THE PUBLISHING HOUSE
OF THE ROMANIAN ACADEMY

PROCEEDINGS OF THE ROMANIAN ACADEMY, Series A
Volume 26, Number 2/2025, pp. 123–133
DOI: 10.59277/PRA-SER.A.26.2.03

THE DIOPHANTINE EQUATION $\frac{x}{y}+\frac{y}{x}+\frac{z}{w}+\frac{w}{z}=n$

Nguyen Duy TAN[1], Nguyen Xuan THO

Faculty of Mathematics and Informatics, Hanoi University of Science and Technology, Hanoi, Vietnam
Corresponding author: Nguyen Xuan THO, E-mail: `tho.nguyenxuan1@hust.edu.vn`

Abstract. This paper shows that the equation in the title has no solutions in the positive integers if (i) n has prime factor congruent to 3 (modulo 4); or (ii) $8|n$; or $8|n-1$. Case (i) follows from an elementary argument. Case (ii) follows from the previous works of E. Dofs and the second author. Case (iii) follows from a standard Brauer-Manin obstruction argument.

***Keywords**:* Azumaya algebras, Brauer-Manin obstruction, elliptic curves, rational points.

Mathematics Subject Classification (MSC2020): 14G12, 11D25, 11G05.

1. INTRODUCTION

We are interested in the following problem.

PROBLEM 1. *Let n be a positive integer. Find positive rational numbers x_1, x_2, x_3, x_4 such that*

$$\begin{cases} x_1x_2x_3x_4 = 1, \\ x_1+x_2+x_3+x_4 = n. \end{cases} \tag{1}$$

The following result was proved in [3, 6].

THEOREM 1 [3, 6]. *Let n be a positive integer. Assume that $8|n$ or $n=4m$ with $m^2-1=2^{2h}k$ with $h,k\in\mathbb{Z}^+$, $h\geq 2$, and $8|k-1$. Then the equation*

$$n=\frac{x}{y}+\frac{y}{z}+\frac{z}{w}+\frac{w}{x}$$

has no solutions in the positive integers. Equivalently, system (1) has no solutions in the positive rationals.

In this paper, we study system (1) with an additional condition $x_1x_2 = x_3x_4 = 1$. The main result is the following.

THEOREM 2. *Let $n>4$ be a positive integer. Assume that n has a prime factor congruent to 3 modudo 4 or $8|n$ or $8|n-1$. Then the equation*

$$n=\frac{x}{y}+\frac{y}{x}+\frac{z}{w}+\frac{w}{z} \tag{2}$$

has no solutions in the positive integers.

---

[1] E-mail: `tan.nguyenduy@hust.edu.vn`

We prove the first two cases of Theorem 2 using an elementary argument and Theorem 1 respectively, and study the last case using the Brauer-Manin obstruction framework.

2. PRELIMINARIES

2.1. Brauer-Manin obstruction

This section mostly follows Colliot-Thélène and Skorobogatov [2, Chapter 13] and Poonen [7, Chapter 8]. Let k be a number field, let Ω be the set of all places of k, and let $\mathbb{A}_k$ be the adèle ring of k. Let X be a proper, smooth, geometrically irreducible variety defined over k. Let $\mathrm{Br}(X)$ be the Brauer group of X, that is the group of equivalence classes of Azumaya algebras over X. In 1970, Manin [4] introduced the Brauer-Manin paring

$$X(\mathbb{A}_k) \times \mathrm{Br}(X) \to \mathbb{Q}/\mathbb{Z},$$

sending $(P_v) \in X(A_k)$ and $\mathscr{A} \in \mathrm{Br}(X)$ to

$$\mathrm{ev}_A((P_v)) = \sum_{v\in\Omega} \mathrm{inv}_v(A(P_v)) \in \mathbb{Q}/\mathbb{Z},$$

where for each valuation v and each Azumaya algebra $\mathscr{A}$ in $\mathrm{Br}(X)$, $\mathrm{inv}_v\colon \mathrm{Br}(k_v) \to \mathbb{Q}/\mathbb{Z}$ is the local invariant map from class field theory and $\mathscr{A}(P_v)$ is defined as follows. A point $P_v \in X(k_v)$ gives a map $\mathrm{Spec}(k_v) \to X$, and hence induces a pullback map $\mathrm{Br}(X) \to \mathrm{Br}(k_v)$. We write $\mathscr{A}(P_v)$ for the image of $\mathscr{A}$ under this map. The Brauer set of $X(\mathbb{A}_k)^{\mathrm{Br}}$ is given

$$X(\mathbb{A}_k)^{\mathrm{Br}} = \left\{(P_v) \in X(\mathbb{A}_k) \text{ such that } \mathrm{ev}_{\mathscr{A}}((P_v)) = 0 \text{ for all } \mathscr{A} \in \mathrm{Br}(X)\right\}.$$

The following theorem is due to Manin [4].

THEOREM 3. *Let k be a number field and let X be a variety defined over k. The Brauer-Manin set $X(\mathbb{A}_k)^{Br}$ contains the closure of the image of the diagonal map* : $X(k) \to X(\mathbb{A}_k)$.

If $X(\mathbb{A}_k)^{\mathrm{Br}} \neq X(\mathbb{A}_k)$ then we say there is a Brauer-Manin obstruction to weak approximation for X. Our model problem is that for a given variety X defined over k, we want to show $X(k)_{\mathscr{P}} = \emptyset$, where $X(k)_{\mathscr{P}}$ is the set of all points in $X(k)$ having a property $\mathscr{P}$. The guiding principle is to construct an Azumaya algebra $\mathscr{A} \in \mathrm{Br}(X)$ such that

$$\mathrm{ev}_{\mathscr{A}}((P_v)) \neq 0 \text{ for all } P \in X(k)_{\mathscr{P}},$$

where $(P_v) \in X(\mathbb{A}_k) = \prod_{v\in\Omega} X(k_v)$ is the image of $P \in X(k)$ under the diagonal map.

2.2. The local Hilbert symbol

This sections follows Serre [8, Chapter III]. Let p be a finite prime. For a nonzero p-adic number a, denote $v_p(a)$ the highest power of q dividing a. Let $k = \mathbb{Q}_p$ or $k = \mathbb{R}$. For a and b in k^*, the local Hilbert symbol $(a,b)_p$ is defined as

$$(a,b)_p = \begin{cases} 1 \text{ if } ax^2 + by^2 = z^2 \text{ has a point } (x,y,z) \text{ in } \mathbb{P}^2(k), \\ -1 \text{ otherwise.} \end{cases}$$

(i) Let $a, b, c \in \mathbb{Q}_p^*$. Then

$$\begin{aligned} &(a, b^2)_p = 1, \\ &(a, bc)_p = (a,b)_p(a,c)_p, \\ &(a,b)_\infty \prod_{p \text{ prime}} (a,b)_q = 1. \end{aligned}$$

(ii) Let $a=p^\alpha u$, $b=p^\beta v$, where $\alpha=v_p(a)$ and $\beta=v_p(b)$. Then

$$\begin{aligned}(a,b)_p&=(-1)^{\alpha\beta(p-1)/2}\left(\frac{u}{p}\right)^\beta\left(\frac{v}{p}\right)^\alpha \text{ if } p\neq 2,\\ (a,b)_p&=(-1)^{(u-1)(v-1)/4+\alpha(v^2-1)/8+\beta(u^2-1)/8} \text{ if } p=2,\end{aligned}$$

where $\left(\frac{\cdot}{\cdot}\right)$ denotes the Legendre symbol.

3. PROOF OF THEOREM 2

PROPOSITION 1. *Let n be a positive integer with a prime factor congruent to* 3 *modulo* 4, *then equation* (2) *has no solutions in the positive integers.*

Proof. Assume that there exist positive integers x,y,z,w satisfying (2). We can further assume that $\gcd(x,y)=1$ and $\gcd(z,w)=1$. Let p be a prime factor of n such that $p\equiv 3 \pmod 4$. Let $n=pm$ with $m\in\mathbb{Z}^+$. By (2),

$$pmxyzw=(x^2+y^2)zw+(z^2+w^2)xy. \tag{3}$$

Since $\gcd(x,y)=\gcd(z,w)=1$, we have $xy|zw$ and $zw|xy$. Hence $xy=zw$ and by (3),

$$pmxy=x^2+y^2+z^2+w^2. \tag{4}$$

Since $x=zw/y$, we have

$$\begin{aligned}pmxy&=\frac{z^2w^2}{y^2}+y^2+z^2+w^2\\&=\frac{(y^2+z^2)(y^2+w^2)}{y^2}.\end{aligned}$$

Hence $p|(y^2+z^2)(y^2+w^2)$. Without loss of generality, we assume that $p|y^2+z^2$. Since $\left(\frac{-1}{p}\right)=1$, it follows that $p|y,z$. By (4), $p|x^2+w^2$. So $p|x,w$. Hence $\gcd(x,y,z,w)>1$, which gives a contradiction. □

PROPOSITION 2. *Let n be a positive integer such that* $8|n$. *Then equation* (2) *has no solutions in the positive integers.*

Proof. This follows directly from Theorem 1. □

PROPOSITION 3. *Let* $n>4$ *be a positive integer such that* $8|n-1$. *Then equation* (2) *has no solutions in the positive integers.*

We briefly discuss the proving strategy of Proposition 3. Equation (2) is first transformed into an elliptic curve E of the form

$$y^2=x(x^2+Ax+B)$$

with $A,B\in\mathbb{Q}$. Positive integer solutions of (2) correspond to rational points on E in the bounded component $x<0$. To show the nonexistence of positive integer solutions is the same as to show the nonexistence of rational points (x,y) with $x<0$. Then Lemma 1 below is used to construct an Azumaya algebra $\mathscr{M}$ in $\mathrm{Br}(\mathbb{Q}(E))$, such that for all $P=(x,y)\in E(\mathbb{Q})$ with $x<0$ then

$$\mathrm{inv}_v(\mathscr{M}(P_v))=\begin{cases}0 & \text{if } v=p, \text{ a finite prime},\\ \frac{1}{2} & \text{if } v=\infty,\end{cases} \quad ,$$

where (P_v) is the image of P in $E(\mathbb{A}_{\mathbb{Q}})$, which contradicts Theorem 3. See Tan and Tho [5] for another application of this strategy.

Proof. Assume that (2) has a solution (x_0,y_0,z_0,w_0) with positive integers x_0,y_0,z_0,w_0. Let $a_0 = x_0/y_0$ and $b_0 = z_0/w_0$. Then (2) becomes

$$n = a_0 + \frac{1}{a_0} + b_0 + \frac{1}{b_0}.$$

So $[a_0 : b_0 : 1]$ is a point on the genus one projective curve C defined by

$$(ab+c^2)(a+b) = nabc.$$

Note that $[0:1:0]$ is a point on C. Using Magma [1], we obtain that a Weierstrass form of C is

$$E\colon y^2 = x(x^2+(n^2-8)x+16). \tag{5}$$

A map ϕ from C to E is given by

$$\phi([0:1:0]) = \infty \text{ and } \phi([a:b:c]) = (x,y),$$

where

$$\begin{cases} x &= \dfrac{-4a}{c}, \\ y &= \dfrac{-4(2ab+2b^2+nbc)}{ac}. \end{cases}$$

Let $(u,v) = \phi([a_0 : b_0 : 1])$. Then

$$u = -4a_0,\ v = \frac{-4(2a_0b_0+2b_0^2+nb_0)}{a_0}.$$

Since $a_0, b_0 > 0$, we have $u < 0$. Let $\mathbb{Q}(E)$ be the function field of E.

LEMMA 1. *Let A, B, and C be quaternion algebras over* $\mathbb{Q}(E)$ *with* $A = (x, 4-n)$*,* $B = (x^2+(n^2-16)x+16, 4-n)$*, and* $C = (1+(n^2-16)/x+16/x^2)$*. Then A, B, and C represent the same class of an Azumaya algebra in* $Br(E)$*.*

Proof. Since $A+B = (y^2, 4-n)$, we have $A = B$. Since $B-C = (x^2, 4-n)$, we have $B = C$. Hence $A = B = C$. Let U_1, U_2, and U_3 be the maximal open subsets of E where x,$x^2+(n^2-8)x+16$, and $1+(n^2-8)/x+16/x^2$ have no zeros or poles respectively. Then $A \in \mathrm{Br}(U_1)$, $B \in \mathrm{Br}(U_2)$, and $C \in \mathrm{Br}(U_3)$. Then $E = U_1 \cup U_2 \cup U_3$.

We have $U_1 = E - \{(0,0),\infty\}$, $U_2 = E - \{(\alpha_1,0),(\alpha_2,0),\infty\}$, where α_1 and α_2 are roots of $x^2+(n^2-8)x+16 = 0$. So $U_1 \cup U_2 = E - \{\infty\}$. However, at ∞ we have $x^{-1}(\infty) = 0$. Therefore

$$(1+\frac{n^2-16}{x}+\frac{16}{x^2})(\infty) = 1 \neq 0.$$

Therefore $\infty \in U_3$. So $E = U_2 \cup U_3$. ☐

Let $P = (x,y)$ be a point in $E(\mathbb{Q})$ with $x < 0$. Let $(P_v)_{v\in\Omega} \in E(\mathbb{A}_{\mathbb{Q}}) = \prod_v E(\mathbb{Q}_v)$ be the image of P under the diagonal map $E(\mathbb{Q}) \to E(\mathbb{A}_{\mathbb{Q}})$.

LEMMA 2. *Let p be an odd prime. Then*

$$\mathrm{inv}_p(A(P_p)) = 0. \tag{6}$$

Proof. It suffices to show that

$$(x, 4-n)_p = 1. \tag{7}$$

Case 1: $v_p(x)<0$. Let $x=p^{-r}x_1$ with $r\in\mathbb{Z}^+$ and $v_p(x_1)=0$. Then

$$y^2=\frac{x_1(x_1^2+p^r(n^2-8)x_1+16p^{2r})}{p^{3r}}. \tag{8}$$

Thus $-3r=v_p(y^2)$, so that $2|r$. Let $z=p^{3r/2}y$. Then $v_p(z)=0$ and (8) becomes

$$z^2=x_1(x_1^2+p^r(n^2-8)x_1+16p^{2r}). \tag{9}$$

Reducing (9) modulo p gives $x_1\equiv$ square (mod p). Hence $x_1\in\mathbb{Z}_p^2$. It follows that $x=p^{-r}x_1\in\mathbb{Q}_p^2$ and $(x,4-n)_p=1$.

Case 2: $v_p(x)=0$.

Case 2.1: $v_p(4-n)=0$. Then x and $4-n$ are units in $\mathbb{Z}_p$ and $(x,4-n)_p=1$.

Case 2.2: $v_p(4-n)>0$. Then $n\equiv 4$ (mod p) and

$$y^2\equiv x(x^2+8x+16)\equiv x(x+4)^2 \pmod p.$$

If $p\nmid x+4$ then $x\equiv(y/(x+4))^2$ (mod p). It follows that $x\in\mathbb{Z}_p^2$ and $(x,4-n)_p=1$.

If $p|x+4$ then $x\equiv -4$ (mod p). Let $x+4=p^ra$ and $n-4=p^sb$ with $r,s\in\mathbb{Z}^+$ and $v_p(a)=v_p(b)=0$. Then

$$\begin{aligned} x^2+(n^2-8)x+16&=(x+4)^2+(n^2-16)x\\ &=p^{2r}a^2+p^sb(p^sb+8)x. \end{aligned} \tag{10}$$

If $2r<s$ then

$$x^2+(n^2-8)x+16=p^{2r}(a^2+p^{s-2r}b(p^sb+8)x).$$

Hence $x^2+(n^2-8)x+16\in\mathbb{Z}_p^2$. It follows that

$$x=\frac{y^2}{x^2+(n^2-8)x+16}\in\mathbb{Q}_p^2$$

and $(x,4-n)_p=1$.

If $2r=s$ then

$$\begin{aligned} (x,4-n)_p&=(x,-p^{2r}b)_p\\ &=(x,-b)_p\\ &=1 \quad (\text{since } x,b\in\mathbb{Z}_p^\times) \end{aligned}$$

If $s<2r$ then

$$\begin{aligned} y^2&=x(x^2+(n^2-8)x+16)\\ &=xp^s(p^{2r-s}a^2+b(p^sb+8)x). \end{aligned}$$

Thus $s=v_2(y^2)$, so that $2|s$ and

$$\begin{aligned} (x,4-n)_p&=(x,-p^sb)_p\\ &=(x,-b)_p\\ &=1 \quad (\text{since } x,b\in\mathbb{Z}_p^\times). \end{aligned}$$

Case 3: $v_p(x)>0$. Let $x=p^rx_1$ with $r\in\mathbb{Z}^+$ and $v_p(x_1)=0$. Then

$$y^2=p^rx_1(p^{2r}x_1^2+p^r(n^2-8)x_1+16). \tag{11}$$

Thus $r = v_p(y^2)$, so that $2|r$. Since $p^{2r}x_1^2 + p^r(n^2-8)x_1 + 16 \in \mathbb{Z}_p^2$, it follows from (11) that

$$x_1 = \frac{y^2}{p^r(p^{2r}x_1^2 + p^r(n^2-8)x_1 + 16)} \in \mathbb{Z}_p^2.$$

Hence $x = p^r x_1 \in \mathbb{Z}_p^2$ and $(x, 4-n)_p = 1$. □

LEMMA 3. *Let $p = 2$. Then*

$$\mathrm{inv}_2(A((P_2))) = 0. \tag{12}$$

Proof. It suffices to show that

$$(x, 4-n)_2 = 1. \tag{13}$$

Case 1: $v_2(x) < 0$. Let $x = 2^{-r}x_1$ with $r \in \mathbb{Z}^+$ and $v_2(x_1) = 0$. By (5),

$$y^2 = \frac{x_1(x_1^2 + 2^r(n^2-8)x_1 + 2^{2r+4})}{2^{3r}}. \tag{14}$$

Thus $v_2(y^2) = -3r$, so that $2|r$ and because $r > 0$, we have $r \geq 2$. Let $z = 2^{3r/2}y$. Then $v_2(z) = 0$ and by (14),

$$z^2 = x_1(x_1^2 + 2^r(n^2-8)x_1 + 2^{2r+4}). \tag{15}$$

Reducing (15) modulo 4 gives $x_1 \equiv 1 \pmod 4$. Since $2|r$ and $8|n-1$, we obtain

$$\begin{aligned}(x, 4-n)_2 &= (2^r x_1, 4-n)_2\\ &= (x_1, 4-n)_2\\ &= (-1)^{(x_1-1)(3-n)/4}\\ &= 1.\end{aligned}$$

Case 2: $v_2(x) = 0$. Let $x = -r/s$ with $r, s \in \mathbb{Z}^+$, $\gcd(r,s) = 1$, and $2 \nmid rs$. By (5),

$$y^2 = \frac{r((n^2-8)rs - r^2 - 16s^2)}{s^3}.$$

Therefore $rs((n^2-8)rs - r^2 - 16s^2))$ is a perfect square. Since r, s and $(n^2-8)rs - r^2 - 16s^2$ are pairwise coprime, we conlude that r, s, and $(n^2-8)rs - r^2 - 16s^2$ are perfect squares. Since r, s are positive odd integers, there exist pairwise coprime positive integers a, b, c with a, b odd such that

$$r = a^2,\ s = b^2,\ (n^2-8)rs - r^2 - 16s^2 = c^2.$$

Hence

$$(nab)^2 - (a^2+4b^2)^2 = (n^2-8)a^2b^2 - a^4 - 16b^4 = c^2.$$

So (a^2+4b^2, c, nab) is a Pythagorean triple with a^2+4b^2 odd. Therefore there exist positive integers u, v, d with $\gcd(u,v) = 1$ such that

$$nab = d(u^2+v^2),\ a^2+4b^2 = d(u^2-v^2),\ c = 2duv. \tag{16}$$

Hence

$$a^2 + 4b^2 + nab = 2du^2, \tag{17}$$

$$nab - a^2 - 4b^2 = 2dv^2. \tag{18}$$

Since $d|c^2$, $d|nab$, and $\gcd(c, ab) = 1$, it follows that $d|n$ and $\gcd(d, ab) = 1$. Since $d|a^2+4b^2$, $2 \nmid ab$, and $\gcd(a,b) = 1$, every prime factor of d is congruent to 1 modulo 4. Hence $d \equiv 1 \pmod 4$. Since $d|n$ and $2 \nmid n$,

$\gcd(d,n+4)=1$. Then

$$\left(\frac{d}{n+4}\right)=(-1)^{(d-1)(n+3)/4}\left(\frac{n+4}{d}\right)=\left(\frac{4}{d}\right)=1. \tag{19}$$

By (17) and (18),

$$(a-2b)^2+(n+4)ab=2du^2,\ (n+4)ab-(a+2b)^2=2dv^2. \tag{20}$$

Since $n+4\equiv 5 \pmod 8$, $n+4$ is not a square, so there exists a prime factor p of $n+4$ with $v_p(n+4)$ odd. Since $n+4$ is odd, p is odd. Since $d|n$, $2\nmid ab$, $\gcd(a,b)=1$, it follows from (17) and (18) that $p\nmid d$. We claim that

$$\left(\frac{2}{p}\right)=\left(\frac{d}{p}\right). \tag{21}$$

Case $p\nmid u$. By (20), $2du^2\equiv(a-2b)^2 \pmod p$, and (21) follows.

Case $p|u$. By (20), $p|a-2b$. Let $u=p^{\alpha}u_1$ and $a-2b=p^{\beta}t$ with $\alpha,\beta,u_1,t\in\mathbb{Z}$, $p\nmid u_1,t$, and $\alpha,\beta>0$. By (20),

$$\begin{aligned}(n+4)ab&=2du^2-(a-2b)^2\\&=2dp^{2\alpha}u_1^2-p^{2\beta}t^2.\end{aligned}$$

If $\alpha\neq\beta$ then $v_p(n+4)=\min\{2\alpha,2\beta\}$, which is impossible since $2\nmid v_p(n+4)$.

If $\alpha=\beta$ then

$$(n+4)ab=p^{2\alpha}(2du_1^2-t^2).$$

Since $v_p(n+4)$ is odd, $p|2du_1^2-t^2$, which implies (21) since $p\nmid u_1t$.

Using (21), we obtain

$$\begin{aligned}\left(\frac{2}{n+4}\right)&=\prod_{p|n+4,2|v_p(n+4)}\left(\frac{2}{p}\right)^{v_p(n+4)}\times\prod_{p|n+4,2\nmid v_p(n+4)}\left(\frac{2}{p}\right)^{v_p(n+4)}\\&=\prod_{p|n+4,2|v_p(n+4)}\left(\frac{d}{p}\right)^{v_p(n+4)}\times\prod_{p|n+4,2\nmid v_p(n+4)}\left(\frac{d}{p}\right)^{v_p(n+4)}\\&=\left(\frac{d}{n+4}\right)\\&=(-1)^{(n+3)(d-1)/4}\left(\frac{n+4}{d}\right)\\&=1\quad(\text{since }4|d-1).\end{aligned}$$

Then

$$\begin{aligned}n-4&=\prod_{q\text{ primes},\ q|n-4,\ q\nmid u}q^{v_q(n-4)}\times\prod_{q\text{ primes},\ q|n-4,\ q|u,\ 2|v_q(n-4)}q^{v_q(n-4)}\times\prod_{q\text{ primes},\ q|n-4,\ q|u,\ 2\nmid v_1(n-4)}q^{v_q(n-4)}\\&\equiv\prod_{q\text{ primes},\ q|n-4,\ q\nmid u}(\pm1)^{v_q(n-4)}\times\prod_{q\text{ primes},\ q|n-4,\ q|u,\ 2|v_q(n-4)}1\times\prod_{q\text{ primes},\ q|n-4,\ q|u,\ 2\nmid v_1(n-4)}(\pm1)^{v_q(n-4)}\pmod 8\\&\equiv\pm1\pmod 8,\end{aligned}$$

which is impossible since $n\equiv 1 \pmod 8$.

Case 3: $v_2(x)>0$. Let $x=2^tx_1$ with $t\in\mathbb{Z}^+$ and $v_2(x_1)=0$. By (5),

$$y^2=2^tx_1(2^{2t}x_1^2+2^t(n^2-8)x_1+16). \tag{22}$$

Case 3.1: $t=1$. By (22),

$$y^2=2^2x_1(2x_1^2+(n^2-8)x_1+8). \tag{23}$$

Thus $v_2(y)=1$ and

$$(\frac{y}{2})^2 = x_1(2x_1^2+(n^2-8)x_1+8). \tag{24}$$

Reducing (24) modulo 4 gives

$$1 \equiv 2x_1+1 \mod 4,$$

which is impossible since $v_2(x_1)=0$.

Case 3.2: $t=2$. Let $x=-4r/s$ with $r,s\in\mathbb{Z}^+$, $\gcd(r,s)=1$, and $2\nmid rs$. By (22),

$$y^2 = \frac{16r((n^2-8)rs-4r^2-4s^2)}{s^3}.$$

Thus $rs((n^2-8)rs-4r^2-4s^2))$ is a square. Since r,s, and $(n^2-8)rs-4r^2-4s^2$ are pairwise coprime odd positive integers, there exist pairwise coprime odd positive integers a,b,c such that

$$r=a^2,\, s=b^2,\, (n^2-8)rs-4r^2-4s^2=c^2.$$

Thus

$$(n^2-8)a^2b^2-4a^4-4b^4=c^2.$$

So

$$(nab)^2 = 4(a^2+b^2)^2+c^2.$$

Therefore $(2(a^2+b^2),c,nab)$ is a Pythagorean triple with c odd. Thus there exist positive integers d,u,v with $\gcd(u,v)=1$ such that

$$nab=d(u^2+v^2),\, a^2+b^2=duv,\, c=d(u^2-v^2). \tag{25}$$

Since $d|nab$, $d|a^2+b^2$, and $\gcd(a,b)=1$, we have $d|n$, $ab|u^2+v^2$, and $\gcd(d,ab)=1$. Since $d|a^2+b^2$, $\gcd(a,b)=1$, $ab|u^2+v^2$, $\gcd(u,v)=1$, every prime factor of a,b,d is congruent to 1 modulo 4. By (25),

$$d(u+v)^2=2a^2+2b^2+nab,\, d(u-v)^2=nab-2a^2-2b^2.$$

Hence

$$d(u+v)^2=2(a-b)^2+(n+4)ab,\, d(u-v)^2=(n+4)ab-2(a+b)^2. \tag{26}$$

Let p be a prime factor of $n+4$. Then p is odd. If $p|d$ then by (26), $p|2(a-b)^2$ and $p|2(a+b)^2$. It follows that $p|a-b$ and $p|a+b$, and hence $p|a$ and $p|b$, which is impossible since $\gcd(a,b)=1$. Therefore $p\nmid d$. Since $n+4\equiv d\equiv 1 \pmod 4$, we obtain

$$\left(\frac{d}{n+4}\right) = (-1)^{(n+3)(d-1)/4}\left(\frac{n+4}{d}\right) = \left(\frac{4}{d}\right) = 1. \tag{27}$$

Since $\gcd(u,v)=1$, p cannot divide both $u-v$ and $u+v$. If $p\nmid u+v$, then by (26), $d(u+v)^2\equiv 2(a-b)^2$ (mod p). If $p\nmid u-v$, then by (26), $d(u-v)^2\equiv 2(a+b)^2$ (mod p). In either case,

$$\left(\frac{2}{p}\right) = \left(\frac{d}{p}\right)$$

This is true for very prime factor of $n+4$. Combining this with (27) gives

$$\left(\frac{2}{n+4}\right) = \left(\frac{d}{n+4}\right)$$
$$= 1,$$

which is impossible since $n\equiv 1 \pmod 8$.

Case 3.3: $t=3$. By (22),

$$y^2=2^6x_1(8x_1^2+(n^2-8)x_1+2).$$

Thus $v_2(y)=3$ and

$$(\frac{y}{8})^2=x_1(8x_1^2+(n^2-8)x_1+2). \tag{28}$$

Reducing (28) modulo 4 gives

$$1=1+2x_1 \pmod 4,$$

which is impossible since $v_2(x_1)=0$.

Case 3.4: $t=4$. Let $x=-16r/s$ with $r,s\in\mathbb{Z}^+$, $\gcd(r,s)=1$, and $2\nmid r,s$. By (22),

$$y^2=\frac{256r((n^2-8)rs-16r^2-s^2)}{s^3}.$$

Thus $rs((n^2-8)rs-16r^2-s^2)$ is a perfect square. Since $r,s,(n^2-8)rs-16r^2-s^2$ are pairwise coprime positive integers with r,s odd, there exist pairwise coprime positive integers a,b,c with a,b odd such that

$$r=a^2, s=b^2, (n^2-8)rs-16r^2-s^2=c^2.$$

Hence

$$(n^2-8)a^2b^2-16a^4-b^4=c^2.$$

Thus

$$(nab)^2-(4a^2+b^2)^2=c^2.$$

So $(4a^2+b^2,c,nab)$ is a Pythagorean triple with $4a^2+b^2$ odd. Therefore there exist positive integers u,v,d with $\gcd(u,v)=1$ such that

$$nab=d(u^2+v^2), 4a^2+b^2=d(u^2-v^2), c=2duv.$$

Hence

$$nab+4a^2+b^2=2du^2, nab-4a^2-b^2=2dv^2.$$

So

$$(n+4)ab+(2a-b)^2=2du^2, (n+4)ab-(2a+b)^2=2dv^2. \tag{29}$$

Let p be a prime factor of $n+4$ with $v_p(n+4)$ odd. Since $n+4$ is odd, p is odd. If $p|d$ then by (29), $p|2a-b$ and $p|2a+b$. It follows that $p|a$ and $p|b$, which is impossible since $\gcd(a,b)=1$. Hence $p\nmid d$. We claim that

$$\left(\frac{2}{p}\right)=\left(\frac{d}{p}\right). \tag{30}$$

If $p\nmid u$ then $2du^2\equiv(2a-b)^2 \pmod p$, which implies (30).
If $p|u$ then $p|2a-b$. Let $u=p^{\alpha}u_1$ and $2a-b=p^{\beta}t_1$ with $\alpha,\beta,u_1,t_1\in\mathbb{Z}$, $p\nmid u_1t$, and $\alpha,\beta>0$. By (29),

$$(n+4)ab=2dp^{2\alpha}u_1^2-p^{2\beta}t_1^2. \tag{31}$$

If $\alpha\neq\beta$ then by (31), $v_p(n+4)=\min\{2\alpha,2\beta\}$, which is impossible since $v_p(n+4)$ is odd.
If $\alpha=\beta$ then since $v_p(n+4)$ is odd, it follows from (31) that $p|2du_1^2-t_1^2$, which implies (30). Using (30) we

obtain

$$\begin{aligned}\left(\frac{2}{n+4}\right) &= \prod_{p|n+4,\,2|v_p(n+4)}\left(\frac{2}{p}\right)^{v_p(n+4)} \times \prod_{p|n+4,\,2\nmid v_p(n+4)}\left(\frac{2}{p}\right)^{v_p(n+4)}\\ &= \prod_{p|n+4,\,2|v_p(n+4)}\left(\frac{d}{p}\right)^{v_p(n+4)} \times \prod_{p|n+4,\,2\nmid v_p(n+4)}\left(\frac{d}{p}\right)^{v_p(n+4)}\\ &= \left(\frac{d}{n+4}\right) = (-1)^{(n+3)(d-1)/4}\left(\frac{n+4}{d}\right) = 1 \quad (\text{since } 4|d-1),\end{aligned}$$

which is impossible since $n \equiv 1 \pmod 8$).

Case 3.5: $t > 4$. By (22),

$$y^2 = 2^{4+t}x_1(2^{2t-4}x_1^2 + 2^{t-4}x_1(n^2-8)+1).$$

Hence $v_2(y^2) = t+4$. So that $2|t$ and because $t > 4$, we have $t \geq 6$. Then

$$(2^{-2-t/2}y)^2 = x_1(2^{2t-4}x_1^2 + 2^{t-4}x_1(n^2-8)+1). \tag{32}$$

Reducing (32) modulo 4 gives $x_1 \equiv 1 \pmod 4$. Then

$$\begin{aligned}(x,4-n)_2 &= (2^r x_1, 4-n)_2\\ &= (x_1,4-n)_2 \quad (\text{since } 2|r)\\ &= (-1)^{(x_1-1)(3-n)/4}\\ &= 1.\end{aligned}$$

□

LEMMA 4. *We have*

$$\mathrm{inv}_\infty(\mathscr{A}(P_\infty)) = \frac{1}{2}.$$

Proof. Because $x < 0$ and $4-n < 0$, we have $(x,n-4)_\infty = -1$. It follows that $\mathrm{inv}_\infty(\mathscr{A}(P_\infty)) = \frac{1}{2}$. □

Combining 2, 3, and 4 gives

$$\mathrm{ev}_{\mathscr{A}}(P) = \mathrm{inv}_\infty(\mathscr{A}(P_\infty)) + \sum_{p<\infty}\mathrm{inv}_v(A(P_p)) = \frac{1}{2},$$

which is impossible since for all rational points M in $E(\mathbb{Q})$ then

$$\mathrm{ev}_{\mathscr{A}}(M)) = 0.$$

This completes the proof of Proposition 3 and hence the proof of Theorem 2. □

ACKNOWLEDGEMENTS

The authors would like to thank the anonymous reviewer for his/her valuable comments. The authors are supported by the Vietnam National Foundation for Science and Technology Development (NAFOSTED) (grant number 101.04-2023.21). Nguyen Duy Tan is supported by Vietnam Institute for Advanced Study in Mathematics (VIASM) from March 2025 to May 2025. Nguyen Xuan Tho is supported by Vietnam Institute for Advanced Study in Mathematics (VIASM) from April 2025 to May 2025. The authors really appreciate the Institute for their help and funding.

REFERENCES

[1] Bosma W, Cannon J, Playoust C. The MAGMA algebra system. I. The user language. J. Symbolic Comput. 1997; 24(3-4): 235–265. `https://doi.org/10.1006/jsco.1996.0125`

[2] Colliot-Thélène JL, Skorobogatov AN. The Brauer-Grothendieck group. A Series of Modern Surveys in Mathematics 71. Springer; 2021.

[3] Dofs E, Tho NX. The Diophantine equation $x_1/x_2 + x_2/x_3 + x_3/x_4 + x_4/x_1 = n$. Int. J. Number Theory. 2021; 18(1): 75–87. `https://doi.org/10.1142/S1793042122500075`

[4] Manin YI. Le groupe de Brauer-Grothendieck en géométrie diophantienne. Actes du Congrès International des Mathématiciens. 1971; Tome 1, pp. 401–411. Nice; 1970.

[5] Tan ND, Tho NX. An extension of Bremner and Macleod's theorem. Rocky Mountain J. Math. 2024; 54(3): 885–893.

[6] Tho NX, On a Diophantine equation. Vietnam J. Math. 2022; 50(1): 183–194. `https://doi.org/10.1007/s10013-021-00503-w`

[7] Poonen B. Rational points on varieties. Graduate Studies in Mathematics 186. AMS; 2017.

[8] Serre JP, A course in arithmetic. Graduate Texts in Mathematics 7. New York: Springer; 1973.

Received July 26, 2024