KYUNGPOOK Math. J. 55(2015), 587-595
http://dx.doi.org/10.5666/KMJ.2015.55.3.587
pISSN 1225-6951 eISSN 0454-8124
© Kyungpook Mathematical Journal

The Diophantine Equation $ax^6 + by^3 + cz^2 = 0$ in Gaussian Integers

Farzali Izadi and Foad Khoshnam*
Department of Mathematics, Faculty of Science, Urmia university, Urmia 165-57153, Iran
e-mail : f.izadi@urmia.ac.ir *and* khoshnam@azaruniv.edu

Abstract. In this article, we will examine the Diophantine equation $ax^6 + by^3 + cz^2 = 0$, for arbitrary rational integers a, b, and c in Gaussian integers and find all the solutions of this equation for many different values of a, b, and c. Moreover, two equations of the type $x^6 \pm iy^3 + z^2 = 0$, and $x^6 + y^3 \pm \omega z^2 = 0$ are also discussed, where i is the imaginary unit and ω is a third root of unity.

1. Introduction

The fundamental problem when studying a given diophantine equation is whether a solution exists, and, in the case of existence, how many solutions are there and how one can find them.

The diophantine equations of the type $ax^p + by^q + cz^r = 0$ are called super-Fermat equations which is one of the most well-known diophantine equations. Simple heuristic reasoning shows that if $1/p+1/q+1/r < 1$, we expect only a finite number of solutions up to a reasonable notion of equivalence, and if $1/p+1/q+1/r > 1$, we expect infinitely many solutions. The intermediate case $1/p + 1/q + 1/r = 1$ reduces to the study of elliptic curves, and the existence or not of solutions essentially depends on the rank of the curve and its torsion subgroup. lt is clear that up to permutation of p, q, and r we have $(p, q, r) = (3, 3, 3), (4, 4, 2)$, or $(6, 3, 2)$ (see section 6.5 of [1]).

The cases $(p, q, r) = (3, 3, 3)$ and $(4, 4, 2)$ have studied in Gaussian integers recently.

* Corresponding Author.

Received July 16, 2014; accepted February 21, 2015.
2010 Mathematics Subject Classification: Primary 14D25; Secondary 11D41, 11G05.
Key words and phrases: Diophantine equations, Gaussian integers, Elliptic curves, ranks, torsion group.

For the case of $(p,q,r) = (4,4,2)$, F. Najman [6] showed that The equation $x^4 - y^4 = iz^2$ has only trivial solutions in Gaussian integers and the only non-trivial solutions satisfying $\gcd(x,y,z) = 1$ in Gaussian integers of the equation $x^4 + y^4 = iz^2$ are (x,y,z), where $x,y \in \{\pm i, \pm 1\}$ and $z = \pm i(1+i)$.
Also for the case of $(p,q,r) = (3,3,3)$, E. Lampakis [3], showed that in the ring of Gaussian integers $\mathbb{Z}[i]$, the solutions of the Diophantine equation $x^3 + y^3 = z^3$ are trivial, namely, $xyz = 0$. It is thus natural to study the last case here, i.e., $ax^6 + by^3 + cz^2 = 0$, where a, b, and c are arbitrary rational integers.

For an elliptic curve E over a number field $\mathbb{K}$, it is well known, by the Mordell-Weil theorem, that the set $E(\mathbb{K})$ of $\mathbb{K}$-rational points on E is a finitely generated abelian group. The group $E(\mathbb{K})$ is isomorphic to $T \oplus \mathbb{Z}^r$, where r is a non-negative integer and T is the torsion subgroup. We will be interested in the case when $\mathbb{K} = \mathbb{Q}(i)$. We will work only with elliptic curves with rational coefficients and by a recent result of Najman (see [7]), if an elliptic curve has rational coefficients, then the torsion of the elliptic curve over $\mathbb{Q}(i)$ is either cyclic group of order m, where $1 \leq m \leq 10$ and $m = 12$, or of the form $\mathbb{Z}_2 \oplus \mathbb{Z}_{2m}$, where $1 \leq m \leq 4$, or $\mathbb{Z}_4 \oplus \mathbb{Z}_4$.

In order to determine the torsion subgroup of $E(\mathbb{Q}(i))$, we use the extended Lutz-Nagell theorem [9], which is a generalization of the Lutz-Nagell theorem from$E(\mathbb{Q})$ to $E(\mathbb{Q}(i))$. Therefore throughout this article, the following extension of the Lutz-Nagell theorem is used to compute the torsion groups of elliptic curves.

Theorem 1.1. *Let $E : y^2 = x^3 + Ax + B$*
with $A, B \in \mathbb{Z}(i)$. If a point $(x,y) \in E(\mathbb{Q}(i))$ has finite order, then

1. *Both $x, y \in \mathbb{Z}[i]$, and*
2. *Either $y = 0$ or $y^2 | 4A^3 + 27B^2$.*

It is well-known (see e.g. [10]) that if an elliptic curve E is defined over $\mathbb{Q}$, then the rank of E over $\mathbb{Q}(i)$ is given by

$$rank(E(\mathbb{Q}(i))) = rank(E(\mathbb{Q})) + rank(E_{-1}(\mathbb{Q}))$$

where E_{-1} is the (-1)-*twist* of E over $\mathbb{Q}$. We use it during the proofs of this article.

2. New Results

We star off with some definitions.

Definition 2.1.(Trivial Solution) The solution (x,y,z) of the equation $ax^6 + by^3 + cz^2 = 0$ is called trivial if $xyz = 0$.

Definition 2.2.(Twisted Projective Equivalence) We will say that two nonzero Gaussian rational solutions (x,y,z) and (x',y',z') of the equation $ax^6+by^3+cz^2 = 0$

are the same under twisted projective equivalence if there exists $\lambda \in \mathbb{Q}^*(i)$ such that $x' = \lambda x, y' = \lambda^2 y, z' = \lambda^3 z$.

We note that there is a one-to-one correspondence between the nonzero Gaussian rational solutions of $ax^6 + by^3 + cz^2 = 0$ up to twisted projective equivalence and the nonzero points of

$$E: \quad Y^2Z = X^3 - ab^2c^3Z^3,$$

where the point $(0, -bc, b^2c)$ corresponds to the zero point $\mathcal{O}$ on E. More precisely, we have the following mutually inverse correspondences

$$(2.1) \qquad \begin{aligned} (x, y, z) &\mapsto (X, Y, Z) = (-bcxy, bc^2z, x^3). \\ (X, Y, Z) &\mapsto (x, y, z) = (bcZ, -bcXZ, b^2cYZ^2). \end{aligned}$$

It follows that our equation has a solution with nonzero x if and only if either the curve E has nonzero rank, in which case it has infinitely many inequivalent solutions, or if E has nontrivial torsion.

To see this, we divide the equation $ax^6+by^3+cz^2 = 0$ by x^6 and do the variable change $r = -y/x^2$, $s = z/x^3$, to get $cs^2 = br^3-a$. Multiplying this equation by b^2c^3, we obtain $b^2c^4s^2 = b^3c^3r^3-ab^2c^3$. Again with a variable change $X = bcr$, $Y = bc^2s$, we get the equation defining the required elliptic curve $E : Y^2 = X^3 - ab^2c^3$, which is the affine model of the above projective curve. Now we are ready to state our main results.

Theorem 2.3. *For the diophantine equation $ax^6 + by^3 + cz^2 = 0$, where a, b, and c are rational integers, the followings hold .*

1. *If $-ab^2c^3 = m^6$ is a sixth power, the only nontrivial solutions in Gaussian integers of the equation $ax^6 + by^3 + cz^2 = 0$ under twisted projective equivalence are $(bc, -2bcm^2, \pm 3b^2cm^3)$.*

2. *If $ab^2c^3 = m^6$ is a sixth power, the only nontrivial solutions in Gaussian integers of the equation $ax^6 + by^3 + cz^2 = 0$ under twisted projective equivalence are $(bc, 2bcm^2, \pm 3ib^2cm^3)$.*

Proof. (1) Suppose (x, y, z) be a nontrivial solution. If $-ab^2c^3 = m^6$ is a sixth power with the correspondent relation (2.1), we obtain the equation defining the elliptic curve

$$E : Y^2 = X^3 + m^6,$$

with $X, Y \in \mathbb{Q}(i)$. This curve is isomorphic to

$$E' : Y'^2 = X'^3 + 1,$$

with $X', Y' \in \mathbb{Q}(i)$, where $X' = X/m^2$ and $Y' = Y/m^3$. Therefore to obtain the torsion subgroup of E over $\mathbb{Q}(i)$ we look for the torsion subgroup of E' over $\mathbb{Q}(i)$.

From the extended Lutz-Nagell theorem for E', we have $4A^3 + 27B^2 = 27$. Then for any torsion point $\infty \neq (X', Y') \in E'(\mathbb{Q}(i))$ the possibilities for Y' are

$$0, \qquad \pm 1, \qquad \pm i, \qquad \pm 3, \qquad \pm 3i.$$

Substituting each Y' into the equation, we obtain the "possible" torsion points as

$$(-1, 0), \qquad (0, \pm 1), \qquad (2, \pm 3).$$

Clearly $(-1, 0)$ has order 2. Also it can be checked that each of the points $(0, \pm 1)$ has order 3, and each of the points $(2, \pm 3)$ has order 6. Thus the torsion subgroup of $E'(\mathbb{Q}(i))$ in this case is

$$\{\infty, \qquad (-1, 0), \qquad (0, \pm 1), \qquad (2, \pm 3)\},$$

which is indeed a cyclic group of order 6. Since $E'(\mathbb{Q}(i))_{tors} = \mathbb{Z}/6\mathbb{Z}$, therefore $E(\mathbb{Q}(i))_{tors}$ is $\mathbb{Z}/6\mathbb{Z}$ with the torsion points

$$\{\infty, \qquad (-m^2, 0), \qquad (0, \pm m^3), \qquad (2m^2, \pm 3m^3)\}.$$

Obviously the points $(-m^2, 0)$ and $(0, \pm m^3)$ lead to trivial solutions. But the point $(2m^2, \pm 3m^3)$, by the correspondences (2.1) leads us to the solutions $(bc, -2bcm^2, \pm 3b^2cm^3)$. Now the only thing that we need to prove that $rank(E(\mathbb{Q}(i))) = 0$.
It is clear that (-1)-*twist* of E' over $\mathbb{Q}$ is

$$E'_{-1} : Y^2 = X^3 - 1.$$

Using the Mwrank program [2], we see that the rank of the curves E' and E'_{-1} are 0. These imply that the rank of the curves E and E_{-1} are also 0. Therefore $rank(E(\mathbb{Q}(i))) = 0$.

(2) The proof for this case is similar. □

Corollary 2.4. *For some specific values of the parameters, the solutions in the Gaussian integers of the equation $ax^6 + by^3 + cz^2 = 0$, are:*

1. *The only nontrivial solutions of the equation $x^6 + y^3 = z^2$ under twisted projective equivalence are $(-1, 2, \pm 3)$.*

2. *The only nontrivial solutions of the equation $x^6 + y^3 = -z^2$ under twisted projective equivalence are $(1, 2, \pm 3i)$.*

3. *The only nontrivial solutions of the equation $x^6 \pm iy^3 + z^2 = 0$, under twisted projective equivalence are $(\pm i, \pm 2i, \pm 3)$.*

4. *The only nontrivial solutions of the equation* $x^6 + y^3 = -\omega z^2$ *under twisted projective equivalence are* $(\omega, 2\omega, \pm 3i\omega)$.

5. *The only nontrivial solutions of the equation* $x^6 + y^3 = \omega z^2$ *under twisted projective equivalence are* $(-\omega, 2\omega, \pm 3\omega)$.

Theorem 2.5. *For the diophantine equation* $ax^6 + by^3 + cz^2 = 0$*, where* a*,* b*, and* c *are rational integers, the followings hold.*

1. *If* $-ab^2c^3/432 = m^6$ *is a sixth power, the only nontrivial solutions in Gaussian integers of the equation* $ax^6 + by^3 + cz^2 = 0$ *under twisted projective equivalence are* $(bc, 12bcm^2, \pm 36ib^2cm^3)$.

2. *If* $ab^2c^3/432 = m^6$ *is a sixth power, the only nontrivial solutions in Gaussian integers of the equation* $ax^6 + by^3 + cz^2 = 0$ *under twisted projective equivalence are* $(bc, -12bcm^2, \pm 36b^2cm^3)$.

Proof. (1) Suppose (x, y, z) be a nontrivial solution. If $-ab^2c^3/432 = m^6$ is a sixth power, with the correspondent relation (2.1), we obtain the equation defining the elliptic curve

$$E : Y^2 = X^3 + 432m^6,$$

with $X, Y \in \mathbb{Q}(i)$. This curve is isomorphic to

$$E' : Y'^2 = X'^3 + 432,$$

with $X', Y' \in \mathbb{Q}(i)$, where $X' = X/m^2$ and $Y' = Y/m^3$. Therefore to obtain the torsion subgroup of E over $\mathbb{Q}(i)$, we look for the torsion subgroup of E' over $\mathbb{Q}(i)$. From the extended Lutz-Nagell theorem for E', we have $4A^3 + 27B^2 = 5038848$. Then for any torsion point $\infty \neq (X', Y') \in E'(\mathbb{Q}(i))$, it can be checked that Y' must be one of the followings:

$$0, \quad , \pm\varepsilon, \quad , \pm\varepsilon i, \quad , \pm\varepsilon_1(i+1), \quad , \pm\varepsilon_1(i-1),$$

where ε runs over all elements of the set

$$\begin{aligned} \Omega =& \{1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 24, 27, 36, 48, 54, \\ & 72, 81, 108, 144, 162, 216, 324, 432, 648, 1296\}. \end{aligned} \tag{2.2}$$

and ε_1 runs over all the elements of the set Ω mines the numbers $\{16, 48, 144, 432, 1296\}$. By solving directly for $x \in \mathbb{Z}$ (with some help from the Maple software), we obtain all the possible torsion points as

$$(-12, \pm 36i).$$

Each of these points has order 3. Thus the torsion subgroup of $E'(\mathbb{Q}(i))$ in this case is

$$\{\infty, \qquad (-12, \pm 36i)\}.$$

Since $E'(\mathbb{Q}(i))_{tors} = \mathbb{Z}/3\mathbb{Z}$, then $E(\mathbb{Q}(i))_{tors}$ is $\mathbb{Z}/3\mathbb{Z}$ with the torsion points

$$\{\infty, \qquad (-12m^2, \pm 36m^3 i)\}.$$

The point $(-12m^2, \pm 36m^3 i)$, by the correspondences (2.1) lead us to the solutions $(bc, 12bcm^2, \pm 36b^2cim^3)$. Now the only thing that we need to prove that $rank(E(\mathbb{Q}(i))) = 0$.
It is clear that (-1)-*twist* of E' over $\mathbb{Q}$ is

$$E'_{-1} : Y^2 = X^3 - 432.$$

Using the Mwrank program [2], we see that the rank of curves E' and E'_{-1} are 0. These imply that the rank of curves E and E_{-1} are also 0. Therefore
$rank(E(\mathbb{Q}(i))) = 0$.

(2) The proof for this case is similar. □

Corollary 2.6. *For some specific values of the parameters, the solutions in the Gaussian integers of the equation* $ax^6 + by^3 + cz^2 = 0$, *are:*

1. *The only nontrivial solutions of the equation* $-4x^6 + 2y^3 + 3z^2 = 0$ *under twisted projective equivalence are* $(6, 72, \pm 2i \times 6^3)$.

2. *The only nontrivial solutions of the equation* $3x^6+6y^3+2z^2 = 0$ *under twisted projective equivalence are* $(12, -144, \pm 2 \times 6^4)$.

3. Infinitely many Solution

From (2.1) it is obvious that the equation $ax^6 + by^3 + cz^2 = 0$ has infinitely many solutions up to twisted projective equivalence if and only if E has nonzero rank. On the other hand, if the rank is zero then there is either finitely many solutions up to twisted projective equivalence or only trivial solutions. In this section, we will show that unlike the above cases the results can be different for the different values of the rational integers a, b, and c. We distinguish the following cases.

Case 1. Let $\pm ab^2c^3$ be square free, then we should have $b = c = 1$, and $E : Y^2 = x^3 - a$. For example for the values of $a = 6, 3, 2, 26$, and $5^6 + 16 \times 6^6 = 762121$, the corresponding elliptic curves all have trivial torsion subgroup but ranks $0, 1, 2, 3$, and ≥ 4 respectively, (see the table 1). It follows that the corresponding diophantine equations have the trivial solution for the first and infinitely many solutions for the others in Gaussian integers.

Case 2. Let $\pm a/c = m^2$ be a square and not a sixth power, then the corresponding elliptic curve is $E : Y^2 = X^3 \mp d^2$, where $d = bmc^2$. Let $b = c = 1$ and $m = 4$, then we get $E : y^2 = x^3 - 16$. It has rank 0 and torsion subgroup of order 3. If $b = c = 1$ and $m = 2$, then we get $E : y^2 = x^3 - 4$. It has rank 1 and torsion subgroup of order 3. For the other values of the parameters see the table 1. Again we see that the diophantine equation can have either finite or infinitely many solutions in Gauusian integers.

case 3. Let $-a/b = m^3$ be a cube and not a sixth power, then the corresponding elliptic curve is $Y^2 = X^3 + d^3$, where $d = bmc$.
In this case, we see that for the values of $d = 27, 8, 6, 30$, the corresponding elliptic curves all have torsion subgroup of order 2 and ranks $0, 1, 1, 1$, respectively. Therefore the diophantine equation has finitely many solutions in the first case and infinitely many solutions in the last three cases.

Table 1: $Y^2 = X^3 + AX + B$

n	[A,B]	Torsion over $\mathbb{Q}(i)$	Torsion point	Rank over $\mathbb{Q}$	Generation
1	$[0, 2]$	trivial	$\mathcal{O}$	1	[-1:1:1]
2	$[0, -2]$	trivial	$\mathcal{O}$	1	[3:5:1]
3	$[0, 3]$	trivial	$\mathcal{O}$	1	[1:2:1]
4	$[0, -3]$	trivial	$\mathcal{O}$	0	-
5	$[0, 4]$	$\mathbb{Z}/3\mathbb{Z}$	[0,-2]	0	-
6	$[0, -4]$	$\mathbb{Z}/3\mathbb{Z}$	[0,2i]	1	[2:2:1]
7	$[0, 6]$	trivial	$\mathcal{O}$	0	-
8	$[0, -6]$	trivial	$\mathcal{O}$	0	-
9	$[0, 8]$	$\mathbb{Z}/2\mathbb{Z}$	[-2,0]	1	[1:3:1]
10	$[0, -8]$	$\mathbb{Z}/2\mathbb{Z}$	[2,0]	0	-
11	$[0, 9]$	$\mathbb{Z}/3\mathbb{Z}$	[0,-3]	1	[-2:1:1]
12	$[0, -9]$	$\mathbb{Z}/3\mathbb{Z}$	[0,-3i]	0	-
13	$[0, 16]$	$\mathbb{Z}/3\mathbb{Z}$	[0,-4]	0	-
14	$[0, -16]$	$\mathbb{Z}/3\mathbb{Z}$	[0,-4i]	0	-
15	$[0, 25]$	$\mathbb{Z}/3\mathbb{Z}$	[0,5]	0	-
16	$[0, -25]$	$\mathbb{Z}/3\mathbb{Z}$	[0,5i]	1	[5:10:1]

Continued on next page

Table 1 - continued from previous page

n	[A,B]	Torsion over $\mathbb{Q}(i)$	Torsion point	Rank over $\mathbb{Q}$	Generation
17	$[0, 26]$	trivial	$\mathcal{O}$	1	[-1:5:1]
18	$[0, -26]$	trivial	$\mathcal{O}$	2	[3:1:1],[35:207:1]
19	$[0, 27]$	$\mathbb{Z}/2\mathbb{Z}$	[-3,0]	0	-
20	$[0, -27]$	$\mathbb{Z}/2\mathbb{Z}$	[3,0]	0	-
21	$[0, 5^6 + 16 \times 6^6]$	trivial	$\mathcal{O}$	4	[-60:739:1],[-58:753:1], [-25:864:1],[2:873:1]
22	$[0, -(5^6 + 16 \times 6^6)]$	trivial	$\mathcal{O}$	$0 \leq r \leq 4$	-
23	$[0, (3 \times 49)^2]$	$\mathbb{Z}/3\mathbb{Z}$	$[0, -147]$	1	[-12:141:1]
24	$[0, -(3 \times 49)^2]$	$\mathbb{Z}/3\mathbb{Z}$	$[0, -147i]$	$0 \leq r \leq 2$	-
25	$[0, (3 \times 5 \times 49)^2]$	$\mathbb{Z}/3\mathbb{Z}$	$[0, -735]$	0	-
26	$[0, -(3 \times 5 \times 49)^2]$	$\mathbb{Z}/3\mathbb{Z}$	$[0, -735i]$	1	$[\frac{1694915427}{41781923}:\frac{-339987829040}{41781923}:1]$
27	$[0, 6^3]$	$\mathbb{Z}/2\mathbb{Z}$	$[-6, 0]$	0	-
28	$[0, -6^3]$	$\mathbb{Z}/2\mathbb{Z}$	$[6, 0]$	1	[10:28:1]
29	$[0, 30^3]$	$\mathbb{Z}/2\mathbb{Z}$	$[-30, 0]$	0	-
30	$[0, -30^3]$	$\mathbb{Z}/2\mathbb{Z}$	$[30, 0]$	1	[2838:28756:27]

References

[1] H. Cohen, *Number Theory Volume I: Tools and Diophantine Equations*, Graduate Texts in Mathematics 239, Springer-Verlag, ISBN 978-0-387-49922-2. page 389.

[2] J. Cremona, *mwrank program*, Available at http://maths.nottingham.ac.uk/personal /jec/ftp/progs/.

[3] E. Lampakis, *In Gaussian integers, $x^3 + y^3 = z^3$ has only trivial solutions*, Elec. J. Comb. N. T, **8**(2008), #A32.

[4] M. A. Kenku, F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J., **109**(1988), 125-149.

[5] T. Nagell, *Introduction to number theory*, Chelsea Publ. Comp., New York, 1981.

[6] F. Najman, *The diophantine equation $x^4 \pm y^4 = iz^2$ in Gaussian integers*, Amer. Math. Monthly, **117**(2010), 637-641.

[7] F. Najman, *Torsion of elliptic curves over quadratic cyclotomic fields*, Math. J. Okayama Univ..

[8] F. Najman, *Complete classification of torsion of elliptic curves over quadratic cyclotomic fields*, J. Number Theory.

[9] J. H. Silverman and J. Tate, *Rational points on elliptic curves*, Undergraduate Texts in Mathemathics, Springer-Verlag, New York, 1992.

[10] U. Schneiders and H. G. Zimmer, *The rank of elliptic curves upon quadratic extensions*, Computational Number Theory (A. Petho, H. C. Williams, H. G. Zimmer, eds.), de Gruyter, Berlin, 1991, 239-260.