

THE DIOPHANTINE EQUATION $x^4 + 2^n y^4 = 1$ IN QUADRATIC NUMBER FIELDS

ANDREW LI 

(Received 19 August 2020; accepted 27 August 2020; first published online 6 November 2020)

Abstract

Aigner showed in 1934 that nontrivial quadratic solutions to $x^4 + y^4 = 1$ exist only in $\mathbb{Q}(\sqrt{-7})$. Following a method of Mordell, we show that nontrivial quadratic solutions to $x^4 + 2^n y^4 = 1$ arise from integer solutions to the equations $X^4 \pm 2^n Y^4 = Z^2$ investigated in 1853 by V. A. Lebesgue.

2020 *Mathematics subject classification*: primary 11D25; secondary 11R11, 11D45.

Keywords and phrases: quartic Diophantine equations, quadratic number fields.

1. Introduction

In 1934, Aigner [1] showed that only in $\mathbb{Q}(\sqrt{-7})$ do nontrivial quadratic solutions to $x^4 + y^4 = 1$ exist. This result was reproven by Faddeev in 1960 [2] and by Mordell in 1967 [5]. We seek to generalise this result and find all solutions to

$$x^4 + 2^n y^4 = 1 \tag{1.1}$$

where x, y are in some quadratic number field and n is a natural number.

To do so, we require some related results. Lebesgue [3, Theorem II, I] proved in 1853 that

$$X^4 - 2^n Y^4 = Z^2 \quad \text{and} \quad X^4 + 2^n Y^4 = Z^2 \tag{1.2}$$

have nontrivial integer solutions only for $n \equiv 1 \pmod{4}$ and $n \equiv 3 \pmod{4}$, respectively, in which case infinitely many solutions exist. By following the method Mordell outlined in [5], we will prove the following result.

THEOREM 1.1. *If the Diophantine equation $x^4 + 2^n y^4 = 1$ has a solution (x, y) in a quadratic number field, then $n \not\equiv 2 \pmod{4}$. Furthermore:*

- *If $n \equiv 0 \pmod{4}$, the field is $\mathbb{Q}(\sqrt{-7})$.*
- *If $n \equiv 1 \pmod{4}$, the field is $\mathbb{Q}(\sqrt{c})$ and the solution is $(\sqrt{c}/a, b/a)$ where (a, b, c) is an integer solution to $X^4 - 2^n Y^4 = Z^2$.*

- If $n \equiv 3 \pmod 4$, the field is $\mathbb{Q}(\sqrt{c})$ and the solution is $(a/\sqrt{c}, b/\sqrt{c})$ where (a, b, c) is an integer solution to $X^4 + 2^n Y^4 = Z^2$.

EXAMPLE 1.2. For $n = 1$, we verify that an integer solution to $X^4 - 2Y^4 = Z^2$ is

$$(113)^4 - 2(84)^4 = (7967)^2$$

and we observe that $(\sqrt{7967}/113)^4 + 2(84/113)^4 = 1$.

EXAMPLE 1.3. For $n = 3$, we verify that an integer solution to $X^4 + 8Y^4 = Z^2$ is

$$(7)^4 + 8(6)^4 = (113)^2$$

and we observe that $(7/\sqrt{113})^4 + 8(6/\sqrt{113})^4 = 1$.

1.1. Background. It suffices to examine (1.1) for $n = 1, 2, 3$ since we can express any $n = 4m + k$ and rewrite (1.1) as $x^4 + 2^{4m+k}y^4 = x^4 + 2^k(2^m y)^4 = 1$. Aigner handled the $n = 0$ case in [1].

We also note some additional curves that will be useful in finding quadratic solutions. With the change of variables $(x, y) = (Z/X^2, Y/X)$, we can rewrite (1.2) and focus on rational solutions to

$$x^2 + 2^n y^4 = 1 \quad \text{and} \quad x^2 - 2^n y^4 = 1$$

respectively. We can generate solutions to these two rational equations by examining their related elliptic curves. Note that $x^2 + 2^n y^4 = 1$ is birationally equivalent to the elliptic curve $v^2 = u^3 + 2^{n+2}u$ by the maps,

$$(x, y) \rightarrow \left(-\frac{2^{n+1}y^2}{x-1}, -\frac{2^{n+2}y}{x-1} \right), \quad (u, v) \rightarrow \left(\frac{v^2 - 2^{n+3}u}{v^2}, \frac{2u}{v} \right).$$

For $n = 2, 3$, the elliptic curve $v^2 = u^3 + 2^{n+2}u$ has rank 0. But for $n = 1$ the curve has rank 1 with generator $(1, 3)$ of infinite order [6, Elliptic Curve 256.b2], so the curve has infinitely many rational points. A similar birational equivalence exists between $x^2 - 2^n y^4 = 1$ and $v^2 = u^3 - 2^{n-2}u$ defined by the maps,

$$(x, y) \rightarrow \left(\frac{2^{n-1}y^2}{x-1}, \frac{2^{n-1}y}{x-1} \right), \quad (u, v) \rightarrow \left(\frac{v^2 + 2^{n-1}u}{v^2}, \frac{u}{v} \right).$$

Likewise, $n = 3$ is the only case where $v^2 = u^3 - 2^{n-2}u$ has rank 1 with generator $(-1, 1)$ of infinite order [6, Elliptic Curve 256.b1]. For $n = 1, 2$ the curve has rank 0. All these observations are in accordance with Lebesgue’s results. The two exceptional rank 1 curves are summarised below in Table 1.

TABLE 1. Exceptional equations and corresponding elliptic curves with rank 1.

	Integer equation	Rational equation	Elliptic curve	Generators
$n = 1$	$X^4 - 2Y^4 = Z^2$	$x^2 + 2y^4 = 1$	$v^2 = u^3 + 8u$	$(1, 3)$
$n = 3$	$X^4 + 8Y^4 = Z^2$	$x^2 - 8y^4 = 1$	$v^2 = u^3 - 2u$	$(-1, 1)$

Lebesgue also showed that the equation $X^4 + 2^n Y^2 = Z^4$ has no nontrivial integer solutions regardless of n [3, Theorem IV], which equivalently means that $x^4 + 2^n y^2 = 1$ has no nontrivial rational solutions. Additionally, he showed that $2^n X^4 - Y^4 = Z^2$ has no nontrivial integer solutions for $n = 3$ [3, Theorem III].

2. Mordell’s method

ASSUMPTION 2.1. Suppose there exists a quadratic number field $\mathbb{Q}(\sqrt{d})$ in which we have a solution $x, y \in \mathbb{Q}(\sqrt{d})$ to (1.1).

It follows that $x^2, y^2 \in \mathbb{Q}(\sqrt{d})$ as well. Motivated by [4], we introduce the following parameterisation of the equation $x^4 + 2^n y^4 = 1$. Suppose that $y^2 = -(x^2 + 1)/t$. Then $t = -(x^2 + 1)/y^2 \in \mathbb{Q}(\sqrt{d})$. Thus

$$x^2 = \frac{2^n - t^2}{2^n + t^2} \quad \text{and} \quad y^2 = \frac{2t}{2^n + t^2}.$$

There are two cases which we handle separately. In the case that t is rational, we will show quadratic solutions (x, y) exist, in fact an infinite number, of the forms described in the theorem. In the case that t is irrational, there are no quadratic solutions.

2.1. t is rational. Since t is rational, then x^2 and y^2 are necessarily rational and $x, y \in \mathbb{Q}(\sqrt{d})$ are either rational or rational multiples of \sqrt{d} . If both x, y are rational, then we have a nontrivial rational solution to $x^4 + 2^n y^4 = 1$. But this leads to a contradiction, because then we can exhibit a nontrivial rational solution to $x^4 + 2^n y^2 = 1$ which is impossible as noted in Section 1.1. This also excludes the case $x \in \mathbb{Q}, y \notin \mathbb{Q}$.

2.1.1. x irrational, y rational. In this case, we have a nontrivial rational solution to $x^2 + 2^n y^4 = 1$. Therefore, based on Section 1.1, we must have $n = 1$. Further, using the birational equivalence between $x^2 + 2y^4 = 1$ and the elliptic curve $v^2 = u^3 + 8u$, this nontrivial rational solution corresponds to a rational point on the elliptic curve. Conversely, a rational point on $v^2 = u^3 + 8u$ can be used to generate the nontrivial rational solution to $x^2 + 2y^4 = 1$. Through the change of variables in Section 1.1, this rational solution can be rewritten as $(c/a^2)^2 + 2(b/a)^4 = 1$ for an integer solution (a, b, c) to $X^4 - 2Y^4 = Z^2$, which gives a quadratic solution $(\sqrt{c}/a)^4 + 2(b/a)^4 = 1$ to (1.1) in $\mathbb{Q}(\sqrt{c})$.

EXAMPLE 2.2. Using the generator $(1, 3)$ of $v^2 = u^3 + 8u$ mentioned in Section 1.1 we can find the rational solution $(7/9)^2 + 2(2/3)^4 = 1$ by the map given in Section 1.1.

This yields the quadratic solution to (1.1) in $\mathbb{Q}(\sqrt{7})$,

$$\left(\frac{\sqrt{7}}{3}\right)^4 + 2\left(\frac{2}{3}\right)^4 = 1.$$

2.1.2. *x, y irrational.* In this case, we conclude that $x = a\sqrt{d}$ and $y = b\sqrt{d}$ since $x^2, y^2 \in \mathbb{Q}$. Observe then that

$$\frac{2^n - t^2}{2t} = \frac{x^2}{y^2} = \frac{a^2d}{b^2d} = s^2$$

where s is rational. So we have a nontrivial rational solution to $t^2 + 2ts^2 = 2^n$. Mapping $(p, q) = (t + s^2, s)$, this becomes $p^2 - 2^n = q^4$ and dividing by q^4 we get a nontrivial rational solution to $x^2 - 2^n y^4 = 1$. Therefore, from Section 1.1, we must have $n = 3$.

Furthermore, a nontrivial solution to $x^2 - 8y^4 = 1$ arises from an integer solution (a, b, c) to $X^4 + 8Y^4 = Z^2$, which gives $(a/\sqrt{c})^4 + 8(b/\sqrt{c})^4 = 1$ in $\mathbb{Q}(\sqrt{c})$.

EXAMPLE 2.3. To generate nontrivial rational solutions to $x^2 - 8y^4 = 1$, we use rational points on the corresponding elliptic curve $v^2 = u^3 - 2u$ and follow the map specified in Section 1.1. For example, from the generator $(-1, 1)$ of $v^2 = u^3 - 2u$ mentioned in Section 1.1, we get the rational solution $(-3)^2 - 8(-1)^4 = 1$. This yields the quadratic solution to (1.1) in $\mathbb{Q}(\sqrt{-3})$,

$$\left(\frac{1}{\sqrt{-3}}\right)^4 + 8\left(-\frac{1}{\sqrt{-3}}\right)^4 = 1.$$

EXAMPLE 2.4. The rational point $(338, 6124)$ on $v^2 = u^3 - 2u$ yields the rational solution $(57123/239^2)^2 - 8(13/239)^4 = 1$. This gives the quadratic solution

$$\left(\frac{239}{\sqrt{57123}}\right)^4 + 8\left(\frac{13}{\sqrt{57123}}\right)^4 = 1.$$

REMARK 2.5. Note that in both Sections 2.1.1 and 2.1.2 there are an infinite number of fields $\mathbb{Q}(\sqrt{c})$ in which solutions to (1.1) exist. Suppose for a contradiction there are a finite number of such $\mathbb{Q}(\sqrt{c})$. Clearly, by the procedures outlined in these sections, we can generate infinitely many quadratic solutions to (1.1), so one of the finitely many $\mathbb{Q}(\sqrt{c})$ must then contain infinitely many solutions to (1.1). However, by Faltings’s theorem, a curve of genus 3, such as (1.1), can only have finitely many solutions over any number field. Thus there must be an infinite number of such fields $\mathbb{Q}(\sqrt{c})$.

2.2. t is irrational. Since $t \in \mathbb{Q}(\sqrt{d})$ is irrational, $t = a + b\sqrt{d}$ with $b \neq 0$. By definition, t is also the root of an irreducible quadratic $F(z) = z^2 + Bz + C$.

REMARK 2.6. In deriving a contradiction to Assumption 2.1 that there exists a field $\mathbb{Q}(\sqrt{d})$ with a solution to (1.1), it will suffice to show that no such $F(z)$ can exist. By showing $F(z)$ cannot exist, it follows no t can exist, thus the field $\mathbb{Q}(\sqrt{d})$ from which t comes cannot exist either.

To keep everything in terms of t we perform a change of basis in $\mathbb{Q}(\sqrt{d})$ and write $K = \{a + bt : a, b \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{d})$. We shall define new elements $\mathbb{X}, \mathbb{Y} \in K$,

$$\mathbb{X} = (2^n + t^2)xy \quad \text{and} \quad \mathbb{Y} = (2^n + t^2)y.$$

Squaring,

$$\mathbb{X}^2 = 2t(2^n - t^2) \quad \text{and} \quad \mathbb{Y}^2 = 2t(2^n + t^2).$$

For $\mathbb{X}, \mathbb{Y} \in K$ we can also write $\mathbb{X} = a_1 + b_1 t$ and $\mathbb{Y} = a_2 + b_2 t$ for $a_1, b_1, a_2, b_2 \in \mathbb{Q}$. Thus, t is the root of the polynomials

$$(a_1 + b_1 z)^2 - 2z(2^n - z^2) \tag{2.1}$$

$$(a_2 + b_2 z)^2 - 2z(2^n + z^2). \tag{2.2}$$

It follows that $F(z)$ divides (2.1) and (2.2) in $\mathbb{Q}[z]$, so we have the identities

$$(a_1 + b_1 z)^2 - 2z(2^n - z^2) = F(z)(P_1 + Q_1 z) \tag{2.3}$$

$$(a_2 + b_2 z)^2 - 2z(2^n + z^2) = F(z)(P_2 + Q_2 z) \tag{2.4}$$

for $P_1, Q_1, P_2, Q_2 \in \mathbb{Q}$. We shall investigate the roots of the linear terms $P_1 + Q_1 z$ and $P_2 + Q_2 z$ to better characterise $F(z)$. Clearly $z = -P_1/Q_1$ is a rational root of the right-hand side of (2.3) so it must be a root of the left-hand side, the polynomial (2.1). Likewise, we conclude $z = -P_2/Q_2$ is a rational root of (2.2). So, we are interested in rational roots of (2.1) and (2.2). In fact, for $y_i = a_i + b_i z$ and $x_i = z$, these rational roots are nontrivial rational points on the elliptic curves

$$y_1^2 = 2x_1(2^n - x_1^2) \tag{2.5}$$

$$y_2^2 = 2x_2(2^n + x_2^2). \tag{2.6}$$

Mapping $(u, v) = (-2x_i, 2y_i)$, we observe these are exactly the elliptic curves noted in Section 1.1. As noted, (2.5) has rank 1 for $n = 3$ as does (2.6) for $n = 1$, otherwise they have rank 0. For $n = 2$, both elliptic curves have rank 0, so we handle this simpler case first.

2.2.1. $n = 2$. Both (2.5) and (2.6) have only trivial points. For (2.5), they are $(0, 0), (\pm 2, 0)$ so $z_1 = 0, \pm 2$ are roots of (2.1). For (2.6) it is $(0, 0)$ so $z_2 = 0$ is the only root of (2.2).

Case 1: $z_1 = 0, z_2 = 0$. Since $z_1 = 0$ is a root of (2.1), from (2.3) we conclude $a_1 = 0$ and $P_1 = 0$. Since $z_2 = 0$, from (2.4) we get $a_2 = 0$ and $P_2 = 0$. After substituting and dividing by z , the identities (2.3) and (2.4) become,

$$Q_1 F(z) = 2z^2 + b_1^2 z - 8$$

$$Q_2 F(z) = -2z^2 + b_2^2 z - 8.$$

Comparing coefficients, clearly $8 \neq -8$, so evidently no such $F(z)$ exists.

Case 2: $z_1 = 2, z_2 = 0$. From (2.3) and the root $z_1 = 2$, we get $a_1 = -2b_1$ and $P_1 = -2Q_1$ so (2.3) becomes

$$(-2b_1 + b_1z)^2 - 2z(4 - z^2) = F(z)(-2Q_1 + Q_1z).$$

After factoring and dividing by $z - 2$, this produces the system

$$Q_1F(z) = 2z^2 + (b_1^2 + 4)z - 2b_1^2$$

$$Q_2F(z) = -2z^2 + b_2^2z - 8.$$

Observe that $2b_1^2 = -8$ is impossible, so again no such $F(z)$ exists.

Case 3: $z_1 = -2, z_2 = 0$. Following the same process, $a_1 = 2b_1$ and $P_1 = 2Q_1$, giving

$$Q_1F(z) = 2z^2 + (b_1^2 - 4)z + 2b_1^2$$

$$Q_2F(z) = -2z^2 + b_2^2z - 8.$$

So $b_1^2 - 4 = -b_2^2$ and $2b_1^2 = 8$. This means that $b_1 = \pm 2$, but then $b_2 = 0$ which is a contradiction since $F(z) = z^2 - 4$ is not irreducible. Therefore, the case $n = 2$ produces no quadratic solutions.

2.2.2. $n = 1$. The only rational point on (2.5) is $(0, 0)$ so $z_1 = 0$ is the only root of (2.1). From (2.3), $a_1 = 0$ and $P_1 = 0$ so

$$Q_1F(z) = 2z^2 + b_1^2z - 4. \tag{2.7}$$

Next, (2.6) has infinitely many rational points with $x_2 \geq 0$. First we shall handle the case where $x_2 = z_2 = 0$ is a root of (2.2). This gives $a_2 = 0$ and $P_2 = 0$, producing

$$Q_2F(z) = -2z^2 + b_2^2 - 4.$$

Comparing coefficients with (2.7) shows this is impossible. So we turn to the general case. Let (x_2, y_2) be one of infinitely many rational points on (2.6) with $x_2 > 0$. By definition, we have $a_2 = y_2 - b_2x_2$ and since $z_2 = x_2$ is a root of (2.2), it follows that $P_2 = -Q_2x_2$. So, (2.4) becomes

$$((y_2 - b_2x_2) + b_2z)^2 - 2z(2 + z^2) = F(z)(-Q_2x_2 + Q_2z).$$

Dividing by $z - x_2$,

$$Q_2F(z) = -2z^2 + (b_2^2 - 2x_2)z + (-x_2b_2^2 + 2y_2b_2 - 2x_2^2 - 4). \tag{2.8}$$

Equating coefficients between (2.7) and (2.8) gives the system

$$\begin{aligned} b_1^2 &= -(b_2^2 - 2x_2) \\ 4 &= -x_2b_2^2 + 2y_2b_2 - 2x_2^2 - 4. \end{aligned} \tag{2.9}$$

Note that the discriminant of (2.9) with respect to b_2 is equal to $-4(2x_2^3 + 8x_2 - y_2^2)$. Substituting (2.6), the discriminant becomes $-4(4x_2)$. Since $x_2 > 0$, the discriminant must always be negative. So there is no rational b_2 and thus $F(z)$ does not exist, and the $n = 1$ case yields no additional solutions.

2.2.3. $n = 3$. We follow a similar process to the $n = 1$ case. The only rational point on (2.6) is $(0, 0)$, so $z_2 = 0$ is the only root of (2.2). From (2.4), $a_2 = 0$ and $P_2 = 0$ so

$$Q_2F(z) = -2z^2 + b_2^2z - 16. \tag{2.10}$$

Now (2.5) has infinitely many rational points without any conditions on x and y . Again we shall handle the point $(0, 0)$ first, so $z_1 = 0$ is a root of (2.1), yielding

$$Q_1F(z) = 2z^2 + b_1^2z - 16.$$

As in the $n = 1$ case, this is impossible. So we turn to the general case. Let (x_1, y_1) be one such rational point on (2.5) with $x_1, y_1 \neq 0$. From (2.3), we conclude $P_1 = -Q_1x_1$ and the identity becomes

$$((y_1 - b_1x_1) + b_1z)^2 - 2z(8 - z^2) = F(z)(-Q_1x_1 + Q_1z).$$

Again dividing by $z - x_1$,

$$Q_1F(z) = 2z^2 + (b_1^2 + 2x_1)z + (2y_1b_1 - b_1^2x_1 + 2x_1^2 - 16). \tag{2.11}$$

Equating coefficients from (2.10) and (2.11) we get a similar system,

$$b_2^2 = -(b_1^2 + 2x_1) \tag{2.12}$$

$$16 = 2y_1b_1 - b_1^2x_1 + 2x_1^2 - 16. \tag{2.13}$$

The discriminant of (2.13) in b_1 is $-4(32x_1 - 2x_1^3 - y_1^2)$ which reduces to $-4(16x_1) = -64x_1$. For positive x_1 , clearly no $F(z)$ exists as in the $n = 1$ case. But for negative x_1 , because $b_1 \in \mathbb{Q}$ by assumption, we see that $-x_1$ must be a perfect square. So $-x_1 = e^2$ for some positive rational e . Rewriting in terms of e , (2.5) becomes

$$y_1^2 = -2e^2(8 - e^4) \implies y_1 = \pm e\sqrt{2e^4 - 16}.$$

Further, in terms of e , (2.13) becomes the following quadratic in b_1 ,

$$0 = e^2b_1^2 + (\pm 2e\sqrt{2e^4 - 16})b_1 + (2e^4 - 32). \tag{2.14}$$

Solving (2.14) and squaring,

$$b_1 = \frac{\sqrt{2e^4 - 16} \pm 4}{e} \quad \text{or} \quad b_1 = \frac{-\sqrt{2e^4 - 16} \pm 4}{e} \implies b_1^2 = \frac{2e^4 \pm 8\sqrt{2e^4 - 16}}{e^2}.$$

We also know from (2.12) that $b_1^2 - 2e^2 = -b_2^2$ so it follows that

$$\begin{aligned} -b_2^2 &= \frac{2e^4 \pm 8\sqrt{2e^4 - 16}}{e^2} - 2e^2 \\ &= \frac{2e^4 \pm 8\sqrt{2e^4 - 16} - 2e^4}{e^2} \\ &= \pm \frac{8\sqrt{2e^4 - 16}}{e^2}. \end{aligned}$$

We discard the positive sign as it is impossible. So for b_2 to be rational, $2\sqrt{2e^4 - 16}$ must be square, or equivalently, $\sqrt{2e^4 - 16} = 2f^2$ for some rational f . It follows that $2e^4 - 16 = 4f^4$ and thus $e^4 - 2g^2 = 2f^4$ for $g = 2$. Multiplying by a common denominator exhibits a solution $E^4 = 2G^2 + 2F^4$ with $E, F, G \in \mathbb{Z}$. Evidently, $2 \mid E^4$ so $2 \mid E$ and we can reduce the equation further to $8E_1^4 = G^2 + F^4$ for $2E_1 = E$. But this is impossible as noted in Section 1.1. Thus no such rational f exists and $b_2 \notin \mathbb{Q}$. There are no additional solutions for $n = 3$ and the proof is complete. \square

Acknowledgement

I want to thank my advisor, Dr. Griff Elder, for providing this research opportunity as well as his patience and guidance in completing this paper.

References

- [1] A. Aigner, 'Über die möglichkeit von $x^4 + y^4 = z^4$ in quadratischen körpern', *Jahresber. Dtsch. Math.-Ver.* **43** (1934), 226–229.
- [2] D. K. Faddeev, 'Group of divisor classes on the curve defined by the equation $x^4 + y^4 = 1$ ', *Soviet Math. Dokl.* **1** (1960), 1149–1151.
- [3] V. A. Lebesgue, 'Résolution des équations biquadratiques (1), (2) $z^2 = x^4 \pm 2^m y^4$, (3) $z^2 = 2^m x^4 - y^4$, (4), (5) $2^m z^2 = x^4 \pm y^4$ ', *J. Math. Pures Appl.* **18** (1853), 73–86. <https://archive.org/details/s1journaldemat18liou/page/72/mode/2up>.
- [4] E. D. Manley, 'On quadratic solutions of $x^4 + py^4 = z^4$ ', *Rocky Mountain J. Math.* **36**(3) (2006), 1027–1031.
- [5] L. J. Mordell, 'The Diophantine equation $x^4 + y^4 = 1$ in algebraic number fields', *Acta Arith.* **14** (1967/68), 347–355.
- [6] The LMFDB Collaboration, 'The L-functions and modular forms database', <http://www.lmfdb.org>, (online; accessed 28 July 2020).

ANDREW LI, Department of Mathematics,
University of Nebraska Omaha, Omaha, NE 68182, USA
e-mail: ali01@unomaha.edu