Advances in Social Science, Education and Humanities Research (ASSEHR), volume 130
2nd International Forum on Management, Education and Information Technology Application (IFMEITA 2017)

Elliptic Curve Integral Points on $y^2 = x^3 + 19x - 46$

Jianhong Zhao[1, a], Lixing Yang[2,b]

[1]Department of Teachers and Education, Lijiang Teachers College, Lijiang, 674199, Yunnan, China

[2]Department of Teachers and Education, Lijiang Teachers College, Lijiang, 674199, Yunnan, China
[a]E-mail: 312508050@qq.com, [b]37574990@qq.com

Keywords: Elliptic Curve; Pell equation; integer solution; common solution; Legendre symbol.
Abstract. By using congruence and Legendre Symbol, it can be proved that elliptic curve $y^2 = x^3 + 19x - 46$ has only one integer point: $(x, y) = (2,0)$.

Introduction

The positive integer points and integral points of elliptic curves are very important in the theory of number and arithmetic algebra, it has a wide range of applications in cryptography and other fields. There are some results of positive integer points of elliptic curve

$$y^2 = x^3 + ax + b, a, b \in Z \tag{1}$$

In 1987, D. Zagier [1] submit the question of the integer points on elliptic curve (1) while $a = -27, b = 62$, that is $y^2 = x^3 - 27x + 62$, it counts a great deal to the study of the arithmetic properties of elliptic curves.

In 2009, Zhu H L and Chen J H [2] solved the problem what D. Zagier submitted by using algebraic number theory and P-adic analysis method.

In 2010, By using the elementary method, Wu H M [3] obtain all the integral points of elliptic curves $y^2 = x^3 - 27x - 62$.

In 2015, Li Y Z and Cui B J [4] solved the problem of the integer points on $y^2 = x^3 - 21x - 90$ By using the elementary method.

In 2016, Guo J [5] solved the problem of the integer points on $y^2 = x^3 + 27x + 62$ by using the elementary method.

In 2017, Guo J [6] proved that $y^2 = x^3 - 21x + 90$ has no integer points by using the elementary method.

Put in a nutshell, Scholars studied the integer points on elliptic curve (1) while $a_1 = -27, b_1 = 62; a_2 = -27, b_2 = -62; a_3 = -21, b_3 = -90; a_4 = 27, b_4 = 62; a_5 = -21, b_5 = 90$.

Up to now, there is no relevant conclusions while $a = 19, b = -46$.

Key lemma

Key lemma [7] Let D to be a square-free positive integer, then the equation $x^2 - Dy^4 = 1$ will have two sets of positive integer solutions (x, y) at most.

When $D = 2^{4s} \times 1785$,where $s \in \{0,1\}$, we can get that $(x_1, y_1) = (169, 2^{1-s})$ and $(x_2, y_2) = (6525617281, 2^{1-s} \times 6214)$;

Otherwise when $D \neq 2^{4s} \times 1785$, $(x_1, y_1) = (u_1, \sqrt{v_1})$ and $(x_2, y_2) = (u_2, \sqrt{v_2})$, where (u_n, v_n) is a positive integer solution of the Pell equation $U^2 - DV^2 = 1$, if $x^2 - Dy^4 = 1$ has only one set of positive integer solution (x,y) and the positive integer n is suitable for $(x,y^2)=(u_n,v_n)$, then $n=2$ consequently ; otherwise if n is an even number; otherwise if n is an odd number, then $n=1$ or p, here p is a prime numbers and $p\equiv 3(mod4)$.

Proof of main theorem

By using elementary method such as congruence and Legendre Symbol, the integer points on $y^2=x^3+19x-46$ can be obtained.

Theorem

Elliptic curve

$$y^2=x^3+19x-46 \tag{2}$$

has only one integer point $(x,y)=(2,0)$.

Proof of the main theorem

Elliptic curve (2) is equivalent to

$$y^2=(x-2)(x^2+2x+23) \tag{3}$$

Primary analysis

Obviously $(x,y)=(2,0)$ is an integer point of the elliptic curve (3), suppose (x,y) is another integer point of the elliptic curve (3).

Because $x^2+2x+23=x(x-2)+4(x-2)+31=(x+4)(x-2)+31$.

$gcd(x-2,x^2+2x+23)=gcd(x-2,(x+4)(x-2)+31)=gcd(x-2,31)$, and the divisor of the prime number 31 is 1 or 31, then $gc\,d(x-2,31)=1$, or $gc\,d(x-2,31)=31$, in other words, the range of this greatest common divisor is $\{1,31\}$. as a result, we have to discuss in two cases of the elliptic curve (3):

Case I $x-2=a^2, x^2+2x+23=b^2, y=ab, gc\,d(a,b)=1, a,b\in Z$.

Case II $x-2=31a^2, x^2+2x+23=31b^2, y=31ab, gc\,d(a,b)=1, a,b\in Z$.

Discussion on Case I

$\because\ a^2\equiv 0,1(mod4)$.

$\therefore\ x=a^2+2\equiv 2,3(mod4)$.

$\therefore x^2+2x+23\equiv 2,3(mod4)$.

At the same time $b^2=x^2+2x+23\equiv 0,1(mod4)$.

Then we will get $2,3(mod4)\equiv 0,1(mod4)$, it is self-contradiction, this shows that (3) has no integer points.

Discussion on Case II

Divide integers into two categories as $2\nmid a$ and $2|a$ discuss separately.

First step: suppose $2\nmid a$.

$\because\ 2\nmid a.\ \therefore\ a^2\equiv 1(mod4). \therefore x=31a^2+2\equiv 1(mod4).\ \therefore\ x^2+2x+23\equiv 2(mod4)$.

At the same time $b^2\equiv 0,1\,(mod4)$.

$\therefore\ 31b^2=x^2+2x+23\equiv 0,3(mod4)$,it means $2(mod4)\equiv 0,3(mod4)$, it is self-contradiction, this shows that (3) has no integer points as well.

Second step: suppose $2|a$.

$\because$ $2|a$, let $a = 2c, c \in Z$, and $x - 2 = 31a^2$.$\therefore$ $x = 124c^2 + 2$.

Go a step further $x^2 + 2x + 23 = (x+1)^2 + 22 = (124c^2+3)^2 + 22 = 31b^2$, it is $(12c^2+1)^2 + 352c^4 = b^2$, it is equivalent to:

$$(b + 12c^2 + 1)(b - 12c^2 - 1) = 352c^4 \tag{4}$$

$\because 2|a$, and $x - 2 = 31a^2$, $\therefore 2|31a^2 + 2$. $\therefore$ $2|x$.

$\because$ $x^2 + 2x + 23 = 31b^2$.$\therefore 2 \nmid x^2 + 2x + 23$. $\therefore 2 \nmid 31b^2$. $\therefore$ $2 \nmid b$. $\therefore$ $2|b$.

Taken together, $2|[b - (12c^2 + 1)]$.

$$\begin{aligned}\therefore \gcd(b + 12c^2 + 1, b - 12c^2 - 1) &= \gcd(24c^2 + 2, b - 12c^2 - 1)\\ &= 2\gcd(12c^2 + 1, b - 12c^2 - 1)\\ &= 2\gcd(12c^2 + 1, b).\end{aligned}$$

Let $d = \gcd(12c^2 + 1, b)$, Then $d|b, d|12c^2 + 1$, so, $d|(b + 12c^2 + 1)$, Therefore, $d|352c^4$.

$\gcd(12c^2 + 1, 352c^4) = \gcd(12c^2 + 1, 11)$.

The divisor of the prime number 11 is 1 or 11, then $gcd(12c^2 + 1,352c^4) = 1$, or $gcd(12c^2 + 1,352c^4) = 11$, in other words, the range of this greatest common divisor is $\{1,11\}$.

If $gcd(12c^2 + 1,352c^4) = 11$.

$12c^2 + 1 \equiv 0(mod 11)$.

$\therefore 12c^2 \equiv -1(mod 11)$.

Because the Legendre symbol value is $\left(\frac{12c^2}{11}\right) = \left(\frac{3}{11}\right) = 1$, while the Legendre symbol value is $\left(\frac{-1}{11}\right) = -1$, it is self-contradiction, this shows that $gcd(12c^2 + 1,352c^4) = 11$ is false. It must be $gcd(12c^2 + 1,352c^4) \neq 11$.

Therefore, $gcd(12c^2 + 1,352c^4) = 1$.

$\therefore$ $\gcd(b + 12c^2 + 1, b - 12c^2 - 1) = 2$.

Furthermore $352 = 2^5 \times 11$, equation (4) can be divided into:

$$\begin{cases} b + 12c^2 + 1 = 2gm^4 \\ b - 12c^2 - 1 = \frac{146}{g}n^4, \\ c = mn \end{cases} \tag{5}$$

Where $gcd(m,n) = 1, gcd\left(g, \frac{88}{g}\right) = 1, g = 1,11,2^3 = 8, 2^3 \times 11 = 88$.

From the first two formulas (5), we will get:

$$12c^2 + 1 = gm^4 - \frac{88}{g}n^4. \tag{6}$$

Making an equivalent of the modulus 4 on (6), we will get:

$$1 \equiv gm^4 - \frac{88}{g}n^4(mod 4) \tag{7}$$

When $g = 11$, (7) is equivalent to:

$$1 \equiv 3m^4(mod 4) \tag{8}$$

$\because$ $m^4 \equiv 0,1(mod 4)$. $\therefore$ $1 \equiv 3m^4(mod 4) \equiv 0,3(mod 4)$.

It is self-contradiction, this shows that (8) is impossible.

When $g = 2^3 \times 11$, (7) is equivalent to:

$$1 \equiv -n^4(mod 4) \tag{9}$$

$\because$ $n^4 \equiv 0,1(mod 4)$. $\therefore$ $1 \equiv -n^4(mod 4) \equiv 0,3(mod 4)$.

It is self-contradiction, this shows that (9) is impossible.

When $g=2^3$, the (6) is equivalent to $12c^2+1=8m^4-11n^4$, from $c=mn$ and $12c^2+1=gm^4-\frac{88}{g}n^4$, we will get:

$$12m^2n^2+1=8m^4-11n^4 \tag{10}$$

(10) is equivalent to:

$$(4m^2-3n^2)^2=31n^4+2 \tag{11}$$

Making an equivalent of the modulus 4 on (11), we will get:

$$(4m^2-3n^2)^2\equiv(n^4+2)(mod10) \tag{12}$$

We will get $2\nmid n$ from (10), and $2\nmid 4m^2-3n^2$ from (11).

$\therefore\ n^4\equiv 1{,}5(mod10)$.

On the other hand, $(4m^2-3n^2)^2\equiv 1{,}5{,}9(mod10)$.

$\therefore\ n^4+2\equiv 3{,}7(mod10)$.

Taken together, we will get:

$1{,}5{,}9\equiv(4m^2-3n^2)^2\equiv n^4+2\equiv 3{,}7(mod10)$. It is self-contradiction, this shows that (12) is impossible.

When $g=1$, the (6) is equivalent to $12c^2+1=m^4-88n^4$, from $c=mn$ and $12c^2+1=gm^4-\frac{88}{g}n^4$, we will get:

$$12m^2n^2+1=m^4-88n^4 \tag{13}$$

(13) is equivalent to:

$$(m^2-6n^2)^2=124n^4+1 \tag{14}$$

Let $s=m^2-6n^2, s\in Z^+$, (14) is equivalent to:

$$s^2=124n^4+1 \tag{15}$$

Let $r=2n^2, r\in Z^+$, (15) is equivalent to:

$$s^2-31r^2=1 \tag{16}$$

We know that (15) has only one positive integer point from the Key lemma, suppose (s,n) is the positive integer point, then the Pell equation (16) has positive integer point $(s,r)=(s,2n^2)$.

$(1520{,}273)$ is a fundamental solution of the Pell equation (16), therefore all of the positive integer point can be represented as:

$$s_k+r_k\sqrt{31}=(1520+273\sqrt{31})^k, k\in Z^+. \tag{17}$$

Therefore all of the positive integer point of (11) satisfied:

$$(m^2-6n^2)+2n^2\sqrt{31}=(1520+273\sqrt{31})^k, k\in Z^+. \tag{18}$$

$\therefore\ m^2-6n^2=s_k,\ 2n^2=r_k, k\in Z^+$.

$$\therefore\ r_{k+2}=3040r_{k+1}-r_k, r_0=0, r_1=273. \tag{19}$$

Making an equivalent of the modulus 2 on recurrent sequence (19), we will get the residue class sequence $0,1,0,1,\cdots$, cycle for 2.

And just when $k\equiv 1(mod2)$, $r_k\equiv 1(mod2)$.

Just when $k\equiv 0(mod2)$, $r_k\equiv 0(mod2)$.

$\because\ 2n^2=r_k$. $\therefore\ r_k$ is even. $\therefore\ k\equiv 0(mod2)$.

We can get $k=2$ or $2\nmid k$ from the Key lemma.

So, we will get

$$m^2 - 6n^2 + n^2\sqrt{124} = m^2 - 6n^2 + 2n^2\sqrt{31}$$
$$= \left(1520 + 273\sqrt{31}\right)^2$$
$$= 4260799 + 829920\sqrt{31}.$$

Taken together, we will get:

$m^2 - 6n^2 = 4260799$, $2n^2 = 829920$, $n^2 = 414960$. All appearance it has no integer points, this shows that equation (15) has no integer points.

In conclusion, elliptic curve $y^2 = x^3 + 19x - 46$ has only one integer point $(x, y) = (2,0)$.

References

[1] D. Zagier. *Lager Integral Point on Elliptic Curves* [J]. Math Comp, 1987,48:425-436.

[2] Zhu H L, *Chen J H. Integral point on* $y^2 = x^3 + 27x - 62$ [J]. Math Study, 2009, 42(2): 117-125.

[3] Wu H M . *Points on the Elliptic Curves* $y^2 = x^3 - 27x - 62$ [J] . J Acta Mathematica Curve Sinica,2010,53(1):205-208.

[4] Li Y Z, Cui B J. *Points on the Elliptic* $y^2 = x^3 - 21x - 90$ [J]. Journal of Yanan University (Natural Science Edition), 2015, 34(3):14-15.

[5] Guo J. *The Integral Points on the Elliptic Curve* $y^2 = x^3 + 27x + 62$ [J]. Journal of Chongqing Normal University (Natural Science), 2016,33(5): 50- 53.

[6] Guo J. *The Positive Integral Points on the Elliptic Curve* $y^2 = x^3 - 21x + 90$ [J]. Mathematics in Practice and Theory,2017,47(8):288-291.

[7] Togbé A.,*Voutier P.M.,and Walsh P.G.,Solving a family of Thue equations with an application to the equation* $x^2 - dy^2 = 1$.Acta. Arith.,2005,120(1) :39-58.