Journal of Inequalities and Applications
a SpringerOpen Journal

RESEARCH Open Access

The upper bound estimate of the number of integer points on elliptic curves $y^2 = x^3 + p^{2r}x$

Jin Zhang[1] and Xiaoxue Li[2*]

*Correspondence:
lxx20072012@163.com
[2]Department of Mathematics, Northwest University, Xi'an, Shaanxi, P.R. China
Full list of author information is available at the end of the article

Abstract

Let p be a fixed prime and r be a fixed positive integer. Further let $N(p^{2r})$ denote the number of pairs of integer points $(x, \pm y)$ on the elliptic curve $E : y^2 = x^3 + p^{2r}x$ with $y > 0$. Using some properties of Diophantine equations, we give a sharper upper bound estimate for $N(p^{2r})$. That is, we prove that $N(p^{2r}) \leq 1$, except with $N(17^{2(2s+1)}) = 2$, where s is a nonnegative integer.

MSC: 11G05; 11Y50

Keywords: elliptic curve; integer point; Diophantine equation

1 Introduction

Let $\mathbb{Z}$, $\mathbb{N}$ be the sets of all integers and positive integers, respectively. Let p be a fixed prime and k be a fixed positive integer. Recently, the integer points (x, y) on the elliptic curve

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

have been investigated in many papers (see [1, 2] and [3]). In this paper we deal with the number of integer points on (1.1) for even k. Then (1.1) can be rewritten as

$$y^2 = x^3 + p^{2r}x, \tag{1.2}$$

where r is a positive integer.

An integer point (x, y) on (1.2) is called trivial or non-trivial according to whether $y = 0$ or not. Obviously, (1.2) has only the trivial integer point $(x, y) = (0, 0)$. Notice that if (x, y) is a non-trivial integer point on (1.2), then $(x, -y)$ is also. Therefore, (x, y) along with $(x, -y)$ are called by a pair of non-trivial integer points and denoted by $(x, \pm y)$, where $y > 0$. For any positive integer n, let

$$u(n) = \frac{1}{2}\left(\alpha^n + \beta^n\right), \qquad v(n) = \frac{1}{2\sqrt{2}}\left(\alpha^n - \beta^n\right), \tag{1.3}$$

where

$$\alpha = 3 + 2\sqrt{2}, \qquad \beta = 3 - 2\sqrt{2}. \tag{1.4}$$

Using some properties of Diophantine equations, we give a sharper upper bound estimate for $N(p^{2r})$, the number of pairs of non-trivial integer points $(x, \pm y)$ on (1.2). That is, we shall prove the following results.

Theorem 1.1 *All non-trivial integer points on* (1.2) *are given as follows.*

(i) $p = u(2^m)$, $r = 2s+1$, $(x, \pm y) = (p^{2s}v^2(2^m), \pm p^{3s}v(2^m)(v^2(2^m)+1))$, *where* m, s *are nonnegative integers.*

(ii) $p \equiv 1 \pmod 8$, $r = 2s+1$, $(x, \pm y) = (p^{2s+1}X^2, \pm p^{3s+2}XY)$, *where* s *is a nonnegative integer,* (X, Y) *is a solution of the equation*

$$X^4 - pY^2 = 1, \quad X, Y \in \mathbb{N}. \tag{1.5}$$

Theorem 1.2 *Let* p *be an odd prime,* r *be a positive integer. Then for any nonnegative integer* s, *we have* $N(p^{2r}) \le 1$, *except with* $N(17^{2(2s+1)}) = 2$. *Moreover, if* $p \not\equiv 1 \pmod 8$, *then* $N(p^{2r}) = 0$, *except with* $N(3^{2(2s+1)}) = 1$.

2 Lemmas

Lemma 2.1 ([4, Theorem 244]) *Every solution* (u, v) *of the equation*

$$u^2 - 2v^2 = 1, \quad u, v \in \mathbb{N} \tag{2.1}$$

can be expressed as $(u, v) = (u(n), v(n))$, *where* n *is a positive integer.*

Lemma 2.2 *If* $p = u(n)$, *then* $n = 2^m$, *where* m *is a nonnegative integer.*

Proof Assume that n has an odd divisor d with $d > 1$. Then we have either $u(1)|u(n)$ and $1 < u(1) < u(n)$ or $u(n/d)|u(n)$ and $1 < u(n/d) < u(n)$. Therefore, since p is a prime, it is impossible. Thus, we get $n = 2^m$. The lemma is proved. □

Any fixed positive integer a can be uniquely expressed as $a = bc^2$, where b, c are positive integers with b is square free. Then b is called the quadratfrei of a and denoted by $Q(a)$.

Lemma 2.3 *For any positive integer* m, *we have* $3|Q(v(2^m))$.

Proof By (1.3) and (1.4), we get

$$v\left(2^m\right) = 2^{m+1}\prod_{i=0}^{m-1} u\left(2^i\right) \tag{2.2}$$

and

$$u\left(2^i\right) = 2u^2\left(2^{i-1}\right) - 1, \quad i \in \mathbb{N}. \tag{2.3}$$

Since $(2/3) = -1$, where $(2/3)$ is the Legendre symbol, we see from (2.3) that $3 \nmid u(2^i)$ for $i \ge 1$. Therefore, since $u(1) = 3$, by (2.2), we obtain $3 \parallel v(2^m)$. It implies that $3|Q(v(2^m))$. The lemma is proved. □

Let D be a non-square positive integer. It is a well known fact that if the equation

$$U^2 - DV^2 = -1, \quad U, V \in \mathbb{N} \tag{2.4}$$

has solutions (U, V), then it has a unique solution (U_1, V_1) such that $U_1 + V_1\sqrt{D} \leq U + V\sqrt{D}$, where (U, V) through all solutions of (2.4). For any odd positive integer l, let

$$U(l) + V(l)\sqrt{D} = (U_1 + V_1\sqrt{D})^l.$$

Then $(U, V) = (U(l), V(l))$ $(l = 1, 3, \ldots)$ are all solutions of (2.4).

Lemma 2.4 ([5, Theorem 1]) *The equation*

$$X^4 - DY^2 = -1, \quad X, Y \in \mathbb{N} \tag{2.5}$$

has at most one solution (X, Y). *Moreover, if the solution* (X, Y) *exists, then* $(X^2, Y) = (U(l), V(l))$, *where* $l = Q(U_1)$.

Lemma 2.5 ([5, Theorem 3]) *If* $3|Q(U_1)$, *then* (2.5) *has no solutions* (X, Y).

Lemma 2.6 *If* $p = u(2^m)$, *where* m *is a positive integer with* $m > 1$, *then* (1.5) *has no solutions* (X, Y).

Proof Since $p = u(2^m)$ with $m > 1$, by (2.3), we have

$$p = 2u^2\left(2^{m-1}\right) - 1 = 4v^2\left(2^{m-1}\right) + 1. \tag{2.6}$$

We see from (2.6) that the equation

$$U^2 - pV^2 = -1, \quad U, V \in \mathbb{N} \tag{2.7}$$

has solution (U, V) and its fundamental solution is $(U_1, V_1) = (2v(2^{m-1}), 1)$. Further, since $m - 1 \geq 1$, by Lemma 2.3, we have $3|Q(v(2^{m-1}))$. Hence, we get $3|Q(U_1) = Q(2v(2^{m-1}))$. Therefore, by Lemma 2.5, the lemma is proved. □

Lemma 2.7 ([6]) *The equation*

$$2X^2 + 1 = Y^n, \quad X, Y, n \in \mathbb{N}, n > 3 \tag{2.8}$$

has no solutions (X, Y, n).

Lemma 2.8 *The equation*

$$X^2 - Y^4 = p^{2n}, \quad X, Y, n \in \mathbb{N}, \gcd(X, Y) = 1 \tag{2.9}$$

has only the solutions $(p, X, Y, n) = (u(2^m), v^2(2^m) + 1, v(2^m), 1)$, *where* m *is a nonnegative integer.*

Proof Assume that (p, X, Y, n) is a solution of (2.9). If $p = 2$, since $\gcd(X, Y) = 1$, then we have $2 \nmid XY$, $\gcd(X + Y^2, X - Y^2) = 2$, $X + Y^2 = 2^{2n-1}$, $X - Y^2 = 2$ and $Y^2 = 2^{2n-2} - 1$. But since $Y^2 + 1$ is not a square, it is impossible.

If p is an odd prime, then we have $\gcd(X+Y^2, X-Y^2)=1$, and by (2.9), we get $X+Y^2=p^{2n}$, $X-Y^2=1$,

$$2X = p^{2n}+1 \tag{2.10}$$

and

$$2Y^2 = p^{2n}-1. \tag{2.11}$$

By Lemma 2.7, we get from (2.11) that $n=1$ and

$$p^2-2Y^2=1. \tag{2.12}$$

Further, applying Lemma 2.1 to (2.12) yields

$$p=u(n), \qquad Y=v(n), \quad n\in\mathbb{N}. \tag{2.13}$$

Further, by Lemma 2.2, we see from the first equality of (2.13) that $n=2^m$. Thus, by (2.10) and (2.13), the lemma is proved. □

3 Proof of Theorem 1.1

Assume that $(x,\pm y)$ is a pair of non-trivial integer points on (1.2). Since $y>0$, we have $x>0$ and x can be expressed as

$$x=p^t z, \quad t\in\mathbb{Z}, t\geq 0, z\in\mathbb{N}, p\nmid z. \tag{3.1}$$

Substituting (3.1) into (1.2) yields

$$p^t z\left(p^{2t}z^2+p^{2r}\right)=y^2. \tag{3.2}$$

We first consider the case that $r>t$. By (3.2), we have

$$p^{3t}z\left(z^2+p^{2r-2t}\right)=y^2. \tag{3.3}$$

Since $p\nmid z$, we have $p\nmid z^2+p^{2r-2t}$ and $\gcd(z, z^2+p^{2k-2r})=1$. Hence by (3.3), we get

$$\begin{aligned} &t=2s, \qquad z=f^2, \qquad z^2+p^{2r-2t}=g^2, \qquad y=p^{3s}fg,\\ &\quad s\in\mathbb{Z}, s\geq 0, f,g\in\mathbb{N}, \gcd(f,g)=1, \end{aligned} \tag{3.4}$$

whence we obtain

$$g^2-f^4=p^{2r-4s}. \tag{3.5}$$

Applying Lemma 2.8 to (3.5) yields

$$p=u\left(2^m\right), \qquad 2r-4s=2, \qquad f=v\left(2^m\right), \qquad g=v^2\left(2^m\right)+1, \quad m\in\mathbb{Z}, m\geq 0. \tag{3.6}$$

Therefore, by (3.1), (3.4), and (3.6), the integer points of type (i) are given.

We next consider the case that $r = t$. Then we have

$$p^{3r}z\left(z^2+1\right) = y^2. \tag{3.7}$$

Since $p \nmid z$, $\gcd(z, z^2+1) = 1$ and z^2+1 is not a square, we see from (3.7) that

$$\begin{aligned} &r = 2s+1, \qquad z = f^2, \qquad z^2+1 = pg^2, \qquad y = p^{3s+2}fg, \\ &\quad s \in \mathbb{Z}, s \geq 0, f, g \in \mathbb{N}, \gcd(f,g) = 1. \end{aligned} \tag{3.8}$$

By (3.8), we get

$$f^4 - pg^2 = -1. \tag{3.9}$$

It implies that $(X, Y) = (f, g)$ is a solution of (1.5). Therefore, by (3.1) and (3.8), we obtain the integer points of type (ii).

We finally consider the case that $r < t$. Then we have

$$p^{t+2r}z\left(p^{2t-2r}z^2+1\right) = y^2. \tag{3.10}$$

Since $p \nmid z(p^{2t-2r}z^2+1)$ and $\gcd(z, p^{2t-2r}z^2+1) = 1$, we see from (3.10) that $p^{2t-2r}z^2+1$ is a square, a contradiction.

To sum up, the theorem is proved.

4 Proof of Theorem 1.2

By (2.3), if $p = u(2^m)$ with $m \geq 1$, then $p \equiv 1 \pmod 8$. Therefore, by Theorem 1.1, if $p \not\equiv 1 \pmod 8$, then (1.2) has only the non-trivial integer point

$$p = 3, \qquad r = 2s+1, \qquad (x, \pm y) = \left(3^{2s} \cdot 4, \pm 3^{3s} \cdot 10\right). \tag{4.1}$$

It implies that the theorem is true for $p \not\equiv 1 \pmod 8$.

For $p \equiv 1 \pmod 8$, let N_1 and N_2 denote the number of pairs of non-trivial integer points of types (i) and (ii) in Theorem 1.1, respectively. Obviously, we have

$$N\left(p^{2r}\right) = N_1 + N_2 \tag{4.2}$$

and $N_1 \leq 1$. By Lemma 2.4, we get $N_2 \leq 1$. Hence, by (4.2), we have $N(p^{2r}) \leq 2$ for $p \equiv 1 \pmod 8$. Since $u(2) = 17$ and (1.5) has the solution $(X, Y) = (2, 1)$ for $p = 17$, by Theorem 1.1, we get

$$\begin{aligned} &p = 17, \qquad r = 2s+1, \qquad (x, \pm y) = \left(17^{2s} \cdot 144, \pm 17^{3s} \cdot 1{,}740\right) \quad \text{and} \\ &\left(17^{2s+1} \cdot 4, \pm 17^{3s+2} \cdot 2\right) \end{aligned} \tag{4.3}$$

and $N(17^{2(2s+1)}) = 2$. However, by Lemma 2.6, if $p = u(2^m)$ with $m > 1$, then $N_2 = 0$. Therefore, by (4.2), if $p \equiv 1 \pmod 8$, then $N(p^{2r}) \leq 1$, except with $N(17^{2(2s+1)}) = 2$. The theorem is proved.

Competing interests
The authors declare that they have no competing interests.

Authors' contributions
JZ obtained the theorems and completed the proof. XL corrected and improved the final version. Both authors read and approved the final manuscript.

Author details
[1]School of Mathematics and Computer Engineering, University of Arts and Science, Xi'an, Shaanxi, P.R. China.
[2]Department of Mathematics, Northwest University, Xi'an, Shaanxi, P.R. China.

Acknowledgements
The authors would like to thank the referees for their very helpful and detailed comments, which have significantly improved the presentation of this paper. This work is supported by the P.E.D. (2013JK0573) and N.S.F. (11371291) of P.R. China.

Received: 22 January 2014 Accepted: 20 February 2014 Published: 04 Mar 2014

References

1. Bremner, A, Cassels, JWS: On the equation $Y^2 = X(X^2 + p)$. Math. Comput. **42**, 247-264 (1984)
2. Draziotis, KA: Integer points on the curve $Y^2 = X^3 \pm p^k X$. Math. Comput. **75**, 1493-1505 (2006)
3. Walsh, PG: Integer solutions to the equation $y^2 = x(x^2 \pm p^k)$. Rocky Mt. J. Math. **38**(4), 1285-1302 (2008)
4. Hardy, GH, Wright, EM: An Introduction to the Theory of Numbers, 5th edn. Oxford University Press, Oxford (1979)
5. Cohn, JHE: The Diophantine equation $x^4 + 1 = Dy^2$. Math. Comput. **66**, 1347-1351 (1997)
6. Nagell, T: Sur l'impossibilité de quelques equations à deux indéterminées. Norsk Mat. Forenings Skr. **13**(1), 65-82 (1921)

10.1186/1029-242X-2014-104
Cite this article as: Zhang and Li: The upper bound estimate of the number of integer points on elliptic curves $y^2 = x^3 + p^{2r}x$. *Journal of Inequalities and Applications* 2014, 2014:104