Hang Lung Mathematics Awards
Vol. 8 (2018), pp. 151–169

INVESTIGATION ON MORDELL'S EQUATION

TEAM MEMBER
Tin Wai LAU

TEACHER
Mr. Ho Fung LEE

SCHOOL
Pui Ching Middle School

Abstract. This paper aims to investigate the integral solutions of the Mordell's Equation $y^2 = x^3 + k$ for a particular class of integers k. We employ some classical approaches, i.e. factorization in number fields and quadratic reciprocity. When $k = p^2$ for certain primes p, we can determine the set of solutions. Two other classes of integers k are also solved in this paper.

1. Introduction

Finding rational points of Elliptic curves is an important aspect in mathematics. In 1922, Mordell proved the group of rational points in elliptic curve, i.e. $E(\mathbb{Q})$, is finitely generated. Mazur in 1977 further found all possible torsion subgroups, which describe all possible groups of $E(\mathbb{Q})$. Nowadays, there are already algorithms [1] that effectively compute the rational points in elliptic curves.

However, there are still a lot to be found on computing integral points in elliptic curves. As $\mathbb{Z}$ is not a field, so $E(\mathbb{Z})$ is usually not a subgroup of $E(\mathbb{Q})$. The only famous result for $E(\mathbb{Z})$ was in 1928, Siegel has proved that $E(\mathbb{Z})$ is finite. In seeing of this, this paper aims to study a specific type of elliptic curves, i.e. Mordell Curve and tries to develop some results.

The Mordell's Equation $y^2 = x^3 + k$ has not only properties in elliptic curves, but also some insights when we employ classical means, e.g. when we factorize the equation in Gaussian integers, we are able to solve the equation in a class of integers k. Hence we choose Mordell's equation as a subject to study. Specifically, we want to employ classical approaches to solve the Mordell's equation.

To deal with three different classes of k, this paper is divided into 3 parts. Each section is guided by different intuitions to approach the problem, and lead to different results via classical means, namely (i) Factorization in $\mathbb{Z}$, (ii) Quadratic Reciprocity Method, and (iii) Factorization in Number Fields.

Notations Unless otherwise specified, all variables in this paper are integers, while variable n only stands for natural numbers. p and q are denoted as primes. We write (a, b) as the greatest common divisor of a and b. For set theory, $\mathbb{N}$ stands for the set of natural numbers which excludes zero while $\mathbb{Z}^+$ includes zero, $\mathbb{F}_p$ stands for finite field with p elements.

In this paper, we let K be a number field, where $\mathcal{O}_K$ is the ring of integers of K, and $\mathcal{O}_K^\times$ is the group of units of $\mathcal{O}_K$. The Norm of an element is same as usual in algebra, i.e.

Definition 1. *Let $\alpha \in K$ have degree n, and set $k = \deg K/n$. The Norm of α is*

$$N_{K/\mathbb{Q}}(\alpha) = \prod(\textit{Galois Conjugates of } \alpha)^k$$

Particularly, if $K = \mathbb{Q}(i)$ and $\alpha = a + bi \in K$, the Norm is

$$N(a + bi) = a^2 + b^2$$

If $K = \mathbb{Q}(\sqrt[3]{2})$ and $\alpha = a + b\sqrt[3]{2} + c\sqrt[3]{4}$. the Norm [2] *is*

$$N(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = a^3 + 2b^3 + 4c^3 - 6abc$$

1.1. Investigation Background

In this section, we will present remarkable results using the theory of elliptic curves, focusing on the case of Mordell curve over integers. They also serve as a background motivation while we approach the problem.

Theorem 2. *(Siegel, 1928) Let $A, B \in \mathbb{Z}$ and E be an elliptic curve given by the equation*

$$E : y^2 = x^3 + Ax + B$$

Then the integral solution set $E(\mathbb{Z}) : \{(x, y) \in \mathbb{Z}^2 \mid y^2 = x^3 + Ax + B\}$ is a finite set.

This theorem shows us there are only finitely many solutions in Mordell's Equation. Indeed in all our theorems, they only show finitely many solutions.

Theorem 3. *(Hasse, 1922) Let $A, B \in \mathbb{F}_p$ and E be an elliptic curve given by the equation*

$$E : y^2 = x^3 + Ax + B$$

Then we have the inequality:

$$|\#E(\mathbb{F}_p) - (p + 1)| \leq 2\sqrt{p}$$

This theorem actually shows us that we cannot prove Mordell Equation has no solutions simply by taking modulo p, as $p + 1 > 2\sqrt{p}$, so there are at least one solution taking modulo p.

We now give a theorem about Mordell's equation specifically, instead of a general Elliptic Curve:

Theorem 4. *(Baker, 1968* [3]*) For any given $k \in \mathbb{Z}$, the integral solutions (x, y) in the equation $y^2 = x^3 + k$ must satisfy the inequality:*

$$\max(|x|, |y|) \leq \exp(10^{10}|k|^{10^4})$$

This gives us an theoretical bound to compute all integral points.

2. Unique Factorization on $\mathbb{Z}$

We first consider some special cases of the number k such that some factorization in $\mathbb{Z}$ can hold. For example, if k is a square number, i.e. $k = m^2$, then we have:

$$x^3 = y^2 - m^2 = (y + m)(y - m)$$

if $y + m$ and $y - m$ are relatively prime to each other, then they are a cube itself, which can be proved by considering the prime factorization of $y + m$ and $y - m$ in $\mathbb{Z}$. Guided by this motivation, we will repeatedly use this fact.

In this section, we first consider the solutions of the three cases $k = 1, 4, 16$, and by using the results we can generalize into all solutions of $y^2 = x^3 + 4^n$. These three cases are dealt with individually, with not necessary elementary method.

2.1. Preliminaries

Two important theorems are needed in Section 1:

Theorem 5. *(Catalan Conjecture, 2002* [4]*) The only positive integral solution (x, y, r, s) with $x, y, r, s \geq 2$ of the Diophantine equation $x^r - y^s = 1$ is $(3, 2, 2, 3)$.*

This theorem can imply our Lemma 12.

The next theorem we need to state is Dirichlet's Unit Theorem in the special case $K = \mathbb{Q}(\sqrt[3]{2})$, which we have to state several definitions first.

The following definition can be found in [5].

Definition 6. *Let K be a number field, and set*

$$r_1 = \textit{number of real embeddings,}$$
$$r_2 = \textit{number of pairs of complex embeddings.}$$

The signature of K is then defined as the pair (r_1, r_2).

As only the case $K = \mathbb{Q}(\sqrt[3]{2})$ is needed, all examples are concerned on this number field.

Example 7. *Let $K = \mathbb{Q}(\sqrt[3]{2})$, and let ω be the cube root of unity. The elements of K are*

$$a + b\sqrt[3]{2} + c\sqrt[3]{4}, \text{ where } a, b, c \in \mathbb{Q}.$$

The signature is $(1,1)$, because the three embeddings are

$$\sigma_1 : \sqrt[3]{2} \to \sqrt[3]{2}, \quad \sigma_2 : \sqrt[3]{2} \to \sqrt[3]{2}\omega, \quad \sigma_3 : \sqrt[3]{2} \to \sqrt[3]{2}\omega^2.$$

The first is real and the latter two are conjugate pairs.

Definition 8. *Let $\mu(\mathcal{O}_K)$ denote the set of roots of unity contained in a number field K. Notice that it is a finite group under multiplication.*

Now we can state the Dirichlet's Unit Theorem, which gives us a picture of what units in $\mathcal{O}_K$ are.

Theorem 9. *(Dirichlet's Unit Theorem) Let K be a number field with signature (r_1, r_2) and set $s = r_1 + r_2 - 1$. Then there exists units $u_1, u_2, u_3, \dots, u_s$ such that every $\alpha \in \mathcal{O}_K^\times$ can be written uniquely in the form*

$$\alpha = \omega \cdot u_1^{n_1} \dots u_s^{n_s}$$

for $\omega \in \mu(\mathcal{O}_K), n_1, \dots, n_s \in \mathbb{Z}$.

In the example of $K = \mathbb{Q}(\sqrt[3]{2})$, we have:

Example 10. *Let $K = \mathbb{Q}(\sqrt[3]{2})$ with signature $(1,1)$. Then $s = 1$, so we have exactly one fundamental unit which is $1 + \sqrt[3]{2} + \sqrt[3]{4}$. So*

$$\mathcal{O}_K^\times = \{\pm(1 + \sqrt[3]{2} + \sqrt[3]{4})^n, n \in \mathbb{Z}\}$$

This ends our preliminary, now we put all these into practice:

2.2. Results on $k = 4^n$

Our main result in this section is the solution in $y^2 = x^3 + 4^n$, given by the theorem below:

Theorem 11. *The only integral solutions to $y^2 = x^3 + 4^n$ (with $n \in \mathbb{N}$) are*

$$(x, y) = \begin{cases} (0, \pm 2^n), (2^{2n/3+1}, \pm 3 \times 2^n), (-2^{2n/3}, 0) & \text{if } n \equiv 0 \pmod 3 \\ (0, \pm 2^n) & \text{otherwise} \end{cases}$$

But before we provide the proof, three lemmas are required.

Lemma 12. *The only integral solutions to $y^2 = x^3 + 1$ are*

$$(x, y) = (2, \pm 3), (0, \pm 1), (-1, 0)$$

This lemma follows from Catalan Conjecture, while some technical work is still needed.

Proof. If $x, y \geq 2$, then by Catalan Conjecture, the only solution is $(x, y) = (2, 3)$. If $-1 \leq x < 2$, by exhaustion we have the three trivial solutions $(0, \pm 1)$ and $(-1, 0)$, similar argument also holds if $-1 \leq y < 2$. If $x \leq -2$, then notice $y^2 = x^3 + 1 < 0$, which is impossible, hence there are no solutions. At last we are left with case $x \geq 2$ and $y \leq -2$. Now write $y' = -y$, then we still have essentially the same equation $y'^2 = x^3 + 1$ with $y' \geq 2$ and $x > 2$, so by Catalan Conjecture we have $(x, y') = (2, 3)$, which corresponds to $(x, y) = (2, -3)$. Hence they are all possible solutions. □

Lemma 13. *The only integral solutions to $y^2 = x^3 + 4$ are $(x, y) = (0, \pm 2)$.*

Proof. From the equation, we have $(y - 2)(y + 2) = x^3$. If y is odd, then $y + 2$ and $y - 2$ is relatively prime. Therefore the two factors are cubes. However, no two odd cubes differ by 4, so we obtain a contradiction. Hence y is even, write $y = 2y_1$.

We obtain the equation:

$$4y_1^2 = x^3 + 4$$

Notice that x is even. Write $x = 2x_1$ we have:

$$y_1^2 = 2x_1^3 + 1$$

Notice that y_1 is odd. Write $y_1 = 2m + 1$ we have:

$$(2m + 1)^2 = 4m^2 + 4m + 1 = 2x_1^3 + 1$$

simplifying both sides yields:

$$2m(m + 1) = x_1^3$$

Once again we have x_1 as an even number, write $x_1 = 2x_2$, we obtain that $m(m + 1) = 4x_2^3$. As m and $m + 1$ are relatively prime, then the only two possibilities are:

$$m = a^3 \quad \text{and} \quad m + 1 = 4b^3$$

and

$$m = 4a^3 \quad \text{and} \quad m + 1 = b^3$$

This yields to the final Diophantine equation concerning on $4b^3 - a^3 = 1$ and $b^3 - 4a^3 = 1$, which are essentially Skolem Equation $x^3 + dy^3 = 1$ for $d = -4$. We claim that this equation has no nontrivial integral solution.

We consider the equation in $K = \mathbb{Q}(\sqrt[3]{2})$, notice that $N(-a + b\sqrt[3]{4}) = 4b^3 - a^3 = 1$, so $-a + b\sqrt[3]{4}$ is a unit by the equation, hence by Dirichlet's Unit Theorem, there exists $g \in \mathbb{Z}$ such that

$$a - b\sqrt[3]{4} = \pm(1 + \sqrt[3]{2} + \sqrt[3]{4})^g$$

Notice that R.H.S must consists of a cube root of 2 (for $g > 0$), which contradict to L.H.S, hence there is no integer solution for $g > 0$. For $g < 0$, notice that $(1 + \sqrt[3]{2} + \sqrt[3]{4})^{-1} = \sqrt[3]{2} - 1$ which must consist of a cube root of 2. Hence $g = 0$ which we have $a = \pm 1$ and $b = 0$.

Hence the only solutions are $(a, b) = (-1, 0)$ and $(0, 1)$ respectively, which corresponds to $x_1 = 0$, and $(x, y) = (0, 2)$. Hence $(x, y) = (0, \pm 2)$. □

Lemma 14. *The only integral solutions to $y^2 = x^3 + 16$ are $(x, y) = (0, \pm 4)$.*

Proof. Rewrite the equation as $(y-4)(y+4) = x^3$. Assume y is odd then $y+4$ and $y-4$ are relatively prime. Hence they are both odd cubes but that is impossible as no odd cubes differ by 8. Hence y is even and so x is even too.

The R.H.S. of the equation is divisible by 8, so we have $4 \mid y$. Let $y = 4y'$, then $16y'^2 = x^3 + 16$, therefore $4 \mid x$. Let $x = 4x'$, then $y'^2 = 4x'^3 + 1$, showing that y' is odd. Further we let $y' = 2m + 1$, then $m^2 + m = x'^3$.

Notice that $m(m + 1) = x'^3$. As $(m, m + 1) = 1$, so both of them are cubes. The only consecutive cubes are $\{-1, 0, 1\}$, hence m or $m + 1$ are 0. Therefore $x' = 0$. Hence $x = 0$ and $y = \pm 4$. □

Notice that our three lemmas are just first three cases of our main theorem, where $n = 0, 1, 2$. In our proof of our main theorem, we will reduce the equation into our three forms in our lemmas.

Proof of main theorem 11. By Lemma 12-14, we can assume $n > 2$. Rewrite the equation as

$$x^3 = y^2 - 4^n = (y + 2^n)(y - 2^n)$$

If y is odd, consider the greatest common divisor $d = (y+2n, y-2n)$. As $y+2^n$ and $y-2^n$ are odd, d must be odd. However d must divides $(y+2^n)-(y-2^n) = 2n+1$, hence $d = 1$, i.e. they are relatively prime. Hence they are both cubes. Now write $u^3 = y + 2^n$ and $v^3 = y - 2^n$ (Notice u and v are odd). Consider the equation $u^3 - v^3 = (u - v)(u^2 + uv + v^2) = 2^{n+1}$. Since $u^2 + uv + v^2 \equiv 1^2 + 1 \times 1 + 1^2 \equiv 1 \pmod 2$, which is odd, but that results in $u - v = 2n + 1$ and $u^2 + uv + v^2 = 1$. We claim that it has no solutions.

Write $u = v + 2^{n+1}$. Substitution yields $(v + 2^{n+1})^2 + v(v + 2^{n+1}) + v^2 = 1$, which implies that $3v^2 + 2^{n+1} \cdot 3v + 2^{2n+2} = 1$. Considering the discriminant of the quadratic equation in v, we have $\Delta = 12(1 - 2^{2n}) < 0$. Hence the equation has no real solutions.

Now we have x and y is even. The R.H.S. of equation $y^2 = x^3 + 4^n$ is divisible by 8, so $4 \mid y$. Writing $y = 4y'$, we have $16y'^2 = x^3 + 4^n$. Therefore $4 \mid x$. Write $x = 4x'$, so $y'^2_1 = 4x'^3 + 4^{n-2}$. Then we have $2 \mid y'$ again, write $y' = 2y_1$ and we attain

$$y'^2_1 = x'^3_1 + 4^{n-3}$$

Notice that this is the same equation as the original one, except now 4^n is reduced by 4^{n-3}. We can repeat the process until we have

Case 1: $n = 3k$ Denote $x_k = 4^{-k}x$ and $y_k = 8^{-k}y$ similarly, we have:

$$y_k^2 = x_k^3 + 1$$

by Lemma 12, the only integral solutions are $(x_k, y_k) = (2, \pm 3)$ with trivial solutions $(0, \pm 1)$ and $(-1, 0)$, which corresponds to $(x, y) = (2^{2k+1}, \pm 3 \times 8^k), (0, 8^k)$ and $(-4^k, 0)$ for $n = 3k$.

Case 2: $n = 3k + 1$ Now we have

$$y_k^2 = x_k^2 + 4$$

By Lemma 13, the only solutions are $(x_k, y_k) = (0, \pm 2)$. Hence, $(x, y) = (0, \pm 2^{3k+1})$.

Case 3: $n = 3k + 2$ Now we have

$$y_k^2 = x_k^2 + 16$$

By Lemma 14, we have $x_k = 0$ and $y_k = \pm 4$, which corresponds to $(x, y) = (0, \pm 2^{3k+2})$. □

3. Quadratic Reciprocity Method

We notice that performing factorization in $\mathbb{Z}$ only works in a small class of integers k. Hence we want to switch to another completely different approach to proceed.

This time, we try to use the factorization identity $x^3 + m^3 = (x + m)(x^2 - mx + m^2)$. That is, $k = m^3 - k_1$.

We have

$$y^2 + k_1 = x^3 + m^3 = (x + m)(x^2 - mx + m^2)$$

The intuition is to consider a modulo p version of the equation. By the theory of Quadratic Residue, there will be restrictions on the congruence condition on p. However if we can find a prime factor that doesn't satisfy the congruence condition in R.H.S., then by choosing a suitable p, a contradiction will arise.

Lemma 15 will be in great use later, so we present the result first.

Lemma 15. *Let p be a prime. Then*

1. *-1 is a quadratic residue modulo p if and only if $p \equiv 1 \pmod 4$;*
2. *2 is a quadratic residue modulo p if and only if $p \equiv 1, 7 \pmod 8$;*
3. *-2 is a quadratic residue modulo p if and only if $p \equiv 1, 3 \pmod 8$.*

In this section, we present four propositions.

Proposition 16. *The equation $y^2 = x^3 + k$ has no solutions if there exists $m, b \in \mathbb{Z}$ such that $k = m^3 - b^2$ in which $m \equiv 2 \pmod 4$ and b is an odd number.*

Proof. Assume the contrary, i.e. there exists a set of integral solution (x, y).

If x is even then $y^2 = x^3 + k \equiv k \equiv m^3 - b^2 \equiv 7 \pmod 8$, but that is impossible as 7 is not a quadratic residue of 8. Hence x is odd.

We have

$$y^2 + b^2 = x^3 + m^3 = (x+m)(x^2 - mx + m^2) = (x+m)\left(\left(x - \frac{m}{2}\right)^2 + \frac{3m^2}{4}\right)$$

As x and $\frac{m}{2}$ are both odd, $\left(x - \frac{m}{2}\right)^2 + \frac{3m^2}{4} \equiv 3 \pmod 4$. Since the product of primes that are in the form $4k+1$ still have residue 1 modulo 4, the above expression must have a prime factor $p \equiv 3 \pmod 4$.

The same p divides the left hand side of the equation, i.e. $y^2 + b^2$. Hence, $y^2 \equiv -b^2 \pmod p$. We consider $\left(\frac{-b^2}{p}\right) = \left(\frac{b^2}{p}\right)\left(\frac{-1}{p}\right)$, which is equal to -1 as $(\frac{x^2}{p}) = 1$ for all x and $(\frac{-1}{p}) = -1$ for $p \not\equiv 1 \pmod 4$.

Hence, by considering the equation modulo p with $p \equiv 3 \pmod 4$, we have a contradiction. □

Proposition 17. *The equation $y^2 = x^3 + k$ has no solutions if there exists $m, b \in \mathbb{Z}$ such that $k = -m^3 - 4b^2$ where $m \equiv 1 \pmod 4$.*

Proof. Assume the contrary, i.e. there exists a set of solution (x, y). Take modulo 4 in the whole equation.

Here is the table of values of y^2 and $x^3 - 1$ modulo 4.

y	$y^2 \pmod 4$	x	$x^3 - 1 \pmod 4$
0	0	0	3
1	1	1	0
2	0	2	3
3	1	3	2

The only common value of y^2 and $x^3 - 1$ modulo 4 is 0, so y is even and $x \equiv 1 \pmod 4$. Now $y^2 + 4b^2 = x^3 - m^3 = (x-m)(x^2 + mx + m^2)$. Consider factor $x^2 + mx + m^2 = \left(x - \frac{m}{2}\right)^2 + \frac{3m^2}{4} \geq 0$. As $x \equiv 1 \pmod 4$, $x^2 + mx + m^2 \equiv m^2 + m + 1 \equiv 3 \pmod 4$, so there exist a prime factor p in $x^2 + mx + m^2$ such that $p \equiv 3 \pmod 4$. Then we have $y^2 + 4b^2 \equiv 0 \pmod p$, so p must be congruent 1 modulo 4, contradiction. □

Proposition 18. *The equation $y^2 = x^3 + k$ has no solutions if there exist $m, b \in \mathbb{Z}$ such that $k = -m^3 + 2b^2$ where $m \equiv 2 \pmod 8$ and b is an odd number.*

Proof. Assume the contrary, i.e. there exists a set of solution (x, y).

If x is even then $y^2 \equiv k \equiv -m^3 + 2b^2 \equiv -2^3 + 2 \equiv 2 \pmod 8$, which is not a square. Therefore x is odd and so y is odd too.

We then have $x^3 = y^2 - k \equiv 1 + 6 \equiv 7 \pmod 8$. Since x is odd, $x^3 - x \equiv x(x^2 - 1) \equiv x(1-1) \equiv 0 \pmod 8$. Hence $x \equiv x^3 \equiv 7 \pmod 8$. Since

$$y^2 - 2b^2 = x^3 - m^3 = (x - m)(x^2 + mx + m^2),$$

we further know that $x^2 + mx + m^2 \equiv 7^2 + 7m + m^2 \equiv m^2 - m + 1 \equiv 3 \pmod 8$ by $m \equiv 2 \pmod 8$. Hence there exists a prime factor p of $x^2 + mx + m^2$ with residue $\pm 3 \pmod 8$.

However, $y^2 \equiv 2b^2 \pmod p$, which corresponds to the congruent relation $p \equiv \pm 1 \pmod 8$ by Lemma 15 and similar argument as above. It leads to contradiction. The result follows. □

Proposition 19. *The equation $y^2 = x^3 + k$ has no solutions if there exist $m, b \in \mathbb{Z}$ such that $k = m^3 - 2b^2$ in which $m \equiv 2 \pmod 8$ and $b \equiv 1 \pmod 8$.*

Proof. Assume the contrary, i.e. there exists a set of solution (x, y).

If x is even, then $y^2 \equiv k \equiv m^3 - 2b^2 \equiv 6 \pmod 8$, which is not a square. Hence x is odd and so y is odd. Then $x^3 \equiv x \equiv y^2 - k \equiv 1 - 6 \equiv 3 \pmod 8$. Now, $y^2 + 2b^2 = x^3 + m^3 = (x + m)(x^2 - mx + m^2)$. Since for all prime factor p in $x^2 - mx + m^2$ we have $y^2 + 2b^2 \equiv 0 \pmod p$, so $p \equiv 1, 3 \pmod 8$ by Lemma 15, but that results in all prime factors p of $x^2 - mx + m^2 \equiv 1, 3 \pmod 8$, which contradicts the fact that $x^2 - mx + m^2 \equiv m^2 - 3m + 9 \equiv 7 \pmod 8$. □

4. Factorization in Number fields

Although considering Quadratic Residue is quite powerful, it can only prove the Mordell's Equation has no integral solution. Hence some Mordell's Equation with solutions (be it trivial or non-trivial) should not be solved by the trick in simple manner. In order to solve some class of Mordell's Equation with solutions, we are forced to consider factorization again. Consider the Mordell's Equation:

$$y^2 = x^3 + k$$

this time we try to factorized in Number field, i.e.

$$y^2 - k = (y + \sqrt{k})(y - \sqrt{k}) = x^3$$

By similar argument, if the two factors in L.H.S are relatively prime and the Number field $\mathbb{Q}(\sqrt{k})$ are Unique Factorization Domain (UFD)[1], then they are both cubes.

4.1. Results using factorization in Principal Ideal Domain

Let us begin with Proposition 20, illustrating our method.

Proposition 20. *The only integral solution to $y^2 = x^3 - 1$ is $(x, y) = (1, 0)$.*

Proof. Similar to above, we first check the parity of x and y. Suppose x is even, then $y^2 + 1 = x^3 \equiv 0 \pmod 8$. Hence, $y^2 \equiv -1 \pmod 8$. But that is impossible given by Lemma 15. Contradiction. Hence x is odd and so y is even.

We then rewrite the equation as

$$x^3 = y^2 + 1$$

in which when we factorize it in $\mathbb{Z}[i]$, we get

$$x^3 = (y + i)(y - i)$$

We now claim that $y + i$ and $y - i$ are relatively prime. Let δ be a common divisor of them. Since $\delta \mid (y + i) - (y - i) = 2i$, we have $N(\delta) \mid N(2i) = 4$.

Furthermore, $N(\delta) \mid N(y + i) = y^2 + 1 = x^3$ which is odd by its definition, and we deduce that $N(\delta)$ divides 4 and is odd. Hence $N(\delta) = 1$ and δ is a unit in $\mathbb{Z}[i]$, and so $y + i$ and $y - i$ are relatively prime.

Now notice that since they are relatively prime and their product is a cube, each factor must be a cube up to unit multiple, by unique factorization in $\mathbb{Z}[i]$. Moreover, notice that every unit in $\mathbb{Z}[i]$ are cubes, i.e. $1 = 1^3, -1 = (-1)^3, i = (-i)^3, -i = i^3$. Hence the unit multiples can be absorbed into the cubes. Thus, $y + i$ and $y - i$ are both cubes.

Therefore, by the above argument we must have

$$y + i = (m + ni)^3$$

for some $m, n \in \mathbb{Z}$. Expanding the cube and equating real and and imaginary parts, we get

$$y = m^3 - 3mn^2 = m(m^2 - 3n^2), \quad 1 = 3m^2n - n^3 = n(3m^2 - n^2)$$

The equation on the right tells us $n = \pm 1$. We separate into two cases: If $n = 1$, then $1 = 3m^2 - 1 \implies 3m^2 = 2$, which has no integral solutions. If $n = -1$, then $1 = -(3m^2 - 1) \implies m = 0$. Therefore $y = 0$ and $x^3 = y^2 + 1 = 1$. Thus $x = 1$.

Hence the only integral solution to $y^2 = x^3 - 1$ is $(x, y) = (1, 0)$. □

[1] In this project, we would not deal with non-principal ideal domain.

Theorem 21. *Given that p is a prime such that $p \equiv 3 \pmod 4$, all solutions of equation $y^2 = x^3 - p^2$ are given below:*

1. *If there exist $m \in \mathbb{N}$ such that $p = 3m^2 - 1$, then the only 2 solutions are $(x, y) = (m^2 + 1, \pm(m^3 - 3m))$.*
2. *If there exist $m \in \mathbb{N}$ such that $p^2 = 3m^2 + 1$, then the only 2 solutions are $(x, y) = (4m^2 + 1, \pm(8m^3 + 3m))$.*

These two cases are mutually exclusive and if p are not one of the cases, it will have no solutions.

Proof. Before we factorize the equation, notice that by taking the equation modulo 4, i.e. $y^2 \equiv x^3 - p^2 \equiv x^3 - 1$, referencing on the parity argument of Proposition 17, we have y is even and x is odd.

We factorize the equation into $x^3 = (y + pi)(y - pi)$. We want to show that $y + pi$ and $y - pi$ are relatively prime.

Let δ be a common divisor of $y + pi$ and $y - pi$. Then $\delta \mid (y + pi) - (y - pi) = 2pi$ and $\delta \mid (y + pi) + (y - pi) = 2y$. $N(\delta) | N(2pi) = 4p^2$. At the same time, $N(\delta) \mid N(y + pi) = y^2 + p^2 = x^3 \equiv 1 \pmod 2$. Hence $N(\delta)$ is odd. Hence the only possibilities of $N(\delta)$ is $1, p$ and p^2. We have to rule out the possibility of p and p^2.

Write $\delta = a + bi$, where $a, b \in \mathbb{Z}$. If $N(\delta) = p$, then $p = a^2 + b^2$. However as $p \equiv 3 \pmod 4$, so it cannot be written sum of two squares. Hence we derive a contradiction.

Similar holds to the case of p^2, we have $a^2 + b^2 = p^2$. By the famous Pythagorean triple generator, we have a pair of integer m and n with a scale factor g such that $a = g(m^2 - n^2), b = g(2mn)$ and $p = g(m^2 + n^2)$. Now we have $g = 1$ or p.

If $g = 1$ then we have $m^2 + n^2 = p$. As $p \equiv 3 \pmod 4$, it cannot be written as sum of two squares, so the case is impossible.

If $g = p$, we have $\delta = p$ (or pi, which only have a difference of unit). Hence we have p divides both x and y. Write $x = pu$ and $y = pv$ we obtain,

$$v^2 = pu^3 - 1$$

However by modulo p, we have -1 is a quadratic residue modulo p, which is impossible as $p \equiv 3 \pmod 4$ by Lemma 15.

Hence we also derive a contradiction. This left to $N(\delta) = 1$, which is a unit.

With a similar argument as above, every unit in $\mathbb{Z}[i]$ are cubes, and so $y + pi$ and $y - pi$ are both cubes.

We can write

$$y + pi = (m + ni)^3$$

for some $m, n \in \mathbb{Z}$ now. Equating real and imaginary parts, we get

$$y = m(m^2 - 3n^2), \quad p = n(3m^2 - n^2).$$

We consider the latter equation, i.e. $p = n(3m^2 - n^2)$. Since n is a factor of p, we know that $n = \pm 1, \pm p$ as p is a prime. We will closely analyze this four cases separately.

Case of $n = -1$: We have $3m^2 = -p + 1$. But this is impossible as $p > 2 \implies -p + 1 < 0$ which cannot be a positive multiple of a square.

Case of $n = 1$: We have $n = 1$ and $3m^2 = p + 1$, hence p can be written as the form $3m^2 - 1$, then we have $y = m(m^2 - 3)$, and $x^3 = y^2 + p^2 = (m^3 - 3m)^2 + (3m^2 - 1)^2 = (m^2 + 1)^3$, hence if $p = 3m^2 - 1$, then we obtain solution $(x, y) = (m^2 + 1, \pm(m^3 - 3m))$. Notice if p can be written in this form, we have 2 solutions.

Case of $n = p$: We have $3m^2 = p^2 + 1$. This cannot be achieved as -1 is not a quadratic residue modulo 3 by Lemma 15.

Case of $n = -p$: We have $p^2 = 3m^2 + 1$. If p can be written as this form, then $y = -8m^3 - 3m$ and $x = 4m^2 + 1$. Hence we have the solution $(x, y) = (4m^2 + 1, \pm(8m^3 + 3m))$. We have 2 solutions.

We now prove that the two cases are mutually exclusive. Assume not, we have $p^2 = (3m_1^2 - 1)^2 = 3m_2^2 + 1$, then $m_1^2(3m_1^2 - 2) = m_2^2$, which means that $3m_1^2 - 2$ is a square. Write $h^2 = 3m_1^2 - 2$. Notice that $p = 3m_1^2 - 1$. Hence we have $p = h^2 + 1$, which cannot be represented by a sum of two squares. Hence we derive a contradiction. □

The above theorem can be further generalized to the proposition below:

Proposition 22. *Given that p, q are distinct primes such that $p, q \equiv 3 \pmod 4$, all solutions of equation $y^2 = x^3 - (pq)^2$ are given below:*

1. *If there exists $m \in \mathbb{N}$ such that $pq = 3m^2 - 1$, then*

$$(x, y) = (m^2 + 1, \pm(m^3 - 3m))$$

are solutions.

2. *If there exists $m \in \mathbb{N}$ such that $p^2 + q = 3m^2$, then*

$$(x, y) = (m^2 + p^2, \pm m(m^2 - 3p^2))$$

are solutions.

3. If there exists $m \in \mathbb{N}$ such that $q^2 + p = 3m^2$, then

$$(x, y) = (m^2 + q^2, \pm m(m^2 - 3q^2))$$

are solutions.

4. If there exists $m \in \mathbb{N}$ such that $(pq)^2 = 3m^2 + 1$, then

$$(x, y) = (4m^2 + 1, \pm(8m^3 + 3m))$$

are solutions.

Proof. Similarly, y is even and x is odd. We have

$$x^3 = (y + pqi)(y - pqi)$$

Let δ be a common divisor of $y+pqi$ and $y-pqi$. Then $\delta \mid (y+pqi)(y-pqi) = 2pqi$ and $\delta \mid (y + pqi) + (y - pqi) = 2y$. We have $N(\delta) \mid N(2pqi) = 4p^2q^2$. At the same time, $N(\delta) \mid N(y + pi) = y^2 + p^2 = x^3 \equiv 1 \pmod 2$. Hence $N(\delta)$ is odd. Hence the only possibilities of $N(\delta)$ is $1, p, p^2, q, pq, q^2, p^2q, pq^2$ and p^2q^2. We rule out the possibilities of the rest by similar argument. Hence $y + pqi$ and $y - pqi$ are both cubes. Write

$$y + pqi = (m + ni)^3$$

for some $m, n \in \mathbb{Z}$. Equating real and imaginary parts, we get

$$y = m(m^2 - 3n^2), \quad pq = n(3m^2 - n^2)$$

We have $n = \pm 1, \pm p, \pm q$ and $\pm pq$.

Case of $n = -1$: We have $3m^2 = -pq + 1$. But this is impossible as $pq > 2 \implies -pq + 1 < 0$ which cannot be a positive multiple of a square.

Case of $n = 1$: We have $3m^2 = pq + 1$, hence pq can be written as the form $3m^2 - 1$, then we have $y = m(m^2 - 3)$, and $x^3 = y^2 + (pq)^2 = (m^3 - 3m)^2 + (3m^2 - 1)^2 = (m^2 + 1)^3$, hence if $pq = 3m^2 - 1$, then we obtain solution $(x, y) = (m^2 + 1, \pm(m^3 - 3m))$. Notice if pq can be written in this form, we have 2 solutions.

Case of $n = p$ and $n = q$: We have $3m^2 = p^2 + q$, if it can be written as this form, we have $y = m(m^2 - 3p^2)$ and $x = m^2 + p^2$. Hence we will have $(x, y) = (m^2 + p^2, \pm m(m^2 - 3p^2))$. Similarly, if $p + q^2$ can be rewritten as $3n^2$, then we have $(x, y) = (n^2 + q^2, \pm n(n^2 - 3q^2))$.

Case of $n=-p$ and $n=-q$: We have $3m^2=p^2-q$. Consider the equation modulo 4, we have $3m^2\equiv 3^2-3\equiv 2 \pmod 4$, which is impossible.

Case of $n=pq$: We have $(pq)^2+1=3m^2$, which cannot be achieved considering modulo 4.

Case of $n=-pq$: We have $(pq)^2-1=3m^2$. If pq can be written as this form, then $y=-8m^3-3m$ and $x=4m^2+1$. Hence we have the solution $(x,y)=(4m^2+1,\pm(8m^3+3m))$.

□

[See reviewer's comment (3)]

We bravely proceed to a more terrible case.

Theorem 23. *Given that $p_1,p_2,\dots,p_j$ are distinct primes such that $p_i\equiv 3 \pmod 4$ for all $1\le i\le j$, all solutions of the equation $y^2=x^3-k^2$, where $k=p_1p_2\dots p_j$ are given below:*

If there exists $m\in\mathbb{N}$ and $n=\pm p_1^{a_1}p_2^{a_2}\dots p_j^{a_j}$, where $a_i\in\{0,1\}$ for all $1\le i\le j$ such that

$$3m^2=\frac{k}{n}+n^2,$$

then $(x,y)=(m^2+n^2,\pm m(m^2-3n^2))$ are solutions.

Proof. We still have y is even and x is odd. We have

$$x^3=(y+ki)(y-ki)$$

Let δ be a common divisor of $y+ki$ and $y-ki$. Then $\delta\mid(y+ki)-(y-ki)=2ki$ and $\delta\mid(y+ki)+(y-ki)=2y$. We have $N(\delta)\mid N(2ki)=4p_1^2p_2^2\dots p_j^2$. At the same time, $N(\delta)\mid N(y+ki)=y^2+k^2=x^3\equiv 1 \pmod 2$. Hence $N(\delta)$ is odd. Hence the only possibilities of $N(\delta)$ is $p_1^{a_1}p_2^{a_2}\dots p_j^{a_j}$, where $a_i\in\{0,1,2\}$ for all $1\le i\le j$. We have to rule out all possibilities except 1.

If there exists $1\le i\le j$ such that a_i is odd, then it cannot be represented by a sum of two squares.

If it is not the case, then a_i is even for all $1\le i\le j$. Let $N(\delta)=a^2+b^2$. We use Pythagorean triple generator again for this situation. We have a pair of integers α and β with a scale factor g such that $a=g(\alpha^2-\beta^2), b=g(2\alpha\beta)$ and $\sqrt{N(\delta)}=g(\alpha^2+\beta^2)$. If g is composed of even powers of primes, then $\frac{\sqrt{N(\delta)}}{g}$ cannot be represented by a sum of two squares. Hence g must be composed of odd powers of primes.

Then we have $g \mid x$ and $g \mid y$. Write $x = gx_1$ and $y = gy_1$. We obtain:

$$y_1^2 = gx_1^3 - \frac{k^2}{g^2}$$

Consider modulo prime p which is $p \mid g$, we obtain a contradiction. Hence $y + ki$ and $y - ki$ are both cubes. Write

$$y + ki = (m + ni)^3$$

for some $m, n \in \mathbb{Z}$. Equating real and imaginary parts, we get

$$y = m(m^2 - 3n^2), \quad k = n(3m^2 - n^2).$$

We have $n = \pm p_1^{a_1} p_2^{a_2} \dots p_j^{a_j}$, where $a_i = 0, 1$ for all $1 \leq i \leq j$ and the result follows. □

This ends our results. However, we cannot solve for the case $p \equiv 1 \pmod 4$. We propose a conjecture for this matter:

Conjecture 24. *Given that p is a prime such that $p \equiv 1 \pmod 4$, all solutions of equation $y^2 = x^3 - p^2$ are given below:*

1. *If there exist $m \in \mathbb{N}$ such that $p = m^2 + 1$, then the only 2 solutions are $(x, y) = (p, pm)$.*
2. *If there exist $m \in \mathbb{N}$ such that $p^2 = 3m^2 + 1$, then the only 2 solutions are $(x, y) = (4m^2 + 1, \pm(8m^3 + 3m))$.*

These two cases are mutually exclusive and if p is not in one of the cases, it will have no solution.

[See reviewer's comment (4)]

5. Conclusion

In this project, we have discussed two main classical approaches, factorizing in number fields and Quadratic Reciprocity method.

In the first section, we consider the case of $k = 4^n$, for $n \in \mathbb{N}$. We reduce the equation into the cases $k = 1, 4, 16$ and successfully obtain all solutions.

In the second section, we consider congruence and quadratic residue to prove a certain set of k have no integral solutions, as presented in Proposition 16 to 19.

In the last section, we consider factorizing in number field, and we solved the case when $k = -p^2$, where p is a prime congruent to 1 modulo 4.

REFERENCES

[1] J. E. Cremona, *Algorithm for Modular Elliptic Curves*, (1997) 62-103.

[2] K. Conrad, *Trace and Norm*, 1-11

[3] A. Baker, *On the representation of integers by binary forms*, Philos. Trans. A 263 (1968) 173-208

[4] P. Mihailescu, *On Catalan's Conjecture* (2002) 1-2.

[5] E. Chen, *An Infinitely Large Napkin.* (2017) 379-395.

[6] K. Conrad, *Examples of Mordell's equation.* 1-11.

Reviewer's Comments

The aim of this paper is to investigate the solutions of the Mordell's equation $y^2 = x^3 + k$ for some special classes of k. The first section is an introduction. The second section uses basic number theory, together with a result of Mihailescu. (The reviewer was unable to find the reference [4] with the exact title.) He also made use of the law of quadratic reciprocity in Section 3. For the results in Section 4, the main tool is the unique factorization in the ring of Gaussian integers $\mathbb{Z}[i]$.

This paper is well-written and the results are correct as far as the reviewer can tell. Regarding the originality of this paper, a search of the reference articles shows that this paper is based on the paper by K. Conrad (reference [6] in the paper), in which a number of explicit numerical examples of the Mordell equation are worked out. Nevertheless, the author was able to generalize these examples and carried out detailed analysis in a number of cases. The methods are somewhat ad-hoc and it is desired that a more systematic viewpoint can be applied to study or classify this equation. Nevertheless, this is nice work for a high school student and the reviewer hopes the author will continue the investigation in the future.

Regarding the style, the reviewer has the following comments:

- The references are not cited at all. Only the titles of the papers/books are given but not the publisher information, which makes it hard to locate the exact reference. For example the reviewer was unable to locate the reference [4]. As the references are not cited, it is not clear to me how they are related to this paper (e.g. the reference [5] is an encyclopedia consisting of 600+ pages and it is unclear which section in that paper is relevant).
- Some of the "bigger" results (e.g. Dirichlet's unit theorem, law of quadratic reciprocity and Lemma 15) are not referenced or proved. It is desirable to cite a proper reference for these results.
- There are a number of notations and definitions in Section 1 which are not used in the later sections. For example, "Galois conjugates" are not defined, the symbols $\mathcal{O}_K$, $\mathcal{O}_K^\times$ are also not used at all.
- Since the results are scattered and they are proved in a case-by-case basis, it would be much more helpful if a table is set up to list the different cases of k for easier comparison. The table may look like:

k	**Result**	**All solutions** (x, y)
1	Lemma 12	$(0, \pm 1), (2, \pm 3), (-1, 0)$
4	Lemma 13	$(0, \pm 2)$
$\cdots$	$\cdots$	$\cdots$

There are some typos/mistakes in the paper:

1. The reviewer has comments on the wordings, which have been amended in this paper.

2. In a number of places, it is mentioned that if $p \equiv 3 \pmod 4$, then p cannot be expressed as a sum of squares without further comment. This appears a number of times in the proof of Theorem 21 and also in the proof of Theorem 23. The reviewer thinks it is better to add a lemma similar to Lemma 26 below as a corollary to Lemma 15 to make it clear to the reader.
3. In fact, in the proof of Theorem 22, the proof that $y \pm pqi$ are relatively prime is omitted, and the analogous part in the proof of Theorem 23 looks a bit messy. The reviewer would suggest writing it in a more systematic way similar to Theorem 30 below.
4. Conjecture 24 (1) is not true (and it should read "only 2 solutions are $(x, y) = (p, \pm pm)$. "). A counterexample is $m = 6$ so that $p = 37 = m^2 + 1$ and $p^2 = 1369$. Besides the solutions $(x, y) = (37, \pm 222)$, the pairs $(x, y) = (185, \pm 2516)$ also satisfy $y^2 = x^3 - 1369$.

Below the reviewer will give a proof of a generalization Theorem 23, which in the reviewer's opinion is more systematic than the treatment in the paper.

Notation 25. *$a \equiv_n b$ means $a \equiv b \pmod{\mathrm{n}}$.*

Lemma 26. *If p is a prime such that $p \equiv_4 3$, then $a^2 + b^2 \equiv_p 0$ has only trivial solution $a \equiv_p 0$ and $b \equiv_p 0$.*

Proof. Suppose not, without loss of generality $b \not\equiv_p 0$, then $0 \equiv_p a^2 + b^2$ implies $(ab^{-1})^2 \equiv_p -1$, contradicting $p \equiv_4 3$ (Lemma 15 in the paper). □

By pigeonhole principle and unique factorization, we have

Lemma 27. *If p is an irreducible element such that $p^n | a_1 \cdots a_k$ (in either $\mathbb{Z}$ or $\mathbb{Z}[i]$), then $p^{\lceil \frac{n}{k} \rceil}$ divides one of the a_i.*

Lemma 28. *If $q, a, b \in \mathbb{Z}$ such that $q | a + bi$ or $q | a - bi$, then $q^2 | (a + bi)(a - bi)$.*

Proof. If $q | a + bi$, then taking the conjugate implies $q | a - bi$. The result follows. □

Combining Lemma 27 and Lemma 28,

Lemma 29. *Let p be a prime number with $p \equiv_4 3$. If $p^n | w\overline{w}$ for some $w \in \mathbb{Z}[i]$, then $p^{2\lceil \frac{n}{2} \rceil} | w\overline{w}$.*

Similarly if $p^n | x^3$ for some $x \in \mathbb{Z}$, then $p^{3\lceil \frac{n}{3} \rceil} | x^3$.

Theorem 30 (Generalization of Theorem 23). *Theorem 4.4 is true if $k = p_1^{\beta_1} \cdots p_j^{\beta_j}$ where $\beta_j \in \{1, 2\}$ and p_i are distinct primes with $p_i \equiv_4 3$.*

Outline of the proof. As in the proof in the paper, the keypoint is the following **Claim**: $y + p_1^{\beta_1} \cdots p_j^{\beta_j} i$ and $y - p_1^{\beta_1} \cdots p_j^{\beta_j} i$ are relatively prime.

Reason: Suppose there exists an irreducible (which is non-unit by definition) common factor $\delta = a + bi$ of $y + p_1^{\beta_1} \cdots p_j^{\beta_j} i$ and $y + p_1^{\beta_1} \cdots p_j^{\beta_j} i$.

As in the paper, $\delta | 2p_1^{\beta_1} \cdots p_j^{\beta_j}$ implies $N(\delta)$ is of the form $p_1^{\gamma_1} \cdots p_j^{\gamma_j}$ where one of the γ_i is ≥ 1. But $\delta\overline{\delta}$ is the unique factorization of $N(\delta)$ in $\mathbb{Z}[i]$ and regarding $p_i \in \mathbb{Z}[i]$, we conclude that $N(\delta)$ is either p_i or p_i^2 for some i. Without loss of generality, $N(\delta) = p_1$ or $N(\delta) = p_1^2$. Let $q = p_2^{\beta_2} \cdots p_j^{\beta_j}$ and write $p = p_1$, $\beta = \beta_1$. Then from the above, $a^2 + b^2 \equiv_p 0$. By Lemma 26, $p|a$ and $p|b$. But then by irreducibility this is only possible if $\delta = \pm p$ or $\pm pi$. So we have

$$\begin{aligned}
&p|y \\
\Rightarrow &p^2|y^2 + p^{2\beta}q^2 = x^3 \\
\Rightarrow &p^3|x^3 = (y + p^\beta qi)(y - p^\beta qi) && \text{(Lemma 29)} \\
\Rightarrow &p^4|(y + p^\beta qi)(y - p^\beta qi) = x^3 && \text{(Lemma 29)} \\
\Rightarrow &p^6|x^3 = (y + p^\beta qi)(y - p^\beta qi) && \text{(Lemma 29)} \\
\Rightarrow &p^3|y + p^\beta qi \text{ or } p^3|y - p^\beta qi && \text{(Lemma 27)}
\end{aligned}$$

In both cases, by considering the imaginary part we have $p^3|p^\beta q$ which is impossible as $\beta \leq 2$.

The rest of the proof is similar to Theorem 23. □