ACADÉMIE
DES SCIENCES
INSTITUT DE FRANCE

Comptes Rendus

Mathématique

Tho Nguyen Xuan

Note on a symmetric Diophantine equation

Volume 363 (2025), p. 985-988

Online since: 5 September 2025

https://doi.org/10.5802/crmath.785

The Comptes Rendus. Mathématique *are a member of the*
Mersenne Center for open scientific publishing
www.centre-mersenne.org — e-ISSN : 1778-3569

ACADÉMIE DES SCIENCES
INSTITUT DE FRANCE

Comptes Rendus. Mathématique
2025, Vol. 363, p. 985-988
https://doi.org/10.5802/crmath.785

Research article / *Article de recherche*
Number theory / *Théorie des nombres*

Note on a symmetric Diophantine equation

Note sur une équation diophantienne symétrique

Tho Nguyen Xuan [a]

[a] Faculty of Mathematics and Informatics, Hanoi University of Science and Technology, Hanoi, Vietnam
E-mail: tho.nguyenxuan1@hust.edu.vn

Abstract. Using an elementary argument, we show that for all rational numbers α such that neither α nor 3α is a rational square, the equation

$$x^4 - 4\alpha x^2 - 4\alpha y^2 + y^4 = -6\alpha^2$$

has no rational solutions. This answers Hindes' two questions and generalizes his theorem (Theorem 1.1) in "Rational points on certain families of symmetric equations", *Int. J. Number Theory* **11** (2015), no. 6, pp. 1821–1838.

Résumé. En utilisant un argument élémentaire, nous montrons que pour tous les nombres rationnels α tels que ni α ni 3α n'est un carré rationnel, l'équation

$$x^4 - 4\alpha x^2 - 4\alpha y^2 + y^4 = -6\alpha^2$$

n'a pas de solutions rationnelles. Ceci répond aux deux questions de Hindes et généralise son théorème (Theorem 1.1) dans "Rational points on certain families of symmetric equations", *Int. J. Number Theory* **11** (2015), no. 6, pp. 1821–1838.

Keywords. Arithmetic geometry, Diophantine equations, rational points.

Mots-clés. Géométrie arithmétique, équations diophantiennes, points rationnels.

2020 Mathematics Subject Classification. 14G05, 14G12.

Funding. The author is supported by the Vietnam National Foundation for Science and Technology Development (NAFOSTED) (grant number 101.04-2023.21) and by Vietnam Institute for Advanced Study in Mathematics (VIASM) from April 2025 to May 2025. The author gratefully acknowledges the Institute for their support and funding.

Manuscript received 4 May 2025, revised and accepted 15 July 2025.

1. Introduction

Let $a, b \in \mathbb{Q}$. Consider the symmetric quartic equation

$$x^4 + ax^2 + ay^2 + y^4 = b \tag{1}$$

with rational numbers x, y. When $a = 0$, equation (1) reduces to the Fermat quartic

$$x^4 + y^4 = b. \tag{2}$$

Dem'janenko [6] studied rational solutions of (2) using the elliptic curve $y^2 = x(x^2 + b)$. Silverman [10] extended Dem'janenko's result to number fields. Hindes [8] further extended

Dem'janenko's method to study rational solutions of a family of equations (1) with $a \neq 0$. For each pair of rational numbers (a, b) with $b(a^2+4b)(a^2+2b) \neq 0$, let us define the curves

$$\begin{cases} F = F_{(a,b)}: x^4 + ax^2 + ay^2 + y^4 = b, \\ E = E_{(a,b)}: y^2 = x\big(x^2 - 4ax - (16b + 4a^2)\big). \end{cases} \tag{3}$$

There are two maps $\phi_1, \phi_2 \colon F_{(a,b)} \to E_{(a,b)}$ given by

$$\begin{cases} \phi_1(x, y) = \big(-4x^2, x(8y^2 + 4a)\big), \\ \phi_2(x, y) = \big(-4y^2, y(8x^2 + 4a)\big). \end{cases}$$

For each squarefree positive integer α, let $F^{(\alpha)} = F_{(\alpha\cdot a, \alpha^2 \cdot b)}$ and $E^{(\alpha)} = E_{(\alpha\cdot a, \alpha^2\cdot b)}$. Hindes [8, Theorem 1.1] proved the following theorem.

Theorem 1. *Let F and E be the symmetric quartic and elliptic curves defined in* (3) *corresponding to* $(a, b) = (-4, -6)$. *Then the following statements hold.*

(1) *If p is a prime number such that $p \equiv 1 \bmod 24$, then $F^{(p)}$ is everywhere locally solvable.*
(2) *The global root number $W(E^{(p)}) = -1$ for all positive, odd primes.*
(3) *If $\alpha > 7 \cdot 10^{74}$ is square-free and* $\operatorname{rank}\big(E^{(\alpha)}(\mathbb{Q})\big) \leq 1$, *then $F^{(\alpha)}(\mathbb{Q}) = \varnothing$.*
(4) *If $p \not\equiv \pm 1 \bmod 16$, then* $\operatorname{rank}(E^{(p)}) \leq 2$.
(5) *Assuming the parity conjecture, if $p > 3 \cdot 10^{74}$ and $p \equiv 25 \bmod 48$, then $F^{(p)}(\mathbb{Q}) = \varnothing$, and $F^{(p)}$ breaks the Hasse principle.*

Hindes posed the following two questions about Theorem 1.

(1) Is part (3) of Theorem 1 still true when $\alpha < 7 \cdot 10^{74}$ and $\alpha \neq 3$?
(2) Is $F^{(577)}(\mathbb{Q})$ empty?

In this paper, we answer these two questions by proving the following theorem.

Theorem 2. *Let α be a rational number such that α and 3α are not rational squares. Then the equation*

$$x^4 - 4\alpha x^2 - 4\alpha y^2 + y^4 = -6\alpha^2 \tag{4}$$

has no rational solutions.

Theorem 2 provides a significant generalization of parts (3) and (5) of Theorem 1. The conditions $\alpha > 7 \cdot 10^{74}$ and $\operatorname{rank}\big(E^{\alpha}(\mathbb{Q})\big) \leq 1$ in part (3) are not necessary. The assumption of the parity conjecture and the condition $p > 3 \cdot 10^{74}$ in part (5) are not required. In contrast to Hindes' approach, our proof of Theorem 1 is short and elementary. For other studies on the rational solutions to (2), see Bremner and Morton [3], Serre [9], Flynn and Wetherell [7], Cohen [5], and Bremner and Tho [4].

Combining part (1) of Theorem 1 with Theorem 2, we obtain the following corollary.

Corollary 3. *Let p be a prime number such that $p \equiv 1 \bmod 24$. Then:*

(1) *$F^{(p)}$ is everywhere locally soluble;*
(2) *$F^{(p)}(\mathbb{Q}) = \emptyset$.*

In particular, $F^{(p)}$ is a counterexample to the Hasse principle.

2. Proof of Theorem 2

Proof. Assume that (x, y) is a rational solution to (4). Equation (4) can be written in the form

$$(x^2 - 2\alpha)^2 + (y^2 - 2\alpha)^2 = 2\alpha^2. \tag{5}$$

Since the equation $X^2+Y^2=2$ has a parameterization

$$X=\frac{-t^2-2t-1}{t^2+1},\quad Y=\frac{t^2-2t-1}{t^2+1},$$

it follows from (5) that there exists a rational number t such that

$$\begin{cases} x^2-2\alpha &= \dfrac{(-t^2-2t-1)\alpha}{t^2+1},\\ y^2-2\alpha &= \dfrac{(t^2-2t-1)\alpha}{t^2+1}.\end{cases}$$

Hence

$$\begin{cases} x^2 &= \dfrac{(t^2-2t+3)\alpha}{t^2+1},\\ y^2 &= \dfrac{(3t^2-2t+1)\alpha}{t^2+1}.\end{cases} \tag{6}$$

Let $v=xy/\alpha$. Then we obtain

$$v^2=(t^2-2t+3)(3t^2-2t+1). \tag{7}$$

Let $\mathscr{C}$ be the quartic curve defined by (7). Since $\mathscr{C}$ has a rational point $(1,2)$, it is an elliptic curve. MAGMA [2] shows that a Weierstrass model of $\mathscr{C}$ is

$$y^2=x^3-x^2-2x, \tag{8}$$

which has the Mordell–Weil group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. Note that $\mathscr{C}$ with model (8) is labeled as 96A in Table I in the classical book of Birch and Kuyk [1]. The table also shows that $\mathscr{C}$ has rank 0 with the Mordell–Weil group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$.

Since equation (7) has four rational solutions $(t,v)=(\pm1,\pm2)$, they are all rational solutions of (7). It follows from (6) that if neither α nor 3α is a rational square, then (4) admits no rational solutions, completing the proof of Theorem (2). □

Acknowledgments

The author is indebted to the anonymous referee for pointing out the error in the previous version of the paper and sincerely appreciates the suggestion, which helped correct the error and improve the presentation of the paper.

Declaration of interests

The author does not work for, advise, own shares in, or receive funds from any organization that could benefit from this article, and has declared no affiliations other than their research organizations.

References

[1] B. J. Birch and W. Kuyk (eds.), *Modular functions of one variable. IV. Proceedings of the International Summer School on Modular Functions of One Variable and Arithmetical Applications, RUCA, University of Antwerp, Antwerp, July 17–August 3, 1972*, Lecture Notes in Mathematics, Springer, 1975, iv+151 pages.

[2] W. Bosma, J. Cannon and C. Playoust, “The Magma algebra system. I. The user language”, *J. Symb. Comput.* **24** (1997), no. 3-4, pp. 235–265.

[3] A. Bremner and P. Morton, “A new characterization of the integer 5906”, *Manuscr. Math.* **44** (1983), no. 1-3, pp. 187–229.

[4] A. Bremner and N. X. Tho, "On the Diophantine equation $x^4 + y^4 = c$", *Acta Arith.* **204** (2022), no. 2, pp. 141–150.

[5] H. Cohen, *Number theory. Vol. I. Tools and Diophantine equations*, Graduate Texts in Mathematics, Springer, 2007, xxiv+650 pages.

[6] V. A. Dem'janenko, "The indeterminate equations $x^6 + y^6 = az^2 x^6 + y^6 = az^3$, $x^4 + y^4 = az^4$", in *American Mathematical Society Translations, Ser. 2, Vol. 119* (L. J. Leifman, ed.), American Mathematical Society Translations, Series 2, vol. 119, American Mathematical Society, 1983, pp. 27–34.

[7] E. V. Flynn and J. L. Wetherell, "Covering collections and a challenge problem of Serre", *Acta Arith.* **98** (2001), no. 2, pp. 197–205.

[8] W. Hindes, "Rational points on certain families of symmetric equations", *Int. J. Number Theory* **11** (2015), no. 6, pp. 1821–1838.

[9] J.-P. Serre, *Lectures on the Mordell-Weil theorem* (M. Brown and M. Waldschmidt, eds.), Aspects of Mathematics, Vieweg & Sohn, 1989, x+218 pages.

[10] J. H. Silverman, "Rational points on certain families of curves of genus at least 2", *Proc. Lond. Math. Soc. (3)* **55** (1987), no. 3, pp. 465–481.