Note on the diophantine equation $X^t + Y^t = BZ^t$  

Benjamin Dupuy (Talence)†

1 Introduction

Let $t > 3$ be a prime number, $B$ be a nonzero rational integer. Consider the equation

$$X^t + Y^t = BZ^t$$

where $X, Y, Z$ are coprime non zero rational integers.

Definition 1.1 Let $t > 3$ be a prime number. We say that $t$ is a good prime number if and only if

- its index irregularity $\iota(t)$ is equal to zero
- or
- $t \nmid h_t^+$ and none of the Bernoulli numbers $B_{2nt}$, $n = 1, \ldots, \frac{t-3}{2}$ is divisible by $t^3$.

For a prime number $t$ with $t < 12.10^6$, it has been recently proved that none of the Bernoulli numbers $B_{2nt}$, $n = 1, \ldots, \frac{t-3}{2}$ is divisible by $t^3$ (see [2]). Furthermore, $h_t^+$ is prime to $t$ for $t < 7.10^6$. In particular, every prime number $t < 7.10^6$ is a good prime number in the previous meaning.

As usual, we denote by $\phi$ the Euler’s function. For the following, we fix $t > 3$ a good prime number, and a rational integer $B$ prime to $t$, such that for every prime number $l$ dividing $B$, we have $-1 \mod t \in \langle l \mod t \rangle$ the subgroup of $\mathbb{F}_t^\times$ generated by $l \mod t$. For example, it is the case if for every prime number $l$ dividing $B$, $l \mod t$ is not a square.

In this paper, using a descent method on the number of prime ideals, we prove the following theorem

Theorem 1.2 The equation (1) has no solution in pairwise relatively prime non zero integers $X, Y, Z$ with $t \mid Z$. 

†Université Bordeaux 1, Institut de Mathématiques, 351 cours de la Libération, 33405 Talence, France
In particular, using a recent result of Bennett et al, we deduce the

**Corollary 1.3** Suppose that \( B^{t-1} \neq 2^{t-1} \mod t^2 \) and \( B \) has a divisor \( r \) such that \( r^{t-1} \neq 1 \mod t^2 \). Then the equation \( (1) \) has no solution in pairwise relatively prime non zero integers \( X, Y, Z \).

## 2 Proof of the theorem

First, we suppose that \( \nu(t) = 0 \). Let us prove the following lemma.

**Lemma 2.1** Let \( \zeta \) be a primitive \( t \)-th root of unity and \( \lambda = (1 - \zeta)(1 - \overline{\zeta}) \). Suppose there exist algebraic integers \( x, y, z \) in the ring \( \mathbb{Z}[\zeta + \overline{\zeta}] \), an integer \( m \geq t \), and a unit \( \eta \) in \( \mathbb{Z}[\zeta + \overline{\zeta}] \) such that \( x, y, z \) and \( \lambda \) are pairwise coprime and verify

\[
x^t + y^t = \eta \lambda^m B z^t.
\]

Then \( z \) is not a unit of \( \mathbb{Z}[\zeta + \overline{\zeta}] \). Moreover, there exist algebraic integers \( x', y', z' \) in \( \mathbb{Z}[\zeta + \overline{\zeta}] \), an integer \( m' \geq t \), and a unit \( \eta' \) in \( \mathbb{Z}[\zeta + \overline{\zeta}] \) such that \( x', y', z', \lambda \) and \( \eta' \) verify the same properties. The algebraic number \( z' \) divides \( z \) in \( \mathbb{Z}[\zeta] \). The number of prime ideals of \( \mathbb{Z}[\zeta] \) counted with multiplicity and dividing \( z' \) is strictly less than that of \( z \).

**Proof** The equation \( (2) \) becomes

\[
(x + y) \prod_{a=1}^{t-1} (x + \zeta^a y) = \eta \lambda^m B z^t.
\]

By hypothesis, for every prime number \( l \) dividing \( B \), we have \(-1 \mod t \in < l \mod t > \). In particular \( B \) is prime to \( \frac{x^t + y^t}{x+y} \). In fact, suppose there exist \( l \) a prime factor of \( B \) in \( \mathbb{Z}[\zeta] \) such that \( l | \frac{x^t + y^t}{x+y} \). Then there exist \( a \in \{1, \ldots, t-1\} \), such that \( l | x + \zeta^a y \). Let \( l \) be the rational prime number under \( l \). Since \(-1 \mod t \) is an element of the subgroup of \( \mathbb{F}_l^\times \) generated by \( l \mod t \), we deduce that the decomposition group of \( l \) contains the complex conjugation \( j \in \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \) that is \( \nu = l \). Particularly, \( l | x + \zeta^a y \) implies that \( l | x + \zeta^{-a} y \) since \( x, y \) are real. So \( l | (\zeta^a - \zeta^{-a}) y \). Since \( l \) is a prime ideal, we deduce that \( l | y \) or \( l | \zeta^a - \zeta^{-a} \). But since \( x \) and \( y \) are coprime, \( y \) is prime to \( l \). Since \( (B, p) = 1 \) and \( \zeta^a - \zeta^{-a} \) is a generator of the only prime ideal of \( \mathbb{Z}[\zeta] \) above \( p \), we can not have \( l | \zeta^a - \zeta^{-a} \): we get a contradiction. So \( B \) and \( \frac{x^t + y^t}{x+y} \) are coprime as claimed. In fact, we have proved the following result: \( B \) is prime to every factor of the form \( \frac{a^t + b^t}{a+b} \) where \( a \) and \( b \) are coprime elements of \( \mathbb{Z}[\zeta + \overline{\zeta}] \).

Then \( B | x + y \) in \( \mathbb{Z}[\zeta] \). Therefore we get

\[
\frac{x + y}{B} \prod_{a=1}^{t-1} (x + \zeta^a y) = \eta \lambda^m z^t.
\]
Following the same method as in section 9.1 of [3], one can show that there exist real units \( \eta_0, \eta_1, \ldots, \eta_{t-1} \in \mathbb{Z}[\zeta + \overline{\zeta}]^\times \) and algebraic integers \( \rho_0, \rho_1, \ldots, \rho_{p-1} \in \mathbb{Z}[\zeta] \) such that

\[
x + y = \eta_0 B \lambda^{m-t} \rho_0^t, \quad \frac{x + \zeta^a y}{1 - \zeta^a} = \eta_a \rho_a^t, \quad a = 1, \ldots, t - 1.
\]

(3)

Let us show that \( z \) is not a unit. As \( \rho_1 \) divides \( z \) in \( \mathbb{Z}[\zeta] \), it is thus enough to show that \( \rho_1 \) is not one. Put \( \alpha = \frac{x + \zeta y}{1 - \zeta} \). One has

\[
\alpha = -y + \frac{x + y}{1 - \zeta} \equiv -y \mod (1 - \zeta)^2.
\]

So \( \frac{\alpha}{\overline{\alpha}} \equiv 1 \mod (1 - \zeta)^2 \). Suppose that \( \rho_1 \) is a unit. Then, the quotient \( \frac{\alpha}{\rho_1} \) is a unit of modulus 1 of the ring \( \mathbb{Z}[\zeta] \), thus a root of the unity of this ring by Kronecker theorem. However, the only roots of the unity of \( \mathbb{Z}[\zeta] \) are the \( 2t \)-th roots of the unity (see [3]). As the unit \( \eta_1 \) is real, thus there exists an integer \( l \) and \( \epsilon = \pm 1 \) such as

\[
\eta_1 \cdot \rho_1^t \eta_1 \cdot \rho_1^t = \epsilon \zeta^l.
\]

Therefore, we have

\[
\frac{\alpha}{\overline{\alpha}} = \epsilon \zeta^l.
\]

As \( \frac{\alpha}{\overline{\alpha}} \equiv 1 \mod (1 - \zeta)^2 \), we get \( \epsilon \zeta^l \equiv 1 \mod (1 - \zeta)^2 \), so \( \epsilon \zeta^l = 1 \), i.e. \( \frac{\alpha}{\overline{\alpha}} = 1 \). So

\[
\frac{x + \zeta y}{1 - \zeta} = \frac{x + \overline{\zeta} y}{1 - \overline{\zeta}},
\]

because \( x \) and \( y \) are real numbers. From this equation, we deduce that

\[
\frac{x + \zeta y}{1 - \zeta} = \frac{\zeta x + y}{\zeta - 1}, \quad \text{i.e.} \quad (x + y)(\zeta + 1) = 0.
\]

We get a contradiction. So the algebraic integer \( \rho_1 \) (and then \( z \)) is not a unit. This completes the proof of first part of the lemma.

Let us prove the existence of \( x', y', z', \eta', \) and \( m' \). It is just an adaptation of the computations done in paragraph 9.1 of chapter 9 of [3] for the second case of the Fermat equation. We give here the main ideas. Let \( a \in \{1, \ldots, p - 1\} \) be a fixed integer. We take \( \lambda_a = (1 - \zeta^a)(1 - \zeta^{-a}) \). By (3), there exist a real unit \( \eta_a \) and \( \rho_a \in \mathbb{Z}[\zeta] \) such that

\[
\frac{x + \zeta^a y}{1 - \zeta^a} = \eta_a \rho_a^t,
\]

and taking the conjugates (we know that \( x, y \in \mathbb{R} \)), we have

\[
\frac{x + \zeta^{-a} y}{1 - \zeta^{-a}} = \eta_a \overline{\rho_a^t}.
\]

\(^1\)Recall that \( t \nmid h_t^+ \) since \( \iota(t) = 0 \).
Thus 
\[ x + \zeta^a y = (1 - \zeta^a)\eta_0 \rho_a^t, \quad x + \zeta^{-a} y = (1 - \zeta^{-a})\eta_0 \rho_a^t. \]

Multiplying the previous equalities, we obtain
\[ x^2 + y^2 + (\zeta^a + \zeta^{-a})xy = \lambda_a \eta_0^2 (\rho_a \overline{\rho_a})^t. \]  
(4)

Taking the square of \( x + y = \eta_0 B \lambda^m \frac{-1}{2} \rho_0^t \) gives
\[ x^2 + y^2 + 2xy = \eta_0^2 B^2 \lambda^{2m-t+1} \rho_0^{2t}. \]  
(5)

The difference between equations (5), (4) and then the division by \( \lambda_a \) give
\[ -xy = \eta_0^2 (\rho_a \overline{\rho_a})^t - \eta_0^2 B^2 \lambda^{2m-t+1} \rho_0^{2t} \lambda^{-1}_a. \]  
(6)

As \( t > 3 \), there exists an integer \( b \in \{1, \ldots, t-1\} \) such that \( b \not\equiv \pm a \mod t \). For this integer \( b \), we get
\[ -xy = \eta_0^2 (\rho_a \overline{\rho_a})^t - \eta_0^2 B^2 \lambda^{2m-t+1} \rho_0^{2t} \lambda^{-1}_b. \]  
(7)

The difference of between equations (6) and (7) gives after simplifying
\[ \eta_0^2 (\rho_a \overline{\rho_a})^t - \eta_0^2 (\rho_b \overline{\rho_b})^t = \eta_0^2 B^2 \lambda^{2m-t+1} \rho_0^{2t} (\lambda_a^{-1} - \lambda_b^{-1}). \]

But as \( b \not\equiv \pm a \mod t \), we have \( \lambda_a^{-1} - \lambda_b^{-1} = \frac{(\zeta^b - \zeta^{-a})(\zeta^{a+b} - 1)}{\lambda_a \lambda_b} = \frac{\delta'}{X} \), where \( \delta' \) is a unit. We know that \( \lambda_a, \lambda_b \) and \( \lambda \) are real numbers, then the unit \( \delta' \) is a real unit. So there exists a real unit \( \eta' = \frac{\delta' \eta_0^2}{\eta_b} \) such that
\[ \left( \frac{\eta_a}{\eta_b} \right)^2 (\rho_a \overline{\rho_a})^t + (\rho_b \overline{\rho_b})^t = \eta' B^2 \lambda^{2m-t} \left( \rho_0^2 \right)^t. \]  
(8)

The condition \( \varphi(t) = 0 \) implies that \( \frac{\eta_a}{\eta_b} \) is a \( t \)-th power in \( \mathbb{Z}[\zeta + \overline{\zeta}] \). Thus there exists \( \xi \in \mathbb{Z}[\zeta + \overline{\zeta}] \) such that \( \frac{\eta_a}{\eta_b} = \xi^t \). In fact, we know that
\[ \eta_a \rho_a^t = \frac{x + \zeta^a y}{1 - \zeta^a}, \quad x + y = \eta_0 B \lambda^m \frac{-1}{2} \rho_0^t \equiv 0 \mod (1 - \zeta)^{2m-t+1}. \]

Then
\[ \eta_a \rho_a^t = -y + \frac{x + y}{1 - \zeta^a} \equiv -y \mod (1 - \zeta)^{2m-t} \equiv -y \mod t. \]

Also \( \eta_b \rho_b^t \equiv -y \mod t \), where \( \frac{\eta_a}{\eta_b} \equiv \left( \rho_a \rho_b \right)^t \mod t \). But Lemma 1.8 in [3] shows that \( \left( \rho_a \rho_b \right)^t \) is congruent to an integer \( l \in \mathbb{Z} \) modulo \( t \), therefore the existence of an integer \( l \) such that
\[ \frac{\eta_a}{\eta_b} \equiv l \mod t, \quad l \in \mathbb{Z}. \]
By Theorem 5.36 of [3], the unit \( \frac{a}{b} \) is a \( t \)-th power in \( \mathbb{Z}[\zeta] \) so we have the existence of \( \zeta_1 \in \mathbb{Z}[\zeta] \) such that \( \frac{a}{b} = \zeta_1^t \). As the unit \( \frac{a}{b} \) is real, one has

\[
\zeta_1^t = \overline{\zeta_1}.
\]

Therefore, there exists an integer \( g \) such that \( \overline{\zeta_1} = \zeta^g \zeta_1 \). Taking \( \xi = \zeta^h \zeta_1 \) where \( h \) is the inverse of \( 2 \) mod \( t \), we have

\[
\xi = \zeta, \quad \xi^t = \zeta_1^t = \frac{\eta a}{\eta b},
\]

i.e. \( \frac{a}{b} = \xi^t \), where \( \xi \in \mathbb{Z}[\zeta + \overline{\zeta}] \). We put

\[
x' = \xi^2 \rho_a \overline{\rho_a}, \quad y' = -\rho_b \overline{\rho_b}, \quad z' = \rho_0^2, \quad m' = 2m - t.
\]

One can verify that

\[
x'' + y'' = \eta' B^2 \lambda^{m'} z'^n.
\]

Obviously, \( B^2 \) is prime to \( t \) and for all prime \( l \) dividing \( B^2 \), we have \(-1 \mod t \in \langle l \mod t \rangle \) the subgroup of \( \mathbb{F}_t^\times \) generated by \( l \mod t \). Moreover, one have already seen that the algebraic integer \( \rho_1 \) is not a unit in \( \mathbb{Z}[\zeta] \). As \( \rho_0 \rho_1 \) divides \( z \) in \( \mathbb{Z}[\zeta] \), the number of prime ideals counted with multiplicity and dividing \( z' \) in \( \mathbb{Z}[\zeta] \) is then strictly less than that of \( z \) and \( m' = 2m - t \geq 2t - t = t \). This completes the proof of the lemma. \( \square \)

Now let \((X, Y, Z)\) be a solution of (11) in pairwise relatively prime non zero integers with \( t|Z \). Let \( Z = t^u Z_1 \) with \( t \nmid Z_1 \). Equation (11) becomes

\[
X^t + Y^t = B t^u Z_1^t.
\]

Let \( \zeta \) be a primitive \( t \)-th root of unity and \( \lambda = (1 - \zeta)(1 - \overline{\zeta}) \). The previous equation becomes

\[
X^t + Y^t = B \frac{t^u}{\lambda^u - 1} \lambda^{u/t - 1} Z_1^t.
\]

The quotient \( \eta = \frac{t^u}{\lambda^u - 1} \) is a real unit in the ring \( \mathbb{Z}[\zeta + \overline{\zeta}] \). Take \( m = tv^{-1} \geq t \). We have just proved that there exist \( \eta \in \mathbb{Z}[\zeta + \overline{\zeta}]^\times \) and an integer \( m \geq t \) such that

\[
X^t + Y^t = \eta B \lambda^m Z_1^t, \quad (9)
\]

where \( X, Y, \lambda \) and \( Z_1 \) are coprime.

We can apply the lemma (2,1) to equation (9). By induction, one can prove the existence of the sequence of algebraic \( Z_i \) such that \( Z_{i+1}/Z_i \) in \( \mathbb{Z}[\zeta] \) and the number of prime factors in \( \mathbb{Z}[\zeta] \) is strictly decreasing. So there is \( n \) such that \( Z_n \) is a unit. But Lemma 2,1 indicates that each of the \( Z_i \) is not a unit. We get a contradiction. The theorem is proved in the case \( i(t) = 0 \).

In the other case, \((t, h_1^t) = 1 \) and none of the Bernoulli numbers \( B_{2nt}, \ n = 1, \ldots, \frac{t-3}{2} \) is divisible by \( t^3 \). In particular, with the notation of the proof of the lemma, it exists \( \xi \in \mathbb{Z}[\zeta + \overline{\zeta}] \) such that \( \frac{a}{b} = \xi^t \) (see [3], page 174 – 176). So the results of the previous lemma are valid in the second case. We conclude as before. The theorem is proved.
3 Proof of the corollary

Let $X, Y, Z$ be a solution in pairwise relatively prime non zero integers of the equation (1). By the theorem, the integer $Z$ is prime to $t$. Furthermore, $B\phi(B)$ is coprime to $t$, $B^{t-1} \neq 2^{t-1} \mod t^2$ and $B$ has a divisor $r$ such that $r^{t-1} \neq 1 \mod t^2$. So by the theorem 4.1 of [1], the equation (1) has no solution for such $t$ and $B$.

Acknowledgments I thank Professor Yuri Bilu and Florian Luca for very helpful suggestions.

References

[1] Bennett, M.A. Gyory, K. Mignotte, M. Pintèr, A. Binomial Thue equations and polynomial powers. Compos. Math. 142, 2006, 1103 – 1121.

[2] Buhler, J. Crandall, R. Ernvall, R. Metsankyla, T. Shokrollahi, A. Irregular Primes and cyclotomic invariants to 12 million. J. Symbolic Computation, 31, (2001), 89 – 96.

[3] Washington, L. Introduction to Cyclotomic Fields, Springer, Berlin, second edition, 1997.