Theoretical Mathematics & Applications, vol.5, no.2, 2015, 31-70
ISSN: 1792-9687 (print), 1792-9709 (online)
Scienpress Ltd, 2015

On Admissible Mordell Equations and Hall conjecture

Olufemi O. Oyadare[1]

Abstract

We introduce the notion of an *admissible* Mordell equation and establish some basic results concerning properties of its integral solutions. A non class-number and complete parametrization, with the most minimal set of conditions, for generating *all* the integral solutions of admissible Mordell equations was then proved. An effective and efficient algorithm for computing the integral solutions of admissible Mordell equations was also established from a proof of the *Hall conjecture.* One of our major results concerns the upper-bound for the number of integral solutions of each of these equations which we show may be explicitly computed. The analysis of these results leads us to the problem of deriving a general expression for the number of integral solutions of the Mordell equations. This problem is completely solved.

Mathematics Subject Classification: 11R04
Keywords: Mordell equations; Polynomial equations; Hall conjecture

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

Article Info: *Received* : January 12, 2015. *Revised* : March 14, 2015.
Published online : April 30, 2015.

1 Introduction

Mordell equations are the members of a family of equations given as $y^2 = x^3 + k,\ k \in \mathbb{Z}$, whose solutions, (x, y), are sought in integers. The case of $k = 1$ is a *Catalan equation* (being also a member of the family of equations $y^m = x^n + 1,\ m, n \in \mathbb{N}$) and has a long interesting history starting from *Euler's theorem* (1738) which states that, apart from the trivial solutions $(x, y) = (-1, 0), (0, \pm 1)$, the only non-trivial *integral* solutions of the equation $y^2 = x^3 + 1$ are $(x, y) = (2, \pm 3)$. However a general technique for isolating integrally solvable Mordell equations, for generating all their integral solutions and for knowing how many of such solutions to expect have been a challenge to mathematicians. This challenge has led to the propagation of conjectures, some of which were deduced and discussed based on available numerical data, and to the proofs of these conjectures using isolated techniques.

We put the results of [8], where we had given a new proof of Euler's theorem on the Catalan's equation, in proper perspective by studying integral solutions of Mordell equations $y^2 = x^3 + k$ for all $k \in \mathbb{Z}$. Among other results, our study introduces a natural platform for studying Mordell equations (indeed any Diophantine equation) and gives completely satisfying answers to the trio challenge of isolating integrally solvable Mordell equations (contained in Definition 3.1), of generating all its integral solutions (by giving explicit expressions for them in Theorem 3.3 and Corollary 3.4) and of knowing how many of such solutions to expect (as shown in Theorem 5.2). The Hall conjecture is also established in Theorem 4.1 as a consequence of the expressions given in Theorem 3.3, which leads to a proof of the effectiveness of our approach to this study (in Theorem 4.2). We refer to [1] and [9] for the status report on integral solutions of Mordell equations and the upper-bounds for the number of these solutions, respectively. We now give a more detailed description of our results.

The present study is conducted by reformulating the problem of seeking integral solutions of Mordell equations into the systematic investigation of a corresponding third-order polynomial in $\mathbb{Z}[X]$, with indeterminates $X \in \mathbb{Z}$. In particular, we study these equations through the introduction of what we term *admissible integers* derived from a detailed look at the result of applying the *Euclid's division algorithm* to this third-order polynomial in §3. These investigations lead to a new and complete parametrization of the integral solutions of those integrally solvable Mordell equations among $y^2 = x^3 + k$, given as

$$x = x(k, \gamma, t) = \frac{1}{t}(900 + k + 10t - (300 + t)\gamma + 30\gamma^2 - \gamma^3)$$

and

$$y = y(k, \gamma, t) = \pm\frac{1}{t}(900 + k + 10t - 300\gamma + 30\gamma^2 - \gamma^3),$$

for some $(k, \gamma, t) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$, which unifies the two major and hitherto isolated cases of $k = 0$ and $k \in \mathbb{Z} \setminus \{0\}$, and is in line with the method of solving Diophantine equations via the study of their corresponding *Diophantine polynomials* introduced in [7] to study Fermat equations.

Indeed this parametrization gives the first known complete method of generating *all* the integral solutions, (x, y), of *all* the integrally-solvable members of the equations $y^2 = x^3 + k,\ k \in \mathbb{Z}$. Some of the results of the present paper may be seen as solutions to the open problems raised in [8.] while one of our major results contained in §5. is an improvement on the different upper-bounds, $b(k)$, of the number, $n = n(k)$, of integral solutions given in [9] by earlier authors, which is brought down to

$$b(k) = 120 \mid k \mid^{3+|k|} - 6$$

while $n(k)$ is shown to be explicitly given as

$$n(k) = 120 \mid k \mid^{3+|k|} - \rho(k) - 6\nu(k) - 6,$$

for every $k \in \mathbb{Z} \setminus \{0\}$ with the functions $\rho : \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{Z}^{\geq 0}$ and $\nu : \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{Z}^{\geq 0}$ as defined in §5. A general finite-step algorithm (in Corollary 3.8) was established to give all integral solutions of *admissible* Mordell equations. The *Hall conjecture* is then shown with an explicit calculation of the *Hall constant* in Theorem 4.1. Ultimately the effectiveness of our approach is established in Theorem 4.2. An example showing the typical steps of this algorithm and effectiveness of our approach is given in Example 4.1.

Investigation of the *minimal set* of admissible integers that give *all* distinct integral solutions to every $y^2 = x^3 + k,$ with $k \in \mathbb{Z} \setminus \{0\}$, and its relationship with the number of these solutions are listed at the end of the paper as open problems. We believe that the problem of computing the integral (resp., rational integral) solutions to a Diophantine equation and their exact number could easily be solved when there is a firm platform for understanding the interactions among components of the equations. Such a platform is via a study of their corresponding *Diophantine* polynomials introduced in [7] for the *Fermat equations* which is further pursued in [8] for a Catalan equation and in the present paper for Mordell equations. The results of this paper strongly assure us that there is an *elementary* path to *Mihăilescu's theorem* (2002) on *Catalan's problem.*

2 Preliminaries

Let $f_n : \mathbb{Z} \to \mathbb{Z}$, be given as $f_n(\zeta) = (\zeta + 10)^n,\ n \in \mathbb{N},\ \zeta \in \mathbb{Z}$. 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 $4 = (\pm 2)^2$). 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 set of polynomials f_n as assured by the following Lemma.

Lemma 2.1 ([7]). *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 $\{f_n(\zeta) : \zeta \in \mathbb{Z}, n \in \mathbb{N}\}$.

Proof. Define $\rho : \{f_n(\zeta) : \zeta \in \mathbb{Z}, n \in \mathbb{N}\} \to \mathfrak{E}$ as $\rho(f_n(\zeta)) := \xi^n$, with $\xi = 10 + \zeta,\ \zeta \in \mathbb{Z}, n \in \mathbb{N}$. ρ is clearly 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 $m^{2n},\ m \in \mathbb{Z} \setminus \{0\},\ n \in \mathbb{N}$. The article [7] contains a constructive approach to defining

f_n. We now use the truth of the above Lemma to *transform* the equation $y^2 = x^3 + k,\ k \in \mathbb{Z}$, as follows.

Set $x^3 = f_3(\zeta + a)$ and $y^2 = f_2(\zeta),\ \zeta,\ a \in \mathbb{Z}$, to have

$$f_2(\zeta) = f_3(\zeta + a) + k,$$

which translates to

$$a^3 + (30 + 3\zeta)a^2 + (300 + 60\zeta + 3\zeta^2)a + (900 + k + 280\zeta + 29\zeta^2 + \zeta^3) = 0.$$

This is a monic cubic polynomial equation in a whose coefficients are polynomials in $\mathbb{Z}[\zeta]$ and whose roots are sought in $\mathbb{Z}$. We call it *Mordell's polynomial equation* and denote it by

$$m_{\zeta,k}(a) = 0,$$

$\zeta, k, a \in \mathbb{Z}$. Our aim is to study the Mordell equations via the considerations of Mordell's polynomial equation. It should be noted that we are aware that Mordell equations form a class of elliptic curves whose integral solutions could be predicted and abstractly handled using the general methods of elliptic curves. However we present here a completely new approach to studying Mordell equations by a method which breaks down the component parts, y^3 and x^2, of each of the equations and regroups them into appropriate terms of a $1-$determinte polynomial equation, $m_{\zeta,k}(a) = 0$, whose coefficients,

$$1,\ \ 30 + 3\zeta,\ \ 300 + 60\zeta + 3\zeta^2,\ \ 900 + k + 280\zeta + 29\zeta^2 + \zeta^3,$$

measure the contributions and interactions of the individual parts, thus encoding the properties of the integral solutions of the equations. An attainment of such a feat would lay the properties of the equations and their integral solutions before us through a detailed information on the polynomial. This is exactly what has been achieved by the above transformation of Mordell equations to the polynomial equations $m_{\zeta,k}(a) = 0$ and their study in the next section.

The third-order polynomial equation, $m_{\zeta,k}(a) = 0$, has at least a real root, say $a = -\gamma,\ \gamma \in \mathbb{R}$. Since for a Mordell equation to have an integral solution it is expected from above that $a \in \mathbb{Z}$, we conclude in this case that $\gamma \in \mathbb{Z}$. Note that an integral solution pair (x, y) (if it exists) of $y^2 = x^3 + k$ would be called *trivial* whenever $xy = 0$ or *non-trivial* whenever $xy \neq 0$.

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, $q_{\zeta,\gamma,k}(a)$ and $r_{\gamma,k}(\zeta)$ respectively; [1.], p. 28), we arrive at

$$m_{\zeta,k}(a) = a^3 + (30+3\zeta)a^2 + (300+60\zeta+3\zeta^2)a + (900+k+280\zeta+29\zeta^2+\zeta^3)$$

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

$$:= (a+\gamma)\cdot(a^2 + ([30-\gamma]+3\zeta)a + (300-30\gamma+\gamma^2+3[20-\gamma]\zeta+3\zeta^2))$$
$$+ ((900+k-300\gamma+30\gamma^2-\gamma^3) + (280-60\gamma+3\gamma^2)\zeta + (29-3\gamma)\zeta^2+\zeta^3) = 0.$$

Since $(a+\gamma)$ is a factor of $m_{\zeta,k}(a)$ we expect that the remainder polynomial $r_{\gamma,k}(\zeta)$, which is essentially equal to $m_{\zeta,k}(-\gamma)$, satisfies $r_{\gamma,k}(\zeta)=0$. That is

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

Now $r_{\gamma,k}(\zeta)=0$ is viewed as a monic cubic polynomial equation in ζ whose coefficients are polynomials in $\mathbb{Z}[\gamma]$ and may be shown to be of discriminant

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

The important point to note on the roots of $r_{\gamma,k}(\zeta)=0$ is that:

> *The above reformulation of Mordell equation, $y^2 = x^3+k$, requires that we seek integral roots, ζ, to $r_{\gamma,k}(\zeta)=0$, for $\gamma\in\mathbb{Z}$.*

A systematic study of these integral roots and their contributions to the existence, nature and explicit expressions of the integral solutions of Mordell equations are the focus of the next section. We develop a correspondence between integral roots of $r_{\gamma,k}(\zeta)=0$ and integral solutions (whenever they exist) of Mordell equations. This study is conducted once and for all for any arbitrary constant $k\in\mathbb{Z}$ as against the case-by-case or group-by-group treatments often employed before now at getting integral solutions of the equations ($cf.$ [1.], p. 392 and [6], p. 202). The immediate consequences of this general view of Mordell equations are (i.) a practical and unified parametrization of all integral solutions of Mordell equations (with any number of integral solutions) which is very effective and contains the most minimal and elementary set of conditions known to the author and (ii.) bounds of these solutions (not based on numerical analysis of a collection of data in any range; $cf.$ [4.]) which lead to the verification of the Hall conjecture and an explicit method of calculating the Hall constant. This approach also allowed us to derive the hitherto unknown explicit expression for the number of integral solutions of an integrally solvable Mordell equation.

3 Integral solutions of Mordell equations

Mordell equations $y^2 = x^3 + k$ may be parameterized by the choice of $k \in \mathbb{Z}$ and classified into *non-trivial* and *trivial* types according to the finiteness or otherwise of the number of its integral solutions, (x, y). We may then write the equations as

$$M(k) : \ y^2 = x^3 + k,$$

where $k \in \mathbb{Z}$ and $(x, y) \in M(k)$ are sought in $\mathbb{Z} \times \mathbb{Z}$.

It is well-known that when $k = 0$, the equation $y^2 = x^3 + k$ (which may be termed *trivial*) has an infinite integral solution-set, $M(0)$, given as

$$M(0) = \{(x, y) = (\delta^2, \pm\delta^3) : \delta \in \mathbb{Z}\},$$

while the integral solution-set, $M(k)$, for $k \in \mathbb{Z} \setminus \{0\}$, is finite and constitutes a non-trivial challenge to compute when k is arbitrary chosen. We start by considering some *basic* results on the configuration of $M(k)$ which will be needed later in some of our major results. Our first observation is the fact that no two integral solution-sets may have a common element. That is, no integral solution of any Mordell equation may solve any other Mordell equation.

Lemma 3.1 *Let $k_1, k_2 \in \mathbb{Z}$ be chosen such that $M(k_1), M(k_2) \neq \emptyset$. Then*

$$M(k_1) \cap M(k_2) \neq \emptyset \ \ \textit{iff} \ \ k_1 = k_2.$$

In this case $M(k_1) = M(k_2)$. *Proof.* Define a non-empty set $L(M)$ as

$$L(M) := \mathbb{Z} \times \mathbb{Z}.$$

The relation $\diamond$ on $L(M)$ given as

$$(x_1, y_1) \diamond (x_2, y_2) \quad \text{iff} \quad y_1^2 - x_1^3 = y_2^2 - x_2^3$$

is an equivalence relation, whose equivalence classes are the integral solution-sets $M(k),\ k \in \mathbb{Z}$. □

It is clear that $L(M) = \coprod_{k\in\mathbb{Z}} M(k)$. That is, the collection of integral solution-sets, $M(k)$, of the Mordell equations partitions the whole of $\mathbb{Z}\times\mathbb{Z} := L(M)$ into non-overlapping subsections. The fact that the above disjoint union exhausts the entire *Diophantine plane,* $\mathbb{Z}\times\mathbb{Z}$, may be the source of the central position occupy by Mordell equations among other Diophantine equations. We may also conclude from Lemma 3.1 that *every* $k \in \mathbb{Z}$ *uniquely determines the members of* $M(k)$.

Lemma 3.2. *If* $(x, y) \in M(k)$ *then* $(x, -y) \in M(k)$.

Proof. Let $(x, y) \in M(k)$ be given according to Lemma 2.1 as $x^3 = f_3(\zeta+a)$ and $y^2 = f_2(\zeta)$ then $y = \sqrt{f_2(\zeta)} = \pm(\zeta + 10) = -[\mp(\zeta + 10)]$, implying therefore that $(x, -y) \in M(k)$. □

The above Lemma may be seen from the simple fact that $y^2 - x^3 = (-y)^2 - x^3$ which, when viewed in the light of Lemma 3.1, shows that $(x, \pm y)$ belong to the same equivalence class or the same integral solution-set, $M(k)$. Notwithstanding the simplicity of Lemma 3.2 the existing relationship between (x, y) $(\in M(k))$ and $(-x, y)$ is non-trivial as may be seen at the tail-end of Corollary 3.1.

Lemma 3.3. *Let* $(x, y) \in M(k)$, *for some* $k \in \mathbb{Z}$, *such that* $x \neq 0$. *Then*

(i.) $(-x, y) \notin M(k)$;

(ii.) $(-x, y) \in M(k^{'})$ *iff* $x^3 = \frac{1}{2}(k^{'} - k)$ *and* $y^2 = \frac{1}{2}(k^{'} + k)$.

Moreover $k = n - m$ *and* $k^{'} = n + m$, *for some* $m, n \in \mathbb{Z},\ m \neq 0$. *Proof.* *(i.)* The hypothesis $(x, y) \in M(k)$ means that $y^2 - x^3 = k$. Now as

$$y^2 - (-x)^3 = y^2 + x^3 \neq k,$$

it follows that $(-x,y) \notin M(k)$.

$(ii.)$ Let $(x,y) \in M(k)$ and $(-x,y) \in M(k^{'})$ then $y^2 - x^3 = k$ and $y^2 + x^3 = k^{'}$ which, when solved simultaneously, gives $x^3 = \frac{1}{2}(k^{'} - k)$ and $y^2 = \frac{1}{2}(k^{'} + k)$. In the converse, we see that $y^2 - (-x^3) = y^2 + x^3 = \frac{1}{2}(k^{'} + k) + \frac{1}{2}(k^{'} - k) = k^{'}$. That is $(-x,y) \in M(k^{'})$.

¿From $(ii.)$ $k^{'} + k = 2n$ and $k^{'} - k = 2m$, for some $m, n \in \mathbb{Z}$, which solve to give $k = n - m$ and $k^{'} = n + m$. We claim that $m \neq 0$, for otherwise $k = n = k^{'}$, hence $x^3 = 0$ which contradict $x \neq 0$. □

For example we know that $(2, \pm 3) \in M(1)$. In order to locate $k^{'} \in \mathbb{Z} \setminus \{0\}$ for which $(-2, \pm 3) \in M(k^{'})$ we solve either $2^3 = \frac{1}{2}(k^{'} - 1)$ or $(\pm 3)^2 = \frac{1}{2}(k^{'} + 1)$ to get $k^{'} = 17$ and conclude that $(-2, \pm 3) \in M(17)$. The above Lemmas shall be employed in §4. in simplifying the proof of *Hall conjecture* to those integral solutions, (x,y), of $y^2 = x^3 + k$ for which $y > 0$.

Corollary 3.1. *Let $a, b \in \mathbb{Z}$ be given such that $a \neq 0$.*

$(i.)$ $(a,y) \in M(k)$ iff $(-a,y) \in M(2a^3 + k)$;

$(ii.)$ $(x,b) \in M(k)$, with $x \neq 0$, iff $(-x,b) \in M(2b^2 - k)$.

Hence $(a,b) \in M(k)$, with $a \neq 0$, iff $M(2a^3 + k) = M(2b^2 - k)$. *Proof.* We solve $a^3 = \frac{1}{2}(k^{'} - k)$ for the *'only if'* of $(i.)$ and $b^2 = \frac{1}{2}(k^{'} + k)$ for the *'only if'* of $(ii.)$. Now if $(-a,y) \in M(2a^3 + k)$ then $(a,y) = (-(-a),y) \in M(2(-a)^3 + (2a^3 + k)) = M(k)$. In the same way, if $(-x,b) \in M(2b^2 - k)$ then $(x,b) = (-(-x),b) \in M(2b^2 - (2b^2 - k)) = M(k)$.

Also $(a,b) \in M(k)$ iff $b^2 = a^3 + k$ iff $2a^3 + k = 2b^2 - k$ iff $M(2a^3 + k) \cap M(2b^2 - k) \neq \emptyset$ (from Lemma 3.1) iff $M(2a^3 + k) = M(2b^2 - k)$ (since each $M(k)$ is an equivalence class of $L(M)/\diamond$). □

The last part of Corollary 3.1 gives a useful characterization of membership of *almost all* the non-trivial members of each of the integral solution-sets, $M(k),\ k \in \mathbb{Z}$. The exception to the characterization being those integral solutions of the form $(0, b)$.

The finiteness of $M(k),\ k \in \mathbb{Z} \setminus \{0\}$, is a version of the celebrated Siegel's theorem for these equations and the difficulty of its explicit realization may be glanced from the volume of intricate results on algebraic number theory that goes into solving only one of the members in the family $y^2 = x^3+k,\ k \in \mathbb{Z}\setminus\{0\}$, in [1]. This challenge is, in the present paper, completely surmounted by the trio of Theorems 3.3, 4.2 and 5.2.

Next to those values of $k \in \mathbb{Z} \setminus \{0\}$ for which the integral solution-set of $y^2 = x^3 + k$ is empty are those values of k for which the integral solution-set is a singleton. We shall therefore start our investigation by considering Mordell equations with unique solutions. The unique integral solutions of such Mordell equations may be quickly isolated in the following. Indeed the next theorem proves that the unique integral solution of a Mordell equation (with such a solution) is necessarily a trivial one while Theorem 3.2 gives the explicit form of this trivial solution.

It should however be noted that the proofs of these Theorems do not yet require the entire machinery of Mordell polynomial equation,

$$m_{\zeta,k}(a) = (a + \gamma) \cdot q_{\zeta,\gamma,k}(a) + r_{\gamma,k}(\zeta) = 0,$$

developed in §2. until Corollary 3.5. We only employ Lemma 2.1 via Lemma 3.2

Theorem 3.1. *Let the Mordell equation $y^2 = x^3 + k,\ k \in \mathbb{Z} \setminus \{0\}$, have a unique integral solution, (x, y). Then $xy = 0$. That is, every Mordell equation with a unique integral solution has only the trivial solution.* *Proof.* Application of the hypothesis of uniqueness to Lemma 3.2 implies that $y = 0$, so that

$xy = 0.$ □

Corollary 3.2. *Every Mordell equation with a non-trivial integral solution has more than one integral solution.*

It should be noted that the above Theorem is not invalidated by the examples of trivial integral solutions, (x, y), of $y^2 = x^3 + k,\ k \in \mathbb{Z} \setminus \{0\}$, of the form $(x, y) = (0, \pm\sqrt{k})$, where k is a perfect square of some non-zero integer. If anything at all, such examples of trivial integral solutions only show that the converse of Theorem 3.1 is false. They actually reveal that the trivial integral solutions of the form $(x, y) = (0, \pm\sqrt{k})$ *cannot* be of unique type (since of course $+\sqrt{k} \neq -\sqrt{k}$, if $k \neq 0$) while affirming that *only* the integral solutions of the form $(x, y) = (\sqrt[3]{-k}, 0)$, where k is a perfect cube of some non-zero integer, *may be* of unique type.

These observations may be formalized as follows and is a strengthening of Theorem 3.1

Theorem 3.2. *Let the Mordell equation $y^2 = x^3 + k,\ k \in \mathbb{Z} \setminus \{0\}$, have a unique integral solution, (x, y). Then $x \neq 0$ and $y = 0$.* *Proof.* If the Mordell equation $y^2 = x^3 + k,\ k \in \mathbb{Z} \setminus \{0\}$, has a unique integral solution (x, y) then, from the proof Theorem 3.1, we already know that $y = 0$. We only need to show that $x \neq 0$.

Suppose on the contrary that $x = 0$. That is, $(x, y) = (0, 0)$. Substituting this into $y^2 = x^3 + k$ leads to the conclusion that $k = 0$, which contradicts the hypothesis. Hence $x \neq 0$. □

It therefore follows from Corollary 3.1 above that if an integral solution-set $M(k),\ k \in \mathbb{Z} \setminus \{0\}$ is a singleton then $M(2a^3 + k) = M(-k)$, for some $a \in \mathbb{Z} \setminus \{0\}$ and $M(k) = \{(a, 0)\}$.

Corollary 3.3. *Every Mordell equation $y^2 = x^3 + k,\ k \in \mathbb{Z} \setminus \{0\}$, with a non-trivial integral solution or a trivial integral solution of the form $(x, y) = (0, \sqrt{k})$ has more than one integral solution.*

Corollary 3.2 may help us to know from the start which of the equations may have non-unique integral solutions. Clearly $x = \sqrt[3]{-k}$ in Theorem 3.2, with k as a perfect cube of some non-zero integer. These results show that Mordell equation with unique integral solution is capable of an independent study and that its contributions to those equations with non-unique integral solutions (as seen in Corollaries 3.2 and 3.3) is enormous. *It appears that a Mordell equation, $y^2 = x^3 + k,\ k \in \mathbb{Z} \setminus \{0\}$, has a unique integral solution iff $y = 0$ and $x = \sqrt[3]{-k}$.*

We are not aware if these Theorems or Corollaries given above on Mordell equations with unique solution may be established in any other way independent of the perfect-square-generating polynomial function $f_2(\zeta)$ (as seen in the crucial Lemma 3.2) or if there has been any systematic study of the contributions of trivial and unique integral solutions to the understanding of Mordell equations. We shall revisit this aspect of the work in Corollary 3.5.

In order to have a firm handle on the solution-set of Mordell equations with either trivial or non-trivial integral solutions we introduce the following notions that would track down members of the equations $y^2 = x^3 + k,\ k \in \mathbb{Z} \setminus \{0\}$, with integral solution(s), affords us the opportunity of deriving general expression for these solutions and study their properties, which are then used to establish effectiveness of our approach.

Definition 3.1.

(i.) A pair $(k, \gamma) \in \mathbb{Z} \times \mathbb{Z}$ is said to be *admissible for the Mordell equation* $y^2 = x^3 + k$ whenever $r_{\gamma,k}(\zeta) = 0$ has (at least) an integral root. This pair is said to be *purely admissible* for the Mordell equation $y^2 = x^3 + k$ whenever $r_{\gamma,k}(\zeta) = 0$ has *only* integral roots. A Mordell equation, $y^2 = x^3 + k$, is called *admissible* (resp., *purely admissible*) if (k, γ) is *admissible* (resp., *purely admissible*) for some $\gamma \in \mathbb{Z}$.

(ii.) The sets $\mathcal{A}(k) := \{\gamma \in \mathbb{Z} : r_{\gamma,k}(\zeta) = 0 \text{ has an integral root}\}$ and $\mathcal{A}_0(k) := \{\gamma \in \mathbb{Z} : r_{\gamma,k}(\zeta) = 0 \text{ has only integral roots}\}$ are the respective sets of *admissible* and *purely admissible integers* for the Mordell equations, $y^2 = x^3 + k,\ k \in \mathbb{Z}$.

It may then be established that a Mordell equation has an integral solution (*i.e.*, is *integrally solvable*) if, and only if, it is admissible (*i.e.*, if, and only if, $\mathcal{A}(k) \neq \emptyset$). Hence the above notion of admissibility adequately ensures the existence of an integral solution to those integrally solvable members of the family of equations $y^2 = x^3 + k,\ k \in \mathbb{Z} \setminus \{0\}$, so that we do not fall into the trap of proving results for the integral solutions of an equation that is not integrally solvable. It also follows that $k \in \mathbb{Z} \setminus \{0\}$ if, and only if, the cardinality, $\mid \mathcal{A}(k) \mid$, of the set $\mathcal{A}(k)$ of admissible integers satisfies $\mid \mathcal{A}(k) \mid < \infty$.

We already know that $\mathcal{A}(0)$ is an infinite subset of $\mathbb{Z}$ and that it is explicitly given as

$$\mathcal{A}(0) = \{-(\delta^2 \pm \delta^3) : \delta \in \mathbb{Z}\}$$

(*since the polynomial equarion* $r_{-(\delta^2 \pm \delta^3),0}(\zeta) = 0$ *has an integral root for every* $\delta \in \mathbb{Z}$, *where we see that* $\gamma = -(\delta^2 \pm \delta^3)$, *and that this equation has no integral roots for other values of* $\gamma \in \mathbb{Z}$). It is also clear that $\mathcal{A}_0(k) \subset \mathcal{A}(k)$, for all $k \in \mathbb{Z}$. A general formula for computing the members of the finite set $\mathcal{A}(k)$, for each $k \in \mathbb{Z}$, which reduces to the above expression for $\mathcal{A}(0)$ when $k = 0$, is given in Corollary 3.6 while the situation with members of the collection of sets $\mathcal{A}_u(k),\ k \in \mathbb{Z} \setminus \{0\}$, whose Mordell equations have unique integral solutions is treated in Corollary 3.5. Some explicit computations of members of $\mathcal{A}(k)$, for some $k \in \mathbb{Z} \setminus \{0\}$, from Definition 3.1 (*ii.*) show that

$$\mathcal{A}(-8) = \{\cdots, -2, \cdots\},\ \mathcal{A}(1) = \{\cdots, -5, -1, 1, \cdots\},\ \mathcal{A}(2) = \{\cdots, 2, \cdots\},$$

$\mathcal{A}(6) = \emptyset$, $\mathcal{A}(8) = \{\cdots, 2, \cdots, 266, \cdots\}$ and $\mathcal{A}(9) = \{\cdots, -9, -3, 1, 3, 9, \cdots\}$.

The extent to which we should seek such γ in $\mathbb{Z}$, for any arbitrarily chosen $k \in \mathbb{Z} \setminus \{0\}$, will be given later in Theorem 4.2. This Theorem contains the open interval within which members of $\mathcal{A}(k)$ are to be found and therefore gives the effectiveness of every result in this paper.

It may be deduced from Theorem 14.2.3 (*c.*) of [1], *p.* 392, that

$$\mathcal{A}(k) = \emptyset \ \text{ if } \ k \neq \pm 1 - 3k_1, \ \text{ with } \ k_1 \in \mathbb{Z}.$$

However the result of Theorem 14.2.3 (*a.*) $-$ (*b.*) in [1.], containing the best known parametrization of integral solutions of $y^2 = x^3 + k$ does not include all $k \in \mathbb{Z} \setminus \{0\}$. Indeed this well-known parametrization is only valid for *some* non-zero integers k, not for all negative or all positive $k \in \mathbb{Z} \setminus \{0\}$. One of our aims in this paper is to give a complete, effective and self-contained parametrization for integral solutions of all integrally solvable Mordell equations. That is, parametrization of solutions $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ of $y^2 = x^3 + k$ for all $k \in \mathbb{Z}$ with $\mathcal{A}(k) \neq \emptyset$.

We now consider the first of our major results which gives a new, complete and *elementary* parametrization of *all* the integral solutions of any admissible Mordell equation (See [9.]). The main features of this parametrization are that it works for every integrally solvable Mordell equation (*i.e*, for equation $y^2 = x^3 + k$ in which $\mathcal{A}(k) \neq \emptyset$), it contains very few hypotheses and, apart from being the first elementary parametrization of the integral solutions of admissible Mordell equations known to the author, it gives the same method in computing these solutions for both $k = 0$ (where there is an infinite number of integral solutions) and *all* $k \in \mathbb{Z} \setminus \{0\}$ (where there is a finite number of integral solutions).

> *A unified solution technique, for both $k = 0$ (whose integral solutions could easily be parameterized as done in $M(0)$) and all $k \in \mathbb{Z} \setminus \{0\}$ (whose integral solutions have hitherto required much of algebraic number theory without commensurate success), would allow the use of algebraic number theory methods (available for all $k \in \mathbb{Z} \setminus \{0\}$) to the trivial Mordell equation (which has always been isolated and said to be of little interest) and be of help in completely understanding the intrinsic nature of the trivial case of $k = 0$ and*

> *in using this understanding to de-mystify the non-trivial case. We hope to initiate this connection in this paper.*

The result given in the following theorem solves one of the open problems listed in [8] and may be compared with Theorem 14.2.3 of [1] that contains the well-known *congruence cum class-number* parametrization of integral solutions of *some* of the Mordell equations. Indeed Theorem 3.3 below gives the first known complete method of generating *all* the integral solutions, (x, y), of the integrally solvable members of the family of equations $y^2 = x^3 + k,\ k \in \mathbb{Z}$, whose effectiveness is deferred till Theorem 4.2 before an example is considered.

Theorem 3.3. *Let $k \in \mathbb{Z}$ be fixed such that $\mathcal{A}(k) \neq \emptyset$. Then every integral solution, (x, y), of $y^2 = x^3 + k$ is given by $x = x(k, \gamma, t)$ and $y = y(k, \gamma, t)$ where*

$$x(k, \gamma, t) = \frac{1}{t}(900 + k + 10t - (300 + t)\gamma + 30\gamma^2 - \gamma^3)$$

and

$$y(k, \gamma, t) = \pm\frac{1}{t}(900 + k + 10t - 300\gamma + 30\gamma^2 - \gamma^3),$$

for those $t \in \mathbb{Z} \setminus \{0\}$ in which $\frac{1}{t}(900 + k - 300\gamma + 30\gamma^2 - \gamma^3)$ is an integral zero of $r_{\gamma,k}(\zeta)$ and all $\gamma \in \mathcal{A}(k)$. *Proof.* It is generally known that if $w = \frac{p}{q}$, with $p, q \in \mathbb{Z},\ q \neq 0$, is a rational integral zero of $a_n w^n + \cdots + a_0 \in \mathbb{Z}[w],\ n \in \mathbb{N}$, then $p|a_0$ and $q|a_n$. Hence every rational integral zero of a *monic* member of $\mathbb{Z}[w]$ is integral. It then follows that the integral factors of the integer $900 + k - 300\gamma + 30\gamma^2 - \gamma^3$ are the only candidates for the integral roots of $r_{\gamma,k}(\zeta)$.

Therefore if ζ' is an integral zero of $r_{\gamma,k}(\zeta)$ (which exists since k is chosen such that $\mathcal{A}(k) \neq \emptyset$), then $\zeta'|(900 + k - 300\gamma + 30\gamma^2 - \gamma^3)$. That is, $\zeta' t = 900 + k - 300\gamma + 30\gamma^2 - \gamma^3$, for some $t \in \mathbb{Z} \setminus \{0\}$. Substituting the expression for ζ' into both $x^3 = f_3(\zeta' - \gamma)$ and $y^2 = f_2(\zeta')$ gives the result. □

A first-glance feature of the above Theorem is that the values of $k \in \mathbb{Z}\setminus\{0\}$ enters *linearly* into the integral solutions

$$x = x(k, \gamma, t) \text{ and } y = y(k, \gamma, t)$$

of admissible Mordell equations, $y^2 = x^3 + k$. However this should not be surprising as there are (two (2)) other parameters, $\gamma = \gamma_k$ and $t = t_{\gamma=\gamma_k}$, depending on the value of the fixed integer k and which contribute to the integral solutions,

$$x = x(k, \gamma, t) = x(k, \gamma_k, t_{\gamma_k}) \text{ and } y = y(k, \gamma, t) = y(k, \gamma_k, t_{\gamma_k}).$$

The highest order of the contribution of k to these solutions, which from Theorem 3.3 seems linear, may be more explicit than in this Theorem if these parameters are explicitly written in terms of k and are eliminated from $x = x(k, \gamma_k, t_{\gamma_k})$ and $y = y(k, \gamma_k, t_{\gamma_k})$. If and whenever the parameters

$$\gamma = \gamma_k =: \gamma(k) \text{ and } t = t_{\gamma_k} =: t(k)$$

are explicitly computed in terms of k (via *Cardano's formula*) then the integral solutions

$$x = x(k, \gamma, t) = x(k, \gamma(k), t(k)) \text{ and } y = y(k, \gamma, t) = y(k, \gamma(k), t(k))$$

would eventually become $x = x(k)$ and $y = y(k)$, respectively, giving the full order of contribution of k into the integral solutions and a direct proof of Hall conjecture.

Remarks 3.1. It may be worthwhile to show that the above expression for (x, y) reduces to $(\delta^2, \pm\delta^3)$, $\delta \in \mathbb{Z}$, for those t satisfying Theorem 3.3 when $k = 0$. It is clear that a finite number of such t in Theorem 3.3 is sufficient in the case when $k \in \mathbb{Z} \setminus \{0\}$.

For example, when $k = 1$, the consideration of $\gamma = 1$ gives $900 + k - 300\gamma + 30\gamma^2 - \gamma^3 = 630$ from where we see that the factors $t_1 = -90$, $t_2 = -70$ and

$t_3 = -63$, of 630, lead respectively to $\zeta_1 = -7,\ \zeta_2 = -9$ and $\zeta_3 = -10$, which are the only integral zeros of $r_{1,1}(\zeta)$. Since any other $\gamma \in \mathcal{A}(1) = \{\cdots, -5, \cdots, -1, 1, \cdots\}$ and $t \in \mathbb{Z} \setminus \{0\}$ for which $\frac{1}{t}(901 - 300\gamma + 30\gamma^2 - \gamma^3)$ is an integral zero of $r_{\gamma,1}(\zeta)$ re-produces either $\zeta_1 = -7,\ \zeta_2 = -9$ or $\zeta_3 = -10$ as the only integral zeros, we arrive in this way at *all* the integral solutions, $x = x(1, \gamma, t)$ and $y = y(1, \gamma, t)$, of $y^2 = x^3 + 1$ from $\zeta_1,\ \zeta_2$ and ζ_3. It will soon be clear from Theorem 4.2 that $\mathcal{A}(1) = \{-5, -1, 1\}$.

Theorem 3.3 may indeed be given in a more explicit and compact form resulting from the fusion of the two (2) conditions on t into a single condition, as follows (*cf.* [3], *p.* 202).

Corollary 3.4. *Every integral solution, (x, y), of $y^2 = x^3 + k$ with $k \in \mathbb{Z}$ and $\mathcal{A}(k) \neq \emptyset$ is given by $x = x(k, \gamma, t)$ and $y = y(k, \gamma, t)$ where*

$$x(k, \gamma, t) = \frac{1}{t}(900 + k + 10t - (300 + t)\gamma + 30\gamma^2 - \gamma^3)$$

and

$$y(k, \gamma, t) = \pm\frac{1}{t}(900 + k + 10t - 300\gamma + 30\gamma^2 - \gamma^3),$$

for every $t \in \mathbb{Z}\backslash\{0\}$ which satisfies the third-order polynomial equation $\mathfrak{D}_{\gamma,k}(t) =$

$$(900+k-300\gamma+30\gamma^2-\gamma^3)t^3+(280-60\gamma+3\gamma^2)(900+k-300\gamma+30\gamma^2-\gamma^3)t^2+$$

$$(29 - 3\gamma)(900 + k - 300\gamma + 30\gamma^2 - \gamma^3)^2 t + (900 + k - 300\gamma + 30\gamma^2 - \gamma^3)^3 = 0,$$

for all $\gamma \in \mathcal{A}(k)$. *Proof.* We substitute $\zeta = \zeta' = \frac{(900+k-300\gamma+30\gamma^2-\gamma^3)}{t}$ into $r_{\gamma,k}(\zeta) = 0$ and clear the fractions to have the polynomial equation $\mathfrak{D}_{\gamma,k}(t) = 0$. □

It follows that non-zero integral roots of the third-order polynomial in Corollary 3.4 generate all integral solutions of any admissible Mordell equation and their explicit realization in terms of this polynomial gives the most efficient algorithm for systematic generation of all these solutions. We have thus succeeded in reducing the not-easily tractable problem of seeking integral solutions, (x, y), of $y^2 = x^3 + k$ with $k \in \mathbb{Z}$ and $\mathcal{A}(k) \neq \emptyset$ into the simpler one of seeking only the integral values of t satisfying the third-order polynomial in the Corollary (*cf.* [6]).

The simplicity of this deduction may be compared with the methods of congruence and class-number given in Theorem 14.2.3 of [1]. Furthermore, the realization of the full contribution of k into the solutions given in Theorem 3.3 depends on explicit realization of the non-zero integral roots of $\mathfrak{D}_{\gamma,k}(t) = 0$ via *Cardano's formula.*

It may then be deduced from Theorem 3.3 that the integral solution-set, $M(k)$, for every $y^2 = x^3 + k$ is given as

$$M(k) = \{(x, y) = (x(k, \gamma, t), y(k, \gamma, t)) : (\gamma, t) \in \mathcal{A}(k) \times (\mathbb{Z} \backslash \{0\}) \text{ with } \mathfrak{D}_{\gamma,k}(t) = 0\},$$

for all $k \in \mathbb{Z}$. For each $k \in \mathbb{Z} \setminus \{0\}$, $M(k)$ is finite since $\mathcal{A}(k)$ is finite (indeed $M(k) = \emptyset$ if, and only if, $\mathcal{A}(k) = \emptyset$) while the infinite cardinality of $\mathcal{A}(0)$ implies that $M(0)$ is infinite.

> *It follows therefore that the only exercise in getting the integral solutions of an admissible Mordell equation is in computing the set, $\mathcal{A}(k)$, of admissible integers from Definition* 3.1 (*ii.*). *How far we should look in $\mathbb{Z}$ when seeking admissible integers for each $k \in \mathbb{Z} \backslash \{0\}$ is completely addressed in Theorem* 4.2, *whose proof depends on our establishment of the celebrated Hall conjecture.*

We may now revisit our study of Mordell equations with unique solutions in the light of Corollary 3.4 and the above remark on $\mathcal{A}(k)$, by giving the explicit form of their corresponding sets of admissible integers. At this point the machinery of Mordell polynomial equation, $m_{\zeta,k}(a) = 0$, developed above has now been employed, having been used in Theorem 3.3.

Corollary 3.5. *Let the Mordell equation $y^2 = x^3 + k,\ k \in \mathbb{Z} \setminus \{0\}$, have a unique integral solution and let $\mathcal{A}_u(k)$ denote its corresponding set of admissible* *integers. Then* $\mathcal{A}_u(k) = \{\sqrt[3]{k}\}$. *Proof.* We already know, from Theorem 3.2, that if (x, y) is the unique solution of Mordell equation $y^2 = x^3+k,\ k \in \mathbb{Z}\backslash\{0\}$, then $x = \sqrt[3]{-k}$ and $y = 0$. Choosing $(\gamma, t) \in \mathcal{A}(k) \times (\mathbb{Z} \setminus \{0\})$ as in Corollary 3.4 we then have

$$0 = y = \pm\frac{1}{t}(900 + k + 10t - 300\gamma + 30\gamma^2 - \gamma^3),$$

which when employed to simplify

$$\sqrt[3]{-k} = x = \frac{1}{t}(900 + k + 10t - (300 + t)\gamma + 30\gamma^2 - \gamma^3),$$

gives $\gamma = \sqrt[3]{k}$. □

It is therefore necessary (though not sufficient) that $k \in \mathbb{Z}\backslash\{0\}$ be a perfect cube of some non-zero integers in order for $y^2 = x^3+k$ to have a unique integral solution. *It appears that necessary and sufficient conditions for* $y^2 = x^3 + k$ *to have a unique integral solution are that* $k \in \mathbb{Z} \setminus \{0\}$ *be a perfect cube of some non-zero integers and that* $\mathcal{A}(k)$ *be the singleton* $\{\sqrt[3]{k}\}$. A first generalization of the above Corollary to accommodate other Mordell equations is the following.

Corollary 3.6. *Let* $k \in \mathbb{Z}$ *be fixed such that* $\mathcal{A}(k) \neq \emptyset$. *Then*

$$\mathcal{A}(k) = \{\gamma = \pm y - x : y^2 = x^3 + k\}.$$

Proof. From Corollary 3.4, we have that

$$\pm y(k, \gamma, t) = \frac{1}{t}(900 + k + 10t - 300\gamma + 30\gamma^2 - \gamma^3).$$

Hence

$$\pm y(k, \gamma, t) - x(k, \gamma, t)$$

$$= \frac{1}{t}(900+k+10t-300\gamma+30\gamma^2-\gamma^3)-\frac{1}{t}(900+k+10t-(300+t)\gamma+30\gamma^2-\gamma^3)$$

$$= \gamma.$$ □

It is clear from Corollary 3.6 that $\mid\mid y \mid - \mid x \mid\mid = \mid\mid \pm y \mid - \mid x \mid\mid \leq \mid \pm y - x \mid \leq \mid \gamma \mid$ and $\mid \gamma \mid = \mid \pm y - x \mid \leq \mid y \mid + \mid x \mid$. Hence the control of values of $\mid \gamma \mid$ is given by

$$\mid\mid y \mid - \mid x \mid\mid \leq \mid \gamma \mid \leq \mid y \mid + \mid x \mid .$$

The above form of $\mathcal{A}(k)$ shall be employed in Theorem 4.2 to prove the effectiveness of our approach for all $k \in \mathbb{Z} \backslash \{0\}$, leading to the explicit computation of the cardinality of $M(k)$. In the mean time lower bounds for both $\mid x \mid$ and $\mid y \mid$ may be given here.

Corollary 3.7. *Let $k \in \mathbb{Z}$ be fixed such that $\mathcal{A}(k) \neq \emptyset$ and let $(\gamma, t) \in \mathcal{A}(k) \times (\mathbb{Z} \setminus \{0\})$ correspond to k as in Corollary* 3.4. *Then the following inequalities hold;*

$$\{\frac{1- \mid t \mid}{2 \mid t \mid}\} \mid x(k,\gamma,t) \mid \leq \mid y(k,\gamma,t) \mid, \qquad \{\frac{2 \mid t \mid}{1+ \mid t \mid}\} \mid \gamma \mid \leq \mid x(k,\gamma,t) \mid$$

and

$$\{\frac{1- \mid t \mid}{1+ \mid t \mid}\} \mid \gamma \mid \leq \mid y(k,\gamma,t) \mid .$$

Proof. It may be shown from Corollary 3.4 that $\mid x \mid \leq \mid ty \mid + \mid t\gamma \mid$. Hence $\mid x \mid \leq \mid ty \mid + \mid t\gamma \mid \leq \mid ty \mid + \mid t \mid (\mid y \mid + \mid x \mid) \leq 2 \mid ty \mid + \mid tx \mid$ which proves the first inequality. Also $\mid \gamma \mid \leq \mid y \mid + \mid ty \mid + \mid t\gamma \mid$, so that $(1- \mid t \mid) \mid \gamma \mid (1+ \mid t \mid) \mid y \mid$ which is the third inequality. The second inequality is a consequence of the other two. □

Solutions $(x,y) = (x(0,\gamma,t), y(0,\gamma,t)) = (\delta^2, \pm\delta^3)$, $\delta \in \mathbb{Z}$, of the trivial Mordell equation implies that there are infinitely many integral roots, $t = t_0$, of $\mathfrak{D}_{\gamma_0,0}(t_0) = 0$, with $\gamma = \gamma_0 \in \mathbb{Z}$, for which $y(0,\gamma_0,t_0) = \frac{1}{t_0}(900 + 10t_0 - 300\gamma_0 + 30\gamma_0^2 - \gamma_0^3)$ is the cube, $\pm\delta^3$, and $x(0,\gamma_0,t_0) = \frac{1}{t_0}(900 + 10t_0 - (300 + t_0)\gamma_0 + 30\gamma_0^2 - \gamma_0^3)$ is the square, δ^2, of the same integer δ. In this case (where $x = \delta^2$, $\pm y = \pm\delta^3$ for $\delta \in \mathbb{Z}$) we arrive, from $\mathcal{A}(k) = \{\gamma = \pm y - x : y^2 = x^3 + k\}$ of Corollary 3.6, at the earlier given expression $\mathcal{A}(0) = \{\gamma_0 = -(\delta^2 \pm \delta^3) : \delta \in \mathbb{Z}\}$ and at an expression for the integral values, $t = t_0$, of Corollary 3.4 as

$$t_0 = \frac{1}{\mp\delta^3 - 10}(\pm\delta^9 + 3\delta^8 \pm 3\delta^7 + 31\delta^6 \pm 60\delta^5 + 30\delta^4 \pm 300\delta^3 + 300\delta^2 + 900)$$

$$= -\delta^6 \mp 3\delta^5 - 3\delta^4 \mp 21\delta^3 - 30\delta^2 - 90,$$

for every $\delta \in \mathbb{Z}$.

It may now be directly established from the above expression for $t = t_0$ that $t_0 \in \mathbb{Z} \setminus \{0\}$ and that it satisfies the third-order polynomial of Corollary 3.4. It then follows that every parameter involved in the analysis of the trivial case $k = 0$ may be expressed in terms of a *fixed* integer δ. A corresponding realization of $t = t_u$ may be derived from the above expression of $\mathcal{A}_u(k),\ k \in \mathbb{Z} \setminus \{0\}$, thus taking care of Mordell equations with unique solutions. A more explicit form of all $\mathcal{A}(k)$, for $k \in \mathbb{Z} \setminus \{0\}$, than is given above may also be sought in the way of $k = 0$ by seeking to rewrite each of x and y of Corollary 3.4 in terms of a common parameter (if such exists).

The existence (or otherwise) of integral solutions of $y^2 = x^3 + k,\ k \in \mathbb{Z}\setminus\{0\}$, is therefore essentially determined by the existence (or otherwise) of integral roots of the third-order polynomial in the indeterminates $X \in \mathbb{Z}$ given as $\mathfrak{D}_{\gamma,k}(X) :=$

$$(900+k-300\gamma+30\gamma^2-\gamma^3)X^3+(280-60\gamma+3\gamma^2)(900+k-300\gamma+30\gamma^2-\gamma^3)X^2$$

$$+(29-3\gamma)(900+k-300\gamma+30\gamma^2-\gamma^3)^2X+(900+k-300\gamma+30\gamma^2-\gamma^3)^3,$$

for all $\gamma \in \mathbb{Z}$ (*cf.* [4.], *p.* 132). And when these integral roots do exist, the value of $\gamma \in \mathbb{Z}$ used in $\mathfrak{D}_{\gamma,k}(X) = 0$ leads to a knowledge of the possible integral solutions, (x, y), since $\gamma = \gamma_k := \pm y - x$. It may not be too ambitious to say that the complete understanding of admissible Mordell equations and the nature of their integral solutions are consequences of some properties of $\mathfrak{D}_{\gamma,k}(X) = 0$. In this same way, properties of the non-integral solutions of any Mordell equation may be studied from the viewpoint of the *non-integral* roots of $\mathfrak{D}_{\gamma,k}(X) = 0$.

Another major result of this paper is the following refinement of Siegel's Theorem for non-trivial admissible Mordell equations.

Theorem 3.4. *Let $k \in \mathbb{Z} \setminus \{0\}$ be fixed such that $\mathcal{A}(k) \neq \emptyset$. Then an upper-bound to the number of integral solutions of $y^2 = x^3 + k$ is $2m$, for a* *well-defined fixed constant $m \in \mathbb{N}$.* *Proof.* Let (x, y) be an integral solution of $y^2 = x^3 + k$, then

$$x^3 = f_3(\zeta + a) \text{ and } y^2 = f_2(\zeta),$$

for some $\zeta \in \mathbb{Z}$ and some constants $a = -\gamma \in \mathbb{Z}$. By Siegel's Theorem, there exists a fixed constant $m \in \mathbb{N}$ and a maximal set of distinct roots $\zeta_1, \cdots, \zeta_m \in \mathbb{Z}$ of $r_{\gamma,k}(\zeta) = 0$. Since there is a maximum of two (2) integral solutions, (x, y), for every such ζ_i, $i = 1, \cdots, m$, the result follows. □

That is,

$$1 \leq\mid M(k) \mid\leq 2m,$$

for every $k \in \mathbb{Z}\backslash\{0\}$ with $\mathcal{A}(k) \neq \emptyset$ in which $r_{\gamma,k}(\zeta) = 0$ has exactly m integral roots, ζ. Indeed while Siegel's Theorem assures the finiteness of the number of integral solutions Theorem 3.4 above assures us further that this number may be completely derived from an equivalent expression for $m = m(k)$. We shall derive such an expression after we have enclosed the set, $\mathcal{A}(k)$, in a symmetric open interval in $\mathbb{Z}$. This form of the upper-bound to the number of integral solutions of admissible Mordell equations as established above makes it possible to get these solutions quickly. This suggests a general algorithm for generating these solutions, whose effectiveness will be proved later in Theorem 4.2, where the symmetric open interval containing $\mathcal{A}(k)$ is explicitly given.

Corollary 3.8. *The polynomial equation, $r_{\gamma,k}(\zeta) = 0$, gives a general algorithm for generating all integral solutions of an admissible Mordell equation.*
Proof. Let $k \in \mathbb{Z} \setminus \{0\}$ be fixed such that $\mathcal{A}(k) \neq \emptyset$. Then $r_{\gamma,k}(\zeta) = 0$ has integral roots for every $\gamma \in \mathcal{A}(k)$, which may be sought in the manner given in Theorem 3.3 (or Corollary 3.4). The linear dependence of $n = n(k)$ on the upper-bound, $m = m(k)$, to the number of these roots and Corollary 3.6 mean that the boundary containing the integral solution-set of the admissible Mordell equation is fast attained after a finite number of $\gamma \in \mathcal{A}(k)$ has been used. □

The steps of the algorithm, which will be employed in Example 3.1, are as follows:

> *To solve* $y^2 = x^3 + k$ *for a fixed value of* $k \in \mathbb{Z} \setminus \{0\}$ *with* $\mathcal{A}(k) \neq \emptyset$, *we substitute the given value of* k *into* $\mathfrak{D}_{\gamma,k}(t) = 0$ *which is then solved to get integral roots,* t, *for each of the members,* γ, *of the finite set* $\mathcal{A}(k)$ *(as originally given in Definition* 3.1 $(ii.)$*). We then use Corollary* 3.4 *to generate the integral solutions,* (x, y), *of* $y^2 = x^3 + k$ *corresponding to every such triple* (k, γ, t).

For example, to solve $y^2 = x^3 + 1$ we substitute $k = 1$ into $\mathfrak{D}_{\gamma,k}(t) = 0$ which is then solved to get the integral roots, $t = -90, -70, -63$, for each of the members, γ, of the finite set $\mathcal{A}(1)$. We then use Corollary 3.4 to get the integral solutions $(x, y) = (2, \pm 3)$ corresponding to the triple $(k, \gamma, t) = (1, 1, -90)$, $(x, y) = (0, \pm 1)$ corresponding to the triple $(k, \gamma, t) = (1, 1, -70)$ and $(x, y) = (-1, 0)$ corresponding to the triple $(k, \gamma, t) = (1, 1, -63)$. The other two values of $\gamma \in \mathcal{A}(1)$ for which $\mathfrak{D}_{\gamma,1}(t) = 0$ has integral roots may also be used to arrive at the same solutions for t as above.

Remarks 3.2.

> $(i.)$ Theorem 3.4 may be seen as a refinement of Siegel's finiteness theorem for non-trivial admissible Mordell equations. The number of distinct integral solutions in this Theorem will be less than $2m$ whenever some of the computed values of y $(:= \pm(\zeta_i + 10),\ i = 1, \cdots, m)$ are zero (if any $\zeta_i = -10$), leading the two (2) integral solutions $(x, y) = (\sqrt[3]{f_3(\zeta_i - \gamma)}, \pm(\zeta_i + 10))$ becoming the single solution $(\sqrt[3]{f_3(\zeta_i - \gamma)}, 0)$, or whenever two triples of (k, γ, t) lead to the same integral solution. The combination of Theorems 3.1 and 3.4 imply that the number n of distinct integral solutions to $y^2 = x^3 + k$, in which $k \in \mathbb{Z} \setminus \{0\}$ and $\mathcal{A}(k) \neq \emptyset$, lies between 1 and $2m$, for a fixed $m \in \mathbb{N}$ (which is defined as the number of integral

roots, ζ, of $r_{\gamma,k}(\zeta)=0$ for all $(k,\gamma)\in\mathbb{Z}\setminus\{0\}\times\mathcal{A}(k))$. This result may be compared with those in [9].

($ii.$) It is known (from Remark 3.1 above) that $m=3$ for $y^2=x^3+1$ and that the upper-bound (of a maximum of six (6) integral solutions) is not attained, due to the situation mentioned in ($i.$). A truly interesting problem is to isolate those constants $k\in\mathbb{Z}\setminus\{0\}$ for which $y^2=x^3+k$ has the maximum possible integral solutions and to list *all* Mordell equations with the maximum possible integral solutions. The class, $\mathfrak{M}(p)$, of admissible Mordell equations having $p-$distinct integral solutions, with $1\leq p\leq 2m,\ m\in\mathbb{N}$, may equally be of interesting study. It has been shown above that $\mathfrak{M}(1)$ contains all the Mordell equations each with a unique integral solution, though it is not yet known if this containment is an equality.

4 Effectiveness and efficiency in the computation of the set $\mathcal{A}(k)$

Corollary 3.6 reports that $\mid\gamma\mid$ is controlled by $\mid y\mid+\mid x\mid$. In order to find a bound for members of $\mathcal{A}(k)$, with $k\in\mathbb{Z}\setminus\{0\}$, we shall therefore seek bounds for $\mid x\mid$ and $\mid y\mid$. One could use the already established *Stark Conjecture* ([5.]) : *for any* $\epsilon>0$ *there is a constant* $C_\epsilon>0$ *such that* $\max\{x,y\}\leq C_\epsilon^{|k|^{1+\epsilon}}$. The bound, $C_\epsilon^{|k|^{1+\epsilon}}$, is however *too exponential* for it to be quickly attained. The more efficient estimates that come to mind are

$$\mid x\mid\leq C(k)\mid k\mid^2\quad\text{and}\quad\mid y\mid\leq C(k)\mid k\mid^3,$$

examples of which include

$(\pm378661)^2=5234^3+17$ where $C(17)$ is estimated as $C(17)\geq\dfrac{378661}{17^3}=77.0$;

$(\pm736844)^2=8158^3+24$ where $C(24)$ is estimated as $C(24)\geq\dfrac{736844}{24^3}=53.3$

and

$(\pm 149651610621)^2 = 28187351^3 + 1090$ where $C(1090)$ is estimated as $C(1090) \geq 115.5.$

These examples reflect the *wild* dependence of $C(k)$ on k. In order to be spared of this unreliability of $C(k)$ we seek to cut off its dependence on k and to arrive at the smallest possible value of $C(k)$ that would work for every $k \in \mathbb{Z} \setminus \{0\}$, once and for all.

> *One option is to increase the powers of* $\mid k \mid$ *from the present* 2 *and* 3. *This is the same as transferring the dependence on k from* $C(k)$ *to the powers of* $\mid k \mid$.

The appropriate question would then be: *at what powers of* $\mid k \mid$ *would there be the smallest value of* $C(k)$ *for all* $k \in \mathbb{Z} \setminus \{0\}$? This question is equivalent to asking for a proof of the *Hall conjecture* where the positive and $k-$independent constant c, for some $\epsilon \geq 0$, in both of the inequalities

$$\mid x \mid \leq c \mid k \mid^{2+\epsilon} \quad \textit{and} \quad \mid y \mid \leq c \mid k \mid^{3+\epsilon}$$

is sought-after for all $k \in \mathbb{Z} \setminus \{0\}$. The expected $k-$independence of c does not however stop ϵ from being given in terms of k. Hence we shall seek a specific $\epsilon \geq 0$ in terms of k that would give these two inequalities for all $(x, y) \in L(M)$. Observe that this conjecture is valid with $\epsilon = 0$ for *many* small values of k and for the class of Mordell equations each with a unique integral solution, as may be seen in the following.

Trivium 4.1 *Let the Mordell equation* $y^2 = x^3 + k,\ k \in \mathbb{Z} \setminus \{0\}$, *have a unique integral solution or let* $(x, 0)$ *be a solution of a particular Mordell equation. Then*

$$\mid x \mid < 5 \mid k \mid^2 \quad \textit{and} \quad \mid y \mid < 5 \mid k \mid^3 .$$

Proof. We already know from Theorem 3.2 that if the Mordell equation $y^2 = x^3 + k,\ k \in \mathbb{Z} \setminus \{0\}$, has a unique integral solution then $y = 0$ and $x = \sqrt[3]{-k} = -\sqrt[3]{k}$, for some non-zero perfect cube integer k. It is clearly that

$| x |=| \sqrt[3]{k} |< 5 | k |^2$ and $| y |= 0 < 5 | k |^3$. □

Trivium 4.2 *Integral solutions,* (x, y), *of the Mordell equations* $y^2 = x^3 \pm 1$ *satisfy the inequalities*

$$| x |< 5 \ \ \textit{and} \ \ | y |< 5.$$

Proof. It is already known to Euler (1738) that, apart from the trivial integral solutions $(-1, 0), (0, \pm 1)$, the only non-trivial integral solutions of the equation $y^2 = x^3 + 1$ are $(2, \pm 3)$, while the only integral solution of $y^2 = x^3 - 1$ is $(1, 0)$. Hence $| x |< 5$ and $| y |< 5$ in both equations. □

We now give the proof of the full Hall conjecture with the choice of a value for $\epsilon > 0$. However, in view of Trivia 4.1 and 4.2 above we shall consider only the admissible Mordell equations, $y^2 = x^3 + k$, with $y \neq 0$ (so that $x^3 + k \neq 0$) and the Hall conjecture for only $k \in \mathbb{Z} \setminus \{-1, 0, 1\}$. We shall also only consider Mordell equations with $y > 0$, due to the conclusion of Lemma 3.2, and $x > 0$, due to Corollary 3.1 ($i.$)

Theorem 4.1 (Hall conjecture). *Let* $k \in \mathbb{Z} \setminus \{0\}$ *be given such that* $\mathcal{A}(k) \neq \emptyset$. *Then there exists a fixed positive constant,* $c \leq 5$, *(here called the Hall constant) such that*

$$| x |< c | k |^{2+|k|} \ \ \textit{and} \ \ | y |< c | k |^{3+|k|} .$$

Proof. Let $k \in \mathbb{Z} \setminus \{-1, 0, 1\}$ be fixed such that $\mathcal{A}(k) \neq \emptyset$. If $y \neq 0$ then the non-empty integral solution-set, $M(k)$, is not a singleton and being a finite set of, say cardinality $r \geq 2$, we have that both

$$\max_{1 \leq i \leq r}\{| x_i |\} \quad \text{and} \quad \max_{1 \leq i \leq r}\{| y_i |\}$$

exist in $\mathbb{Z}$, where $(x_i, y_i) \in M(k), \ 1 \leq i \leq r$. It is true, from all the examples of integral solutions of Mordell equations which may be considered and the fact that k uniquely determines members of $M(k)$ (as seen in Lemma 3.1), that $\max_{1 \leq i \leq r}\{| x_i |\}$ and $\max_{1 \leq i \leq r}\{| y_i |\}$ are functions of k, say $q_1(k)$ and $q_2(k)$, respectively. We may then conclude that $x \leq q_1(k)$ and $y \leq q_2(k)$, for every $(x, y) \in M(k)$.

Now let $x > 0$ and $y > 0$ and assume *hypothetically* that

$$q_1(k) = 5 \mid k \mid^{2+|k|} \text{ and } q_2(k) = 5 \mid k \mid^{3+|k|},$$

then it must follow that $x =\mid x \mid \leq 5 \mid k \mid^{2+|k|}$ and $y =\mid y \mid \leq 5 \mid k \mid^{3+|k|}$, for every $(x, y) \in M(k),\ k \in \mathbb{Z} \setminus \{-1, 0, 1\}$. The above assumptions on q_1 and q_2 are seen as the *first approximations* to $\max_{1\leq i\leq r}\{\mid x_i \mid\}$ and $\max_{1\leq i\leq r}\{\mid y_i \mid\}$, which would be further *refined* based on its *accommodation* by the Mordell equation, $y^2 = x^3 + k$. We claim that $x \neq 5 \mid k \mid^{2+|k|}$ and $y \neq 5 \mid k \mid^{3+|k|}$.

Suppose, on the contrary, that $x = 5 \mid k \mid^{2+|k|}$ and $y = 5 \mid k \mid^{3+|k|}$. Then, for $k > 1$, we have

$$\begin{aligned} x^3 + k &= 5^3 \mid k \mid^{6+3|k|} + k \\ &> 5^3 \mid k \mid^{6+2|k|} \quad \text{(since } k > 1) \\ &= 5y^2 > y^2 \ \text{ (since } y^2 \neq 0), \end{aligned}$$

while for $k < -1$,

$$\begin{aligned} x^3 + k &= 5^3 \mid k \mid^{6+3|k|} - k \quad \text{(transforming back to } k > 1) \\ &> \mid k \mid^{|k|} (5^3 \mid k \mid^{6+2|k|} - 1) \quad \text{(from k} < \mid k \mid^{|k|}\text{, since } \mid k \mid > 1) \\ &> \mid k \mid^{|k|} (5^2 \mid k \mid^{6+2|k|}) \quad \text{(since } 5^3 \mid k \mid^{6+2|k|} - 1 > 5^2 \mid k \mid^{6+2|k|}) \\ &= \mid k \mid^{|k|} y^2 > y^2 \ \text{ (since } y^2 \neq 0), \end{aligned}$$

That is, $x^3 + k > y^2$, for $x = 5 \mid k \mid^{2+|k|}$ and $y = 5 \mid k \mid^{3+|k|}$, $k \in \mathbb{Z} \setminus \{-1, 0, 1\}$. Hence

$$x \neq 5 \mid k \mid^{2+|k|} \text{ and } y \neq 5 \mid k \mid^{3+|k|} .$$

In order to then attain equality between $x^3 + k$ and y^2 we have the options of either taking values of x less than $5 \mid k \mid^{2+|k|}$ and/or taking values of y

greater than $5 \mid k \mid^{3+|k|}$. However taking values of y (resp., x) greater than $5 \mid k \mid^{3+|k|}$ (resp., $5 \mid k \mid^{2+|k|}$) contradicts the definition of $q_2(k)$ (resp., $q_1(k)$) as the upper bound of all $y > 0$ (resp., $x > 0$) in the integral solutions of $y^2 = x^3 + k, \ k \in \mathbb{Z} \setminus \{-1, 0, 1\}$. *Indeed if for some* $\delta \in \mathbb{Z} \setminus \{0\}$ *and* $\eta \in \mathbb{Z}^{>0}$ *we have* $(5 \mid k \mid^{3+|k|} + \delta)^2 = (5 \mid k \mid^{2+|k|} - \eta)^3 + k,$ *then*

$$(5 \mid k \mid^{3+|k|} + \delta)^2 = (5 \mid k \mid^{2+|k|} - \eta)^3 + k < (5 \mid k \mid^{2+|k|})^3 + k < ([(5 \mid k \mid^{3+|k|})]^2)^2$$

leading to the conclusion that $\delta < 0$. Thus

$$x < 5 \mid k \mid^{2+|k|} \quad \text{and} \quad y < 5 \mid k \mid^{3+|k|},$$

which when combined with $-x < x$ and $-y < y$ (since $x > 0$ and $y > 0$) lead to the conclusions

$$\mid x \mid < 5 \mid k \mid^{2+|k|} \quad \text{and} \quad \mid y \mid < 5 \mid k \mid^{3+|k|} .$$

The last two inequalities show that our initial hypothetical assumptions should in fact be the general truth that

$$q_1(k) < 5 \mid k \mid^{2+|k|} \quad \text{and} \quad q_2(k) < 5 \mid k \mid^{3+|k|} .$$

Hence,

$$\mid x \mid < 5 \mid k \mid^{2+|k|} \quad \text{and} \quad \mid y \mid < 5 \mid k \mid^{3+|k|},$$

for every $k \in \mathbb{Z} \setminus \{-1, 0, 1\}$ and $(x, y) \in M(k)$.

These, when combined with Trivia 4.1 and 4.2 above, give the result for all $k \in \mathbb{Z} \setminus \{0\}$. □

The conclusion of Theorem 4.1 would also hold if, having shown that $x_1 > 0$ and $y_1 > 0$, we establish that

$$x_{\pi(k')} = x_{\pi(k)+1} > x_{\pi(k)} \quad \text{and} \quad y_{\pi(k')} = y_{\pi(k)+1} > y_{\pi(k)}, \ k \in \mathbb{Z} \setminus \{0\},$$

using the relation $k^{'} = \begin{cases} \frac{1}{2}(l+2) = -k+1, & l \text{ is even,} \\ \\ -\frac{1}{2}(l+1) = -k, & l \text{ is odd,} \end{cases}$ between k and $k^{'}$, where $\{x_{\pi(k)}\}_{\pi(k)=1}^{\infty}$ and $\{y_{\pi(k)}\}_{\pi(k)=1}^{\infty}$ are sequences of real numbers given as

$$x_{\pi(k)} := 5 - \max_{(\gamma,t)\in\mathcal{A}(k)\times\mathbb{Z}\setminus\{0\}}\{\frac{1}{\mid tk^{2+|k|}\mid} \mid 900+k+10t-(300+t)\gamma+30\gamma^2-\gamma^3 \mid\}$$

and

$$y_{\pi(k)} := 5 - \max_{(\gamma,t)\in\mathcal{A}(k)\times\mathbb{Z}\setminus\{0\}}\{\frac{1}{\mid tk^{3+|k|}\mid} \mid 900+k+10t-300\gamma+30\gamma^2-\gamma^3 \mid\},$$

for every $k \in \mathbb{Z}\setminus\{0\}$ where $\pi : \mathbb{Z}\setminus\{0\} \to \mathbb{N}$ is a one-to-one correspondence given as $\pi(k) = \begin{cases} 2k-1, & k>0, \\ \\ -2k, & k<0. \end{cases}$. Also since ϵ may take any non-negative real constant the *minimum value* of ϵ in Theorem 4.1 may also be sought by scaling down $\epsilon = \mid k \mid$. It may be further shown that the Hall constant, c, in Theorem 4.1 may be chosen such that $3 \leq c \leq 5$.

The results of the remaining part of this paper are consequences of Hall conjecture (Theorem 4.1 above). However corresponding results may also be deduced from the already established *Stark's conjecture* (starting with the fact of the inequalities $\mid \gamma \mid \leq \mid y \mid + \mid x \mid \leq 2\max(\mid x \mid, \mid y \mid) \leq 2C_{\epsilon}^{|k|^{1+\epsilon}}$). The beauty of any of the two set of results is in giving all the admissible integers for any $k \in \mathbb{Z}\setminus\{0\}$ before bringing in the convenience of getting all the integral solutions of $y^2 = x^3 + k$ from Corollary 3.4. *In other words the following results show that the proper use of any of these conjectures are in seeking all admissible integers, γ, before all the integral solutions of the Mordell equation are then deduced from Corollary* 3.4. This will be highlighted in Example 3.1.

The presentation has been so far general for arbitrary values of $k \in \mathbb{Z}\setminus\{0\}$ and it may then be asked how *effective* would be the computation of the set $\mathcal{A}(k)$, $k \in \mathbb{Z}\setminus\{0\}$, of admissible integers, hence of the parametrization of solutions of the Mordell equations given in Theorem 3.3 and the algorithm contained in Corollary 3.8. *The following theorem, whose proof rests on the fact that $\mathcal{A}(k)$ may be seen as $\mathcal{A}(k) = \{\gamma = \pm y - x : y^2 = x^3 + k\}$ and the* *already established Hall conjecture (Theorem* 4.1*), therefore addresses the effectiveness of our approach to the study of Mordell equations by telling how far we should look in* $\mathbb{Z}$ *in the computation of the set,* $\mathcal{A}(k)$*, of admissible integers given in Definition* 3.1*, for any arbitrary* $k \in \mathbb{Z} \setminus \{0\}$.

Theorem 4.2. *Let* $k \in \mathbb{Z} \setminus \{0\}$ *be given such that* $\mathcal{A}(k) \neq \emptyset$*. Then every* $\gamma \in \mathcal{A}(k)$ *satisfies* $\mid \gamma \mid < 10 \mid k \mid^{3+2|k|}$. *Proof.* We recall from the expression derived for $\mathcal{A}(k)$ above, that if $\gamma \in \mathcal{A}(k)$ then $\gamma = \pm y - x$, for every $(x, y) \in M(k)$. Hence we have

$$\mid \gamma \mid = \mid \pm y - x \mid \leq \mid y \mid + \mid x \mid \leq 2\max(\mid x \mid, \mid y \mid) < 2\max(5 \mid k \mid^{2+|k|}, 5 \mid k \mid^{3+|k|})$$

$$= 2(5 \mid k \mid^{3+|k|}) = 10 \mid k \mid^{3+|k|}. \qquad \square$$

A second look at Theorem 4.2 shows that it reflects the finiteness of the sets $M(k)$ and $\mathcal{A}(k)$, for every $k \in \mathbb{Z} \setminus \{0\}$, inherited from Siegel's Theorem. This follows if we observe that

$$\mathcal{A}(k) \subset \{\gamma \in \mathbb{Z} : \mid \gamma \mid < 10 \mid k \mid^{3+2|k|}\} = (-10 \mid k \mid^{3+2|k|}, 10 \mid k \mid^{3+2|k|}) \cap \mathbb{Z},$$

for every $k \in \mathbb{Z} \setminus \{0\}$. ¿From this inclusion we then have that $\mathcal{A}(1) = \{-5, -1, 1\}$, as may be computed for any other $k \in \mathbb{Z} \setminus \{0\}$.

The above open and symmetric interval

$$(-10 \mid k \mid^{3+2|k|}, 10 \mid k \mid^{3+2|k|}) \cap \mathbb{Z} =: I_M(k),$$

$k \in \mathbb{Z} \setminus \{0\}$, with the property $I_M(k_1) \supseteq I_M(k_2)$ iff $k_1 \geq k_2$, within which is found the set $\mathcal{A}(k)$ of admissible integers and which may then be termed the *interval of admissible integers for non-trivial Mordell equations,* $y^2 = x^3 + k$, may be used to estimate a corresponding interval for t in Theorem 3.3. A more specific characterization of those non-trivial Mordell equations without integral solutions may also be deduced from Definition 3.1 (*i.*) and Theorem 4.2 as follows.

Corollary 4.1. *A non-trivial Mordell equation, $y^2 = x^3 + k,\ k \in \mathbb{Z} \setminus \{0\}$, has no integral solution (i.e., is non-admissible) iff $r_{\gamma,k}(\zeta)$ has no integral root, for all $\gamma \in I_M(k)$.* *Proof.* The Mordell equation $y^2 = x^3 + k,\ k \in \mathbb{Z} \setminus \{0\}$, has no integral solution iff $\mathcal{A}(k) = \emptyset$ iff $r_{\gamma,k}(\zeta)$ has no integral root, for all $\gamma \in \mathbb{Z}$; in particular, for all $\gamma \in I_M(k)$. □

As an example $y^2 = x^3 - 3$ has no integral solution, hence is a non-trivial non-admissible Mordell equation. We now solve a non-trivial example of a non-trivial admissible Mordell equation with our methods.

Example 4.1. We illustrate in the following how to generate all the integral solutions of the non-trivial integrally solvable Mordell equation $y^2 = x^3 + 9$ using the method established in Theorem 3.3 (or in Corollary 3.4). In this case we have that

$$r_{\gamma,9}(\zeta) = (909 - 300\gamma + 30\gamma^2 - \gamma^3) + (280 - 60\gamma + 3\gamma^2)\zeta + (29 - 3\gamma)\zeta^2 + \zeta^3 = 0,$$

from which we seek values of $\gamma \in \mathbb{Z}$ for which there is at least one integral root, ζ.

We already know, from Theorem 4.2, that $\mid \gamma \mid < 10 \mid 9 \mid^{3+2|9|} = 1094189891 \times 10^{21}$. It may then be shown by considering every integer, γ, of the corresponding interval,

$$I_M(9) = (-1094189891 \times 10^{21}, 1094189891 \times 10^{21}) \cap \mathbb{Z},$$

of admissible integers for $y^2 = x^3 + 9$ in Definition 3.1, that the only integral values of γ for which $r_{\gamma,9}(\zeta) = 0$ has integral roots, $\zeta = \zeta'$, are $\gamma = -293, -21, -9, -3, 1, 3, 9$ and 213 ($i.e,\ \mathcal{A}(9) = \{-293, -21, -9, -3, 1, 3, 9, 213\}$), and that the integral roots are

$$\zeta' = -263 \ \text{(for } \gamma = -293), \qquad \zeta' = -25 \ \text{(for } \gamma = -21),$$

$$\zeta' = -16 \ \text{(for } \gamma = -9), \qquad \zeta' = -13 \ \text{(for } \gamma = -3),$$
$$\zeta' = -11 \ \text{(for } \gamma = 1), \qquad \zeta' = -4, -7, -9 \ \text{(for } \gamma = 3, \ \text{so that } \mathcal{A}_0(9) = \{3\}),$$
$$\zeta' = 5 \ \text{(for } \gamma = 9) \qquad \text{and} \qquad \zeta' = 243 \ \text{(for } \gamma = 213).$$

We then seek (non-zero) integral values of t in which $\frac{1}{t}(909 - 300\gamma + 30\gamma^2 - \gamma^3) = \zeta'$ (as in Theorem 3.3) or in which

$$\mathfrak{D}_{\gamma,9}(t) = (909-300\gamma+30\gamma^2-\gamma^3)t^3+(280-60\gamma+3\gamma^2)(909-300\gamma+30\gamma^2-\gamma^3)t^2+$$
$$(29 - 3\gamma)(909 - 300\gamma + 30\gamma^2 - \gamma^3)^2 t + (909 - 300\gamma + 30\gamma^2 - \gamma^3)^3 = 0,$$

(as in Corollary 3.4), for each of $\gamma = \mathcal{A}(9)$. In either of these approaches we get that

$$t = -105772 \ \text{for } \gamma = -293, \qquad t = -1188 \ \text{for } \gamma = -21,$$
$$t = -423 \ \text{for } \gamma = -9, \qquad t = -162 \ \text{for } \gamma = -3,$$
$$t = -58 \ \text{for } \gamma = 1, \qquad t = -63, -36, -28 \ \text{for } \gamma = 3,$$
$$t = -18 \ \text{for } \gamma = 9 \qquad \text{and} \quad t = -34426 \ \text{for } \gamma = 213.$$

All the possible triples, (k, γ, t), for integral solutions, (x, y), of $y^2 = x^3 + 9$ are therefore $(k, \gamma, t) =$

$$(9, -293, -105772), \ (9, -21, -1188), \ (9, -9, -423), \ (9, -3, -162), \ (9, 1, -58),$$
$$(9, 3, -63), \ (9, 3, -36), \ (9, 3, -28), \ (9, 9, -18), \ (9, 213, -34426).$$

Since there are ten (10) of these triples in all we expect to have a maximum of $2(10) = 20$ integral solutions of $y^2 = x^3 + 9$, counting repetitions if any. With these triples all the integral solutions are then calculated from $x = x(k, \gamma, t) = \frac{1}{t}(900 + k + 10t - (300 + t)\gamma + 30\gamma^2 - \gamma^3)$ and $y = y(k, \gamma, t) = \pm\frac{1}{t}(900 + k + 10t - 300\gamma + 30\gamma^2 - \gamma^3)$ to give

$$M(9) = \{(x, y) = (-2, \pm 1), \ (0, \pm 3), \ (3, \pm 6), \ (6, \pm 15), \ (40, \pm 253)\}.$$

Observe that we do not have the maximum number of twenty (20) integral solutions even though $y = y(k, \gamma, t) \neq 0$ for all triples (k, γ, t). This is due to different triples, (k, γ, t), leading to the same integral solutions. □

Every member of the family of Mordell equations $y^2 = x^3 + k,\ k \in \mathbb{Z} \setminus \{0\}$, may be effectively treated as done in Example 3.1 while any question on their integral solutions may be completely handled by Theorem 3.3. Theorem 3.3 gives the contributions of $k \in \mathbb{Z}$ to the integral solution(s) of every admissible Mordell equation (via k itself and via $\gamma = \gamma(k)$ and $t = t(k)$) and, since we are more interested in these solutions and their properties than in k by itself, we have a completely satisfying platform for the treatment of Mordell equations in this Theorem. The undue attention given to values of k was largely due to insistence on applying the platform of *unique factorization* to different variants of Mordell equations (which leads to various stringent conditions on k, like not being divisible by a sixth power, or being of the form $k_1 b^2 - k_1^3 a^3$, for some $k_1, a, b \in \mathbb{Z}$, *etc*, thereby giving integral solutions to *only* a class of the equations but which are no more necessary due to our present use of Lemma 2.1) and inability to have a general solution of the kind in Theorem 3.3, forcing on us the laborious computations of the integral solutions for each $k \in \mathbb{Z} \setminus \{0\}$ from algebraic number theory before conclusions and *informed* conjectures are made on each Mordell equation, one after the other.

> *Indeed with Theorem* 3.3 *we no longer have to explicitly compute the integral solutions of an integrally solvable Mordell equation before we could study the evolution of the equation and its integral solutions.*

5 Further results and some open problems on Mordell arithmetic functions

(1.) Let $k \in \mathbb{Z} \setminus \{0\}$ and let $y^2 = x^3 + k$ has $n-$distinct integral solutions.

What is the expression for the minimum number, l, of integers $\gamma_i \in \mathcal{A}(k),\ 1 \leq i \leq l = l(n)$, that give all the $n-$distinct integral solutions of $y^2 = x^3 + k$?

That is, what is the least number of t in Corollary 3.4 that would suffice to get all integral solutions of $y^2 = x^3 + k$ for any fixed $k \in \mathbb{Z} \setminus \{0\}$ with $\mathcal{A}(k) \neq \emptyset$? We already know from the main result of [8.] quoted above that for $y^2 = x^3 + 1$ where $n = 5$, we have $l = 1$ and, from Example 3.1, that for $y^2 = x^3 + 9$ where $n = 10$, we have $l = 3$.

(2.) Clearly

$$n = n(k) = \frac{1}{k}\omega(k),$$

for some function $\omega : \mathbb{Z} \to \mathbb{Z}$ with $\omega(0) > 0$, so that $n(0) = \infty$ as may be seen from $M(0) = \{(x, y) = (\delta^2, \pm\delta^3) : \delta \in \mathbb{Z}\}$, as earlier reported in §3.

What is the explicit expression for the function $k \mapsto \omega(k),$ for all $k \in \mathbb{Z}$?

We however know that this subsidiary function $\mathbb{Z} \to \mathbb{Z} : k \mapsto \omega(k)$ is highly *piecewise continuous* on $\mathbb{R}$ and is given in the interval $1 \leq k \leq 14$ as

$$\omega(k) = \begin{cases} 5, & \text{if } k = 1, \\ 2k, & \text{if } 2 \leq k \leq 5, \\ 0, & \text{if } 5 < k < 8, \\ 34k - 216, & \text{if } 8 \leq k \leq 9, \\ -20k + 220, & \text{if } 9 < k < 12, \\ -48k + 624, & \text{if } 12 \leq k \leq 13, \\ 0, & \text{if } k = 14. \end{cases}$$

This problem suggests we seek a real-valued function of real variables whose *Fourier expansion* is exactly ω.

It may be helpful to recall from Theorem 3.4 that:

> *If there are m number of distinct integral roots, ζ, of $r_{\gamma,k}(\zeta) = 0$ for all $\gamma \in \mathcal{A}(k)$ and a fixed $k \in \mathbb{Z}$, then the Mordell equation $y^2 = x^3 + k$ is admissible and has exactly $n = 2m$ number of integral solutions, counting repetitions.*

This is our partial solution to the problem of counting the number of integral solutions of admissible Mordell equations, $y^2 = x^3 + k,\ k \in \mathbb{Z} \setminus \{0\}$. It only remains to deduce the exact dependence of m on k. This is done below while the complete solution to the problem of counting the number of integral solutions of admissible Mordell equations is given thereafter as Theorem 5.2. Also with $m = m(k)$ we have $n(k) = 2m(k)$ so that $m(k) = \frac{1}{2k}\omega(k),\ k \in \mathbb{Z}$, counting repetitions.

However Theorem 4.2 reports (from the symmetricity of $I_M(k)$) that there is a maximum of

$$2(10 \mid k \mid^{3+|k|}) - 1 = 20 \mid k \mid^{3+|k|} -1$$

admissible integers, γ, that are needed in order to arrive at *all* the integral roots, ζ of $r_{\gamma,k}(\zeta) = 0$, for every $k \in \mathbb{Z}\setminus\{0\}$ considered. Hence, since $r_{\gamma,k}(\zeta) = 0$ is *cubic* in ζ, we must have the following.

Lemma 5.1 *For every $k \in \mathbb{Z} \setminus \{0\}$ with $\mathcal{A}(k) \neq \emptyset$,*

$$m = m(k) \leq 3(20 \mid k \mid^{3+|k|} -1) = 60 \mid k \mid^{3+|k|} -3.$$

This means that the upper-bound for the number, $n(k)$, of integral solutions of each of the equations $y^2 = x^3 + k,\ k \in \mathbb{Z} \setminus \{0\}$, could be given as follows. This Theorem, when compared with the main result of [9], shows an improvement in the estimation of the number of integral solutions of a Mordell equation.

Theorem 5.1. *Let $k \in \mathbb{Z} \setminus \{0\}$ such that $\mathcal{A}(k) \neq \emptyset$. Then*

$$1 \leq \mid M(k) \mid = n(k) \leq 120 \mid k \mid^{3+|k|} -6.$$

Proof. We combine $n(k) = 2m(k)$ of Theorem 3.4 with Lemma 5.1. □

The upper bound $b(k) := 120 \mid k \mid^{3+|k|} -6$ of the number, $n = n(k)$, of integral solutions of any admissible Mordell equation, $y^2 = x^3 + k$, may be further reduced by ($i.$) counting and removing the number, $\rho(k) \geq 0$, of repetitions of members of $M(k)$ (when the (integral) roots, ζ, of $r_{\gamma,k}(\zeta) = 0$ are repeated or when some of them are -10, thus leading to $y = 0$ (See Remarks 3.2 ($i.$)) or when two (2) integral roots, $\zeta' \neq \zeta''$, gives the same solution, (x, y)) and by ($ii.$) counting and removing the number, $\nu(k) \geq 0$, of those (non-admissible) integers, τ, in the range $-10 \mid k \mid^{3+|k|} < \tau < 10 \mid k \mid^{3+|k|}$ for which $r_{\tau,k}(\zeta) = 0$ has no integral root (k being fixed in $\mathbb{Z} \setminus \{0\}$), from the total maximum possible number, $b(k) = 120 \mid k \mid^{3+|k|} -6$, of integral solutions of $y^2 = x^3 + k$. Thus we have that

$$n = n(k) = b(k) - \rho(k) - 6\nu(k).$$

This gives the following consequence of Theorem 4.2, containing the first known expression for the number, $n(k)$, of integral solutions of $y^2 = x^3 + k$.

Theorem 5.2. *The cardinality $n(k)$ of the solution-set $M(k)$ is given as*

$$n(k) = 120 \mid k \mid^{3+|k|} -\rho(k) - 6\nu(k) - 6,$$

for every $k \in \mathbb{Z} \setminus \{0\}$ with $\mathcal{A}(k) \neq \emptyset$, where $\rho(k) \geq 0$ and $\nu(k) \geq 0$. *Proof.* As contained in the last paragraph above. □

Explicit expressions for the functions $k \mapsto \rho(k)$ and $k \mapsto \nu(k)$ in terms of k are therefore necessary in order to have a complete solution to the problem of cardinality of $M(k)$, for those $k \in \mathbb{Z} \setminus \{0\}$ with $\mathcal{A}(k) \neq \emptyset$. It is however clear that

$$\nu(k) := \mid I_M(k) \mid - \mid \mathcal{A}(k) \mid = 20 \mid k \mid^{3+|k|} - \mid \mathcal{A}(k) \mid -1,$$

so that $n(k) = 6 \mid \mathcal{A}(k) \mid -\rho(k)$, for every $k \in \mathbb{Z} \setminus \{0\}$.

Example 5.1.

$\underline{k = 1}$: Observe that, since

$$I_M(1) = \{-19, -18, \cdots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \cdots, 18, 19\}$$

and $\mathcal{A}(1) = \{-5, -1, 1\}$ from where we may get $\rho(1) = 19$ and

$$\nu(1) = 20 \mid 1 \mid^4 - \mid \mathcal{A}(1) \mid -1 = 20 - 3 - 1 = 16$$

for $y^2 = x^3 + 1$, we have that $n(1) = 120 \mid 1 \mid^4 -\rho(1) - 6\nu(1) - 6 = 5$ as expected. This calculation may be made as well for $k = 9$, from Example 4.1, and indeed for every $k \in \mathbb{Z} \setminus \{0\}$.

We believe that a comprehensive solution to problem (2.), either via Fourier analysis of $\omega = \omega(k)$ or the consideration of the explicit forms of $\rho = \rho(k)$ and $\nu = \nu(k)$ or of at least their properties, for every $k \in \mathbb{Z} \setminus \{0\}$ with $\mathcal{A}(k) \neq \emptyset$, would suggest a method of solving problem (1.). Indeed the functions

$$k \mapsto \omega(k), \quad k \mapsto \rho(k) \ \text{ and } \ k \mapsto \nu(k)$$

are the *elementary* functions which encode the *arithmetic* of both admissible and non-admissible Mordell equations.

(3.) For a Mordell equation, $y^2 = x^3 + k, \ k \in \mathbb{Z} \setminus \{0\}$, with a unique integral solution we have seen, in Corollary 3.5, the most explicit form of the set $\mathcal{A}_u(k)$ given strictly in terms of the value of k.

> *Is there a more explicit form for* $\mathcal{A}(k), \ k \in \mathbb{Z} \setminus \{0\}$, *than we have in the formula*
>
> $$\mathcal{A}(k) = \{\gamma = \pm y - x : y^2 = x^3 + k\},$$
>
> *which will be in terms of* k *indeed and is not based on the foreknowledge of the integral solutions,* (x, y)*?*

An affirmative answer to this will be of importance in arriving at a concrete expression for t of Corollary 3.4 (as done for $\mathcal{A}(0)$ and may be seen for $\mathcal{A}_u(k) = \{\sqrt[3]{k}\}$). It will in turn pave way to the solution of problems (1.) and (2.) above. Indeed these three problems aim at solving the central problem of being able to effectively count all the integral solutions of any (non-trivial) admissible Mordell equation from the knowledge of k. A cue may be taken from $\mathcal{A}_u(k),\ k \in \mathbb{Z}$, and its corresponding expression for t. A detailed study of the maps

$$(k, \gamma, t) \mapsto x(k, \gamma, t) \text{ and } (k, \gamma, t) \mapsto y(k, \gamma, t)$$

in Theorem 3.3 may also not be out of place. The much we can say presently is that

$$\mathcal{A}(k) \subset \{\gamma \in \mathbb{Z} :\mid \gamma \mid< 10 \mid k \mid^{3+|k|}\} = (-10 \mid k \mid^{3+|k|}, 10 \mid k \mid^{3+|k|}) \cap \mathbb{Z} =: I_M(k),$$

for every $k \in \mathbb{Z} \setminus \{0\}$.

6 Conclusion

It may therefore be concluded that the disparate nature of the integral (resp., rational integral) solutions of Mordell equations is due largely to the difficulty in isolating integral (resp., rational integral) roots of the third-order polynomial equations given as

$$r_{\gamma,k}(\zeta) = 0 \text{ and } \mathfrak{D}_{\gamma,k}(X) = 0, \quad \gamma, k, \zeta, X \in \mathbb{Z}.$$

However with proper handling of these polynomials, as shown in this paper, headways could be made. These observations underscore the need to have a general theory for the integral (resp., rational integral) solutions of nth-order polynomials with integer (resp., rational integral) coefficients, as against only the *radical* roots of polynomials discussed by Galois theory, since each of these polynomials correspond to a particular Diophantine equation. Properties of some of these corresponding polynomials, which may therefore be termed *Diophantine polynomials,* have been successfully exploited to discuss integral solutions of some other important Diophantine equations in [7] and [8].

It will seem that every little observation on the nature of integral solutions of $y^2 = x^3 + k$ always give far-reaching results that have been hard earned or laboriously conjectured from other sources or from numerical data. This is exactly so and the success of this approach is a direct consequence of the transformation of the original Diophantine equation by Lemma 2.1 into a $1-$indeterminate polynomial equation with integral coefficients. Since polynomials are well understood objects of mathematics it should therefore not be a surprise that we are able to prove all these results with so little efforts after the said transformation.

The Diophantine polynomials serve to lay before us the entire physiology of Diophantine equations, furnishing us with the reason for the existence or non-existence of classes of their solutions ([7]), the nature and how to generate the solutions in specific integral domains ([8]), explicit realization of the corresponding Mordell-Weil group ([7]) and the generation of its field of arithmetic. All these could be effectively done for any integrally solvable Diophantine equation without recourse to conjectures or numerical analysis of these equations immediately the *interval of admissible integers* for the Diophantine equations is derived. These polynomials may also serve to simplify the problem of computing integral and non-integral solutions of admissible Mordell equations over a local or global field.

Lemma 2.1 may also be employed to transfer the abstract axioms at the foundation of the theory of polynomials in $\mathbb{Z}[X]$ or $\mathbb{Q}[X]$ into an analogous set of abstract axioms that may serve as the theoretical foundation for Diophantine analysis and the theory of numbers. We hope the modern *number theorists* would see the need to rigourously study the theory of numbers along this line of thoughts.

References

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

[2] M.A. Bennett and Ghadermarzi, Mordell's Equation: A Classical Approach. Available at arXiv:1311.7077v1 [math.NT] 27 Nov 2013.

[3] A. Baker, Contributions to the Theory of Diophantine Equations, II. The Diophantine Equation $y^2 = x^3 + k$, *Phil. Royal Soc. of London*, **263**, 1139, (1968), 193-208.

[4] J. Gebel, A. Peth*ö* and H.G. Zimmer, Computing integral points on Mordell's elliptic curves, *Collect. Math.*, **48**(1-2), (1997),115-136.

[5] J. Gebel, A. Peth*ö*, and H.G. Zimmer, On Mordell's Equations, *Compositio Math.*, **110**(3), (1998), 335-367.

[6] B. Mazur, Questions about Powers of Numbers, *Notices of the AMS*, **47**(2), (2000), 195-202.

[7] O.O. Oyadare, Galois groups of Fermat polynomials and the arithmetic groups of Diophantine curves. To appear in *Scientia Magna*, **10**(2), (2014), Preprint available at www.arXiv.org/abs/1404.1472.pdf

[8] O.O. Oyadare, A new proof of Euler's theorem on Catalan's equation. Under review.

[9] D. Poulakis, The number of solutions of the Mordell equation, *Acta Arithmetica*, LXXXVIII, **2**, (1999), 173-179.