NOTE ON THE DIOPHANTINE EQUATION $X^t + Y^t = BZ^t$

Benjamin Dupuy
Institut de Mathématiques, Université Bordeaux I
benjamin.dupuy@math.u-bordeaux1.fr

Received: 3/8/10, Accepted: 12/29/10, Published: 2/4/11

Abstract

In this paper, we consider the diophantine equation $X^t + Y^t = BZ^t$ where X, Y, Z are nonzero coprime integers. We prove that this equation has no non-trivial solution with the exponent t dividing Z under certain conditions on t and B.

1. Introduction

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

$$X^t + Y^t = BZ^t \tag{1}$$

where X, Y, Z are coprime nonzero rational integers.

Definition 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}, $n = 1, \dots, \frac{t-3}{2}$, 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}, $n = 1, \dots, \frac{t-3}{2}$, 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.

Recently the diophantine Equation (1) has been studied by Preda Mihăilescu in [3]. In his paper, he requires that B is such that $B > 1$, $(t, \phi(Rad(B))) = 1$, and the pairwise relatively prime nonzero integers X, Y, Z satisfy the condition $t^3|BZ$ where t is a prime number such that $t \nmid h_t^+$ and none of the Bernoulli numbers B_{2nt},

$n = 1, \ldots, \frac{t-3}{2}$, is divisible by t^3. Particularly, if B is prime to t, he requires that $t^3|Z$. Unfortunately, the proof of a very fundamental fact in his proof is wrong (see Section 4 of this paper), so that Theorem 1 of [3] has not been yet proved.

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

In this paper, using very similar methods to those used in [3], we prove the following theorem (with a stronger condition on B, but a much weaker condition on Z than that used by Mihăilescu).

Theorem 2 *Equation (1) has no solution in pairwise relatively prime non zero integers X, Y, Z with $t|Z$.*

In particular, using a recent result of Bennett *et al.*, we deduce the following corollary.

Corollary 3 *Suppose that $B^{t-1} \neq 2^{t-1} \bmod t^2$ and B has a divisor r such that $r^{t-1} \neq 1 \bmod t^2$. Then Equation (1) has no solution in pairwise relatively prime nonzero integers X, Y, Z.*

2. Proof of the Theorem

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

Lemma 4 *Let ζ 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 η in $\mathbb{Z}[\zeta + \overline{\zeta}]$ such that x, y, z and λ are pairwise coprime and satisfy*

$$x^t + y^t = \eta \lambda^m B z^t. \tag{2}$$

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 η' in $\mathbb{Z}[\zeta + \overline{\zeta}]$ such that x', y', z', λ and η' satisfy 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 dividing z.

Proof. 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 $-1 \bmod t \in < l \bmod t >$. In particular B is prime to $\frac{x^t+y^t}{x+y}$. In fact, suppose there exists γ a prime factor of B in $\mathbb{Z}[\zeta]$ such that $\gamma | \frac{x^t+y^t}{x+y}$. Then there exist $a \in \{1,\dots,t-1\}$ such that $\gamma \mid (x+\zeta^a y)$. Let l be the rational prime number under γ. Since $-1 \bmod t$ is an element of the subgroup of $\mathbb{F}_t^\times$ generated by $l \bmod t$, we deduce that the decomposition group of γ contains the complex conjugation $j \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ that is $\gamma^j = \gamma$. In particular, $\gamma \mid (x+\zeta^a y)$ implies that $\gamma \mid (x+\zeta^{-a}y)$ since x, y are real. So $\gamma \mid (\zeta^a - \zeta^{-a})y$. Since γ is a prime ideal, we deduce that $\gamma \mid y$ or $\gamma \mid (\zeta^a - \zeta^{-a})$. But x and y are coprime so y is prime to γ. Since $(B,p)=1$ and $\zeta^a - \zeta^{-a}$ is a generator of the only prime ideal of $\mathbb{Z}[\zeta]$ above p, we cannot have $\gamma \mid (\zeta^a - \zeta^{-a})$: 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 $B \mid (x+y)$ 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[1] as in Section 9.1 of [4], one can show that there exist real units $\eta_0, \eta_1, \dots, \eta_{t-1} \in \mathbb{Z}[\zeta+\overline{\zeta}]^\times$ and algebraic integers $\rho_0 \in \mathbb{Z}[\zeta+\overline{\zeta}]$, $\rho_1, \dots, \rho_{t-1} \in \mathbb{Z}[\zeta]$ such that

$$x+y = \eta_0 B \lambda^{m-\frac{t-1}{2}}\rho_0^t, \quad \frac{x+\zeta^a y}{1-\zeta^a} = \eta_a \rho_a^t, \quad a = 1,\dots,t-1. \tag{3}$$

Let us show that z is not a unit. As ρ_1 divides z in $\mathbb{Z}[\zeta]$, it is thus enough to show that ρ_1 is not one. Put $\alpha = \frac{x+\zeta y}{1-\zeta}$. One has

$$\alpha = -y + \frac{x+y}{1-\zeta} \equiv -y \bmod (1-\zeta)^2.$$

So $\frac{\overline{\alpha}}{\alpha} \equiv 1 \bmod (1-\zeta)^2$. Suppose that ρ_1 is a unit. Then, the quotient $\frac{\overline{\rho_1}^t}{\rho_1^t}$ is a unit of modulus 1 of the ring $\mathbb{Z}[\zeta]$, thus a root of the unity of this ring by the Kronecker theorem. However, the only roots of the unity of $\mathbb{Z}[\zeta]$ are the $2t$-th roots of the unity (see [4]). As the unit η_1 is real, thus there exists an integer l and $\epsilon = \pm 1$ such as $\frac{\overline{\eta_1}\cdot\overline{\rho_1}^t}{\eta_1\cdot\rho_1^t} = \frac{\overline{\rho_1}^t}{\rho_1^t} = \epsilon\zeta^l$. Therefore, we have

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

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

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

[1] Recall that $t \nmid h_t^+$ since $\iota(t) = 0$

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

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

We get a contradiction. So the algebraic integer ρ_1 (and then z) is not a unit. This completes the proof of the first part of the lemma.

Let us prove the existence of x', y', z', η', and m'. It is just an adaptation of the computations done in Paragraph 9.1 of Chapter 9 of [4] for the second case of the Fermat equation. Here we give 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 η_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

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

Thus

$$x + \zeta^a y = (1-\zeta^a)\eta_a \rho_a^t, \quad x + \zeta^{-a} y = (1-\zeta^{-a})\eta_a \overline{\rho_a}^t.$$

Multiplying the previous equalities, we obtain

$$x^2 + y^2 + \left(\zeta^a + \zeta^{-a}\right) xy = \lambda_a \eta_a^2 \left(\rho_a \overline{\rho_a}\right)^t. \tag{4}$$

Taking the square of $x + y = \eta_0 B \lambda^{m-\frac{t-1}{2}} \rho_0^t$ gives

$$x^2 + y^2 + 2xy = \eta_0^2 B^2 \lambda^{2m-t+1} \rho_0^{2t}. \tag{5}$$

The difference between equations (5), (4) and then division by λ_a gives

$$-xy = \eta_a^2 \left(\rho_a \overline{\rho_a}\right)^t - \eta_0^2 B^2 \lambda^{2m-t+1} \rho_0^{2t} \lambda_a^{-1}. \tag{6}$$

As $t > 3$, there exists an integer $b \in \{1, \ldots, t-1\}$ such that $b \neq \pm a \bmod t$. For this integer b, we get

$$-xy = \eta_b^2 \left(\rho_b \overline{\rho_b}\right)^t - \eta_0^2 B^2 \lambda^{2m-t+1} \rho_0^{2t} \lambda_b^{-1}. \tag{7}$$

The difference between equations (6) and (7) gives, after simplifying,

$$\eta_a^2 \left(\rho_a \overline{\rho_a}\right)^t - \eta_b^2 \left(\rho_b \overline{\rho_b}\right)^t = \eta_0^2 B^2 \lambda^{2m-t+1} \rho_0^{2t} \left(\lambda_a^{-1} - \lambda_b^{-1}\right).$$

But as $b \neq \pm a \bmod t$, we have $\lambda_a^{-1} - \lambda_b^{-1} = \frac{\left(\zeta^{-b}-\zeta^{-a}\right)\left(\zeta^{a+b}-1\right)}{\lambda_a \lambda_b} = \frac{\delta'}{\lambda}$, where δ' is a unit. We know that λ_a, λ_b and λ are real numbers and so the unit δ' is a real unit. So there exists a real unit $\eta' = \frac{\delta' \cdot \eta_0^2}{\eta_b^2}$ such that

$$\left(\frac{\eta_a}{\eta_b}\right)^2 \left(\rho_a \overline{\rho_a}\right)^t + \left(-\rho_b \overline{\rho_b}\right)^t = \eta' B^2 \lambda^{2m-t} \left(\rho_0^2\right)^t. \tag{8}$$

The condition $\iota(t)=0$ 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

$$\eta_a\rho_a^t = \frac{x+\zeta^a y}{1-\zeta^a}, \quad x+y=\eta_0 B\lambda^{m-\frac{t-1}{2}}\rho_0^t \equiv 0 \bmod (1-\zeta)^{2m-t+1}.$$

Then

$$\eta_a\rho_a^t = -y+\frac{x+y}{1-\zeta^a} \equiv -y \bmod (1-\zeta)^{2m-t} \equiv -y \bmod t.$$

Also $\eta_b\rho_b^t \equiv -y \bmod t$ and $\frac{\eta_a}{\eta_b} \equiv \left(\frac{\rho_b}{\rho_a}\right)^t \bmod t$. But Lemma 1.8 in [4] shows that there exists an integer l such that

$$\frac{\eta_a}{\eta_b} \equiv l \bmod t,$$

with $\left(\frac{\rho_b}{\rho_a}\right)^t$ congruent to l modulo t.

By Theorem 5.36 of [4], the unit $\frac{\eta_a}{\eta_b}$ is a t-th power in $\mathbb{Z}[\zeta]$ so we have the existence of $\xi_1 \in \mathbb{Z}[\zeta]$ such that $\frac{\eta_a}{\eta_b}=\xi_1^t$. As the unit $\frac{\eta_a}{\eta_b}$ is real, one has $\xi_1^t=\overline{\xi_1}^t$. Therefore, there exists an integer g such that $\overline{\xi_1}=\zeta^g\xi_1$. Taking $\xi=\zeta^{gh}\xi_1$ where h is the inverse of 2 mod t, we have

$$\overline{\xi}=\xi, \quad \xi^t=\xi_1^t=\frac{\eta_a}{\eta_b},$$

i.e., $\frac{\eta_a}{\eta_b}=\xi^t$, 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 $x'^t+y'^t=\eta' B^2\lambda^{m'}z'^t$. Obviously, B^2 is prime to t and for all prime l dividing B^2, we have $-1 \bmod t \in \langle l \bmod t \rangle$, the subgroup of $\mathbb{F}_t^\times$ generated by $l \bmod t$. Moreover, we have already seen that the algebraic integer ρ_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 dividing z and $m'=2m-t \geq 2t-t=t$. This completes the proof of the lemma. □

Now let (X,Y,Z) be a solution of (1) in pairwise relatively prime non zero integers with $t|Z$. Let $Z=t^vZ_1$ with $t \nmid Z_1$. Equation (1) becomes

$$X^t+Y^t=Bt^{tv}Z_1^t.$$

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

$$X^t+Y^t=B\frac{t^{tv}}{\lambda^{tv\frac{t-1}{2}}}\lambda^{tv\frac{t-1}{2}}Z_1^t.$$

The quotient $\eta = \frac{t^{tv}}{\lambda^{tv\frac{t-1}{2}}}$ is a real unit in the ring $\mathbb{Z}[\zeta+\overline{\zeta}]$. Take $m = tv\frac{t-1}{2} \geq t$. We have just proved that there exist $\eta \in \mathbb{Z}[\zeta+\overline{\zeta}]^\times$ and an integer $m \geq t$ such that

$$X^t + Y^t = \eta B \lambda^m Z_1^t, \tag{9}$$

where X, Y, λ and Z_1 are pairwise coprime.

We can apply Lemma 4 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 exists an n such that Z_n is a unit. But Lemma 4 indicates that each of the Z_i is not a unit, a contradiction which proves the theorem in the case $\iota(t) = 0$.

In the other case, $(t, h_t^+) = 1$ 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, there exists $\xi \in \mathbb{Z}[\zeta+\overline{\zeta}]$ such that $\frac{\eta_a}{\eta_b} = \xi^t$ (see [4], pp. 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 nonzero integers of Equation (1). By the theorem, the integer Z is prime to t. Furthermore, $B\phi(B)$ is coprime to t, $B^{t-1} \not\equiv 2^{t-1} \bmod t^2$ and B has a divisor r such that $r^{t-1} \not\equiv 1 \bmod t^2$. So by the theorem 4.1 of [1], Equation (1) has no solution for such t and B.

4. Some Remarks on Mihăilescu's Paper

For the reader's convenience, recall "Fact 3:"

Fact 3 of [3] *Let ρ, $\varpi \in \mathbb{Q}[\zeta]^+$; set*

$$\mu_a = \frac{\rho - \zeta^a \varpi}{1-\zeta^a}, \quad C = \frac{\rho^t - \varpi^t}{t(\rho - \varpi)},$$

and suppose $(\mu_a, \mu_b) = 1$ for $a \neq b$. If $\rho^t - \varpi^t = \beta \cdot \gamma^t$ and none of the prime ideals $\tau|\beta$ are totally split, then $(\beta, \mu_a) = 1$ for all $a \in \{1, \ldots, t-1\}$. In particular, $\beta|(\rho - \varpi)$.

His method to prove this fact is the following: he supposes that we can find a prime ideal τ of β such that $\tau|\mu_a$ for some $a \in \{1, \ldots, t-1\}$. By hypothesis, none of the prime ideals of β are totally split in the extension $\mathbb{Q}(\zeta)/\mathbb{Q}$. So there exist

$\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ such that $\sigma(\tau) = \tau$. In particular $\sigma(\tau) = \tau|\sigma(\mu_a)$. So we have $\tau|\mu_a$ and $\tau|\sigma(\mu_a)$.

Then Mihăilescu claims we have a contradiction since (μ_a, μ_b) for all $a \neq b$. But this last argument does not follow. Indeed,

$$\sigma(\mu_a) = \frac{\sigma(\rho) - \sigma(\zeta^a)\sigma(\varpi)}{1 - \sigma(\zeta^a)}$$

and this last number is not of the form μ_b for some $b \in \{1, \ldots, t-1\}$. Indeed, ρ and ϖ are just elements of $\mathbb{Q}[\zeta]^+$.

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

References

[1] M.A. Bennett, K. Gyory, M. Mignotte, A Pintèr, 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] Mihăilescu Preda. On solutions of the equation $X^n + Y^n = BZ^n$ with $n|BZ$. Acta Arithmetica, **136** (2009), 1-6.

[4] Washington, L. *Introduction to Cyclotomic Fields*, Second Ed., Springer, Berlin, 1997.