Journal of Applied Mathematics & Bioinformatics, vol.5, no.4, 2015, 99-106
ISSN: 1792-6602 (print), 1792-6939 (online)
Scienpress Ltd, 2015

A new proof of Euler's theorem on Catalan's equation

Olufemi O. Oyadare[1]

Abstract

This paper contains a new proof of *Euler's theorem,* that the only non-trivial integral solution, (α, β), of $\alpha^2 = \beta^3 + 1$ is $(\pm 3, 2)$. This proof employs only the properties of the ring, $\mathbb{Z}$, of integers without recourse to elliptic curves and is independent of the methods of algebraic number fields. The advantage of our proof, over Euler's isolated and other known proofs of this result, is that it charts a *common* path to a novel approach to the solution of *Catalan's conjecture* and indeed of any Diophantine equation.

Mathematics Subject Classification: 11R04
Keywords: Catalan's equation; Mihăilescu's theorem; Polynomial equations

1 Introduction

Catalan's equation is given as $\alpha^m = \beta^n + 1, m, n \in \mathbb{N}$, whose solutions

[1] Department of Mathematics, Obafemi Awolowo University, Ile-Ife, 220005, Nigeria.
E-mail: femi_oya@yahoo.com

Article Info: *Received* : February 3, 2015. *Revised* : May 12, 2015.
Published online : October 20, 2015.

are sought in integers. *Catalan's conjecture (*1844*)* says that, apart from the trivial integral solutions $(\alpha, \beta) = (0, -1), (\pm 1, 0)$, the only non-trivial *integral* solutions of the equation are $(\alpha, \beta) = (\pm 3, 2)$ and that they occur precisely when $m = 2$ and $n = 3$. We refer to [2] for the history, developments and proof of *Mihăilescu's theorem* (2002) which solved this conjecture after about 158 years.

The case of $m = 2$ and $n = 3$ had earlier been completely solved by Euler in 1738 ([2], *p.* 118) by an *elementary* use of the *method of infinite descent.* Euler's method was elementary because his proof did not involve the use of *objects* outside $\mathbb{Z}$, as against the common practice in modern proofs of the same result on $\alpha^2 = \beta^3 + 1$ ([2], *p.* 19). In addition to this, the known proof of Catalan's conjecture, now called *Mihăilescu's theorem* [2] is *not* elementary, thereby isolating Euler's case from other cases of Catalan's equation. The fact that all the modern proofs of Euler's theorem did not generalize to solving Catalan's conjecture was also responsible for the delay in the eventual solution of the conjecture, thereby motivating us to seek a general platform where the Catalan's equation, $\alpha^m = \beta^n + 1$, could be understood once and for all.

In this paper we give another elementary proof of Euler's theorem and show how our method of proof may lead to both an elementary proof of Catalan's conjecture and a new parametrization of the integral solutions of Mordell equations, $\alpha^2 = \beta^3 + k, \ k \in \mathbb{Z}$, different from those in [4].

2 Main results

Let $f_n : \mathbb{Z} \to \mathbb{Z}$, be given as $f_n(y) = (y + 10)^n, \ n \in \mathbb{N}, \ y \in \mathbb{Z}$. We define an *exact integer* of power n as an integer which may be written as the $nth-$power of some element of $\mathbb{Z}$. In this sense -4 is an exact integer of power 1 only (since $-4 = (-4)^1$), while 4 is an exact integer of powers 1 (since $4 = 4^1$) and 2 (since $4 = (2)^2$). Our point of departure in the consideration of powers of integers is to view the set of *all* exact integers of power n in terms of the polynomials, f_n, as assured by the following Lemma.

Lemma 2.1 ([3], *p.* 3). *Let $\mathfrak{E}$ be the collection of all exact integers, explicitly* *given as*

$$\mathfrak{E} = \{\xi^n : \xi \in \mathbb{Z}^{>0} \textit{ and } n \in 2\mathbb{N}\} \cup \{\xi^n : \xi \in \mathbb{Z} \textit{ and } n \in \mathbb{N} \setminus 2\mathbb{N}\}.$$

Then the set $\mathfrak{E}$ *is in a one-to-one correspondence with the set* $\{f_n(y) : y \in \mathbb{Z},\ n \in \mathbb{N}\}$.

Proof. Define $\rho : \{f_n(y) : y \in \mathbb{Z},\ n \in \mathbb{N}\} \to \mathfrak{E}$ as $\rho(f_n(y)) := \xi^n$, with $\xi = 10 + y,\ y \in \mathbb{Z}$. ρ is a one-to-one correspondence. □

The constant 10 in f_n may clearly be replaced with any other constant in $\mathbb{Z}$, while the definition of $\mathfrak{E}$ is designed to take adequate care of the unnecessary repetition of values brought about by the equality of $(-m)^{2n}$ and $m^{2n},\ m \in \mathbb{Z},\ n \in \mathbb{N}$. See [3.] for a constructive approach to defining f_n. We now use the truth of the above Lemma to *transform* the equation $\alpha^2 = \beta^3 + 1$ as follows. Set $\alpha^2 = f_2(y)$ and $\beta^3 = f_3(y + a),\ y,\ a \in \mathbb{Z},\ a \neq 0$, to have $f_2(y) = f_3(y + a) + 1$, which translates to

$$a^3 + (30 + 3y)a^2 + (300 + 60y + 3y^2)a + (901 + 280y + 29y^2 + y^3) = 0.$$

This is a cubic monic polynomial equation in a whose coefficients are polynomials in $\mathbb{Z}[y]$ and whose solutions are sought in $\mathbb{Z}$. We call it *Catalan's polynomial equation of index* $(2, 3)$ (since it corresponds to the Catalan's equation $\alpha^2 = \beta^3 + 1$) and denote it by $c_y(a) = 0$.

It has at least a real root, say $a = -\gamma,\ \gamma \in \mathbb{R} \setminus \{0\}$ which, since it is expected above that $a \in \mathbb{Z} \setminus \{0\}$, implies that $\gamma \in \mathbb{Z} \setminus \{0\}$. The existence of γ in $\mathbb{Z} \setminus \{0\}$ assures us that the equation $\alpha^2 = \beta^3 + 1$ has *an* integral solution pair (α, β), which could be called trivial (when $\alpha\beta = 0$) or non-trivial (when $\alpha\beta \neq 0$). Employing *Euclid's division algorithm* of the domain $\mathbb{Z}[X]$ (or of $\mathbb{Q}[X]$, in order to have *uniquely determined* quotient and remainder polynomials, $q_{y,\gamma}(a)$ and $r_\gamma(y)$ respectively; [1.], *p.* 28), we arrive at

$$c_y(a) = a^3 + (30 + 3y)a^2 + (300 + 60y + 3y^2)a + (901 + 280y + 29y^2 + y^3)$$

$$= (a + \gamma) \cdot q_{y,\gamma}(a) + r_\gamma(y)$$

$$:= (a + \gamma) \cdot (a^2 + ([30 - \gamma] + 3y)a + (300 - 30\gamma + \gamma^2 + 3[20 - \gamma]y + 3y^2))$$
$$+ ((901 - 300\gamma + 30\gamma^2 - \gamma^3) + (280 - 60\gamma + 3\gamma^2)y + (29 - 3\gamma)y^2 + y^3) = 0.$$

We expect that the remainder polynomial $r_\gamma(y)$, which is essentially $c_y(-\gamma)$, satisfies

$$r_\gamma(y) = (901 - 300\gamma + 30\gamma^2 - \gamma^3) + (280 - 60\gamma + 3\gamma^2)y + (29 - 3\gamma)y^2 + y^3 = 0,$$

since $(a + \gamma)$ is a factor of $c_y(a)$. Now $r_\gamma(y) = 0$ is viewed as a cubic monic polynomial equation in y whose coefficients are polynomials in $\mathbb{Z}[\gamma]$.

The important point to note on the roots of $r_\gamma(y) = 0$ is this:

> *The above reformulation of Catalan's equation,* $\alpha^2 = \beta^3+1$, *requires that we seek only integral roots,* y, *to* $r_\gamma(y) = 0$, *for* $\gamma = -a \in \mathbb{Z} \setminus \{0\}$.

What then are the necessary and sufficient conditions for $r_\gamma(y) = 0$ to have *only* integral solutions? This is addressed in the following *central* result of the paper. We recall here, from [1], *p.* 139, the fact that the discriminant, $D := D(p_3(y))$, of a monic cubic polynomial, $p_3(y) \in \mathbb{Z}[y]$, always satisfies the congruence $D \equiv 0$ or $1 \pmod 4$.

Theorem 2.1. $r_\gamma(y) = 0$ *has only integral solutions if, and only if,* $\gamma = 1$.

Proof. Let $\gamma = 1$, then $r_1(y) = 630 + 223y + 26y^2 + y^3 = 0$, which gives $y = -7, -9, -10 \in \mathbb{Z}$.

Conversely, let $r_\gamma(y) = 0$ has only integral solutions, then the discriminant, $D(r_\gamma(y))$, computed to be

$$D(r_\gamma(y)) = -(23 - 36\gamma - 54\gamma^2 + 4\gamma^3 + 27\gamma^4)$$

must *necessarily* be a perfect square of some integer.

Solving $D(r_\gamma(y)) \equiv 1 \pmod 4$ gives $\gamma = 2n,\ n \in \mathbb{Z}$. However, $D(r_{2n}(y)) < 0$, for all $n \in \mathbb{Z}$, hence $D(r_{2n}(y))$ is not a perfect square of an integer for any $n \in \mathbb{Z}$. In the same way we solve $D(r_\gamma(y)) \equiv 0 \pmod 4$ to get $\gamma = 2n + 1,\ n \in \mathbb{Z}$. We observe in this case that, since $D(r_{2n+1}(y)) < 0$, for all $n \in \mathbb{Z} \setminus \{0\}$, we would still not have the expected perfect squared discriminant from $D(r_{2n+1}(y))$ as long as $n \in \mathbb{Z} \setminus \{0\}$. Indeed $D(r_\gamma(y))$ is a perfect square of some integer only at $\gamma = 2(0) + 1 = 1$. □

Remarks 2.1. Note that $D(r_1(y)) = 36$. The deductions from Theorem 2.1 are that the integral solutions, (α, β), of Catalan's equation, $\alpha^2 = \beta^3 + 1$, have to *necessarily* be *consecutive integers,* since

$$\mid \alpha \mp \beta \mid = \mid \mp a \mid = \mid \pm\gamma \mid = \mid \pm 1 \mid = 1$$

(where we add (respectively, subtract) when $\alpha \leq 0$ (respectively, $\alpha > 0$)), and that the integral values of y for which $r_1(y) = 0$ are completely *sufficient* to solve the (Catalan's) equation in integers.

We now use this information to give a complete solution to $\alpha^2 = \beta^3 + 1$ in $\mathbb{Z} \times \mathbb{Z}$, thereby giving another *elementary* proof of Euler's result on this equation.

Corollary 2.1. *The integral solution set of Catalan's equation* $\alpha^2 = \beta^3 + 1$ *in* $\mathbb{Z} \times \mathbb{Z}$ *is precisely* $\{(\alpha, \beta) = (0, -1), (\pm 1, 0), (\pm 3, 2)\}$.

Proof. We refer to the above reformulation of $\alpha^2 = \beta^3 + 1$, which by Theorem 2.1, needs only be considered for $\gamma = 1$. Hence solving $r_1(y) = 630 + 223y + 26y^2 + y^3 = 0$ gives $y = -7, -9, -10$. Therefore, when

$\underline{y = -7:}$

$\alpha^2 = f_2(y) = f_2(-7) = 9$,
$\beta^3 = f_3(y + a) = f_3(-7 - 1) = 8$. Hence $(\alpha, \beta) = (\pm 3, 2)$;

$\underline{y = -9:}$

$\alpha^2 = f_2(y) = f_2(-9) = 1$,
$\beta^3 = f_3(y + a) = f_3(-9 - 1) = 0$. Hence $(\alpha, \beta) = (\pm 1, 0)$;

$\underline{y = -10:}$
$\alpha^2 = f_2(y) = f_2(-10) = 0$,
$\beta^3 = f_3(y + a) = f_3(-10 - 1) = -1$. Hence $(\alpha, \beta) = (0, -1)$.

□

It may be seen that our approach to the study of $\alpha^2 = \beta^3 + 1$ is based only on the exploration of *in-built* structure of the equation as brought out in Theorem 2.1. In retrospect, we observe that only the properties of $\mathbb{Z}$ and $\mathbb{Z}[X]$ were employed in our proofs. In our opinion, the exploitation of properties of $\mathbb{Z}$ and $\mathbb{Z}[X_1, \cdots, X_n]$ (or of $\mathbb{Q}$ and $\mathbb{Q}[X_1, \cdots, X_n]$), in which $X_i \in \mathbb{Z}$ (or $\mathbb{Q}$), should be the only background on which the *solution* of a *Diophantine equation* is sought. This is what makes the equations *Diophantine.*

3 Directions to Catalan's conjecture and Mordell equations

(1) Catalan's polynomial equation, $c_y(a) = 0$, its remainder polynomial, $r_\gamma(y)$, and quotient polynomial, $q_{y,\gamma}(a)$, may equally prove indispensable in a systematic production and study of *(non-integral) algebraic* solutions of $\alpha^2 = \beta^3 + 1$ in various *quadratic fields* (which, according to Theorem 2.1, must correspond to $\gamma = -a \in \mathbb{Z} \setminus \{0, 1\}$), as well as in the *arithmetic* and *ideal* theories of these fields. A potent quest along this line is to find *how many non-trivial solutions of* $\alpha^2 = \beta^3 + 1$ *are in each of these number fields.* The proof of this may be fashioned on our Theorem 2.1 and may *not* easily be deductable from other proofs of Euler's theorem.

(2) Partial solutions of Catalan's conjecture leading to the 2002 Mihăilescu's theorem may also be subsumed under some properties of $r_\gamma(y), q_{y,\gamma}(a)$ or their generalizations, say $r_{n,\gamma}(y), q_{n-1,y,\gamma}(a)$, in $\alpha^m = \beta^n + 1,\ m, n \in \mathbb{N}$. Indeed if we combine Mihăilescu's theorem with Theorem 2.1 above, we may conclude that:

> *the generalization,* $r_{n,\gamma}(y) = 0$, *of* $r_\gamma(y) = 0$ *in* $\alpha^m = \beta^n + 1$ *has only integral solutions if, and only if,* $m = 2, n = 3$ *and* $\gamma = 1$,

thus giving Mihăilescu's theorem an elementary *outlook.* An independent proof of this statement, hence an elementary proof of Catalan's conjecture, and the systematic study of the contributions of the roots of $r_{n,\gamma}(y) = 0$ to other algebraic solutions of the Catalan's equation and the theory of their number fields may however have to be deduced from a proper handling of the explicit expression for $r_{n,\gamma}(y)$.

(3) The equation $\alpha^2 = \beta^3 + 1$ may also be seen as a representative of members of the family of *Mordell equations,* $\alpha^2 = \beta^3 + k,\ k \in \mathbb{Z}$, where the requirement for the existence of integral solutions may be sought in the form

$$\gamma = f(k),$$

reminiscence of Theorem 2.1, for some function $f : \mathbb{Z} \to \mathbb{Z}$. The required discriminant, $D(r_{\gamma,k}(y))$, of the corresponding reminder polynomial equation

$$r_{\gamma,k}(y) = (900+k-300\gamma+30\gamma^2-\gamma^3)+(280-60\gamma+3\gamma^2)y+(29-3\gamma)y^2+y^3 = 0,$$

of the *Mordell polynomial equation,* has been computed to be

$$D(r_{\gamma,k}(y)) = -27k^2 + (4 + 36\gamma + 54\gamma^2)k - 4\gamma^3 - 27\gamma^4$$

and may be treated like we did $D(r_{\gamma,1}(y)) =: D(r_\gamma(y))$ in the proof of Theorem 2.1. It is however clear from Theorem 2.1 that, for the above mentioned function $f : \mathbb{Z} \to \mathbb{Z}$, we have $f(1) = 1$ and, from Theorem 14.2.3 of [1], that f is going to be a function of functions. The structure and properties of f may ultimately be exploited in further understanding the integral solutions of $\alpha^2 = \beta^3 + k,\ k \in \mathbb{Z}$, which has been completely solved using a different approach in [4].

The ideas outlined in $(1) - (3)$ above or in [4] may be employed to seek and study the solution set and field theory of the equation $\alpha^m = \beta^n + k,\ m, n \in \mathbb{N},\ k \in \mathbb{Z}$.

The above method of reducing Diophantine equations to equations involving members of the *Noetherian domain* $\mathbb{Z}[X_1, \cdots, X_k]$ (or of $\mathbb{Q}[X_1, \cdots, X_k]$, with $X_i \in \mathbb{Z}$ (or $\mathbb{Q}$)), which we termed *Diophantine polynomials,* is a natural technique to the *complete* solution of *any* Diophantine equation (*cf.* [3]) and is a candidate for the much needed *Galois theory of Diophantine equations.*

Acknowledgement

The author is grateful to Professor René Schoof for sharing his thoughts on an earlier draft of this work.

References

[1] Alaca, Ş. and Williams, K. S., *Introductory algebraic number theory*, Cambridge University Press, 2004.

[2] Schoof, R., *Catalan's conjecture*, Springer-Verlag, London, 2008.

[3] Oyadare, O.O., Galois groups of Fermat polynomials and the arithmetic groups of Diophantine curves, to appear in *Scientia Magna*, **10**(2), (2014).

[4] Oyadare, O.O., On admissible Mordell equations and Hall conjecture, to appear in *Theoretical Mathematics and Applications*, **5**(2), (2015).