Czechoslovak Mathematical Journal

Hai Yang; Ruiqin Fu

Integral points on the elliptic curve $y^2 = x^3 - 4p^2x$

Czechoslovak Mathematical Journal, Vol. 69 (2019), No. 3, 853–862

Persistent URL: `http://dml.cz/dmlcz/147793`

INTEGRAL POINTS ON THE ELLIPTIC CURVE $y^2 = x^3 - 4p^2x$

Hai Yang, Ruiqin Fu, Xi'an

Received November 21, 2017. Published online March 26, 2019.

Abstract. Let p be a fixed odd prime. We combine some properties of quadratic and quartic Diophantine equations with elementary number theory methods to determine all integral points on the elliptic curve $E\colon\ y^2 = x^3 - 4p^2x$. Further, let $N(p)$ denote the number of pairs of integral points $(x, \pm y)$ on E with $y > 0$. We prove that if $p \geqslant 17$, then $N(p) \leqslant 4$ or 1 depending on whether $p \equiv 1 \pmod 8$ or $p \equiv -1 \pmod 8$.

Keywords: elliptic curve; integral point; quadratic equation; quartic Diophantine equation

MSC 2010: 11G05, 11D25, 11Y50

1. Introduction

Let $\mathbb{Z}, \mathbb{N}$ be the sets of all integers and positive integers, respectively. For any fixed positive integer n, the elliptic curve

$$E\colon\ y^2 = x^3 - n^2x \tag{1.1}$$

is related to the famous congruent number problem (see [12]). The computation of integral points on (1.1) has been investigated in many papers (see [1], [3], [4], [5], [6], [7], [8], [10], [11], [12], [13], [14] and [15]). For instance, Bremner, Silverman and Tzanakis in [3] determined all integral points on (1.1) for $1 \leqslant n \leqslant 72$.

Let p be a fixed odd prime. In this paper we deal with the integral points on (1.1) for $n = 2p$, namely,

$$E\colon\ y^2 = x^3 - 4p^2x. \tag{1.2}$$

This work is supported by N.S.F. (11226038, 11371012) of P. R. China, the N.S.F. (2017JM1025) of Shaanxi Province, the Education Department Foundation of Shaanxi Province (17JK0323) and Scientific Research Foundation for Doctor of Xi'an Shiyou University (2015BS06).

DOI: 10.21136/CMJ.2019.0529-17

An integral point (x, y) on (1.2) is called trivial or nontrivial according to whether $y = 0$ or not. Obviously, the only trivial integral points on (1.2) are given by $(x, y) = (0, 0)$, $(2p, 0)$ and $(-2p, 0)$. Notice that if (x, y) is a nontrivial integral point on (1.2), then $(x, -y)$ is also. Therefore, (x, y) along with $(x, -y)$ are called a pair of nontrivial integral points and denoted by $(x, \pm y)$ with $y > 0$. We will determine all nontrivial integral points on (1.2) and give an upper bound for their number.

We now introduce some notations and symbols. Let a, b, k be positive integers with $\gcd(a, b) = 1$. Any fixed positive integer c can be uniquely expressed as $c = dm^2$, where d, m are positive integers with d being square free. Then d is called the quadratic free number of c (see [9], Section 2.6), d and m are denoted by $Q(c)$ and $R(c)$, respectively. For any nonnegative integer t let

$$U_t = \frac{1}{2}(\alpha^t + \beta^t), \quad V_t = \frac{1}{2\sqrt{2}}(\alpha^t - \beta^t), \tag{1.3}$$

where

$$\alpha = 1 + \sqrt{2}, \quad \beta = 1 - \sqrt{2}. \tag{1.4}$$

It is a well known fact that $(U, V) = (U_{2i+1}, V_{2i+1})$ $(i = 0, 1, 2, \ldots)$ and $(u, v) = (U_{2i}, V_{2i})$ $(i = 1, 2, \ldots)$ are all solutions of Pell's equations

$$U^2 - 2V^2 = -1, \quad U, V \in \mathbb{N} \tag{1.5}$$

and

$$u^2 - 2v^2 = 1, \quad u, v \in \mathbb{N}, \tag{1.6}$$

respectively (see [9], Theorem 244).

Using certain properties of quadratic and quartic Diophantine equations, we will prove the following result:

Theorem 1.1. *If $p \geqslant 17$, then all nontrivial integral points on (1.2) are given as follows:*

(i) $p = a^4 + b^4$, $(x, \pm y) = (-4a^2b^2, \pm 4ab|a^4 - b^4|)$.

(ii) $p = a^4 + 12a^2b^2 + 4b^4$, $(x, \pm y) = (-2(a^2 - 2b^2)^2, \pm 16ab|a^4 - 4b^4|)$.

(iii) $p = 4V_{2k+1} + 3\delta$, $\delta \in \{1, -1\}$,

$$(x, \pm y) = \begin{cases} (2(U_k^2 + 2V_{k+1}^2)^2, \pm 16U_kV_{k+1}(4V_{k+1}^4 - U_k^4)) \\ \qquad \text{if } 2 \mid k \text{ and } \delta = 1 \text{ or } 2 \nmid k \text{ and } \delta = -1, \\ (2(U_{k+1}^2 + 2V_k^2)^2, \pm 16U_{k+1}V_k(U_{k+1}^4 - 4V_k^4)), \\ \qquad \text{if } 2 \mid k \text{ and } \delta = -1 \text{ or } 2 \nmid k \text{ and } \delta = 1. \end{cases}$$

(iv) $p = Q(U_{4k})$, $(x, \pm y) = (2pU_{4k}, \pm 4p^2V_{4k}R(U_{4k}))$.

Let $N(P)$ denote the number of pairs of nontrivial integer points on (1.2). Recently, Bennett in [1] proved that if $p \geqslant 29$ and $p \equiv \pm 3 \pmod 8$, then $N(P) = 0$. By the above theorem, we obtain an upper bound for $N(P)$ for the remaining cases as follows:

Corollary 1.1. *If $p \geqslant 17$ and $p \equiv \pm 1 \pmod 8$, then*

$$N(p) \leqslant \begin{cases} 4 & \text{if } p \equiv 1 \pmod 8, \\ 1 & \text{if } p \equiv -1 \pmod 8. \end{cases} \tag{1.7}$$

Notice that if $p = 17$, then there exist four pairs of nontrivial integral points $(x, \pm y) = (-16, \pm 120), (-2, \pm 48), (162, \pm 2016)$ and $(578, \pm 13872)$ on (1.2). It implies that the upper bound (1.7) is attainable.

2. Preliminaries

Lemma 2.1 ([9], Theorem 279). *If $p \equiv 1 \pmod 4$, then the equation*

$$X^2 + Y^2 = p, \quad 2 \mid Y, \quad X, Y \in \mathbb{N} \tag{2.1}$$

has exactly one solution (X, Y). If $p \equiv 3 \pmod 4$, then (2.1) has no solution.

Lemma 2.2. *The equation*

$$X^4 + 12X^2Y^2 + 4Y^4 = p, \quad X, Y \in \mathbb{N} \tag{2.2}$$

has at most one solution (X, Y).

Proof. We now assume that (2.2) has two distinct solutions (X, Y) and (X', Y'). Then we have

$$p = (X^2 - 2Y^2)^2 + (4XY)^2 = (X'^2 - 2Y'^2)^2 + (4X'Y')^2. \tag{2.3}$$

Applying Lemma 2.1 to (2.3), we get

$$4XY = 4X'Y' \tag{2.4}$$

and

$$|X^2 - 2Y^2| = |X'^2 - 2Y'^2|. \tag{2.5}$$

By (2.2) and (2.4), we have $(X^2+2Y^2)^2 = X^4+4X^2Y^2+4Y^4 = (X^4+12X^2Y^2+4Y^4)-8X^2Y^2 = p-8X^2Y^2 = p-8X'^2Y'^2 = (X'^4+12X'^2Y'^2+4Y'^4)-8X'^2Y'^2 = (X'^2+2Y'^2)^2$. It implies that

$$X^2+2Y^2 = X'^2+2Y'^2. \tag{2.6}$$

The combination of (2.5) and (2.6) yields either $(X,Y)=(X',Y')$ or $X^2=2Y'^2$, a contradiction. Thus, (2.2) has at most one solution (X,Y). The lemma is proved. □

Lemma 2.3. *If the equation*

$$X^4-12X^2Y^2+4Y^4 = p, \quad X,Y\in\mathbb{N} \tag{2.7}$$

has a solution (X,Y), *then*

$$p = 4V_{2k+1}-3, \quad k\in\mathbb{N}. \tag{2.8}$$

Moreover, if p *satisfies* (2.8), *then* (2.7) *has only the solution*

$$(X,Y)=\begin{cases}(U_{k+1},V_k) & \text{if } 2\mid k,\\ (U_k,V_{k+1}) & \text{if } 2\nmid k.\end{cases} \tag{2.9}$$

Proof. We now assume that (X,Y) is a solution of (2.7). Then we have

$$p=(X^2+2Y^2)-(4XY)^2=(X^2+4XY+2Y^2)(X^2-4XY+2Y^2). \tag{2.10}$$

Notice that $X^2+4XY+2Y^2>1$ and p is an odd prime. By (2.10), we get

$$X^2+4XY+2Y^2=p \tag{2.11}$$

and

$$X^2-4XY+2Y^2=(X-2Y)^2-2Y^2=1. \tag{2.12}$$

We see from (2.12) that (1.6) has the solution $(u,v)=(|X-2Y|,Y)$. Hence, we have

$$X-2Y=\lambda U_{2t},\ Y=V_{2t},\ \lambda\in\{1,-1\},\ t\in\mathbb{N}. \tag{2.13}$$

When $\lambda = 1$, then from (1.3), (1.4) and (2.13), we have

$$X = U_{2t} + 2V_{2t} = \frac{\alpha^{2t} + \beta^{2t}}{2} + \frac{\alpha^{2t} - \beta^{2t}}{\sqrt{2}} = \frac{\alpha^{2t+1} + \beta^{2t+1}}{2} = U_{2t+1}. \tag{2.14}$$

Substituting (2.12), (2.13) and (2.14) into (2.11) yields

$$p = (X^2 - 4XY + 2Y^2) + 8XY = 1 + 8U_{2t+1}V_{2t} = 4V_{4t+1} - 3. \tag{2.15}$$

Let $k = 2t$. We see from (2.15) that p satisfies (2.8) with $2 \mid k$. Moreover, since p is fixed and $\{V_i\}_{i=1}^{\infty}$ is an increasing sequence, by (2.13) and (2.14), if p satisfies (2.8) with $2 \mid k$, then (2.7) has only the solution $(X, Y) = (U_{k+1}, V_k)$.

Similarly, when $\lambda = -1$, let $k = 2t - 1$, then p satisfies (2.8) with $2 \nmid k$, and (2.7) has only the solution $(X, Y) = (U_k, V_{k+1})$. Thus, the lemma is proved. $\square$

Using the same method as in the proof of Lemma 2.3, we can obtain the following lemma:

Lemma 2.4. *If $p > 7$ and the equation*

$$X^4 - 12X^2Y^2 + 4Y^4 = -p, \quad X, Y \in \mathbb{N} \tag{2.16}$$

has a solution (X, Y), then

$$p = 4V_{2k+1} + 3, \quad k \in \mathbb{N}. \tag{2.17}$$

Moreover, if p satisfies (2.17), then (2.16) has only the solution

$$(X, Y) = \begin{cases} (U_k, V_{k+1}) & \text{if } 2 \mid k, \\ (U_{k+1},\ V_k) & \text{if } 2 \nmid k. \end{cases} \tag{2.18}$$

Lemma 2.5. *The equation*

$$U_{2l} = pZ^2, \quad l, Z \in \mathbb{N} \tag{2.19}$$

has at most one solution (l, Z). Moreover, if $p > 11$, then the solution (l, Z) satisfies $2 \mid l$.

Proof. We now assume that (l, Z) is a solution of (2.19). Since $U_{2l}^2 - 2V_{2l}^2 = 1$, by (2.19) we have

$$p^2Z^4 - 2V_{2l}^2 = 1. \tag{2.20}$$

Thus, applying the results of [2] to (2.20), we obtain the lemma immediately. $\square$

Lemma 2.6. *If $p > 11$ and (2.19) has a solution (l, Z), then $p \equiv 1 \pmod 8$.*

P r o o f. By Lemma 2.5 we have $2 \mid l$ and

$$U_{4k} = pZ^2. \tag{2.21}$$

Further, by (1.3), (1.4) and (2.21), we get

$$pZ^2 = \frac{\alpha^{4k} + \beta^{4k}}{2} = \frac{1}{2}((\alpha^{2k} + \beta^{2k})^2 - 2(\alpha\beta)^{2k}) = 2U_{2k}^2 - 1. \tag{2.22}$$

Therefore, since $2 \nmid Z$ and $2 \nmid U_{2k}$, by (2.22) we obtain $p \equiv pZ^2 \equiv 2U_{2k}^2 - 1 \equiv 2 - 1 \equiv 1 \pmod 8$. The lemma is proved. □

3. Proof of the theorem

We now assume that $(x, \pm y)$ is a pair of nontrivial integral points on (1.2). Since $y > 0$, we have either $0 > x > -2p$ or $x > 2p$. The case $0 > x > -2p$ has been solved in [3] as follows:

Lemma 3.1. *If $p \geqslant 17$ and $0 > x > -2p$, then the integral points satisfy either type* (i) *or type* (ii).

For the case $x > 2p$, x can be expressed as

$$x = 2^r p^s z, \quad \gcd(2p,\ z) = 1, \quad r \geqslant 0,\ s \geqslant 0,\ r, s \in \mathbb{Z},\ z \in \mathbb{N}. \tag{3.1}$$

In this respect, by [3] we have the following result:

Lemma 3.2. *If $p \geqslant 17$ and $x > 2p$, then the integral points do not satisfy $r = 0$ or $s = 1$.*

By Lemma 3.1 and 3.2, it suffices to prove the theorem for the following four cases:

Case I: $r = 1$ and $s = 0$.

By (1.2) and (3.1) we have $z = 2z$ and

$$8z(z^2 - p^2) = y^2. \tag{3.2}$$

Since $\gcd(2p, z) = 1$, we get $\gcd(z, 8(z^2 - p^2)) = 1$, and by (3.2),

$$z = f^2, \quad z^2 - p^2 = 8g^2, \quad y = 8fg, \quad 2 \nmid f,\ \gcd(f, g) = 1,\ f, g \in \mathbb{N}. \tag{3.3}$$

By (3.3) we have

$$f^4 - p^2 = 8g^2, \quad p \nmid fg \tag{3.4}$$

and

$$f^2 + \lambda_1 p = 2l^2, \quad f^2 - \lambda_1 p = 4m^2, \quad g = lm,\ 2 \nmid l,\ \gcd(l, m) = 1, \quad \lambda_1 \in \{1, -1\}, \quad l, m \in \mathbb{N}. \tag{3.5}$$

Further, by (3.5) we get

$$f^2 = l^2 + 2m^2 \tag{3.6}$$

and

$$p = \lambda_1(l^2 - 2m^2). \tag{3.7}$$

Furthermore, by (3.6) we have

$$f + \lambda_2 l = 2a^2, \quad f - \lambda_2 l = 4b^2, \quad m = 2ab,\ 2 \nmid a,\ \gcd(a, b) = 1, \quad \lambda_2 \in \{1, -1\},\ a, b \in \mathbb{N}, \tag{3.8}$$

whence we get

$$f = a^2 + 2b^2 \tag{3.9}$$

and

$$l = \lambda_2(a^2 - 2b^2). \tag{3.10}$$

Substituting (3.8) and (3.10) into (3.7) yields

$$p = \lambda_1(a^4 - 12a^2b^2 + 4b^4). \tag{3.11}$$

Therefore, since $p \geqslant 17$, applying Lemma 2.3 and 2.4 to (3.11), by (3.3), (3.8), (3.9) and (3.10), we obtain the integral points of type (iii).

Case II: $r > 1$ and $s = 0$.

Now we see that $x = 2^r z$ and

$$2^{r+2} z(2^{2r-2} z^2 - p^2) = y^2. \tag{3.12}$$

Since $\gcd(z,\ 2^{r+2}(2^{2r-2}z^2 - p^2)) = 1$, by (3.12) we get

$$r = 2t, \quad z = f^2, \quad 2^{2r-2}z^2 - p^2 = g^2, \quad y = 2^{t+1}fg, \quad 2 \nmid fg, \quad \gcd(f, g) = 1, \quad f, g, t \in \mathbb{N}. \tag{3.13}$$

But by the third equality of (3.13), we have

$$0 \equiv 2^{2r-2}z^2 \equiv p^2 + g^2 \equiv 1 + 1 \equiv 2 \pmod 4,$$

a contradiction.

Case III: $r = 1$ and $s > 1$.

Now we see that $x = 2p^s z$ and

$$8p^{s+2}z(p^{2s-2}z^2 - 1) = y^2. \tag{3.14}$$

Since $\gcd(z, 8p^{s+2}(p^{2s-2}z^2 - 1)) = 1$, we get from (3.14) that

$$s = 2t, \quad z = f^2, \quad p^{2s-2}z^2 - 1 = 8g^2, \quad y = 8p^{t+1}fg, \quad 2 \nmid f, \quad \gcd(f,\ g) = 1, \quad f, g, t \in \mathbb{N}, \tag{3.15}$$

whence we obtain

$$(p^{2t-1}f^2)^2 - 2(2g)^2 = 1. \tag{3.16}$$

Comparing (3.16) with (1.6), we have

$$p^{2t-1}f^2 = U_{2l},\ 2g = V_{2l},\ l \in \mathbb{N}. \tag{3.17}$$

Further, since $p \geqslant 17$, applying Lemma 2.5 to the first equality of (3.17), we get $2 \mid l$. So we have $l = 2k$, where k is a positive integer. Therefore, by the definition of quadratic free number, we see from (3.17) that

$$p = Q(U_{4k}),\ p^{t-1}f = R(U_{4k}). \tag{3.18}$$

Thus, by (3.15) and (3.18) we obtain the integral points of type (iv).

Case IV: $r > 1$ and $s > 1$.

Now we see that $x = 2^r p^s z$ and

$$2^{r+2}p^{s+2}z(2^{2r-2}p^{2s-2}z^2 - 1) = y^2. \tag{3.19}$$

Since $\gcd(z, 2^{r+2}p^{s+2}(2^{2r-2}p^{2s-2}z^2 - 1)) = 1$, we see from (3.19) that $2 \mid r$, $2 \mid s$ and

$$2^{2r-2}p^{2s-2}z^2 - 1 = g^2, \quad g \in \mathbb{N}. \tag{3.20}$$

But by (3.20) we get $1 = (2^{r-1}p^{s-1}z)^2 - g^2 \geqslant 2^{r-1}p^{s-1}z + g > 1$, a contradiction.

To sum up, the theorem is proved. $\square$

4. Proof of the corollary

Let $N_i(p)$ $(i = 1, 2, 3, 4)$ denote the numbers of pairs of integral points of type (i), (ii), (iii) and (iv), respectively. Then we have

$$N(p) = \sum_{i=1}^{4} N_i(p). \tag{4.1}$$

By Lemma 2.1 and 2.2, we have

$$N_j(p) \begin{cases} \leqslant 1 & \text{if } p \equiv 1 \pmod 8, \\ = 0 & \text{if } p \equiv -1 \pmod 8) \end{cases} \quad \text{for } j = 1, 2. \tag{4.2}$$

Notice that

$$4V_{2k+1} + 3\delta \equiv \begin{cases} -1 \pmod 8 & \text{if } \delta = 1, \\ 1 \pmod 8 & \text{if } \delta = -1, \end{cases}$$

and $\{4V_{2k+1} + 3\delta\}_{k=1}^{\infty}$ is an increasing sequence, where $\delta \in \{1, -1\}$. Therefore, by Lemma 2.3 and 2.4, we get

$$N_3(p) \leqslant 1. \tag{4.3}$$

By Lemma 2.5 and 2.6, we have

$$N_4(p) \begin{cases} \leqslant 1 & \text{if } p \equiv 1 \pmod 8, \\ = 0 & \text{if } p \equiv -1 \pmod 8. \end{cases} \tag{4.4}$$

Thus, the combination of (4.1), (4.2), (4.3) and (4.4) yields (1.7). The corollary is proved. □

Acknowledgements. The authors would like to thank the anonymous referees for their valuable suggestions.

References

[1] *M. A. Bennett*: Integral points on congruent number curves. Int. J. Number Theory *9* (2013), 1619–1640. zbl MR doi
[2] *M. A. Bennett, G. Walsh*: The Diophantine equation $b^2X^4 - dY^2 = 1$. Proc. Am. Math. Soc. *127* (1999), 3481–3491. zbl MR doi
[3] *A. Bremner, J. H. Silverman, N. Tzanakis*: Integral points in arithmetic progression on $y^2 = x(x^2 - n^2)$. J. Number Theory *80* (2000), 187–208. zbl MR doi
[4] *K. A. Draziotis*: Integer points on the curve $Y^2 = X^3 \pm p^k X$. Math. Comput. *75* (2006), 1493–1505. zbl MR doi

[5] *K. Draziotis, D. Poulakis*: Practical solution of the Diophantine equation $y^2 = x \times (x + 2^a p^b)(x - 2^a p^b)$. Math. Comput. *75* (2006), 1585–1593. zbl MR doi
[6] *K. Draziotis, D. Poulakis*: Solving the Diophantine equation $y^2 = x(x^2 - n^2)$. J. Number Theory *129* (2009), 102-121; corrigendum *129* (2009), 739–740. zbl MR doi
[7] *Y. Fujita, N. Terai*: Integer points and independent points on the elliptic curve $y^2 = x^3 - p^k x$. Tokyo J. Math. *34* (2011), 367–381. zbl MR doi
[8] *Y. Fujita, N. Terai*: Generators and integer points on the elliptic curve $y^2 = x^3 - nx$. Acta Arith. *160* (2013), 333–348. zbl MR doi
[9] *G. H. Hardy, E. M. Wright*: An Introduction to the Theory of Numbers. The Clarendon Press, Oxford University Press, New York, 1979. zbl MR
[10] *B. K. Spearman*: Elliptic curves $y^2 = x^3 - px$ of rank two. Math. J. Okayama Univ. *49* (2007), 183–184. zbl MR
[11] *B. K. Spearman*: On the group structure of elliptic curves $y^2 = x^3 - 2px$. Int. J. Algebra *1* (2007), 247–250. zbl MR doi
[12] *J. B. Tunnell*: A classical Diophantine problem and modular forms of weight 3/2. Invent. Math. *72* (1983), 323–334. zbl MR doi
[13] *P. G. Walsh*: Maximal ranks and integer points on a family of elliptic curves. Glas. Mat., III. Ser. *44* (2009), 83–87. zbl MR doi
[14] *P. G. Walsh*: On the number of large integer points on elliptic curves. Acta Arith. *138* (2009), 317–327. zbl MR doi
[15] *P. G. Walsh*: Maximal ranks and integer points on a family of elliptic curves II. Rocky Mt. J. Math. *41* (2011), 311–317. zbl MR doi

Authors' addresses: Hai Yang, School of Science, Xi'an Polytechnic University, Xi'an, Shaanxi, 710048, P. R. China, e-mail: `xpuyhai@163.com`; Ruiqin Fu, School of Science, Xi'an Shiyou University, Xi'an, Shaanxi, 710065, P. R. China, e-mail: `xsyfrq@163.com`.