Proceedings of the Edinburgh Mathematical Society (2024) **67**, 142–150
doi:10.1017/S0013091523000706

ON THE DIFFERENCE OF TWO FOURTH POWERS

NGUYEN XUAN THO

Hanoi University of Science and Technology Hanoi, Vietnam
(tho.nguyenxuan1@hust.edu.vn)

(Received 2 September 2022)

Abstract We investigate the equation $D = x^4 - y^4$ in field extensions. As an application, for a prime number p, we find solutions to $p = x^4 - y^4$ if $p \equiv 11 \pmod{16}$ and $p^3 = x^4 - y^4$ if $p \equiv 3 \pmod{16}$ in all cubic extensions of $\mathbb{Q}(i)$.

Keywords: Diophantine equations; quartic curves; solutions in field extensions

2020 Mathematics subject classification: Primary 14G25
Secondary 14H50

1. Introduction

We are interested in the following problem.

Problem 1. *Let k be a perfect field of characteristic not equal to 2. Let K be a finite extension of k. Let $D \in k^*$. Find all solutions to the equation*

$$D = x^4 - y^4. \tag{1}$$

By a solution (x, y) to Equation (1), we always mean $(x, y) \in \mathbb{A}^2(K)$ satisfying Equation (1) and $xy \neq 0$.

When $k = K = \mathbb{Q}$, using a variety of methods, many authors have shown that Equation (1) has no solutions if $D = nz^p$ for integers n and prime numbers p; see [1, 2, 4, 6, 7, 11].

It is natural to ask for solutions of Equation (1) when k and K are not the rational field. When k and K are number fields, since Equation (1) defines a curve of genus 3, by Faltings' theorem [8], Equation (1) only has a finite number of solutions, but to find all solutions to Equation (1) is in general a difficult task. We adopt here the method of Cassels' [5] and Bremner's [3], which is effective in finding solutions to Equation (1) in *all* cubic extensions of the base field in many situations. It is also worth mentioning that the work of Silverman [13] on the equation $x^4 + y^4 = D$ (and $x^6 + y^6 = D$) over number fields. But Silverman's method does not apply when finding solutions in cubic extensions of the base field. The main result of this paper is as follows:

Theorem 1. *Let k be a perfect field of characteristic not equal to 2. Let $D \in k$ such that $D \notin \pm k^2$. Assume that*

(i) *every solution $(X, y, z) \in \mathbb{A}^3(k)$ to $X^2 - y^4 = Dz^4$ satisfies $z = 0$,*
(ii) *every solution $(x, Y, z) \in \mathbb{A}^3(k)$ to $x^4 - Y^2 = Dz^4$ satisfies $z = 0$.*

If (x, y) is a solution to $D = x^4 - y^4$ in a cubic extension K of k, then

(1) *(if $-1 \notin k^2$)*

$$K = k(\theta), \quad x = \pm\left(\frac{D}{s\theta} - \frac{s}{4}\right), \quad y = \pm\left(\frac{D}{s\theta} + \frac{s}{4}\right),$$

where $\theta^3 - s^2\theta^2/8 - 2D^2/s^2 = 0$ and $s \in k^*$, and
(2) *(if $-1 \in k^2$)*

$$K = k(\theta), \quad x = \pm\left(\frac{\theta}{s} - \frac{s}{4}\right), \quad y = \pm i\left(\frac{\theta}{s} + \frac{s}{4}\right),$$

where $i = \sqrt{-1}$, $\theta^3 + s^4\theta/16 + Ds^2/2 = 0$, and $s \in k^*$.

A nice corollary of Theorem 1 is

Corollary 1. *Let p be a prime number. Let $D = p$ if $p \equiv 11 \pmod{16}$, and let $D = p^3$ if $p \equiv 3 \pmod{16}$. Then solutions to $D = x^4 - y^4$ in all cubic extensions of $\mathbb{Q}(i)$ are*

(1)

$$x = \pm\left(\frac{D}{s\theta} - \frac{s}{4}\right), \qquad y = \pm\left(\frac{D}{s\theta} + \frac{s}{4}\right),$$

where $\theta^3 - s^2\theta^2/8 - 2D^2/s^2 = 0$ for some $s \in \mathbb{Q}(i)^*$; and
(2)

$$x = \pm\left(\frac{\theta}{s} - \frac{s}{4}\right), \qquad y = \pm i\left(\frac{\theta}{s} + \frac{s}{4}\right),$$

where $\theta^3 + s^4\theta/16 + Ds^2/2 = 0$ for some $s \in \mathbb{Q}(i)^*$.

Remark 1. Theorem 1 finds all possible cubic extensions K of k and solutions to $D = x^4 - y^4$ in K. The defining polynomial of K, $F_s(x) = x^3 - s^2x^2/8 - 2D^2/s^2$ or $F_s(x) = x^3 + s^4x/16 + Ds^2/2$, must be irreducible in $k[x]$, which in general is difficult to check since the irreducibility of $F_s(x)$ depends on s. However, if k is a number field,

https://doi.org/10.1017/S0013091523000706 Published online by Cambridge University Press

by Hilbert's irreducibility theorem [12, Theorem 3.4.1], there exist infinitely many $s \in k$ such that $F_s(x)$ is irreducible in $k[x]$ and Theorem 1 finds all solutions to $D = x^4 - y^4$ in these cases.

2. Proof of Theorem 1

We follow Cassels [5]. Equation (1) can be written in the homogeneous form

$$x^4 - y^4 = Dz^4. \tag{2}$$

Let $\mathcal{C}$ be the projective curve over k defined by Equation (2). Suppose that $P = [x_1 : y_1 : z_1]$is a point on (2) whose coordinates generate a cubic extension K of k. If $z_1 = 0$, then $[x_1 : y_1 : z_1] = [\pm 1 : 1 : 0]$; therefore $K = k$, which is impossible. Therefore, $z_1 \neq 0$. Since $(x_1/z_1)^4 - (y_1/z_1)^4 = D$ and $|K : k| = 3$, we have $x_1/z_1, y_1/z_1 \notin k$. Thus,

$$k\left(\frac{x_1}{z_1}\right) = k\left(\frac{y_1}{z_1}\right) = k\left(\frac{x_1^2}{z_1^2}\right) = k\left(\frac{y_1^2}{z_1^2}\right) = K. \tag{3}$$

Fix an algebraic closure $\overline{k}$ of k. Let $P_i = [x_i : y_i : z_i] \in \mathbb{P}^2(\overline{k})$, $i = 1, 2, 3$, be the Galois conjugates of P. The equation

$$X^2 - Y^2 = DZ^2 \tag{4}$$

has a parametrization

$$[X : Y : Z] = [l^2 + Dm^2 : l^2 - Dm^2 : 2lm].$$

Since $[x_1^2 : y_1^2 : z_1^2]$ satisfies Equation (4), there exist $\lambda, \mu \in k$ such that

$$[x_1^2 : y_1^2 : z_1^2] = [\lambda^2 + D\mu^2 : \lambda^2 - D\mu^2 : 2\lambda\mu]. \tag{5}$$

Since $z_1 \neq 0$, it follows from Equation (5) that $\mu \neq 0$, $\lambda \neq 0$, and

$$[\lambda : \mu] = [x_1^2 + y_1^2 : z_1^2] = [Dz_1^2 : x_1^2 - y_1^2]. \tag{6}$$

Let $\theta = \lambda/\mu$. Then Equations (3) and (6) show that $\theta \notin k$. Hence, $k(\theta) = K$. Therefore, there exists an irreducible cubic polynomial $P(x) = ax^3 + bx^2 + cx + d \in k[x]$ such that $P(\theta) = 0$. In particular, $ad \neq 0$. From Equation (5), we have

$$\left(\frac{x_1}{z_1}\right)^2 : \left(\frac{y_1}{z_1}\right)^2 = \frac{\theta^2 + D}{2\theta} : \frac{\theta^2 - D}{2D}. \tag{7}$$

Step 1: Consider the weighted projective curve

$$\mathcal{C}_1 \colon X^2 - y^4 = Dz^4. \tag{8}$$

By points on $\mathcal{C}_1$, we mean the equivalence classes of points $[X : y : z]$ in $\mathbb{P}^2_{2,1,1}(\overline{k})$ satisfying Equation (8). Since $x_i^2, y_i^2, y_i z_i, z_i^2$ are linearly dependent over k and $x_i \neq 0$, there exist $r, s, t \in \mathbb{Q}$ such that

$$x_i^2 = ry_i^2 + sy_iz_i + tz_i^2,$$

for $i = 1, 2, 3$. Consider the weighted projective curve

$$\mathcal{D}_1 \colon X = ry^2 + syz + tz^2. \tag{9}$$

By the weighted Bézout theorem [Theorem VIII.2][10], the two curves $\mathcal{C}_1$ and $\mathcal{D}_1$ intersect at 4 points in $\mathbb{P}^2_{2,1,1}(\overline{k})$. We know that three of these four points are $[x_i^2 : y_i : z_i]$ for $i = 1, 2, 3$. Let $v_1(T)$ be the fourth point of intersection. Since the set $\{[x_i^2 : y_i : z_i] : i = 1, 2, 3\}$ is stable under the action of $\mathrm{Gal}(\overline{k}/k)$, $v_1(T)$ is fixed by $\mathrm{Gal}(\overline{k}/k)$. Therefore, $v_1(T)$ is a k-rational point. By the assumption in Theorem 1, we have $v_1(T) = [\pm 1 : 1 : 0]$.

- $v_1(T) = [1 : 1 : 0]$. Then Equation (9) gives $r = 1$. Since

$$(X - y^2 - tz^2)^2 - s^2y^2z^2 = 0,$$

the homogeneous quartic in l, m,

$$(l^2 + Dm^2 - (l^2 - Dm^2) - 2tlm)^2 - s^2(l^2 - Dm^2)(2lm),$$

has factors m and $P(l, m)$. Therefore, there exists $q \in k$ such that

$$\begin{aligned}(l^2 + Dm^2 - (l^2 - Dm^2) - 2tlm)^2 - 2lms^2(l^2 - Dm^2) =& 2qm(al^3 + bl^2m \\ &+ clm^2 + dm^3).\end{aligned} \tag{10}$$

Thus,

$$2m(Dm - tl)^2 - ls^2(l^2 - Dm^2) = q(al^3 + bl^2m + clm^2 + dm^3).$$

Therefore,

$$\begin{cases} qa &= -s^2, \\ qb &= 2t^2, \\ qc &= Ds^2 - 4Dt, \\ qd &= 2D^2. \end{cases} \tag{11}$$

Hence,

$$q(c + Da) = -4Dt, \quad q^2bd = 4D^2t^2, \ q \neq 0.$$

Therefore,

$$(c + Da)^2 = 4bd. \tag{12}$$

https://doi.org/10.1017/S0013091523000706 Published online by Cambridge University Press

Since $a, d \neq 0$, system (11) gives

$$\frac{a}{d} \equiv -2 \pmod{k^2}. \tag{13}$$

- $v_1(T) = [-1 : 1 : 0]$. Then Equation (9) gives $r = -1$. Since

$$(X + y^2 - tz^2)^2 - s^2y^2z^2 = 0,$$

the homogeneous quartic in l, m,

$$(l^2 + Dm^2 + l^2 - Dm^2 - 2tlm)^2 - s^2(l^2 - Dm^2)(2lm),$$

has factors l and $P(l, m)$. Therefore, there exists $q \in k$ such that

$$(2l^2 - 2tlm)^2 - s^2(l^2 - Dm^2)(2lm) = 2ql(al^3 + bl^2m + clm^2 + dm^3). \tag{14}$$

Hence,

$$2l(l - tm)^2 - ms^2(l^2 - Dm^2) = q(al^3 + bl^2m + clm^2 + dm^3).$$

Therefore,

$$\begin{cases} qa &= 2, \\ qb &= -4t - s^2, \\ qc &= 2t^2, \\ qd &= Ds^2. \end{cases} \tag{15}$$

Hence,

$$q^2ac = 4t^2, \quad q\left(b + \frac{d}{D}\right) = -4t, \; q \neq 0.$$

Therefore,

$$\left(b + \frac{d}{D}\right)^2 = 4ac. \tag{16}$$

Since $a, d \neq 0$, system (15) also gives

$$\frac{a}{d} \equiv 2D \pmod{k^2}. \tag{17}$$

Step 2: Consider the weighted projective curve

$$\mathcal{C}_2 \colon x^4 - Y^2 = Dz^4. \tag{18}$$

https://doi.org/10.1017/S0013091523000706 Published online by Cambridge University Press

By points on $\mathcal{C}_2$, we mean the equivalence classes of points $[x : Y : z]$ in $\mathbb{P}^2_{1,2,1}(\overline{k})$ satisfying Equation (18). Since $y_i^2, x_i^2, x_i z_i, z_i^2$ are linearly dependent over k and $y_i \neq 0$, there exist $r, s, t \in \mathbb{Q}$ such that

$$y_i^2 = r x_i^2 + s x_i z_i + t z_i^2,$$

for $i = 1, 2, 3$. Consider the weighted projective curve

$$\mathcal{D}_2 \colon Y = r x^2 + s x z + t z^2. \tag{19}$$

By the weighted Bézout theorem [Theorem VIII.2][10], the two curves $\mathcal{C}_2$ and $\mathcal{D}_2$ intersect at 4 points in $\mathbb{P}^2_{1,2,1}(\overline{k})$. We know that three of these four points are $[x_i : y_i^2 : z_i]$ for $i = 1, 2, 3$. Let $v_2(T)$ be the fourth point of intersection. Since the set $\{[x_i : y_i^2 : z_i] : i = 1, 2, 3\}$ is stable under the action of $\mathrm{Gal}(\overline{k}/k)$, $v_2(T)$ is fixed by $\mathrm{Gal}(\overline{k}/k)$. Therefore, $v_2(T)$ is a k-rational point. By the assumption in Theorem 1, we have $v_2(T) = [1 : \pm 1 : 0]$.

- $v_2(T) = [1 : 1 : 0]$. Then Equation (19) gives $r = 1$. We have

$$(Y - x^2 - t z^2)^2 - s^2 x^2 z^2 = 0,$$

so that the homogeneous quartic in l, m,

$$(l^2 - Dm^2 - (l^2 + Dm^2) - 2tlm)^2 - s^2 (l^2 + Dm^2)(2lm),$$

has factors m and $P(l, m)$. Therefore, there exists $q \in k$ such that

$$(l^2 - Dm^2 - (l^2 + Dm^2))^2 - 2tlm)^2 - s^2 (l^2 + Dm^2)(2lm) = 2qmP(l, m). \tag{20}$$

Thus,

$$2m(Dm + rl)^2 - ls^2 (l^2 + Dm^2) = q(al^3 + bl^2 m + clm^2 + dm^3).$$

Hence,

$$\begin{cases} qa &= -s^2, \\ qb &= 2r^2, \\ qc &= 4Dr - Ds^2, \\ qd &= 2D^2. \end{cases} \tag{21}$$

Therefore,

$$q(c - Da) = 4Dr, \quad q^2 bd = 4D^2 r^2, \; q \neq 0.$$

Hence,

$$(c - Da)^2 = 4bd. \tag{22}$$

Since $a, d \neq 0$, system (21) gives

$$\frac{a}{d} \equiv -2 \pmod{k^2}. \tag{23}$$

- $v_2(T) = [1 : -1 : 0]$. Then Equation (19) gives $r = -1$. We have

$$(Y + x^2 - tz^2)^2 - s^2x^2z^2 = 0,$$

so that the homogeneous quartic in l, m,

$$(l^2 - Dm^2 + (l^2 + Dm^2) - 2rlm)^2 - s^2(l^2 + Dm^2)(2lm),$$

has factors l and $P(l, m)$. Thus, there exists $q \in k$ such that

$$\begin{aligned}(l^2 - Dm^2 + (l^2 + Dm^2) - 2tlm)^2 - s^2(l^2 + Dm^2)(2lm) =& 2lq(al^3 + bl^2m \\ &+ clm^2 + dm^3).\end{aligned} \tag{24}$$

Hence,

$$2l(l - tm)^2 - ms^2(l^2 + Dm^2) = q(al^3 + bl^2m + clm^2 + dm^3).$$

Therefore,

$$\begin{cases} qa &= 2, \\ qb &= -4t - s^2, \\ qc &= 2t^2, \\ qd &= -Ds^2. \end{cases} \tag{25}$$

Hence,

$$q^2ac = 4t^2, \quad q\left(b - \frac{d}{D}\right) = -4r, \ q \neq 0.$$

Thus,

$$\left(b - \frac{d}{D}\right)^2 = 4ac. \tag{26}$$

System (25) also gives

$$\frac{a}{d} \equiv -2D \pmod{k^2}. \tag{27}$$

It follows from (23), (27), (13) and (17) and the assumption that $D \notin \pm k^2$ that there are only two compatible cases for $v_1(T)$ and $v_2(T)$.

Case 1: $v_1(T) = [1:1:0]$ and $v_2(T) = [1:1:0]$. From (12) and (22), we have

$$(c - Da)^2 = (c + Da)^2.$$

Since $aD \neq 0$, we have $c = 0$. From (21), we have $r = s^2/4$. Thus,

$$qP(x) = -s^2x^3 + \frac{s^4}{8}x^2 + 2D^2.$$

Therefore θ satisfies

$$\theta^3 - \frac{s^2}{8}\theta^2 - 2\frac{D^2}{s^2} = 0. \tag{28}$$

Then (10) and (20) give

$$\frac{\theta^2 + D}{2\theta} = \left(\frac{s}{4} + \frac{D}{2\theta}\right)^2, \qquad \frac{\theta^2 - D}{2\theta} = \left(\frac{s}{4} - \frac{D}{2\theta}\right)^2. \tag{29}$$

From (7) and (29), we have

$$\frac{x_1}{z_1} = \pm\left(\frac{D}{s\theta} - \frac{s}{4}\right), \qquad \frac{y_1}{z_1} = \pm\left(\frac{D}{s\theta} + \frac{s}{4}\right). \tag{30}$$

Case 2: $v_1(T) = [-1:1:0]$ and $v_2(T) = [1:-1:0]$. This case also implies that $-1 \in k^2$. From (17) and (25), we have

$$\left(b + \frac{d}{D}\right)^2 = \left(b - \frac{d}{D}\right)^2.$$

Since $d \neq 0$, we have $b = 0$. Hence, from (15), we have $t = -s/4$. Therefore,

$$qP(x) = 2x^3 + \frac{s^4}{8}x + Ds^2.$$

Therefore, θ satisfies

$$\theta^3 + \frac{s^4}{16}\theta + \frac{Ds^2}{2} = 0. \tag{31}$$

It follows from (14) and (24) that

$$\frac{\theta^2 + D}{2\theta} = \left(\frac{\theta}{s} - \frac{s}{4}\right)^2, \qquad \frac{\theta^2 - D}{2\theta} = \left(i\left(\frac{\theta}{s} + \frac{s}{4}\right)\right)^2, \tag{32}$$

where $i \in k$ such that $i^2 = -1 \in k$. From (7) and (32), we have

$$\frac{x_1}{z_1} = \pm\left(\frac{\theta}{s} - \frac{s}{4}\right), \qquad \frac{y_1}{z_1} = \pm i\left(\frac{\theta}{s} + \frac{s}{4}\right). \tag{33}$$

https://doi.org/10.1017/S0013091523000706 Published online by Cambridge University Press

3. Proof of Corollary 1

Corollary 1 is a consequence of Theorem 1 and the following lemma due to Izadi et al. [9].

Lemma 1.

(1) *For prime numbers, $p \equiv 3 \pmod{16}$, then the equations $x^2 - y^4 = \pm p^3 z^4$ only have solutions $X = \pm y^2$ and $z = 0$ in $\mathbb{Q}(i)$.*
(2) *For prime numbers, $p \equiv 11 \pmod{16}$, then the equations $X^2 - y^4 = \pm p z^4$ only have solutions $X = \pm y^2$ and $z = 0$ in $\mathbb{Q}(i)$.*

Proof. See Izadi [9, Theorems 3.2 and 3.4]. □

Acknowledgements. The author is supported by the Vietnam National Foundation for Science and Technology Development (NAFOSTED) (grant number 101.04-2023.21).

Competing Interest. The author declares none.

References

(1) A. Bajolet, B. Dupuy, F. Luca and A. Togbe, On the Diophantine equation $x^4 - q^4 = py^r$, *Publ. Math. Debrecen* **79** (2011), 269–282.
(2) M. A. Bennett, Integers presented by $x^4 - y^4$ revisited, *Bull. Aust. Math. Soc.* **76** (2007), 133–136.
(3) A. Bremner, Some quartic curves with no points in any cubic field, *Proc. Lond. Math. Soc.* **52**(3): (1986), 193–214.
(4) Z. Cao, The Diophantine equations $x^4 - y^4 = z^p$ and $x^4 - 1 = dy^q$, *C. R. Math. Rep. Acad. Sci. Canada* **21** (1999), 23–27.
(5) J. W. S. Cassels, The arithmetic of certain quartic curves, *Proc. Roy. Soc. Edinburgh Sect. A* **100**(3–4) (1985), 201–218.
(6) A. Dabrowski, On the integers represented by $x^4 - y^4$, *Bull. Aust. Math. Soc.* **76** (2007), 133–136.
(7) H. Darmon, The equation $x^4 - y^4 = z^p$, *C. R. Math. Rep. Acad. Sci. Canada* **15**(6) (1993), 286–290.
(8) G. Faltings, Endlichkeitssätze für abelsche Varietä ten über Zahlkörpern, *Invent. Math.* **73**(3) (1983), 349–366.
(9) F. Izadi, R. F. Naghdali and P. G. Brown, Some quartic Diophantine equations in Gaussian integers, *Bull. Aust. Math. Soc.* **92** (2015), 187–194.
(10) P. Mondal, *How many zeroes? Counting Solutions of Systems of Polynomials via Toric Geometry at Infinity.* CMS/CAIMS Books in Mathematics, Volume 2 (Switzerland: Springer, 2021).
(11) D. Savin, On the Diophantine equation $x^4 - q^4 = py^5$, *Ital. J. Pure Appl. Math.* **26** (2009), 103–108.
(12) J. P. Serre, *Topics in Galois Theory*, Research Notes in Mathematics, Book 1, 2nd edition (Natick, MA: A K Peters/CRC Press, 2016).
(13) J. H. Silverman, Rational points on certain families of curves of genus at least two, *Proc. Lond. Math. Soc.* **55** (1987), 465–481.