Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2018, 5(1):236-240**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

The Number of Integral Points on the Elliptic Curve

Zhiwei Liu

College of Science, Hezhou University, Hezhou 542899, Guangxi, China

AbstractLet p be a given prime number and k be a given odd integer. Using $N(P^k)$ to denote the number of the integral points $(x,\pm y)$ with $y>0$ on the elliptic curve $E: y^2=x^3+p^k x$. By using the properties of *Diophantine equation*, the author proved that $N(P^K)\leq 2$,beside $N(3)=3$ and $N(3^{4s+5})=4$, where s is nonnegative integer.

KeywordsElliptic curve; Integral points; Diophantine equation

1. Introduction

Let P, P be the set of all integers and the set of positive integers respectively. In recently decades, the arithmetic properties of elliptic curve has become the interesting research issue in the number theory and its related field. Let p be a given prime number and k be a given positive integer. The papers [1-4] discussed integral points (x,y) of the following elliptic curve:

$$E: y^2=x^3+p^k x. \tag{1.1}$$

In this paper, by using the properties of the *Diophantine* equation, we will study the problem of the case that k be the given positive odd numbers.

For the integral points (x,y) of (1.1), if $y=0$, we call the trivial integral point, otherwise we call the nontrivial integer point. Obviously, (1.1) only has the trivial integral point $(x,y)=(0,0)$. On account of that, if (x,y) is the nontrivial integer point of (1.1), then $(x,\text{-}y)$ also is the nontrivial integer point of (1.1). So we will write that with together, which denote by $(x,\pm y)$, where $y>0$. Let s be a nonnegative integer and $a>1$be a positive integer. This paper will determined all the nontrivial integer points of (1.1) under the case that k be the given positive odd numbers, that is:

Theorem 1.1. For the positive odd numbers k ,the elliptic curve (1.1) only has the following nontrivial integer points :

(I) $p=2, k=4s+3, (x,\pm y)=(2^{2s},\pm 2^{3s}\cdot 3)$ and $(2^{2s+3},\pm 2^{3s+3}\cdot 3)$

(II) $p=3, k=1, (x,\pm y)=(1,\pm 2),(3,\pm 6)$ and $(12,\pm 42)$.

(III) $p=3, k=4s+5, (x,\pm y)=(3^{2s}\cdot 121,\pm 3^{3s}\cdot 1342), (3^{2s+2},\pm 3^{3s+3}\cdot 2),$

$(3^{2s+3},\pm 3^{3s+4}\cdot 2)$ and $(3^{2s+3}\cdot 4,\pm 3^{3s+4}\cdot 14)$.

(IV) $p=2a^2+1, k=4s+1, (x,\pm y)=(p^{2s}a^2,\pm p^{3s}a(a^2+1))$.

(V) $p>3,k\equiv n(\text{mod}\,4),(x,\pm y)=(p^{(k+n)|2}Y^2,\pm p^{(3k+n)|4}XY)$, where (X,Y,n) is the solution of the equation

$$X^2-p^nY^4=1,X,Y,n\in N,\quad 2\nmid n. \tag{1.2}$$

Assume that $N(P^K)$ is the class number of nontrivial integer points $(x,\pm y)$ on the elliptic curve (1.1). According to above theorem, we have the upper bound of $N(P^K)$ as follows.

Corollary 1.1. For the positive odd number k , when $p=2$,

$$N(2^k)=\begin{cases}2, & \text{if } k\equiv 3(\text{mod}\,4),\\ 0, & \text{otherwise;}\end{cases}$$

when p is odd number,

$$N(p^k)\begin{cases}=4, & \text{if } p=3,k\geq 5 \text{ and } k\equiv 1(\text{mod}\,4),\\ =3, & \text{if } p=3 \text{ and } k=1,\\ \leq 2, & \text{otherwise.}\end{cases}$$

2.The Lemmas

Let D be an non-square positive integer, and from the Theorem 10.9.1 and Theorem 10.9.2 of [5], it is easy to know the equation

$$U^2-DV^2=1 \quad U,V\in N \tag{2.1}$$

has the solution (u,v), and has an unique solution (u_1,v_1) which satisfies $u_1+v_1\sqrt{D}\leq u+v\sqrt{D}$, here (u,v) is any solution of above equation. Such (u_1,v_1) be called the minimal solution of equation (2.1).

Lemma 2.1. The equation

$$X^2-DY^2=1 \quad X,Y\in N \tag{2.2}$$

has no more than two group solution (X,Y). If the equation has two group solution (X_1,Y_1) and (X_2,Y_2) satisfying $X_1<X_2$, then when $D\neq 1785$ or 28560, there will be

$$(X_1,Y_1^2)=(u_1,v_1),\ (X_2,Y_2^2)=(u_1^2+Dv_1^2,2u_1v_1), \tag{2.3}$$

where (u_1,v_1) is the minimal solution of equation (2.1).

Proof. It can refer to Lemma 2 of [6], so we omit it.

Lemma 2.2 For given $m\in\{1,3\}$, if $p=2$, then the equation

$$X^2-p^mY^4=1 \quad X,Y\in N \tag{2.4}$$

has a solution (X,Y)=(3, 1) when $m=3$; If $p=3$, then (2.4) has the solutions (X,Y)=(2, 1) and (X,Y)= (7, 2) when $m=1$; If $p>3$, then (2.4) has no more than a group solution (X,Y).

Proof. According to all the given solution of (2.2) in [7] for $D\leq 400$, we can know that the lemma holds for the case $p\leq 3$.For $p>3$, by $p^m\neq 1785$ or 28560, thus from Lemma 2.1, we know: if equation (2.4) has two group solution (X_1,Y_1) and (X_2,Y_2) such that $X_1<X_2$, then it satisfy (2.3), where (u_1,v_1) is the minimal solution of equation

$$U^2-p^mV^2=1 \quad U,V\in N \tag{2.5}$$

From (2.3), we have $v_1=Y_1^2$ and

$$2u_1v_1=2u_1Y_1^2=Y_2^2 \tag{2.6}$$

By (2.6), we get

$$\mu_1 = 2a^2, Y_2 = 2aY_1, a \in N \qquad (2.7)$$

Therefore, from (2.5) and (2.7), it is easy to know

$$u_1^2 - p^m v_1^2 = 4a^4 - p^m Y_1^4 = 1. \qquad (2.8)$$

As p is an odd prime number and $\gcd(2a^2+1, 2a^2-1)=1$, thus from (2.8), we have

$$2a^2 + \lambda = b^4, 2a^2 - \lambda = p^m c^4, Y_1 = bc, \lambda \in \{\pm 1\}, b, c \in N \qquad (2.9)$$

However, from [8], the first equality of (2.9) didn't hold for $\lambda = 1$; and from [9], it hold for $\lambda = -1$ under $a = b = 1$. Moreover, from the second equality of (2.9), we have $p^m = 3$, but which contradict with the assumption $p > 3$, then equation (2.5) has no more than one group solution. The proof is complete.

Lemma 2.3. The following equation

$$1 + 2X^2 = Y^n, X, Y, n \in N,\ n > 1, 2 \nmid n \qquad (2.10)$$

only has a solution $(X, Y, n) = (11, 3, 5)$.

Proof. Please refer to [10].

Lemma 2.4. The equation

$$X^2 - Y^4 = p^n, X, Y, n \in N,\ \gcd(X, Y) = 1, 2 \nmid n \qquad (2.11)$$

only has the solutions $(p, n, X, Y) = (2, 3, 3, 1)$, $(3, 5, 122, 11)$ and $(2a^2+1, 1, a^2+1, a)$, where a is a position integer.

Proof. Assume that (p, n, X, Y) is a group solution of (2.11). If $p = 2$, as X and Y are relatively prime positive odd numbers, thus $\gcd(X+Y^2, X-Y^2) = 2$, and from (2.11), we have $X+Y^2 = 2^{n-1}$ and $X - Y^2 = 2$, then

$$X = 2^{n-2} + 1,\ \ Y^2 = 2^{n-2} - 1. \qquad (2.12)$$

Because of $Y^2 + 1 \equiv 2 (\bmod 4)$, and from (2.12), it can obtain that there is only a solution $(p, n, X, Y) = (2, 3, 3, 1)$.

If p is an odd prime number, as X and Y are relatively prime positive odd numbers, and one is odd and another is even, thus $\gcd(X+Y^2, X-Y^2) = 1$, and from (2.11), we get that $X + Y^2 = p^n$, $X - Y^2 = 1$ and

$$2X = p^n + 1,\ \ 2Y^2 = p^n - 1. \qquad (2.13)$$

By $2 \nmid n$, and according to Lemma 2.3 and (2.13), we can know that the equation (2.11) only has the solutions $(p, n, X, Y) =$ (3,5,122,11) and $(2a^2+1, 1, a^2+1, a)$. The proof of Lemma is complete.

3. The Proof of Theorem

The proof of Theorem 1.1. Let $(x, \pm y)$ be a group nontrivial integer points on elliptic curve (1.1),as $y > 0$, thus $x > 0$. Moreover, x can be expressed only as follows:

$$x = p^r z, r \in Z,\ r \geq 0, z \in N, p \nmid z. \qquad (3.1)$$

Substitute (3.1) into (1.1), which implies

$$p^r z(p^{2r} z^2 + p^k) = y^2. \qquad (3.2)$$

As k is a position odd number, thus $k \neq 2r$, therefore, we only need to consider the following two cases:

Case I: $k > 2r$

Now, from (3.2), we have

$$p^{3r} Z(Z^2 + p^{k-2r}) = y^2. \qquad (3.3)$$

As $p \nmid z$, thus $p \nmid z^2 + p^{k-2r}$ and $\gcd(z, z^2 + p^{k-2r}) = 1$, so by (3.3), it can obtain

$$r = 2s, z = f^2, z^2 + p^{k-2r} = g^2, y = p^{3s} fg, s \in Z, s \geq 0, f, g \in N, \gcd(f, g) = 1 、 \qquad (3.4)$$

From (3.4), we have

$$g^2 - f^4 = p^{k-4s} \qquad (3.5)$$

If $p = 2$, according to Lemma 2.4, and from (3.5), it is easy to know $k - 4s = 3, f = 1$ and $g = 3$, thus from (3.4), we have

$$p = 2, \quad k = 4s + 3, \quad (x, \pm y) = (2^{2s}, \pm 2^{3s} \cdot 3) \qquad (3.6)$$

If p is an odd number, according to Lemma 2.4, by (3.4) and (3.5), we get

$$p = 3, \quad k = 4s + 5, \quad (x, \pm y) = (3^{2s} \cdot 121, \pm 3^{3s} \cdot 1342) \qquad (3.7)$$

and

$$p = 2a^2 + 1, \quad k = 4s + 1, \quad (x, \pm y) = (p^{2s} a^2, \pm p^{3s} a(a^2 + 1)) \qquad (3.8)$$

Case II: $k < 2r$

In this case, from (3.2), we have

$$p^{r+k} z(p^{2r-k} z^2 + 1) = y^2. \qquad (3.9)$$

As $p \nmid z(p^{2r-k} z^2 + 1)$ and $\gcd(z, p^{2r-k} z^2 + 1) = 1$, thus from (3.9), we get

$$r + k = 2t, z = f^2, p^{2r-k} z^2 + 1 = g^2, y = p^t fg, t, f, g \in N, \gcd(f, g) = 1 \qquad (3.10)$$

And by (3.10), we have

$$g^2 - p^{2r-k} f^4 = 1. \qquad (3.11)$$

From (3.11), we can know that the equation (1.2) has a solution (X, Y, n) such that

$$(X, Y, n) = (g, f, 2r - k). \qquad (3.12)$$

Because of the first equality of equation (3.10), it is easy to know r is a position odd number, thus $r = 2s + 1$, where s is a nonnegative integer. Moreover, by (3.12), we have $n = 2r - k$, thus from $n \equiv 2r - k \equiv 2 - k(\bmod 4)$, we get $k \equiv n(\bmod 4)$. Therefore, according to the Lemma 2.2, and from (3.10), (3.11) and (3.12), we obtain that there are only the integer points:

$$p = 2, \quad k = 4s + 3, \quad (x, \pm y) = (2^{2s+3}, \pm 2^{3s+3} \cdot 3) \qquad (3.13)$$

$$p = 3, \quad k = 4s + 1, \quad (x, \pm y) = (3^{2s+1}, \pm 3^{3s+1} \cdot 2) \qquad (3.14)$$

$$p = 3, \quad k = 4s + 1, \quad (x, \pm y) = (3^{2s+1} \cdot 4., \pm 3^{3s+1} \cdot 14) \qquad (3.15)$$

and the integer points of Type (V).

Finally, from the equation (3.6) and (3.13), we have the integer points of Type (I) ; Let $a = 1$ and $s = 0$ in (3.8), and $a = 1$, $s = 0$ in (3.14) and (3.15). We can get the integer points of Type (II) ; Let $a = 1$, $s \geq 1$ in (3.8) and let $s \geq 1$in (3.14) and (3.15), then combine with (3.7), it can obtain the integer points of Type (III) ; Let $a > 1$ in (3.8), we have the integer points of Type (IV). To sum up above discussion, which complete the proof of theorem.

Proof of ***Corollary*** **1.1.** From Theorem 1.1, we can immediate obtain that the corollary holds for $p \leq 3$. If $p > 3$, assume that N_4, N_5 are group count which belong to Type (IV) and Type (V) respectively for nontrivial integer points of elliptic curve. Obviously, from the theorem of this paper, we have

$$N(p^k) = N_4 + N_5. \qquad (3.16)$$

As p be given, so when $p = 2a^2 + 1$, where a is also be given, then $N_4 \le 1$. Moreover, as k be given and from Lemma 2.2, we have $N_5 \le 1$. Thus from (3.16), we get $N(p^k) \le 2$. The proof of corollary is complete.

Acknowledgments This research is supported by Scientific Research Foundation of Guangxi EducationDepartment (No. 201012MS210).

References

[1]. Bremner A. and Cassels J.W.S. On the equation $Y^2 = X(X^2 + p)$, Math. comp., 1984, 42:247-262.

[2]. Draziotis K.A. Integer points on the curve $Y^2 = X^3 - p^k X$, Math. comp., 2006, 75:1493-1505.

[3]. Walsh P.G. Integer Solutions to the equation $y^2 = x(x^2 \pm p^k)$, Rocky Mt. J. Math., 2008, 38(4):1285-1302.

[4]. Woo S.S. lrreducibibity of polynomials and diophantine equations, J. Korean Math., 2010, 47(1):101-112.

[5]. Luogeng H. Guide of Number Theory [M]. Beijing: Science Press, 1979.

[6]. Walsh P.G. A note on a theorem of Liunggren and the diophantine equations $x^2 - kxy^2 + y^4 = 1$,4, Arch Math.Based,1999,73(1):119-125.

[7]. Cohn J.H.E. The diophantine equations $x^2 - Dy^4 = 1$, Math. Scand., 1978, 42(2):180-188.

[8]. Liunggren W. Some remarks on the diophantine equation $x^2 - dy^4 = 1$ and $x^4 - dy^4 = 1$, J. london Math .Soc., 1966,41(3): 542-544.

[9]. Cohn J.H.E. The diophantine equation $x^4 + 1 = Dy^4$ [J].Math. comp., 1997, 66:1347-1351.

[10]. Nagell T. Sur I'impossibilit′ee de quelques equations á deuxindéteminées[J]. NorskMat, Forenings Skr., 1921, 13(1):65-82.