A New Approach to Find Integral Solutions for the Mordell's Equation, $y^2 + 2 = x^3$

Ekanayake E. M. P* and Dharmawardane P. M. N.

Department of Mathematical Sciences, Faculty of Applied Sciences, Wayamba University of Sri Lanka

**Email:* piyalekanayake@gmail.com

Abstract— Mordell's equation, $y^2 + 2 = x^3$, which is historically important, was solved using complex numbers and more specifically using the unique factorization method. In this paper, it is shown that Mordell's equation can be solved by using elementary mathematics and the Fermat's little theorem. In the first step, it is shown that if (x, y) is a solution of the aforementioned equation then $x \neq y$ and then the equation is reduced to a cubic equation. In the next step, it is shown that this cubic equation has no other integer solution than $x = 3$ using very elementary mathematics and the Fermat's little theorem, and hence the Mordell's equation has only the well-known solution $x = 3, y = \pm 5$.

Keywords—Cubic equation, Elementary mathematics, Fermat's little theorem, Mordell's equation, Unique factorization method

I. INTRODUCTION

Pierre de Fermat, a famous French mathematician, challenged the Europeans by inviting them to find the integer solutions of the now well-known Mordell's equation $y^2 + 2 = x^3$ (Conrad, 2009; Leyandekkers and Shannon, 2002; Mordell, 1914). It was said that Europeans failed to find the integer solutions and the proof of Fermat was also vague (Leyandekkers and Shannon, 2002). Fermat claimed that he could solve this equation but with no details (Conrad, 2009). Later, very famous Unique Factorization Method, hereafter referred to as UFM, was developed and since then the integer solution of the Mordell's equation was found using the UFM (Conrad, 2009). In the UFM, one has to use complex numbers but the main objective of this paper is to introduce a novel method in which only elementary mathematics and the Fermat's Little Theorem (FLT) are used to obtain the integer solutions of the Mordell's equation. The general case of Mordell's equation, $y^2 = x^3 + k$ for nonzero integer k, defines an elliptic curve over $\mathbb{Q}$. Mordell (1914) showed that there are at most finitely many integer solutions to the aforementioned equation. It must be noted that in the available literature, Stephens (1975) studied the number of co-prime solutions to the general case of Mordell's equation. However, there was no hint to solve the equation when $k = -2$, which is covered in this work.

II. MATERIALS AND METHODOLOGY

Consider the Mordell's equation given by

$$y^2 + 2 = x^3 \qquad (1)$$

To find integer solutions of (1), we shall show the use of elementary mathematics together with Fermat's little theorem. From (1), it is obvious that x is positive and if x is even, then $x^3 \equiv 0 \pmod 8$. Then by (1), we have $y^2 \equiv -2 \pmod 8$. However, $-2 \pmod 8$ is not a square. Therefore, x should be odd and hence y should also be odd (Conrad, 2009). Moreover, $(x, y) = 1$ which follows from (1).

Now, we shall show that $y \neq x$. If $y = x$, then $x^3 - x^2 > 2$ unless $x \neq 1$. It is clear from (1) that x can not be one. Therefore $y \lneqq x$. Now since x and y are odd, together with the aforementioned result we can write $y = x + 2m$, where m is a nonzero integer.

It follows from (1) that

$$x^3 - x^2 - 4mx - 2(1 + 2m^2) = 0 \qquad (2)$$

Since it is obvious from Equation (1) that $x > 0$ and $x \neq 1$ and we proved that x must be odd, the next odd positive integer x can take is 3. When $x = 3$, the Equation (2) becomes $m^2 + 3m - 4 = 0$ and the roots of this quadratic equation are $m = 1, -4$. Conversly, when $m = 1$ or -4, we obtain $x = 3$ as the only integer solution for the cubic Equation (2). Now it is clear that $(m = 1, x = 3)$ and $(m = -4 \ , \ x = 3)$ satisfy the Equation (2), respectively. Moreover, since x is odd, the possible integer roots of $x^3 - x^2 - 4mx - 2(1 + 2m^2) = 0$ are odd. And hence those positive odd integers are factors of $(1 + 2m^2)$. Here, it is noteworthy to mention that:

when $m = 1$, we have positive integer factor of $(1 + 2m^2) = 3$ as $x = 1$ and 3. We choose only $x = 3$ since $x \neq 1$.

When $m = -4$, we have positive integer factors of $(1 + 2m^2) = 33$ as $x = 1$,3, 11 and 33. We choose only $x = 3$. We neglect 1, 11 and 33 since $x \neq 1$ and 11 and 33 do not satisfy the cubic equation.

All the facts mentioned above confirm that the smallest positive integer that x can take is 3.

Now since $y = x + 2m$ and $m = 1$ or $m = -4$, we have $y = \pm 5$. In other words, $x = 3$, $y = \pm 5$ are the solutions of Equation (1).

Next, we shall show that these are the only solutions of this equation.

If $(1 + 2m^2)$ is a prime number solution for x, then from (2), we have

$$m^2(1 + 2m^2) - (2m + 1) = 0 \qquad (3)$$

This means that m should divide 1, and hence $m = 1$ and $x = 3$. Therefore, there is no any other prime number solution which is equal to $1 + 2m^2$ other than $x = 3$. It is important to mention here that when m divides 1, we have $m = \pm 1$.

However, we neglect the case when $m = -1$ since it does not satisfy Equation (3).

Now we assume that $1+2m^2$ is a composite number and $m \not\equiv 0 \text{ (mod 3)}$.

Then we have $1+2m^2 = 3+2(m^2-1) \equiv 0 \text{ (mod 3)}$ from the FLT. Let $1+2m^2 = 3pq$ in this case.

If $x = 3$ is a solution of (2), then $pq = 3-2m > 0$. Therefore, $m = 1$, $pq = 1$, and $x = 3$, again. If p is a solution of the Equation (2), we must have

$$p^2 - p - 2(2m+3q) = 0 \qquad (4)$$

It is clear that there is no integer solution for odd p such that $p \equiv 0 \text{ (mod 3)}$ because it does not divide $2m+3q$ since $m \not\equiv 0 \text{ (mod 3)}$. If $p \not\equiv 0 \text{ (mod 3)}$, consider

$$3pq = 1 + 2\mathrm{m}^2 \qquad (5)$$

Now multiplying (4) by m and combining the result with (5), we get

$$\begin{gathered} m(p^2-p) - 6pq = 6qm - 2 \\ \text{or} \\ m(p^2-1+1-p) - 6pq = 6qm - 2 \end{gathered} \qquad (6)$$

By the FLT, $p^2 - 1 = 0 \text{ (mod 3)}$. Hence, $(p-1)$ or $(p+1)$ is divisible by 3. However, it is clear from (6) that $p-1 \not\equiv 0 \text{ (mod 3)}$. Assume that $p+1 \equiv 0 \text{ (mod 3)}$. Then we have $p = 3k-1$ for some postive integer k. Then from (4), we have

$$2(2m+3q) = (3k-1)(3k-2).$$

In other words,

$$9k^2 - 9k = 4m + 6q - 2 \qquad (7a)$$

$$3(3kq) = 3q + 1 + 2m^2 \qquad (7b)$$

Here (7b) is obtained from (5).

Now, from (7a) and (7b), we obtain

$$9kq + 9k^2 - 9k = 2m^2 + 4m + 9q - 1 \qquad (7c)$$

If $q = 1$, (7c) becomes

$$9k^2 = 2m^2 + 4m + 8 \qquad (7d)$$

Accordingly, k should be even and hence m should also be even which follows from (7d).

Let $m = 2l$. Then (7d) becomes $9k^2 = 8(l^2+l+1)$ and hence we deduce that (7d) never holds since l^2+l+1 is odd for all l. As a deduction from the quadratic equation (4), we get that $(25+16m)$ is not a perfect square for any integer $m > 0$. Again we deduce from (7c) that

$$9kq + 9k^2 - 9k = 2m(m-1) + 6m + 9q - 1$$

If $(m-1)$ is divisible by 3, (7c) never holds. Similarly, (7c) can be written as

$$3kq + 3k^2 - 3k = \frac{2}{3}(m+1)^2 + 3q - 1$$

It is clear that (7c) does not hold even if $m+1 \equiv 0 \text{ (mod 3)}$ and $m \not\equiv 0 \text{ (mod 3)}$. Therefore we conclude that Equation (2) has no integer solution other than $x = 3$ when $m \not\equiv 0 \text{ (mod 3)}$.

Now suppose that $m = 3t$, where t is an integer. $x = 1 + 2m^2$ does not hold unless $m = 1$ as before. Now, let $1 + 2m^2 = pq$ and let $x = p$. Then from (2), we have

$$p^2 - p - 2\,(2m+q) = 0 \qquad (8)$$

Now, $p \not\equiv 0 \text{ (mod 3)}$ since $m \equiv 0 \text{ (mod 3)}$. As before, $p - 1 \not\equiv 0 \text{ (mod 3)}$ since $q \not\equiv 0 \text{ (mod 3)}$.

Assume that $p+1 \equiv 0 \text{ (mod 3)}$. Let $p = 3k-1$ as before and upon substitution we obtain from (8)

$$18k^2 - 18k - 8m = 4q - 4 \qquad (9a)$$

$$72t^2 = 4pq - 4 \qquad (9b)$$

where, (9b) follows from $m = 3t$ and $1 + 2m^2 = pq$.

From (9a) and (9b), we get $72t^2 - 18k^2 + 18k + 24t = 4q(p-1)$ and this leads to the contradiction that $p - 1 \equiv 0 \text{ (mod 3)}$. Therefore, we can conclude that (1) has no other integer solution than $x = 3, y = \pm 5$.

III. RESULTS AND DISCUSSION

Mohanthy (1973) showed that if $N'(k)$ denoted the number of coprime integer solutions x, y to Diophantine equation $y^2 - k = x^3$ for nonzero integer k then $\limsup_{k\to\infty} N'(k) \geq 8$ and two years later, Stephens (1975) showed that

$$\limsup_{k\to\infty} N'(k) \geq 8 \text{ and } \limsup_{k\to-\infty} N'(k) \geq 12.$$

Moreover, Bennett and Ghadermarzi (2015) solved the above equation for all integer k with $|k| \leq 10^7$. As special case for the above equation, when $k = -2$, Beukers (2011) and Conrad (2009) found the integer solutions to the equation $y^2 + 2 = x^3$ by using UFM. In contrast to the above methods we could solve the aforementioned equation, using elementary mathematics and the FLT.

IV. CONCLUSION

In this paper we presented a novel method to solve the special Mordell's equation given by $y^2 + 2 = x^3$. By using elementary mathematics together with FLT we could obtain solutions as $x = 3, y = \pm 5$ of the Mordell's equation.

V. REFERENCES

Bennett, M.A. and Ghadermarzi, A. (2015). Mordell's equation: a classical approach, *LMS J. Comput. Math.* , **18** (1) 633–646

Beukers, F. (2011). Diophantine equations, Available from http://pub.math.leidenuniv.nl/~evertsejh/dio2011-diophantine.pdf (Accessed on July 18, 2021)

Conrad K. (2009). Examples of Mordell's Equations, Available from https://kconrad.math.uconn.edu/blurbs /gradnumthy/mordelleqn1.pdf (Accessed on July 02, 2021)

Leyandekkers, J.V. and Shannon, A.G. (2002). Fermat and the solution of $x^3 - 2 = y^2$, *International Journal of Mathematical Education and Science and Technology,* **33** (1), 91-95, DOI: 10.1080/00207390210211

Mohanthy, S.P. (1973). A note on Mordell's equation $y^2 - k = x^3$, *Proc. Amer. Math. Soc.* **39**, 645-646

Mordell, L. J. (1914). Indeterminate equations of the third and fourth degree, *Quart. J. Pure Appl. Math.*, **45**, 170–186

Stephens, N.M. (1975). On the number of co-prime solutions of $y^2 = x^3 + k$, *Proceeding of the American Mathematical Society*, **48**(2), 325-327, DOI**:** https://doi.org/10.1090/S0002-9939-1975-0357320-4