The positive integral points on the elliptic curve $y^2 = 7px(x^2 + 8)$

Du Xiancun [1], Jianhong Zhao [2,3], and Lixing Yang [3,*]

[1] Honghe University, College of Teachers Education, Mengzi, Honghe,661100, China
[2] West Yunnan University of Applied Sciences, Teaching Department of public basic courses, Dali, Yunnan 671009, China
[3] Lijiang Teachers College, Department of Teachers and Education, Lijiang, Yunnan 674199, China

Abstract. The integral point of elliptic curve is a very important problem in both elementary number theory and analytic number theory. In recent years, scholars have paid great attention to solving the problem of positive integer points on elliptic curve $y^2 = kx(ax^2 + bx + c)$, where k, a, b, c are integers. As a special case of $y^2 = kx(ax^2 + bx + c)$, when $a = 1, b = 0, c = 2^{2t-1}$, it turns into $y^2 = kx(x^2 + 2^{2t-1})$, which is a very important case. However ,at present, there are only a few conclusions on it, and the conclusions mainly concentrated on the case of $t = 1,2,3,4$. The case of $t = 1$, main conclusions reference [1] to [7]. The case of $t = 2$, main conclusions reference [8]. The case of $t = 3$, main conclusions reference [9] to [11]. The case of $t = 4$, main conclusions reference [12] and [13]. Up to now, there is no relevant result on the case of $k = 7p$ when $t = 2$, here the elliptic curve is $y^2 = 7px(x^2 + 8)$, this paper mainly discusses the positive integral points of it. And we obtained the conclusion of the positive integral points on the elliptic curve $y^2 = 7px(x^2 + 8)$. By using congruence, Legendre symbol and other elementary methods, it is proved that the elliptic curve in the title has at most one integer point when $p \equiv 5,7(mod 8)$.

1 Introduction

Elliptic curve is a smooth projective curve with genus 1 over a field, its affine equation is usually called Weierstrass equation, and can be written as

$$y^2 + ay = x^3 + bx^2 + cx + d$$

In number theory, scholars pay more attention to the integral point of elliptic curve.

The integral points of elliptic curve is a very important problem in both elementary number theory and Analytic number theory.

In recent years, scholars have paid much attention to the problem of solving The positive integral points on the elliptic curve

$$y^2 = kx(ax^2 + bx + c) \quad (1)$$

where k, a, b, c are integers.

As a special case of (1), when $a = 1, b = 0, c = 2^{2t-1}$, it turns into

$$y^2 = kx(x^2 + 2^{2t-1}) \quad (2)$$

which is a very important case. However ,at present, there are only a few conclusions on it, and the conclusions mainly concentrated on the case of $t = 1,2,3,4$.

The case of $t = 1$, main conclusions reference [1] to [7].

The case of $t = 2$, main conclusions reference [8].

The case of $t = 3$, main conclusions reference [9] to [11].

The case of $t = 4$, main conclusions reference [12] and [13].

Up to now, there is no relevant result on the case of $k = 7p$ when $t = 2$, here the elliptic curve is $y^2 = 7px(x^2 + 8)$, this paper mainly discusses the positive integral points of it.

2 Critical lemma

Lemma 1[14] The diophantine equation $x^2 - Dy^4 = 1$ has at most one set of positive integer solutions where D is an even number of non-square.

Lemma 2[15] Legendre symbol $\left(\frac{a}{p}\right)$ is a function defined on all integers a for a given prime number p, whose values are specified as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, a \text{ is the square residue of module } p \\ -1, a \text{ is the nonsquare residue of module } p \\ 0, p|a \end{cases}$$

Whether the congruence equation $x^2 \equiv a(mod p)$ where p is an odd prime number and $p \nmid a$ has a solution depends on the value of the Legendre symbol. Specifically, when Legendre symbol $\left(\frac{a}{p}\right) = -1$,the congruence equation has no solution. When Legendre symbol $\left(\frac{a}{p}\right) = 1$, the congruence equation has two solutions.

3 Theorem and proof

Objective: The objective of this paper is to solve a kind of very important elliptic curve in elementary number theory and find the integral point of the curve in title.

* Corresponding author: yanglixing1980@163.com

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (http://creativecommons.org/licenses/by/4.0/).

Methods: Comprehensive use of congruence and Legendre symbols and other important elementary number theory methods.

Conclusion: Elliptic curve $y^2 = 7px(x^2 + 8)$ has only one positive integral point at most in odd prime number $p \equiv 5,7(mod8)$.

3.1. theorem

When odd prime number $p \equiv 5,7(mod8)$, the elliptic curve

$$y^2 = 7px(x^2 + 8) \tag{3}$$

has only one positive integral point at most.

3.2 Proof of main theorem

3.2.1 Primary analysis

Supposing the elliptic curve (3) has positive integral points, we can assume that it is (x, y), where $x, y \in Z^+$.

Because p is an odd prime number, we can get $7p|y$, assume that $y = 7pz$, where $z \in Z^+$. So

$$7pz^2 = x(x^2 + 8) \tag{4}$$

$gcd(x, x^2 + 8) = gcd(x, 8) = 1$ or 2 or 4 or 8, in other words, the range of this greatest common divisor is {1,2,4,8}. As a result, we have to discuss in four cases of the elliptic curve (4):

Case 1 $x = ma^2, x^2 + 8 = 7pmb^2, z = ab, gcd(a, b) = 1$.

Case 2 $x = mpa^2, x^2 + 8 = 7mb^2, z = ab, gcd(a, b) = 1$.

Case 3 $x = 7ma^2, x^2 + 8 = pmb^2, z = ab, gcd(a, b) = 1$.

Case 4 $x = 7pma^2, x^2 + 8 = mb^2, z = ab, gcd(a, b) = 1$.

where $m = 1,2,4,8$, and $a, b \in Z^+$.

3.2.2 Discusion on Case 1

When $x = ma^2, x^2 + 8 = 7pmb^2, z = ab, gcd(a, b) = 1$, where $m = 1,2,4,8$, and $a, b \in Z^+$. The elliptic curve equation $7pz^2 = x(x^2 + 8)$ is discussed as follows:

Obviously $7|7pmb^2$, it means $7pmb^2 \equiv 0(mod7)$.Then we will get

$$x^2 \equiv -8(mod7) \tag{5}$$

from $x^2 + 8 = 7pmb^2$. By calculating Legendre symbols $\left(\frac{-8}{7}\right) = -1$.

According to lemma 2, the congruence formula (5) is not valid, so case 1 is false, this shows that (3) has no integer points in case 1.

3.2.3 Discusion on Case 2

When $x = mpa^2, x^2 + 8 = 7mb^2, z = ab, gcd(a, b) = 1$, where $m = 1,2,4,8$, and $a, b \in Z^+$. The elliptic curve equation $7pz^2 = x(x^2 + 8)$ is discussed as follows:

Similar to the previous proof on case 1, for $7mb^2 \equiv 0(mod7)$,we will get

$$x^2 \equiv -8(mod7) \tag{6}$$

from $x^2 + 8 = 7mb^2$. By calculating Legendre symbols $\left(\frac{-8}{7}\right) = -1$.

According to lemma 2, the congruence formula (6) is not valid, so case 2 is false, this shows that (3) has no integer points in case 2.

3.2.4 Discusion on Case 3

When $x = 7ma^2, x^2 + 8 = pmb^2, z = ab, gcd(a, b) = 1$, where $m = 1,2,4,8$, and $a, b \in Z^+$. The elliptic curve equation $7pz^2 = x(x^2 + 8)$ is discussed as follows:

Similar to the previous proof on case 1 and case 2, for $pmb^2 \equiv 0(modp)$,we will get

$$x^2 \equiv -8(modp) \tag{7}$$

from $x^2 + 8 = 7mb^2$. For odd prime number $p \equiv 5,7(mod8)$, we can calculating Legendre symbols $\left(\frac{-8}{p}\right) = -1$.

According to lemma 2, the congruence formula (7) is not valid, so case 3 is false, this shows that (3) has no integer points in case 3.

3.2.5 Discusion on Case 4

When $x = 7pma^2, x^2 + 8 = mb^2, z = ab, gcd(a, b) = 1$, where $m = 1,2,4,8$, and $a, b \in Z^+$. The elliptic curve equation $7pz^2 = x(x^2 + 8)$ is discussed as follows:

Because $x^2 + 8 = mb^2$, we should discuss it according to $m = 1,2,4,8$.

(i) Discuss on the case of $m = 1$.

When $m = 1$,we can get $x = 7pa^2, x^2 + 8 = b^2, z = ab, gcd(a, b) = 1$. From $x^2 + 8 = b^2$, we will get

$$(b + x)(b - x) = 8 \tag{8}$$

Solve this quadratic equation (8), we can get:

$$\begin{cases} x = 1 \\ b = 3 \end{cases}$$

or

$$\begin{cases} x = \frac{7}{2} \\ b = \frac{9}{2} \end{cases}$$

Examine the first case, $x = 1$, it will contradict $x = 7pa^2$.

Examine the second situation $x = \frac{7}{2}, b = \frac{9}{2}$ and $x, b \in Z^+$ contradictions.

It means case 4 is not valid when $m = 1$, this shows that elliptic curve (3) has no integer points in case 4 when $m = 1$.

(ii) Discuss on the case of $m = 2$.

When $m=2$, we can get $x=14pa^2, x^2+8=2b^2, z=ab, gcd(a,b)=1$. Substituting $x=14pa^2$ for $x^2+8=2b^2$, we will get $256p^2a^4+8=2b^2$,which can be reduced to

$$128p^2a^4+4=b^2 \tag{9}$$

From (9) we can know that b is an even number. Suppose $b=2c, c\in Z^+$,then we will get $128p^2a^4+4=4c^2$from (9), which can be reduced to

$$c^2-32p^2a^4=1 \tag{10}$$

According to Lemma 1, we can know that equation (10) has at most one set of positive integer solutions, at this time, elliptic curve (3) has at most one positive integer point in case 4 when $m=2$.

(iii) Discuss on the case of $m=4$.

When $m=4$,we can get $x=28pa^2, x^2+8=4b^2, z=ab, gcd(a,b)=1$. From $x^2+8=4b^2$, we will get

$$(2b+x)(2b-x)=8 \tag{11}$$

Solve this quadratic equation (11), we can get:

$$\begin{cases} x=1 \\ b=\dfrac{3}{2} \end{cases}$$

or

$$\begin{cases} x=\dfrac{7}{2} \\ b=\dfrac{9}{4} \end{cases}$$

Examine the first case, $x=1$, it will contradict $x=28pa^2$.

Examine the second situation $x=\frac{7}{2}, b=\frac{9}{4}$ and $x,b\in Z^+$ contradictions.

In fact, whether $=1$ or $x=\frac{7}{2}$ will contradict $x,b\in Z^+$.

It means case 4 is not valid when $m=4$, this shows that elliptic curve (3) has no integer points in case 4 when $m=4$.

(iv) Discuss on the case of $m=8$.

When $m=8$,we can get $x=56pa^2, x^2+8=8b^2, z=ab, gcd(a,b)=1$. Substituting $x=56pa^2$ for $x^2+8=8b^2$, we will get $3136p^2a^4+8=8b^2$,which can be reduced to

$$b^2-392p^2a^4=1 \tag{12}$$

According to Lemma 1, we can know that equation (12) has at most one set of positive integer solutions, at this time, elliptic curve (3) has at most one positive integer point in case 4 when $m=8$.

To sum up, when $m=2$ or $m=8$, the elliptic curve may have integer solutions, and the number of integer solutions is at most one at any time.

On the other hand, 2 and 8 are the greatest common factors, so it is impossible to hold both of them at the same time.

Therefore, it can be seen from the above (i) to (iv), elliptic curve (3) has at most one positive integer point in case 4 when $m=2$ in case 4.

4 Conclusion

The positive integer points and integral points of elliptic curves $y^2=kx(ax^2+bx+c), k,a,b,c\in Z$ are very important in the theory of number and arithmetic algebra, it has a wide range of applications in cryptography and other fields. Up to now, there is no relevant result on the case of $k=7p$ when $t=2$, here the elliptic curve is $y^2=7px(x^2+8)$.

In this paper, by using elementary number theory methods, such as congruence and Legendre symbol, it can be proved that elliptic curve $y^2=7px(x^2+8)$ has only one positive integral point at most in odd prime number $p\equiv 5,7(mod8)$.

Acknowledgment

The author would like to thank the referees for thier very helpful and detail comments, which have significantly improved the presentation of this paper.

Supported by Scientific Research Project fund of Education Department of Yunnan Province: 2020J0825.

Supported by Scientific Research Project fund of Education Department of Yunnan Province: 2019J1182.

Supported by Science and technology innovation project of Honghe University: SC1943.

Supported by Golden course of elementary number theory in Lijiang Teachers College.

References

1. Liu Xianbei. A Note on the Positive Integer Solutions of the Elliptic Curve $y^2=px(x^2+2)$ [J]. Journal of Xinxiang University, 2015,32(12):12-13.
2. Zhang Jin. The Criterions for Elliptic Curve $y^2=px(x^2+2)$ Has Positive Integer Points [J]. Mathematics in Practice and Theory, 2015,45(2):232-235.
3. Du Xiao-ying. The Positive Integral Points on Elliptic Curves $y^2=px(x^2+2)$ with $p\equiv 1(mod8)$ [J]. Mathematics in Practice and Theory, 2014,44(8):290-294.
4. Li Min Chen. On the Diophantine Equation $y^2=px(x^2+2)$ [J]. Acta Mathematica Sinica, Chinese Series, 2010,53(1):83-86.
5. Li Ling, Zhang Xu-xu. The integral points on the elliptic curve $y^2=nx(x^2+2)$ [J]. Journal of Xi'an Polytechnic University, 2011,25(3):407-409.
6. LIAO Si-quan, LE Mao-hua. THE POSITIVE INTEGRAL POINTS ON THE ELLIPTIC CURVE $y^2=px(x^2+2)$ [J] . Journal of Mathematics, 2009,29(3):387-390.
7. Yin Jing-jing, GUAN Xun-gui. Integral Points on Elliptic Curve $y^2=px(x^2+2)$ [J]. Journal of Hebei North University (Natural Science Edition),2017,33(7):11-13.
8. WAN Fei, DU Xian-cun. The Positive Integral Point on the Elliptic Curve $y^2=nx(x^2+8)$ [J]. Journal

of Qufu Normal University (Natural Science), 2018,44(1):42-44.

9. Zhao Jianhong. The Integral Points on the Elliptic Curve $y^2 = qx(x^2 + 32)$ [J] . Journal of Dezhou University,2017.33(6):20-22.
10. DU Xiancun, LIN Xing, TANG Lihua. The Integral Points on the Elliptic Curve $y^2 = qx(x^2 + 32)$. Journal of Hubei Minzu University (Natural Science Edition),2016.34(04):391-393.
11. Zhao Jianhong. The Positive Integral Points on the Elliptic Curve $y^2 = qx(x^2 + 32)$ [J] . Journal of Hubei Minzu University (Natural Science Edition),2017,35(2):134-136.
12. Zhao Jianhong, The Integral Points on the Elliptic Curve $y^2 = px(x^2 + 128)$ *[J]. Journal of Qufu Normal University (Natural Science),2017:43 (04):21-24.
13. Zhao Jianhong. ABOUT THE POSITIVE INTEGRAL POINTS ON THE ELLIPTIC CURVE $y^2 = qx(x^2 + 128)$ [J]. Journal of Inner Mongolia University for Nationalities (Natural Sciences),2017:38 (2):100-104.
14. Pan Jiayu. SOME REMARKS ON THE DIOPHANTINE EQUATION $x^2 - Dy^4 = 1$ [J]. Henan Science,1997:15 (1):7-11.
15. Zhu Ping. Elementary number theory and its application in Information Science[M]. Beijing: Tsinghua University Press, 2010:86-98.