Journal of Inequalities and Applications
a SpringerOpen Journal

RESEARCH Open Access

An exact upper bound estimate for the number of integer points on the elliptic curves $y^2 = x^3 - p^k x$

Su Gou[1] and Xiaoxue Li[2*]

*Correspondence: lxx20072012@163.com
[2]School 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 k be a fixed odd positive integer. Further let $N(p^k)$ denote the number of pairs of integer points $(x, \pm y)$ on the elliptic curve $E : y^2 = x^3 - p^k x$ with $y > 0$. Using some properties of the Diophantine equations, we gave an exact upper bound estimate for $N(p^k)$. That is, we proved that $N(p^k) \le 4$.

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 on the elliptic curve

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

have been investigated in many papers (see [1–3] and [4]). In this paper we will deal with the number of integer points on (1.1) for odd k.

An integer point (x, y) on (1.1) is called trivial or non-trivial according to whether $y = 0$ or not. Obviously, for odd k, (1.1) has only the trivial integer point $(x, y) = (0, 0)$. If (x, y) is a non-trivial integer point on (1.1), then $(x, -y)$ is too. Therefore, (x, y) along with $(x, -y)$ are called a pair of non-trivial integer points and denoted by $(x, \pm y)$ with $y > 0$. Let a, b be coprime positive integers and s be a nonnegative integer. Using some properties of the Diophantine equations, we give an exact upper bound estimate for $N(p^k)$. That is, we shall prove the following results.

Theorem 1.1 *For any odd integer $k \ge 1$, all non-trivial integer points on* (1.1) *are given as follows*:

(i) $p = 2$, $k = 4s + 1$, $(x, \pm y) = (-2^{2s}, \pm 2^{3s})$, $(2^{2s+1}, \pm 2^{3s+1})$ *and* $(2^{2s+1} \cdot 169, \pm 2^{3s+1} \cdot 3107)$.

(ii) $p = 2$, $k = 4s + 3$, $(x, \pm y) = (2^{2s} \cdot 9, \pm 2^{3s} \cdot 21)$.

(iii) $p = 23$, $k = 4s + 3$, $(x, \pm y) = (23^{2s} \cdot 6084, \pm 23^{3s} \cdot 474474)$.

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

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

(vi) $p^3 = a^4 + b^2$, $k = 4s + 3$, $(x, \pm y) = (-p^{2s} a^2, \pm p^{3s} ab)$.

(vii) *p is an odd prime with* $p \equiv 1 (\bmod 4)$,

$$k = \begin{cases} 4s+1, \\ 4s+3, \end{cases}$$

$$(x, \pm y) = \begin{cases} (p^{2s+(n+1)/2} Y^2, \pm p^{3s+(n+3)/4} XY), & n \equiv 1 (\bmod 4), \\ (p^{2s+(n+3)/2} Y^2, \pm p^{3s+(n+9)/4} XY), & n \equiv 3 (\bmod 4), \end{cases}$$

where (X, Y, n) *is a solution of the equation*

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

Theorem 1.2 *Let* $N(p^k)$ *denote the number of pairs of non-trivial integer points on* (1.1). *For odd* k, *if* $p \not\equiv 1 (\bmod 4)$, *then*

$$N(p^k) = \begin{cases} 3, & \text{for } p = 2 \text{ and } k \equiv 1 (\bmod 4), \\ 1, & \text{for } p = 2 \text{ and } k \equiv 3 (\bmod 4), p = 23 \text{ and } k \equiv 3 (\bmod 4), \\ & \text{or } p = 2a^2 - 1 \text{ and } k \equiv 1 (\bmod 4), \\ 0, & \text{otherwise.} \end{cases} \tag{1.3}$$

If $p \equiv 1 (\bmod 4)$, *then*

$$N(p^k) \le \begin{cases} 4, & \text{for } k \equiv 1 (\bmod 4), \\ 2, & \text{for } k \equiv 3 (\bmod 4). \end{cases} \tag{1.4}$$

2 Preliminaries

Lemma 2.1 ([5]) *The equation*

$$X^2 - 2Y^4 = -1, \quad X, Y \in \mathbb{N} \tag{2.1}$$

has only the solutions $(X, Y) = (1, 1)$ *and* $(239, 13)$.

Lemma 2.2 ([6, Theorem D]) *Let* D *be a non-square positive integer. If* $D \ge 3$, *then the equation*

$$X^2 - DY^4 = -1, \quad X, Y \in \mathbb{N} \tag{2.2}$$

has at most one solution (X, Y).

Lemma 2.3 ([7]) *The equation*

$$X^2 - Y^n = 1, \quad X, Y, n \in \mathbb{N}, \min\{X, Y, n\} > 1 \tag{2.3}$$

has only the solution $(X, Y, n) = (3, 2, 3)$.

Lemma 2.4 ([8, Proposition 8.1]) *The equation*

$$2X^2 - Y^n = 1, \quad X, Y \in \mathbb{N}, \min\{X, Y\} > 1, 2 \nmid n \tag{2.4}$$

has only the solutions $(X, Y, n) = (78, 23, 3)$ *and* $(a, 2a^2 - 1, 1)$, *where a is a positive integer with* $a > 1$.

Lemma 2.5 *The equation*

$$X^4 - Y^2 = 2^n, \quad X, Y, n \in \mathbb{N}, \gcd(X, Y) = 1 \tag{2.5}$$

has only the solution $(X, Y, n) = (3, 7, 5)$.

Proof By (2.5), since $\gcd(X, Y) = 1$, both X and Y are odd and $\gcd(X^2 + Y, X^2 - Y) = 2$. Hence, we have $X^2 + Y = 2^{n-1}$, $X^2 - Y = 2$ and

$$X^2 = 2^{n-2} + 1, \qquad Y = 2^{n-2} - 1. \tag{2.6}$$

Applying Lemma 2.3 to the first equality of (2.6), we only get $X = 3$ and $n = 5$. Therefore, by the second equality of (2.6), (2.5) has only the solution $(X, Y, n) = (3, 7, 5)$. The lemma is proved. □

Lemma 2.6 *If p is an odd prime, then the equation*

$$X^4 - Y^2 = p^n, \quad X, Y, n \in \mathbb{N}, \gcd(X, Y) = 1, 2 \nmid n \tag{2.7}$$

has only the solutions $(p, X, Y, n) = (23, 78, 6083, 3)$ *and* $(2a^2 - 1, a, a^2 - 1, 1)$, *where a is a positive integer with* $a > 1$.

Proof By (2.7), since $2 \nmid p$ and $\gcd(X, Y) = 1$, we have $2 \mid XY$, $\gcd(X^2 + Y, X^2 - Y) = 1$, $X^2 + Y = p^n$, $X^2 - Y = 1$ and

$$2X^2 = p^n + 1, \qquad 2Y = p^n - 1. \tag{2.8}$$

Since $2 \nmid n$, applying Lemma 2.4 to the first equality of (2.8), we get either $(X, p, n) = (78, 23, 3)$ or $(X, p, n) = (a, 2a^2 - 1, 1)$. Thus, by the second equality of (2.8), the lemma is proved. □

Lemma 2.7 ([9, Theorem 278]) *For any fixed positive integer n, if* $p \equiv 1 \pmod 4$, *then the equation*

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

has exactly one solution (X, Y). *If* $p \equiv 3 \pmod 4$, *then* (2.9) *has no solution.*

Lemma 2.8 ([10, p.630]) *The equation*

$$X^4 + Y^4 = Z^3, \quad X, Y, Z \in \mathbb{N}, \gcd(X, Y) = 1 \tag{2.10}$$

has no solution (X, Y, Z).

Lemma 2.9 ([11, Theorem 1]) *The equation*

$$X^4 + Y^2 = Z^n, \quad X, Y, Z, n \in \mathbb{N}, \gcd(X, Y) = 1, n > 3 \tag{2.11}$$

has no solution (X, Y, Z, n).

3 Proof of Theorem 1.1

Assume that $2 \nmid k$ and $(x, \pm y)$ is a pair of non-trivial integer points on (1.1). Since $y > 0$, we have $x \neq 0$ and either $0 > x > -p^{k/2}$ or $x > p^{k/2}$.

We first consider the case that $0 > x > -p^{k/2}$. Then x can be expressed as

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

Applying (3.1) to (1.1) yields

$$p^{3r} z\left(p^{k-2r} - z^2\right) = y^2. \tag{3.2}$$

Further, since $p \nmid z$ and $p^k > x^2 \geq p^{2r}$, we have $p \nmid z(p^{k-2r} - z^2)$ and $\gcd(z, p^{k-2r} - z^2) = 1$. Therefore, by (3.2), we get

$$r = 2s, \qquad z = f^2, \qquad p^{k-2r} - z^2 = g^2, \qquad y = p^{3s} fg, \quad f, g, s \in N, \gcd(f, g) = 1, \tag{3.3}$$

whence we obtain

$$f^4 + g^2 = p^{k-4s}. \tag{3.4}$$

If $p = 2$, then from (3.4) we get $k - 4s = 1$ and $f = g = 1$. Hence, by (3.1) and (3.3), we obtain

$$p = 2, \qquad k = 4s + 1, \qquad (x, \pm y) = \left(-2^{2s}, \pm 2^{3s}\right). \tag{3.5}$$

If p is an odd prime, applying Lemma 2.9 to (3.4), we get either $k - 4s = 1$ or $k - 4s = 3$. Therefore, by (3.1), (3.3), and (3.4), we obtain the integer points of types (v) and (vi).

We next consider the case that $x > p^{k/2}$. Then x can be expressed as

$$x = p^r z, \quad r \in \mathbb{Z}, r \geq 0, z \in \mathbb{N}, p \nmid z. \tag{3.6}$$

Case I: $k > 2r$.

By (1.1) and (3.6), we have

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

Since $p \nmid z(z^2 - p^{k-2r})$ and $\gcd(z, z^2 - p^{k-2r}) = 1$, by (3.7), we get

$$\begin{gathered} r = 2s, \qquad z = f^2, \qquad z^2 - p^{k-2r} = g^2, \qquad y = p^{3s} fg, \\ s \in \mathbb{Z}, s \geq 0, f, g \in \mathbb{N}, \gcd(f, g) = 1, \end{gathered} \tag{3.8}$$

and hence,

$$f^4 - g^2 = p^{k-4s}. \tag{3.9}$$

If $p = 2$, applying Lemma 2.5 to (3.9), we get $k - 4s = 3$, $f = 3$ and $g = 7$. Therefore, by (3.6) and (3.8), we obtain the integer points of type (ii).

If p is an odd prime, applying Lemma 2.6 to (3.9) yields either $p = 23$, $k - 4s = 3$, $f = 78$ and $g = 6083$ or $p = 2a^2 - 1$, $k - 4s = 1$, $f = a$, and $g = a^2 - 1$. Therefore, by (3.6) and (3.8), we obtain the integer points of types (iii) and (iv).

Case II: $k < 2r$.

Then we have $p^{r+k}z(p^{2r-k}z^2 - 1) = y^2$ and

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

whence we get

$$g^2 - p^{4t-3k} f^4 = -1. \tag{3.11}$$

If $p = 2$, then from (3.11) we get $4t - 3k = 1$. It implies that $t \equiv 1 (\mathrm{mod} 3)$ and $t = 3s + 1$, where s is a nonnegative integer. Hence, we have $k = 4s + 1$ and $r = 2s + 1$. Further, by Lemma 2.1, we get from (3.11) that $(f, g) = (1, 1)$ and $(239, 13)$. Therefore, by (3.6) and (3.10), we obtain

$$p = 2, \qquad k = 4s + 1, \qquad (x, \pm y) = \left(2^{2s+1}, \pm 2^{3s+1}\right), \left(2^{2s+1} \cdot 169, \pm 2^{3s+1} \cdot 3107\right). \tag{3.12}$$

If p is an odd prime, we see from (3.11) that (1.2) has a solution

$$(X, Y, n) = (g, f, 4t - 3k). \tag{3.13}$$

While $n \equiv 1 (\mathrm{mod} 4)$, since $n \equiv 4t - 3k \equiv -3k \equiv 1 (\mathrm{mod} 4)$, we have $k \equiv 1 (\mathrm{mod} 4)$ and $k = 4s + 1$, where s is a nonnegative integer. Hence, we get $t = 3s + (n + 3)/4$ and $r = 2s + (n + 1)/2$. Therefore, by (3.6), (3.10), and (3.13), we obtain

$$k = 4s + 1, \qquad (x, \pm y) = \left(p^{2s+(n+1)/2} Y^2, \pm p^{3s+(n+3)/4} XY\right). \tag{3.14}$$

While $n \equiv 3 (\bmod 4)$, since $n \equiv 4t - 3k \equiv -3k \equiv 3 (\bmod 4)$, we have $k \equiv 3 (\bmod 4)$ and $k = 4s + 3$. Hence, we get $t = 3s + (n + 9)/4$ and $r = 2s + (n + 3)/2$. Therefore, by (3.6), (3.10), and (3.13), we obtain

$$k = 4s + 3, \qquad (x, \pm y) = \left(p^{2s+(n+3)/2} Y^2, \pm p^{3s+(n+9)/4} XY\right). \tag{3.15}$$

Combining of (3.14) and (3.15), we get the integer points of type (vii).

Finally, by (3.5) and (3.12), we obtain the integer points of type (i). To sum up, all nontrivial integer points on (1.1) are determined. The theorem is proved.

4 Proof of Theorem 1.2

Since $p \equiv 1 \pmod 4$ if (1.1) has integer points belonging to one of types (v), (vi), and (vii), by Theorem 1.1, (1.3) is true.

For $p \not\equiv 1 \pmod 4$, let N_j ($j = 4, 5, 6, 7$) denote the number of pairs of integer points of types (iv), (v), (vi), and (vii) respectively. Then we have

$$N(p^k) = N_4 + N_5 + N_6 + N_7. \tag{4.1}$$

Since p and k are fixed, we get

$$N_4 \begin{cases} \le 1, & \text{if } k \equiv 1 \pmod 4, \\ = 0, & \text{if } k \equiv 3 \pmod 4. \end{cases} \tag{4.2}$$

By Lemmas 2.7 and 2.8, we have

$$N_5 \begin{cases} \le 2, & \text{if } k \equiv 1 \pmod 4, \\ = 0, & \text{if } k \equiv 3 \pmod 4, \end{cases} \qquad N_6 \begin{cases} = 0, & \text{if } k \equiv 1 \pmod 4, \\ \le 1, & \text{if } k \equiv 3 \pmod 4. \end{cases} \tag{4.3}$$

On the other hand, for any fixed $\delta \in \{1, 3\}$, by Lemma 2.2, (1.2) has at most one solution (X, Y, n) satisfying $n \equiv \delta \pmod 4$. It implies that

$$N_7 \le 1. \tag{4.4}$$

Therefore, the combination of (4.1)-(4.4) yields (1.4). The theorem is proved.

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

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

Author details
[1]School of Science, Xi'an University of Posts and Telecommunications, Xi'an, Shaanxi, P.R. China. [2]School of Mathematics, Northwest University, Xi'an, Shaanxi, P.R. China.

Acknowledgements
The authors would like to thank the referee for his very helpful and detailed comments, which have significantly improved the presentation of this paper. This work is supported by the S. R. P. F. (12JK0883) of Shaanxi Provincial Education Department and G. I. C. F. (YZZ13075) of NWU.

Received: 4 April 2014 Accepted: 29 April 2014 Published: 13 May 2014

References

1. Draziotis, KA: Integer points on the curve $Y^2 = X^3 \pm p^k X$. Math. Comput. **75**(255), 1493-1505 (2006)
2. Fujita, Y, Terai, N: Integer points and independent points on the elliptic curve $y^2 = x^3 - p^k x$. Tokyo J. Math. **34**(2), 367-381 (2011)
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. Walsh, PG: Maximal ranks and integer points on a family of elliptic curves. Glas. Mat. **44**(1), 83-87 (2009)
5. Ljunggren, W: Zur Theorie der Gleichung $x^2 + 1 = Dy^4$. Avh. Nor. Vidensk. Akad. Oslo **1**(5), 1-27 (1942)
6. Chen, J-H, Voutier, PM: Complete solution of the Diophantine equation $X^2 + 1 = dY^4$ and a related family of quartic Thue equation. J. Number Theory **62**(1), 71-99 (1997)
7. Ko, C: On the Diophantine equation $x^2 = y^n + 1$, $xy \neq 0$. Sci. Sin. **14**(5), 457-460 (1964)
8. Bennett, MA, Skinner, CM: Ternary Diophantine equations via Galois representations and modular forms. Can. J. Math. **56**(1), 23-54 (2004)
9. Hardy, GH, Wright, EM: An Introduction to Number Theory, 5th edn. Oxford University Press, Oxford (1981)
10. Dickson, LE: History of the Theory of Numbers. Chelsea, New York (1971)
11. Bennett, MA, Ellenberg, JS, Ng, NC: The Diophantine equation $A^4 + 2^\delta B^2 = C^n$. Int. J. Number Theory **6**(2), 311-338 (2010)

10.1186/1029-242X-2014-187
Cite this article as: Gou and Li: An exact upper bound estimate for the number of integer points on the elliptic curves $y^2 = x^3 - p^k x$. *Journal of Inequalities and Applications* 2014, 2014:187