AN UNEXPECTED MEETING BETWEEN THE P_1^3-SET AND THE CUBIC-TRIANGULAR NUMBERS

A. DEBBACHE AND S. BOUROUBI*

Abstract. A set of m positive integers $\{x_1, \ldots, x_m\}$ is called a P_1^3-set of size m if the product of any three elements in the set increased by one is a cube integer. A P_1^3-set S is said to be extendible if there exists an integer $y \notin S$ such that $S \cup \{y\}$ still a P_1^3-set. Now, let consider the Diophantine equation $u(u+1)/2 = v^3$ whose integer solutions produce what we called cubic-triangular numbers. The purpose of this paper is to prove simultaneously that the P_1^3-set $\{1, 2, 13\}$ is non-extendible and $n = 1$ is the unique cubic-triangular number by showing that the two problems meet on the Diophantine equation $2x^3 - y^3 = 1$ that we solve using p-adic analysis.

1. Introduction

A set of m positif integers $\{x_1, \ldots, x_m\}$ is called a Diophatine m-tuple or a $D(1)$-m-tuple, if the product of any two elements in the set increased by one is a perfect square, i.e., $x_i x_j + 1 = u_{ij}^2$, where $u_{ij} \in \mathbb{N}^*$, for $1 \le i < j \le m$. Diophantus of Alexandria was the first to look for such sets. He found a set of four positive rational numbers with the above property $\left\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\right\}$. However, Fermat was the first to give $\{1, 3, 8, 120\}$ as an example of a Diophantine quadruple. For a detailed history on Diophantine m-tuples and its results, we refer the reader to Dujella's webpage [3]. Throughout the following we consider in a similar way what we have called a P_1^3-set.

2. Definitions

Definition 1. A P_1^3-set of size m is a set $S = \{x_1, \ldots, x_m\}$ of distinct positive integers, such that $x_i x_j x_k + 1$ is a cube for $1 \le i < j < k \le m$.

Definition 2. A P_1^3-set S is said to be extendible if there exists an integer $y \notin S$ such that $S \cup \{y\}$ is a P_1^3-set.

2010 *Mathematics Subject Classification.* 11D45, 11D09.
Key words and phrases. P_1^3-set, cubic-triangular number, Diophantine equation.
* Corresponding author.

Definition 3. A triangular number is a figurate number that can be represented in the form of an equilateral triangle of points, where the first row contains a single element and each subsequent row contains one more element than the previous one. Let T_n denotes the n^{th} triangular number, then T_n is equal to the sum of the n natural numbers from 1 to n, whose initial values are listed as the sequence A000217 in [1].

$$T_n = \frac{n(n+1)}{2} = \binom{n+1}{2},$$

where $\binom{n}{k}$ is a binomial coefficient.

Definition 4. A cubic-triangular number is a positive integer that is simultaneously cubic and triangular. Such a number must satisfy $T_n = m^3$ for some positive integers n and m, so

$$\frac{n(n+1)}{2} = m^3. \tag{2.1}$$

3. Some Claims

Claim 1. *The triple* $\left\{a-1, a+1, a^4+a^2+1\right\}$ *is an infinite family of* P_1^3*-set for any positive integers* $a \geq 2$.

Proof. Thanks to the identity $x^3 = (x-1)(x^2+x+1)+1$, it is enough to substitute x by a^2 to get,

$$a^6 - 1 = (a-1)(a+1)(a^4+a^2+1).$$

□

Claim 2. *The triple* $\{a, b, a^2b^2+3ab+3\}$ *form an infinite family of* P_1^3*-set for any positive integers* a *and* b*, such that* $1 \leq a < b$.

Proof. The result follows thanks to the identity :

$$(ab+1)^3 - 1 = ab(a^2b^2+3ab+3).$$

□

Remark 1. The triple $\{1, 2, 13\}$ is a P_1^3-set, it belongs to the family in Claim 2, for $a = 1$ and $b = 2$.

4. Main Results

Theorem 3. *Any* P_1^3*-set is finite.*

Proof. Let $S = \{x_1, x_2, x_3, \ldots, x_m\}$ be a P_1^3-set. Suppose that $S \cup \{y\}$ still a P_1^3-set, then by setting

$$\begin{cases} a = x_m x_{m-1}, \\ b = x_m x_{m-2}, \\ c = x_{m-1} x_{m-2}, \end{cases}$$

we get an elliptic curve

$$(ay+1)(by+1)(cy+1) = t^3,$$

which has only finitely many integral solutions [4]. □

In the following, we will restrict our attention to equation (4.1), for which we present a proof for it's uniqueness integer solution, by using p-adic analysis tools.

$$2x^3 - y^3 = 1. \tag{4.1}$$

We first briefly remind Hensel's Lemma and Strassman's Theorem [2].

Lemma 1. (Hensel) *Let $P(X) \in \mathbb{Z}_p[X]$, a monic polynomial. Suppose that $x \in \mathbb{Z}_p$, satisfied:*

(1) $P(x) \equiv 0 \ (mod\ p)$,
(2) $\dfrac{d}{dx}(P(x)) \not\equiv 0 \ (mod\ p)$.

So, there is a unique $y \in \mathbb{Z}_p$ such as $P(y) = 0$ and $y \equiv x \ (mod\ p)$.

Theorem 4. (Strassman) *Let $\mathbb{K}$ be a complete field for the non-archimedean norm $\|.\|$, $\mathcal{A}$ its ring of integers, and let*

$$g(x) = \sum_{n=0}^{+\infty} g_n x^n.$$

Suppose that $g_n \to 0$ (so $g(x)$ converges in $\mathcal{A}$), but with g_n not all zeros, there is at most a finite number of elements b of $\mathcal{A}$ such that $g(b) = 0$. More precisely, there is at most M elements b of $\mathcal{A}$, such that

$$\|g_N\| = \max_n \|g_n\|, \quad \|g_n\| < \|g_N\|, \forall n > M.$$

Lemma 2. *Let $b \in \mathbb{Q}_p, |b|_2 \leq 2^{-2}$ and $|b|_p \leq p^{-1}$ ($p \neq 2$). So, there is a series $\Phi_b(X) = \sum_{n \geq 0} \gamma_n X^n$, with $\gamma_n \in \mathbb{Q}_p$, $\gamma_n \to 0$, such that $\Phi_b(r) = (1+b)^r$, $\forall r \in \mathbb{Z}$.*

By application of these results, we may show

Theorem 5. *The unique positive integer solution of Equation (4.1) is $(1,1)$.*

Proof. Let (a,b) be a solution of Equation (4.1). As $N(2^{\frac{1}{3}}a-b)=2a^3-b^3$, so $2^{\frac{1}{3}}a-b$ is an algebraic unit, especially $\theta=\theta_1=2^{\frac{1}{3}}-1$. For convenience, on all the rest of the paper we will work with the field $\mathbb{K}=\mathbb{Q}(\theta)$. Note $\mathcal{A}$, the integer ring of $\mathbb{K}$ and $\mathcal{U}$ its group of units. We have

$$2=(\theta+1)^3.$$

Hence

$$\theta^3+3\theta^2+3\theta-1=0.$$

Let $f(X)=X^3+3X^2+3X-1$ be the irreducible polynomial of θ. According to Dirichlet's unit theorem $\mathcal{U}=G\times\mathbb{Z}^{r+s-1}$, where G is the root group of the unit of $\mathcal{A}$, r is the number of real zeros of f, and $2s$ is the number of complex zeros of f. Here, $r=s=1$, so $\mathcal{U}=G\times\mathbb{Z}$. Let α be a root of the unit of $\mathcal{A}$, then the dimension of the field $\mathbb{Q}(\alpha)$ divides the dimension of the field $\mathbb{K}$, so it is a divisor of 3. Since $\mathbb{Q}(\alpha)\neq\mathbb{K}$, we have $\mathbb{Q}(\alpha)=\mathbb{Q}$ and $A=\mathbb{Z}$, where A is the ring of the units of $\mathbb{Q}(\alpha)$. However, the only invertible elements of $\mathbb{Z}$ are $+1$ and -1, hence $\mathcal{U}=\{\pm u^n/n\in\mathbb{Z}\}$. Let $u>1$ be the fundamental unit, $\rho e^{i\theta}$ and $\rho e^{-i\theta}$ its conjugates. We have

$$N(u)=u\times\rho e^{i\theta}\times\rho e^{-i\theta}=1.$$

It follows

$$u=\rho^{-2}.$$

In addition

$$disc_{\mathbb{Z}}(u)=(u-\rho e^{i\theta})^2(u-\rho e^{-i\theta})^2(\rho e^{i\theta}-\rho e^{-i\theta})^2=-4(\rho^3+\rho^{-3}-2cos\theta)^2sin^2\theta.$$

For $c=cos\theta$, let us set $g(x)=(1-c^2)(x-2c)^2-x^2$. Then we get

$$g(x)\leq 4(1-c^2),$$

or even

$$(1-c^2)(x-2c)^2\leq x^2+4(1-c^2).$$

Replacing x by $\rho^3+\rho^{-3}$, we obtain

$$(1-c^2)(\rho^3+\rho^{-3}-2c)^2<u^3+u^{-3}+6.$$

This involves that

$$|disc_{\mathbb{Z}}(u)|<4(u^3+u^{-3}+6).$$

Therefore

$$u^3>\frac{d}{4}-6-u^{-3}>\frac{d}{4}-7,$$

where $d = |disc_{\mathbb{Z}}(u)|$.
The discriminant of f equals -108, then $u^3 > 20$. Hence

$$u > 2,7144.$$

Since $\theta^{-1} \simeq 3,8473$, and $u^2 > 7,3680$, we get $u = \theta^{-1}$. We therefore have

$$\mathcal{U} = \{\pm\theta^n / n \in \mathbb{Z}\}.$$

Moreover, $2^{\frac{1}{3}}a - b = (a-b) + (2^{\frac{1}{3}} - 1)a = (a-b) + a\theta$. Since $N(2^{\frac{1}{3}}a - b) = 1$, we have $(a-b) + a\theta \in \mathcal{U}$, i.e., there exists $n \in \mathbb{Z}$ such that

$$(a-b) + a\theta = \pm\theta^n. \tag{4.2}$$

If we take for instance $(a-b) + a\theta = \theta^n$, then we get

$$(a-b) + a\theta_i = \theta_i^n, \text{ pour } i = 1, 2, 3,$$

where $\theta_1 = \theta$, θ_2 and $\theta_3 = \overline{\theta_2}$ are the three zeros of f. We have obviously

$$\frac{1}{f'(\theta_1)} + \frac{1}{f'(\theta_2)} + \frac{1}{f'(\theta_3)} = \frac{1}{(\theta_1-\theta_2)(\theta_1-\theta_3)} + \frac{1}{(\theta_2-\theta_1)(\theta_2-\theta_3)} + \frac{1}{(\theta_3-\theta_1)(\theta_3-\theta_2)} = 0, \tag{4.3}$$

and

$$\frac{\theta_1}{f'(\theta_1)} + \frac{\theta_2}{f'(\theta_2)} + \frac{\theta_3}{f'(\theta_3)} = \frac{\theta_1}{(\theta_1-\theta_2)(\theta_1-\theta_3)} + \frac{\theta_2}{(\theta_2-\theta_1)(\theta_2-\theta_3)} + \frac{\theta_3}{(\theta_3-\theta_1)(\theta_3-\theta_2)} = 0. \tag{4.4}$$

If we multiply (4.3) by $a - b$ and (4.4) by a, we find

$$\frac{(a-b)+a\theta_1}{f'(\theta_1)} + \frac{(a-b)+a\theta_2}{f'(\theta_2)} + \frac{(a-b)+a\theta_3}{f'(\theta_3)} = \frac{\theta_1^n}{f'(\theta_1)} + \frac{\theta_2^n}{f'(\theta_2)} + \frac{\theta_3^n}{f'(\theta_3)} = 0.$$

So, solving the equation $2x^3 - y^3 = 1$, is like finding the zeros of the sequence $(c_n)_{n\in\mathbb{Z}}$ defined by:

$$c_n = \frac{\theta_1^n}{(\theta_1-\theta_2)(\theta_1-\theta_3)} + \frac{\theta_2^n}{(\theta_2-\theta_1)(\theta_2-\theta_3)} + \frac{\theta_3^n}{(\theta_3-\theta_1)(\theta_3-\theta_2)}.$$

Now, let us work locally in $\mathbb{Q}_p$. For this purpose, we are looking for an adequate prime number p that allows us to apply Hensel's Lemma in ordre to find two zeros of f α and $\beta \in \mathbb{Q}_p$, the third one is then given by $\alpha + \beta + \gamma = -3$. Since $f(3) = 2 \times 31 \equiv 0 \ (mod\ 31)$, $f(6) = 11 \times 31 \equiv 0 \ (mod\ 31)$, $f'(3) = 48 \not\equiv 0 \ (mod\ 31)$ and $f'(6) = 147 \not\equiv 0 \ (mod\ 31)$, then according to Hensel's Lemma, there exist a unique α and β in $\mathbb{Z}_{31}$, where $\alpha = 34$ and $\beta = 37$, hence $\gamma = -74$. According to Fermat's little theorem, we have $\alpha^{30} \equiv 1 \ (mod\ 31)$. Thus $\alpha^{30} = 1 + a$. Since

$$\alpha^{30} = 34^{30} \equiv 838 \ (mod\ 31^2).$$

Then

$$a \equiv 837 \ (mod\ 31^2).$$

Similarly,

$$\beta^{30} \equiv 1 \ (mod\ 31).$$

Thus

$$\beta^{30} = 1 + b.$$

Since

$$\beta^{30} = 37^{30} \equiv 869 \ (mod\ 31^2).$$

Then

$$b \equiv 868 \ (mod\ 31^2).$$

Likewise, $\gamma^{30} \equiv 1 \ (mod\ 31)$. Thus

$$\gamma^{30} = 1 + c.$$

Since

$$\gamma^{30} = 74^{30} \equiv 94 \ (mod\ 31^2).$$

Then

$$c \equiv 93 \ (mod\ 31^2).$$

In the rest of the proof we will need the following table:

r	$\alpha^r \ (mod\ 31^2)$	$\beta^r \ (mod\ 31^2)$	$\gamma^r \ (mod\ 31^2)$
1	34	37	-74
30	838	869	94

In addition, we have

$$\begin{aligned} c_{r+30s} &= \frac{\alpha^r}{(\alpha-\beta)(\alpha-\beta)}(\alpha^{30})^s + \frac{\beta^r}{(\beta-\alpha)(\beta-\gamma)}(\beta^{30})^s + \frac{\gamma^r}{(\gamma-\beta)(\gamma-\alpha)}(\gamma^{30})^s \\ &= \frac{\alpha^r}{(\alpha-\beta)(\alpha-\beta)}(1+a)^s + \frac{\beta^r}{(\beta-\alpha)(\beta-\gamma)}(1+b)^s + \frac{\gamma^r}{(\gamma-\beta)(\gamma-\alpha)}(1+c)^s \\ &\equiv c_r \ (mod\ 31), \ \text{for } 1 \le r \le 30. \end{aligned}$$

The calculations show that $c_r \neq 0$ for $r \neq 1, 30$. Since, $c_{r+30s} \equiv c_r \ (mod\ 31)$, we get

$$c_{r+30s} \neq 0, \forall s \in \mathbb{N}, \ \text{for } r \neq 1, 30.$$

Let's say for $r = 1, 30$ and $s \in \mathbb{Q}_{31}$,

$$u_r(s) = \frac{\alpha^r}{(\alpha-\beta)(\alpha-\beta)}(1+a)^s + \frac{\beta^r}{(\beta-\alpha)(\beta-\gamma)}(1+b)^s + \frac{\gamma^r}{(\gamma-\beta)(\gamma-\alpha)}(1+c)^s.$$

To demonstrate the result, it is enough to work only with u_1 and u_{30}. Since $|a|_{31} \le 31^{-1}, |b|_{31} \le 31^{-1}$ and $|c|_{31} \le 31^{-1}$, we deduce from Lemma 2 that u_r is a function that we can develop as a series:

$$\lambda_{0,r} + \lambda_{1,r}s + \lambda_{2,r}s^2 + \cdots$$

We have

$$\lambda_{0,r} = 0, \text{ for } r = 1, 30, \quad \lambda_{j,r} \not\equiv 0 \ \left(mod\ 31^2\right), \text{ for } j \geq 2, \quad r \text{ unspecified},$$

and

$$\lambda_{1,r} = \frac{\alpha^r}{(\alpha-\beta)(\alpha-\gamma)}a + \frac{\beta^r}{(\beta-\alpha)(\beta-\gamma)}b + \frac{\gamma^r}{(\gamma-\beta)(\gamma-\alpha)}c \not\equiv 0 \ (mod\ 31^2),$$

for $r = 1, 30$.

According to Strassman's theorem, the functions $u_r(s)$, $r = 1, 30$, have at most one root. As they have at least one root, they have therefore exactly one root. From Equation (4.2), we have $\theta^0 = 1$ implies $a = 0$ and $b = -1$, which is impossible, and $\theta^1 = \theta$ implies $a = b = 1$.

This completes the proof. □

Corollary 1. *The P_1^3-set $\{1, 2, 13\}$ is nonextendible.*

Proof. Suppose there exists an integer $d > 13$ such that the quadruple $\{1, 2, 13, d\}$ is a P_1^3-set. Then the following system of equations has an integral solution $(u, v, w) \in \mathbb{N}^3$:

$$(S) \begin{cases} 2d + 1 = u^3, \\ 13d + 1 = v^3, \\ 26d + 1 = w^3. \end{cases}$$

The system (S) yields

$$2v^3 - w^3 = 1. \tag{4.5}$$

From Theorem 5, the unique positive integer solution of Equation (4.5) is $(v, w) = (1, 1)$, which is impossible in (S).

This completes the proof. □

Corollary 2. *The unicity of positive integer solution of Equation (4.1) implies the unicity of a cubic-triangular number.*

Proof. Let n be a cubic-triangular number. Since n and $n + 1$ are coprime then according to Equation (2.1), there exists x and y two positive integers such that $m = xy$, $n = y^3$ and $n+1 = 2x^3$, which implies Equation (4.1), that has from Theorem 5, $(x, y) = (1, 1)$ as unique positive integer solution. Thus, $n = 1$ is the unique cubic-triangular number. □

Remark 2. As we can see, the resolution of Equation (4.1) meets the two problems mentioned above that seem to be a priori different.

5. Conclusion

The interest of this work is twofold. Firstly, we showed an unexpected link between two problems, which were a priori distinct. Secondly, we presented a proof for the uniqueness of the positive integer solution of the Diophantine equation $2x^3 - y^3 = 1$, using p-adic analysis tools.

References

[1] "The on-line encyclopedia of integer sequences (oeis)." [Online]. Available: https://oeis.org/

[2] J. W. S. Cassels, *Lectures on elliptic curves*, 1st ed., ser. London Mathematical Society student texts 24. Cambridge University Press, 1991.

[3] A. Dujella. [Online]. Available: https://web.math.pmf.unizg.hr/~duje/dtuples.html

[4] R. T. T. N. Shorey, *Exponential diophantine equations*, ser. Cambridge Tracts in Mathematics. CUP, 1986.

USTHB University, Faculty of Mathematics, LATN Laboratory, P.O. Box 32, El Alia 16111, Bab-Ezzouar, Algiers, Algeria,

E-mail address: `a_debbache2003@yahoo.fr`

USTHB University, Faculty of Mathematics, L'IFORCE Laboratory, P.O. Box 32, El Alia 16111, Bab-Ezzouar, Algiers, Algeria,

Current address: Other Institution, Some Other Department, P. O. Box 0002, 12347 City, Other Country

E-mail address: `sbouroubi@usthb.dz or bouroubis@gmail.com`