |x|^{(p-1)/2} - \sum_{c=1}^{(p-1)/2} S_c R_0 c$, and thus:

$$|x| \leq \sum_c |S_c|/|S| < (p-1)D_1 < 3 \left(\frac{p-3}{2}\right)^{(p-3)/2}.$$  

These bounds are better than the ones in [Mi], and this concludes the clarification.

### 2.3. Link of (3) with the diagonal Nagell–Ljunggren equation.

In order to use the results from [Mi], we relate (3) to the diagonal Nagell–Ljunggren equation

$$X^n - 1 = n^e Y^n, \quad e = \begin{cases} 0 & \text{if } X \equiv 1 \mod n, \\ 1 & \text{otherwise.} \end{cases}$$

First, note that $\delta = \left(\frac{X^n-1}{X-1}\right)n$ and $\delta = n$ exactly when $X \equiv 1 \mod n$. Indeed, from the expansion

$$X^n - 1 = ((X-1)+1)^n - 1 = n + k(X-1),$$

with $k \in \mathbb{Z}$, one deduces the claim $\delta | n$. If $D \neq 1$, then $\delta = n$ and thus $n|(X-1)$ must hold. Conversely, inserting $X \equiv 1 \mod n$ in the previous expression shows that in this case $\delta = n$.

We first show that any solution of (3) leads to a solution of (5). For this, let $\text{rad} \left(\frac{X^n-1}{n(X-1)}\right) = \prod_{i=1}^{K} p_i$. Obviously, $\text{rad} \left(\frac{X^n-1}{n(X-1)}\right) \mid \text{rad} \left((X^n-1)\right)$. Let $\zeta \in \mathbb{C}$ be a primitive $n$–th root of unity. Then the numbers $\alpha_c = \frac{X^{c-1}}{(1-\zeta)^c} \in \mathbb{Z}[\zeta]$, by definition of $e$ and $(\alpha_c, n) = 1$. Since for distinct $c, d \not\equiv 0 \mod n$ we have $(1-\zeta^c)^e \cdot \alpha_d - (1-\zeta^d)^e \cdot \alpha_c = \zeta^c - \zeta^d$, it follows that $(\alpha_c, \alpha_d) \mid (1 - \zeta)$ and in view of $(\alpha_c, n) = 1$, it follows that the $\alpha_c$ are coprime. But $\prod_{c=1}^{n-1} \alpha_c = \frac{X^n-1}{n(X-1)}$.

Thus, for any rational prime $p_i \mid \frac{X^n-1}{n(X-1)}$, all of its conjugates are coprime and thus different: their decomposition group in the $n$–th cyclotomic extension is trivial and they are all totally split. We remind here that such a prime $p_i$ also belongs to $\text{rad} \left((X^n-1)\right)$. For such a prime $p_i$, if $(X, Z; B)$ is a solution of (3), it follows from (11) that $(p_i, B) = 1$, and thus $p_i | Z$; furthermore, (3) implies that there exists $j_i > 0$ such that $p_i^{j_i} \parallel Z^n$ and thus $p_i^{j_i} \parallel \frac{X^n-1}{n(X-1)}$. This holds for all primes $p_i \mid \text{rad} \left(\frac{X^n-1}{n(X-1)}\right)$.

It follows that (3) is verified for $Y = \prod_{i=1}^{K} p_i^{j_i}$ and $Y \mid Z$. We have proved that if $(X, Z)$ is a solution of (3) for the prime $n$, then there exists $C \in \mathbb{Z}$ such that $Z = C \cdot Y$ with $Y$ as above, and:

$$\frac{X^n-1}{n^e(X-1)} = Y^n \quad \text{and} \quad \frac{X-1}{n^e} = B \cdot C^n/n^e.$$

It follows that any integer solution of (3) induces one of (4).

Conversely, if $(X, Y)$ is a solution of (5), then $(X, Y; n^e(X-1))$ is a solution of (3). For instance, the particular solution $(X, Y; B) = (18, 7; 17)$ of (3) stems from

$$\frac{18^3-1}{18-1} = 7^3,$$

which is supposed to be the only non trivial solution of (4).
Remark 1. Note that if \((X, Z)\) verify (3), then \((-X, Z)\) is a solution of \(\frac{X^n + 1}{X + 1} = BZ^n\), so the results apply also to the equation:

\[ X^n + 1 = BZ^n. \]

2.4. Bounds to the solutions of Equation (5). We shall use the following Theorem from [Mi]:

Theorem 3. Suppose that \(X, Y\) are integers verifying (5) with \(n \geq 17\) being a prime. Let \(u = (X \mod n)\). Then there is an \(E \in \mathbb{R}_+\) such that \(|X| < E\). The values of \(E\) in the various cases of the equation are the following:

\[ E = \begin{cases} 
4 \cdot \left(\frac{n-1}{2}\right)^{\frac{n+2}{2}} & \text{if } u \notin \{-1, 0, 1\} \\
(4n)^{\frac{n}{2}} & \text{if } u = 0, \\
4 \cdot (n-2)^n & \text{otherwise}.
\end{cases} \tag{8} \]

By comparing the bounds (3) with (7), it follows that \(|C| < 2n\). In particular, the primes dividing \(C\) do not split completely in \(\mathbb{Q}[[n]]\) – since a prime splitting in this field has the form \(r = 2kn + 1 > 2n\).

Remark 2. Note that \(|C| < 2n\) implies a fortiori that for all primes \(r|C, r^2 \neq 1 \mod n\). Thus the 2 - part of the group \(< r \mod n\) has at least four elements.

2.5. A combinatorial lemma.

Lemma 2. Let \(p\) be an odd prime, \(k \in \mathbb{N}\) with \(1 < k < \log_2(p)\) and \(P = \{1, 2, \ldots, p - 1\}\). If \(S = \{a_1, a_2, \ldots, a_k\} \subset P\) is a set of distinct numbers and \(A = [p^{k/2}]\), then there are \(k\) numbers \(b_i \in \mathbb{Z}\), \(i = 1, 2, \ldots, k\), not all zero, with \(0 \leq |b_i| \leq A\) and such that

\[ \sum_{i=1}^{k} a_i b_i \equiv 0 \mod p. \]

Proof. Let \(T = \{1, 2, \ldots, A\} \subset P\). Consider the functional \(f : T^k \to \mathbb{Z}/(p \cdot \mathbb{Z})\) given by

\[ f(\vec{t}) \equiv \sum_{i=1}^{k} t_i a_i \mod p, \quad \text{with } \vec{t} = (t_1, t_2, \ldots, t_k) \in T^k. \]

Since \(|T^k| > p\), by the pigeon hole principle there are two vectors \(\vec{t} \neq \vec{t}'\) such that \(f(\vec{t}) \equiv f(\vec{t}') \mod p\). Let \(b_i = t_i - t_i'\); by construction, \(0 \leq |b_i| \leq A\) and not all \(b_i\) are zero, since \(\vec{t} \neq \vec{t}'\). The choice of these vectors implies \(\sum_{i=1}^{k} a_i b_i \equiv 0 \mod p\), as claimed. \(\square\)

2.6. Auxiliary facts on the Stickelberger module. The following results are deduced in [Mi] and they shall only be mentioned here without proof.

Let \(\zeta\) be a primitive \(n\)-th root of unity, \(\mathbb{K} = \mathbb{Q}(\zeta)\) the \(n\)-th cyclotomic field and \(G = \text{Gal}(\mathbb{K}/\mathbb{Q})\) the Galois group. The automorphisms \(\sigma_a \in G\) are given by \(\zeta \mapsto \zeta^a\), \(a = 1, 2, \ldots, n - 1\); complex conjugation is denoted by \(\bar{\zeta} \in \mathbb{Z}[G]\). The Stickelberger module is \(I = \vartheta \cdot \mathbb{Z}[G] \cap \mathbb{Z}[G]\), where \(\vartheta = \frac{1}{n} \sum_{c=1}^{n-1} c \cdot \sigma_c^{-1}\) is the Stickelberger element. For \(\theta \in I\) we have the relation \(\theta + \vartheta \theta = \zeta(\theta) \cdot N\), where \(\zeta(\theta) \in \mathbb{Z}\) is called the relative weight of \(\theta\). The Fueter elements are

\[ \psi_k = (1 + \sigma_k - \sigma_{k+1}) \cdot \vartheta = \sum_{c=1}^{n-1} \left( \left\lfloor \frac{(k+1)c}{n} \right\rfloor - \left\lfloor \frac{kc}{n} \right\rfloor \right) \cdot \sigma_c^{-1}, \quad 1 \leq k \leq (n-1)/2. \]
Together with the norm, they generate $I$ as a $\mathbb{Z}$-module (of rank $(n + 1)/2$) and $\zeta(\psi_k) = 1$ for all $k$.

The Fuchsian elements are

$$\Theta_k = (k - \sigma_k) \cdot \vartheta = \sum_{c=1}^{n-1} \left[ \frac{kc}{n} \right] \cdot \sigma_c^{-1}, \quad 2 \leq k \leq n.$$ 

They also generate $I$ as a $\mathbb{Z}$-module. Note that $\Theta_n$ is the norm, and that we have the following relationship between the Fueter and the Fuchsian elements:

$$\psi_1 = \Theta_2$$

$$\psi_k = \Theta_{k+1} - \Theta_k, \quad k \geq 2$$

The Fermat quotient map $I \to \mathbb{Z}/(n \cdot \mathbb{Z})$, given by

$$\varphi : \theta = \sum_{c=1}^{n-1} n_c \sigma_c^{-1} \mapsto \sum_{c=1}^{n-1} n_c / c \mod n,$$

is a linear functional, with kernel $I_f = \{ \theta \in I : \zeta^\theta = 1 \}$ (the Fermat module), and enjoys the properties:

$$\zeta^\theta = \zeta^{\varphi(\theta)},$$

$$(1 + \zeta)^\theta = \zeta^{\varphi(\theta)/2},$$

$$(1 - \zeta)^\theta = \zeta^{\varphi(\theta)/2} \cdot \left( \left( \frac{-1}{n} \right) n \right)^{\varphi(\theta)/2},$$

where $\left( \frac{-1}{n} \right)$ is the Legendre symbol.

The last relation holds up to a sign which depends on the embedding of $\zeta$. For a fixed embedding, we let $\nu = \sqrt{\left( \frac{-1}{n} \right) n}$ be defined by $(1 - \zeta)^\theta = \zeta^{\varphi(\theta)/2} \cdot \nu$. Note that for $\theta \in I$ with $\zeta(\theta) = 2$ we have $(1 - \zeta)^{2\theta} = \zeta^{2\varphi(\theta)} \cdot n^2$ for any embedding.

We define the following additive maps:

$$\rho_0 : \mathbb{F}_n[G] \to \mathbb{Q}[\zeta], \quad \theta = \sum_{c=1}^{n-1} n_c \sigma_c \mapsto \sum_{c \in P} \frac{n_c}{1 - \sigma_c},$$

and

$$\rho : \mathbb{F}_n[G] \to \mathbb{Z}[\zeta], \quad \theta \mapsto (1 - \zeta) \cdot \rho_0[\theta].$$

The $(i)$-th moment of an element $\theta = \sum_{c=1}^{n-1} n_c \sigma_c^{-1}$ of $\mathbb{Z}[G]$ is defined as:

$$\phi^{(i)}(\theta) = \sum_{c=1}^{n-1} n_c c^i \mod n.$$ 

Note that $\phi^{(1)}$ is the Fermat quotient map: $\phi^{(1)} = \varphi$.

Let $\alpha = \frac{X - \zeta}{(1 - \zeta)} \in \mathbb{Z}[\zeta]$, as before, and define $c_e \equiv 1/(X - 1) \mod n$ if $e = 0$ and $c_e = 0$ if $e = 1$. For any $\theta \in I$, there is a Jacobi integer $\beta[\theta] \in \mathbb{Z}[\zeta]$ such that $\beta[\theta]^n = (\zeta - \alpha)^\theta$, normed by $\beta[\theta] \equiv 1 \mod (1 - \zeta)^2$ [Mi]. The definition of $\zeta(\theta)$ implies that

$$\beta[\theta] \cdot \zeta(\theta) = N_{K/Q}(\alpha)^{\zeta(\theta)} = Y^{\zeta(\theta)}.$$
We have for any $\theta \in I$,

\begin{equation}
\beta[\theta]^n = (\zeta^{c_\theta} \alpha)^\theta = (\zeta^{c_\theta} (1 - \zeta)^{1 - e})^\theta \cdot \left(1 + \frac{X - 1}{1 - \zeta}\right)^\theta
\end{equation}

**Lemma 3.** For any $\theta \in 2 \cdot I_f$, for any prime ideal $\mathfrak{P} \mid D$, there is a $\kappa = \kappa_{\mathfrak{P}}(\theta) \in \mathbb{Z}/(n \cdot \mathbb{Z})$ such that

\begin{align*}
\beta[\theta] &\equiv \zeta^{\kappa} \cdot Y^{\xi(\theta)} \mod \mathfrak{P} \quad \text{and} \\
\overline{\beta}[\theta] &\equiv \zeta^{-\kappa} \cdot Y^{\xi(\theta)} \mod \mathfrak{P},
\end{align*}

the second relation not requiring that $\mathfrak{P}$ be fixed under complex conjugation.

**Proof.** Let $\theta_0$ be an element of $I_f$, and let $\theta = 2\theta_0$. Note that from (11) we have $Y^{\xi(\theta_0)n} = \beta[\theta_0]^n \cdot \overline{\beta}[\theta_0]^n$. Thus $\beta[\theta]^n = \beta[\theta_0]^{2n} = Y^{\xi(\theta_0)n} \cdot (\beta[\theta_0]/\overline{\beta}[\theta_0])^n$. Using (10) and the previous observations, we find:

\begin{align*}
\beta[\theta]^n &= Y^{\xi(\theta_0)n} \cdot (\zeta^{c_\theta} (1 - \zeta)^{1 - e})^{(\theta_0 - \kappa\theta_0)} \cdot \left(1 + \frac{X - 1}{1 - \zeta}\right)^{(\theta_0 - \kappa\theta_0)} \\
&= Y^{\xi(\theta_0)n} \cdot \zeta^{2c_\theta + 1} \xi(\theta_0) \cdot (1 + D/(1 - \zeta))^{(\theta_0 - \kappa\theta_0)} \\
\beta[\theta]^n &= Y^{\xi(\theta_0)n} \cdot \left(1 + \frac{D}{1 - \zeta}\right)^{(\theta_0 - \kappa\theta_0)}.
\end{align*}

Thus for any prime ideal $\mathfrak{P} \mid D$ there is a $\kappa = \kappa_{\mathfrak{P}}(\theta) \in \mathbb{Z}/(n \cdot \mathbb{Z})$ such that

\begin{align*}
\beta[\theta] &\equiv \zeta^{\kappa} \cdot Y^{\xi(\theta_0)} \mod \mathfrak{P} \quad \text{and} \\
\overline{\beta}[\theta] &\equiv \zeta^{-\kappa} \cdot Y^{\xi(\theta_0)} \mod \mathfrak{P}.
\end{align*}

The second relation follows from (11) and does not require that $\mathfrak{P}$ be fixed under complex conjugation. Note that the two relations (10) and (11) lead to a binomial series expansion for $\beta[\theta]$. \hfill \square

We will also use the Voronoi identities – see Lemma 1.0 in [Jha] –, which we remind here for convenience:

**Lemma 4.** Let $m$ be an even integer such that $2 \leq m \leq n - 1$. Let $a$ be an integer, coprime to $n$. Then

\[
a^m \sum_{j=1}^{n-1} \left[\frac{aj}{n}\right] j^{m-1} \equiv \frac{(a^{m+1} - a)B_m}{m} \mod n,
\]

where $B_m$ is the $m$-th Bernoulli number. In particular, for $m = n - 1$, we get

\[
\sum_{j=1}^{n-1} \left[\frac{aj}{n}\right] j^{n-2} \equiv \frac{a^n - a}{n} \mod n,
\]

which is the Fermat quotient map of the $a$-th Fuchsian element, $\varphi(\Theta_a)$.

**Lemma 5.** Let $\psi_k$ be the $k$-th Fueter element. Then, there exists no constant $A$ such that, for all $k > 1$, $\phi^{(-1)}(\psi_k) = A \cdot \phi^{(1)}(\psi_k)$.  

Proof. By linearity, we can prove it for the Fuchsian elements and use the definition of the Fueter elements as a function of the Fuchsian elements. Let $\varphi$ be the Fermat quotient map. For any integer $1 < k < n - 1$, we have:

\[(n-k)n-(n-k) \equiv -k^n - n + k \mod n^2 \]

\[\equiv -n \left(\frac{k^n - k}{n} + 1\right) \mod n^2.\]

Dividing both terms by $n$ we find:

\[(12) \quad \varphi(\Theta_{n-k}) = n - (1 + \varphi(\Theta_k)).\]

With this result in mind, assume that such a constant $A$ exists and remember that $\varphi(1) = \varphi$. Using Lemma 4 with $m = 2$, we find that:

\[\varphi(-1)(\Theta_k) = A \cdot \varphi(\Theta_k) \equiv k^3 - k^2 - k \mod n^2.\]

However, $B_2 = 1/6$, and thus the equation becomes:

\[\varphi(\Theta_k) \equiv \frac{1}{12A} \left(k - \frac{1}{k}\right) \mod n, \text{ for all } 1 < k < n - 1.\]

This equation is also true for $\varphi(\Theta_{n-k}) \equiv \frac{1}{12A} \left(n - k - \frac{1}{n-k}\right) \mod n, \text{ for all } 1 < k < n - 1.$

Equation (12) shows that in this case, $A$ would depend on $k$ and $n$. □

The following two lemmas yield computational details for binomial series developments that we shall use.

**Lemma 6.** Let $\theta = \sum_{c=1}^{n-1} n_c \sigma_c \in \mathbb{Z}[G]$ and $f[\theta] = \left(1 + \frac{D}{1-\zeta}\right)^{\theta/n}$. Then,

\[f[\theta] = 1 + \sum_{k=1}^{N} \frac{a_k[\theta]}{k!n^k} D^k + O(D^{N+1}),\]

where

\[a_k[\theta] = \rho_k[\theta] + O\left(\frac{n}{(1-\zeta)^k}\right).\]

**Proof.** We prove this result by induction on the number of components of $\theta$. First, note that

\[\binom{n_c/n}{k} = \frac{1}{k!} \cdot \frac{n^k}{n^k} \cdot (1 + O(n)).\]

Thus, if $\theta = n_c \sigma_c$, then:

\[f[\theta] = 1 + \sum_{k=1}^{n-1} \frac{1}{k!} \cdot \frac{n^k}{n^k} \cdot (1 + O(n)) \cdot \frac{D^k}{(1-\zeta)^k} = 1 + \sum_{k=1}^{N} \frac{a_k[\theta]}{k!n^k} D^k + O(D^{N+1}),\]

where

\[a_k[\theta] = \rho_k[\theta] + O\left(\frac{n}{(1-\zeta)^k}\right).\]

Assume that $\theta = \theta_1 + \theta_2$ with $\theta_i \in I, i = 1, 2$ for which the Lemma holds. Then,

\[f[\theta] = \left(1 + \frac{D}{1-\zeta}\right)^{\theta_1/n} \cdot \left(1 + \frac{D}{1-\zeta}\right)^{\theta_2/n} \]

\[= 1 + \sum_{k=1}^{N} \alpha_k[\theta] D^k + O(D^{N+1}),\]
where
\[ \alpha_k[\theta] = \sum_{j=1}^{k} \frac{a_j[\theta_1]}{\prod_{i=1}^{j}(1-\zeta^i)} \cdot \frac{a_{k-j}[	heta_2]}{\prod_{i=1}^{k-j}(1-\zeta^{k-j+i})} \cdot (1 + O(n)) \]
\[ = \frac{1}{\prod_{l \leq n} (\rho_0[\theta_1] + \rho_0[\theta_2])^k + O \left( \frac{n}{\prod_{l \leq n}(1-\zeta^l)} \right)} \]
\[ = \frac{1}{\prod_{l \leq n}} \rho_0^k[\theta] + O \left( \frac{n}{\prod_{l \leq n}(1-\zeta^l)} \right). \]

This proves the claim by complete induction. \( \square \)

As a consequence, we may deduce that matrices built from the first coefficients occurring in some binary series developments are regular.

**Lemma 7.** Let \( \theta = \sum_{e=1}^{n-1} n_e \sigma_e \in \mathbb{Z}[G] \) such that \( \phi^{(-1)}(\theta) \not\equiv 0 \mod n \), let \( f[\theta] = \left( 1 + \frac{D}{1-c} \right)^{\theta/n} \) and \( 0 < N < n \) be a fixed integer. Then,
\[ f[\theta] = 1 + \sum_{k=1}^{N} b_k[\theta] D^k + O(D^{N+1}), \]
with \( b_k[\theta] \in \mathbb{Z}[\zeta] \), and the matrix
\[ A_N = (b_k[\theta])_{c,k=1} \in GL(\mathbb{K}, N). \]

**Proof.** Let \( \lambda = 1 - \zeta \); we show that the determinant of \( A_N \) is not zero modulo \( \lambda \). Using Lemma 6, we know that we have a development of symbolic power series
\[ f[\theta] = 1 + \sum_{k=1}^{N} a_k[\theta] D^k + O(D^{N+1}), \]
where
\[ a_k[\theta] = \rho_0^k[\theta] + O \left( \frac{n}{(1-\zeta)^k} \right). \]

By definition, \( (1-\zeta)^k \cdot a_k[\sigma, \theta], k = \mathbb{Z}[\zeta] \) for all \( \sigma \in G \). Let \( b_k[\theta] = (1-\zeta)^k \cdot a_k[\theta] \in \mathbb{Z}[\zeta] \). Then, according to Lemma 6
\[ b_k[\sigma, \theta] = (1-\zeta)^k \cdot \left( \rho_0^k[\sigma, \theta] + O \left( \frac{n}{(1-\zeta)^k} \right) \right) \]
\[ = \rho_0^k[\sigma, \theta] + O(n) \]
\[ = \left( \sum_{l=1}^{n-1} n_l \cdot \frac{1}{1-\zeta^l} \right)^k + O(n) \]
\[ = \left( \sum_{l=1}^{n-1} \frac{n_l}{l-\zeta} \right)^k \mod \lambda \]
\[ = \left( \phi^{(-1)}[\theta] \right)^k \mod \lambda. \]

Thus, \( \det A_N \equiv \left( \left( \frac{\phi^{(-1)}[\theta]}{c} \right)^k \right)_{k,c=1}^N \mod \lambda \). We obtained a Vandermonde determinant:
\[ \det A_N \equiv \left( \phi^{(-1)}[\theta] \right)^{N(N-1)/2} \cdot \prod_{i \not= j}^{1 \leq i,j \leq N} \left( \frac{1}{i} - \frac{1}{j} \right) \mod \lambda. \]

The assumption that \( \phi^{(-1)}[\theta] \not\equiv 0 \mod n \), together with \( 1/i \not\equiv 1/j \mod n \) for \( 0 < i \neq j < n \), imply finally that \( \prod_{i \not= j}^{1 \leq i,j \leq N} \left( \frac{1}{i} - \frac{1}{j} \right) \not\equiv 0 \mod n \), which confirms our claim. \( \square \)
3. Proof of Theorem \([\text{I}]\)

It is proved in [\(M\)] that \([\text{I}]\) has no solutions when \((\text{CF})\) holds; as a consequence of the computations in [\(BH\)], it has no solution for \(n \leq 163 \cdot 10^6\), except for \([\text{I}]\).

For values of \(n > 163 \cdot 10^6\), either \((\text{CF})\) does not hold or \(2^{n-1} \equiv 3^{n-1} \equiv 1 \mod n^2\), if there is a non trivial solution. This confirms respectively claims \([\text{A}]\) and \([\text{C}]\) from Theorem \([\text{I}]\) in the sequel we shall show that the only possible solutions are \(X = \pm B/n^e + 1\). We may assume in particular that \(n > 163 \cdot 10^6\).

We have already proved that \(X - 1 = B \cdot C^n/n^e\). If \(C = \pm 1\), then \(X - 1 = \pm B/n^e\), as stated in point \([\text{I}]\) of the Theorem and \(X\) is a solution of \([\text{I}]\). The bounds on \(|X|\) in \([\text{I}]\) imply \(|B| < n^e\), the second claim of \([\text{I}]\).

Consequently, Theorem \([\text{I}]\) will follow if we prove that \(C = \pm 1\); we do this in this chapter.

Assume that there is a prime \(p|C\) with \(p^d|C\) and will show that \(p = 1\). Let \(\mathfrak{B} \subset \mathbb{Z}[[\zeta]]\) be a prime ideal lying above \(p\) and let \(d(p) \subset G\) be its decomposition group. The proof uses local approximations based on expansions in binomial series. We derive the relations which lead to these expansions.

Let \(D = B \cdot C^n/n^e = X - 1\), with \(C\) defined by \([\text{II}]\). Note that \([\text{II}]\) implies that either \((n, D) = 1\), or \(n^2|B\) and \((n, C) = 1\), the last relation following from the bounds \(C^n \leq E < 4(n-2)^n\), hence \(|C| < n\). Then \(1/(1 - \zeta)\) is congruent to an algebraic integer modulo \(D \cdot \mathbb{Z}[[\zeta]]\).

We claim that there are at least two elements, \(\sigma_1, \sigma_2 \in d(p)\) such that \(\sigma_1 \neq j \cdot \sigma_2\).

If \(d(p)\) is not a pure \(2\) - group, it contains a non trivial subgroup of odd order, which fixes the claim. If \(d(p)\) is a \(2\) - group and thus \(j \in d(p)\), it has, by Remark \([\text{II}]\) at least \(4\) elements, which implies our claim in this case, too. Assume that there exist \(l \geq 2\) elements \(\{\sigma_1, \ldots, \sigma_l\} \in d(p)\) such that \(\sigma_i \neq j \cdot \sigma_j\) for \(i \neq j \in \{1 \ldots l\}\). Let \(\sigma_i(\zeta) = \zeta^{c_i}, c_i \in \mathbb{Z}/(n-\mathbb{Z})\). It follows from Lemma \([\text{II}]\) that there are \(h_1, \ldots, h_l \in \mathbb{Z}\) with \(|h_i| \leq n^{1/l}\) and \(\sum_{i=1}^{l} h_i c_i \equiv 0 \mod n\). Let \(\mu = \sum_{i=1}^{l} h_i \sigma_i \in \mathbb{Z}[d(p)] \subset \mathbb{Z}[G]\).

By construction, \(\zeta^\mu = 1\). Since \(\mathbb{K}/\mathbb{Q}\) is abelian and all the primes \(\mathfrak{P}((p))\) have the same decomposition group \(d(p)\), \(\mu\) has the following stronger property: let \(\mathfrak{P}((p))\), \(S \subset G\) be a set of representatives of \(G/d(p)\) and \(\gamma \in \mathbb{Z}[[\zeta]]\) be such that \(\gamma \equiv \zeta^\mu \mod \sigma(\mathfrak{P})\) for all \(\sigma \in S\). Then \(\gamma^\mu \equiv 1 \mod p \mathbb{Z}[[\zeta]]\), as follows directly from \(\zeta^\mu \equiv 1 \mod \sigma(\mathfrak{P})\).

We next build \(\theta_0 \in I_f\) such that \(c(\theta_0) = 2\) and \(\phi^{(1)}(\theta_0) \neq 0 \mod n\). Let \(u, v \in \{2, \ldots, n-1\}\), \(u \neq v\) and let \(\psi_u, \psi_v\) be the associated Fueter elements. By Lemma \([\text{II}]\) the system:

\[
\begin{cases}
  w \cdot \varphi(\psi_u) + z \cdot \varphi(\psi_v) = 0 \\
  w \cdot \phi^{(1)}(\psi_u) + z \cdot \phi^{(1)}(\psi_v) \neq 0
\end{cases}
\]

has a non-trivial solution in \(\mathbb{F}_n \times \mathbb{F}_n\), which we denote by \((w_0, z_0)\). Then, by setting

\[
\theta_0 = \sigma_{w_0} \cdot \psi_u + \sigma_{z_0} \cdot \psi_v,
\]

be obtain a Stickelberger element \(\theta_0\) which verifies our three conditions, namely:

\(\varphi(\theta_0) = 0, c(\theta_0) = 2\) and \(\phi^{(1)}(\theta_0) \neq 0 \mod n\).

Let

\[
\Theta = 2 \cdot \sum_{i=1}^{l} (-1)^{g_i} h_i \sigma_i (j)^{g_i} \theta_0,
\]

where \(g_i = 0\) if \(h_i \geq 0\) and \(g_i = 1\) if \(h_i < 0\).

By construction, \(\Theta \in 2 \cdot I_f\) and \(\phi^{(1)}(\Theta) \neq 0\). Let \(h = 2 \cdot \sum_{i=1}^{l} |h_i| = c(\Theta)/2\). From subsection \([\text{II}]\) we know that there exists a Jacobi integer \(\beta(\Theta) \in \mathbb{Z}[[\zeta]]\) such
that $\beta[\Theta]^n = (\zeta^c(1 - \zeta)^{1-c})^{\Theta} \cdot \left(1 + \frac{x}{1-x}\right)^{\Theta}$ (see (10)). It follows from (11) that in both cases we have $\beta[\Theta] \equiv \mu(\zeta^c) \cdot Y^h \mod \mathfrak{P}$ and thus, by Lemma 3

$$\beta[\Theta] \equiv Y^h \mod p\mathbb{Z}[\zeta].$$

Let $\Theta = 2 \sum_{c=1}^{n-1} n_c \sigma_c,$ for any prime $\mathfrak{P}|(p)$, the binomial series of the $n-$th root of the right hand side in (11) converges in the $\mathfrak{P}$ -adic valuation and its sum is equal to $\beta[\Theta]$ up to a possible $n-$th root of unity $\zeta^c$. Here we make use of the choice of $\Theta$: comparing (13) with the product above, it follows that $\zeta^c = 1$ for all primes $\mathfrak{P}|(p)$. For any $N > 0$, we have $p^{\infty N}|D^N$ and thus

$$\beta[\Theta] \equiv Y^h \prod_{c=1}^{n-1} \left(\sum_{k=0}^{N-1} \left(\frac{D}{1-\zeta^c}\right)^k\right) \mod p^{\infty N}.$$

We develop the product in a series, obtaining an expansion which converges uniformly at primes above $p$ and is Galois covariant:

$$\beta[\sigma_d \Theta] = Y^h \left(1 + \sum_{k=1}^{N-1} \frac{b_k[\sigma_d \Theta]}{(1-\zeta^c)^{nk} k!} \cdot D^k\right) + O(p^{\infty N}).$$

for any $N > 0$ and $b_k[\Theta] \in \mathbb{Z}[\zeta]$. Let $I \subset \{1, 2, \ldots, n-1\}$ of cardinal $N > 1$ and $J \subset \mathbb{Z}[G]$ of the Galois automorphisms of $\mathbb{k}$ indexed by $I$: $J = \{\sigma_c \}_{c \in J}$. Consider the linear combination $\Delta = \sum_{\sigma \in J} \lambda_{\sigma} \cdot \beta[\sigma \cdot \Theta]$ where $\lambda_{\sigma} \in \mathbb{Q}[\zeta]$ verify the linear system:

$$\sum_{\sigma \in J} \lambda_{\sigma} \cdot b_{[N/2]}[\sigma \cdot \Theta] = 1.$$

Applying Lemma 6 we observe that this system is regular for any $N < n$. There exists therefore a unique solution which is not null.

We recall that a power series $\sum_{k=0}^{+\infty} a_k X^k \in \mathbb{C}[[X]]$ is dominated by the series $\sum_{k=0}^{+\infty} b_k X^k \in \mathbb{R}[[X]]$ with non-negative coefficients, if for all $k \geq 0$, we have $|a_k| \leq b_k$. The dominance relation is preserved by addition and multiplication of power series.

Following the proof of Proposition 8.2.1 in [Bilu], one shows that if $r \in \mathbb{R}_{>0}$ and $\chi \in \mathbb{C}$, with $|\chi| \leq 1$, then the binomial series $(1 + \chi T)^r$ is dominated by $(1 - T)^{-r}$. From this, we obtain that $(1 + T)^{\Theta/n}$ is dominated by $(1 - T)^{-w(\Theta)/n}$, where $w(\Theta)$ is the absolute weight of $\Theta$. Applying this to our selected $\Theta$, whose absolute weight is bounded by $4n\sqrt{n}$, we find after some computations that $|b_k[\sigma \cdot \Theta]| < (2n)^{2k}$.

Let $A = \det (b_k[\sigma_c \cdot \Theta])_{c \in I, k=1}^N \neq 0$ be the determinant of the matrix of the system (14), which is non vanishing, as noticed above. Let $\delta = (\delta_{c,[N/2]})^N_{c=1}$ where $\delta_{i,j}$ is Kronecker’s symbol. The solution to our system is $\lambda_{\sigma} = A_{\sigma}/A$, where $A_{\sigma} \in \mathbb{Z}[\zeta]$ are the determinants of some minors of $(b_k[\sigma_c \cdot \Theta])_{c \in I, k=1}^N$ obtained by replacing the respective column by $\delta$. Hadamard’s inequality implies that

$$|A_{\sigma}| \leq (2n)^{2N(N-1)} \cdot (N-1)^{(N-1)/2} \leq (2n)^{2N^2 \cdot N^{N/2}} \quad \text{and} \quad |A| \leq N^{N/2} \cdot n^{N(N-1)}$$
Let $\delta = A \cdot \Delta \in \mathbb{Z}[\zeta]$.

$$\delta = \sum_{\sigma \in J} A_{\sigma} \cdot \beta[\sigma \cdot \Theta] \in \mathbb{Z}[\zeta].$$

We claim that $\delta \neq 0$. Indeed, by choice of the $\lambda$’s, we have $\delta = A + p^{inN}z$ for some $z \in \mathbb{Z}[\zeta]$, and thus $A = -p^{inN}z$. The upper bound for $|A|$ implies a fortiori that $v_p(A) \leq \lfloor N/2 \cdot \log_2 N + (N - 1) \cdot \log_2 n \rfloor$ and the last identity would require that $v_p(A) \geq nN$. The two inequalities for $v_p(A)$ imply $\frac{11}{4}n^{3/4} \log_2 n - 2 \log_2 n - n^{7/4} \geq 0$, which is impossible $n > 4$. Therefore $\delta \neq 0$.

Given the bounds on $A_{\sigma}$, we obtain $|\delta| \leq NY^{h(2n)2N/2}$ and using the fact that $h < 2ln^1/l$ and $Y < n^n$ (Theorem 1.(B)), we find

$$|N_{K/Q}(\delta)| < \left(n^{2ln^1/l} \cdot (2n)^{2N^2} \cdot N^{N/2+1}\right)^{n-1}.$$ 

We can set $N = \lceil n^{3/4} \rceil$ and then, the above bound becomes

$$(15) \quad |N_{K/Q}(\delta)| < \left(2^{2n^{3/2}} \cdot (2n)^{2ln^1/l+2n^{3/2}+\frac{3}{2}n^{3/4}+\frac{1}{4}}\right)^{n-1}.$$ 

The initial homogenous conditions in (14) imply $\delta \equiv 0 \mod p^{in[N/2]}$, therefore $|N_{K/Q}(\delta)| \geq p^{in(n-1)N/2}$. Combining this inequality with (15) and $n \geq 163 \cdot 10^6$, one finds for $l = 2$ (which is possible for all $p$) that $\log p < 1.02$. This shows that $p = 1$ or 2. However, if $p = 2$, one could choose $l = 3 < 27 < \frac{\log n}{\log 2}$ and then $\log p < 0.39$, which would be a contradiction. Thus, $C = \pm 1$, which completes the proof of Theorem 1.

4. Consequences for the general case of the binary Thue equation

In this section we derive the Theorem 2. For this we assume that (3) has a solution with $(\varphi(B), n) = 1$, since our results only hold in this case, a fact which is reflected also in the formulation of the Theorem 2.

Consider the case when $n = p \cdot q$ is the product of two distinct primes. If $(n, B) = 1$, then Theorem 1 holds for both $p$ and $q$ with the value $e = 0$. If $X, Z$ is a solution, then Theorem 1 implies that $X^p = \pm B + 1$ and $X^q = \pm B + 1$. Consequently either $X^p + X^q = 2$ or $X^p - X^q = 2$. This is impossible for $|X| > 2$ and a simple case distinction implies that there are no solutions. As a consequence,

Corollary 1. Consider Equation (3) for fixed $B$ and suppose that $n$ is an integer which has two distinct prime divisors $p > q > 2$ with $(p, B) = (q, B) = 1$. Then (3) has no solutions for which (7) holds.

If all divisors of $n$ are among the primes dividing $B$, we are led to the following equation: $p(X^q - 1) = q(X^p - 1)$, which has no solutions in the integers other than 1. Indeed, assume $X$ to be a solution of the equation (X ≠ 1), and $q = p + t$, $t ≥ 0$. The real function $f(t) = p(X^{p+t} - 1) - (p + t)(X^p - 1)$ is strictly monotonous and $f(0) = 0$. Therefore, the equation $p(X^q - 1) = q(X^p - 1)$ has no solutions. There is only the case left in which $n$ is built from two primes, one dividing $B$ and one not. In this case, one obtains that equation $p(X^q - 1) = X^p - 1$ which can also be shown not to have non trivial solutions, using the above remark, this time with $f(t) = p(X^{p+t} - 1) - (X^p - 1)$. Hence:
ON THE EQUATION $X^n - 1 = BZ^n$

Corollary 2. The equation \([3]\) has no solutions for exponents \(n\) which are divisible by more than one prime and for \(B\) such that \([1]\) holds.

We are left to consider the case of prime powers \(n = p^c\) with \(c > 1\). If \(p \nmid B\), we obtain \(X^{n/p} - 1 = B/p^c\), so in particular \(B/p^c + 1 \geq 2^{p^c-1}\) is a \(p^c-1\)-th power. Since in this case, \([3]\) has in particular a solution for the exponent \(p\), the Theorem \([1]\) implies that \(B < p^p\); combining this with the previous upper bound implies that there are no solutions for \(c > 2\). For \(c = 2\), we deduce that \(|X| < p\) and, after applying the Theorem \([1]\) again and letting \(\xi = \zeta^{1/p}\) be a primitive \(p^2\)-th root of unity, we obtain the equation

$$Yp^2 = \frac{Xp^2 - 1}{p^c(Xp - 1)} = N\langle\xi\rangle/Q(\alpha)$$

$$\alpha = \frac{X - \xi}{(1 - \xi)^p}.$$  

Like usual, the conjugates of the ideal \((\alpha)\) are pairwise coprime. We let \(\mathfrak{A} = (Y, \alpha)\), an ideal with \(N(\mathfrak{A}) = (Y)\); moreover, if \(\mathfrak{L}/\mathfrak{A}\) is a prime ideal and \(N(\mathfrak{L}) = (\ell)\), then the rational prime \(\ell\) is totally split in \(\mathbb{Q}[\xi]\), the factors being the primes \((\ell, \sigma_c(\alpha))\). Being totally split, it follows in particular that \(\ell \equiv 1 \mod p^2\) so \(Y \geq \ell > 2p^2\), in contradiction with \(Y < X < p + 1\). This shows that there are no solutions for \(n = p^2\).

Corollary 3. If the Equation \([3]\) in which \(n = p^c\) is a prime power has non trivial solutions for which \([1]\) holds, then \(c = 1\).

The primes dividing the exponent \(n\) used in the above corollaries are by definition coprime to \(\varphi^*(B)\). As a consequence, if \(n\) is an exponent for which \([3]\) has a solution and \(m|n\) is the largest factor of \(n\) with \(m \in \mathcal{N}(B)\) – as defined in \([2]\) – then the corollaries imply that there is at most one prime dividing \(n/m\) and the exponent of this prime in the prime decomposition of \(n\) must be one. This is the first statement of Theorem \([2]\) which thus follows from these corollaries and Theorem \([3]\).

Acknowledgments: The first author is grateful to the Universities of Bordeaux and Göttingen for providing a stimulating environment during the development of this work. Both authors thank Mike Bennett and Kalman Győry for suggesting this interesting problem for an algebraic investigation.

REFERENCES

[BE] M. A. Bennet: Rational Approximation To Algebraic Numbers Of Small Height: The Diophantine Equation \(|ax^n - by^n| = 1\), J. Reine Angew. Math., 535, pp. 1–49 (2001).

[BGMP] M. A. Bennett, K. Győry, M. Mignotte and Á. Pintér: Binomial Thue equations and polynomial powers, Compositio Math. 142, pp. 1103–1121 (2006).

[BBM] Y. Bilu, Y. Bugeaud and M. Mignotte: The problem of Catalan, Springer (2014).

[Bilu] Y. Bilu: Catalan’s conjecture (after Mihăilescu), Séminaire Bourbaki, Exposé 909, 55ème année (2002-2003); Astérisque 294, pp. 1–26 (2004).

[BHM] Y. Bugeaud, G. Hanrot and M. Mignotte: Sur l’équation diophantienne \(\frac{x^{n-1}}{x-1} = y^9\), III, Proc. London. Math. Soc. 84, pp. 59–78 (2002).

[BH] J. P. Buhler and D. Harvey: Irregular primes to 163 million, Math. Comp., 80:276, pp. 2435–2444 (2011).

[G] K. Győry: Personal communication.

[Jha] V. Jha: The Stickelberger Ideal in the Spirit of Kummer with Application to the First Case of Fermat’s Last Theorem, Queen’s University, Queen’s papers in pure and applied mathematics 93 (1993).
[Mi] P. Mihăilescu: *Class Number Conditions for the Diagonal Case of the Equation of Nagell and Ljunggren*, in *Diophantine Approximation*, Springer Verlag, Development in Mathematics 16, pp. 245–273 (2008).