ACTA ARITHMETICA
XIV (1968)

# The Diophantine equation $x^4+y^4=1$ in algebraic number fields

by

L. J. MORDELL (Cambridge)

An interesting extension of a classical result is to discuss the solution of the equation

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

in an algebraic number field $K$. When $K$ is the rational field $Q$, it is well known that the only solutions are given by

$$x=\pm 1,\ y=0; \quad x=0,\ y=\pm 1. \tag{2}$$

When $K$ is a quadratic field, it has been recently shown by Faddeev [1] that solutions other than (2) occur only when

$$\begin{aligned} &K=Q(i), \quad x=\pm i,\ y=0; \quad x=0,\ y=\pm i,\\ &K=Q(\sqrt{-7}), \quad x=\varepsilon_1\frac{(1+\varepsilon\sqrt{-7})}{2},\ y=\varepsilon_2\frac{(1-\varepsilon\sqrt{-7})}{2}, \end{aligned} \tag{3}$$

where $\varepsilon^2=\varepsilon_1^2=\varepsilon_2^2=1$.

Further when $K$ is a cubic field, he has shown that the only solutions other than (2) and (3), are those given by the intersection of (1) with arbitrary rational lines through each of the points (2), e.g., for one set, with rational $t$, $y=1+tx$ and

$$(t^4+1)x^3+4t^3x^2+6t^2x+4t=0. \tag{4}$$

The proof depends upon very advanced principles and requires considerable technique. It seems desirable to give a very simple elementary proof depending upon first principles.

On putting $1-x^2=ty^2$, a solution of (1) is given parametrically by

$$x^2=\frac{1-t^2}{1+t^2}, \quad y^2=\frac{2t}{1+t^2}. \tag{5}$$

Then if $x$ and $y$ are elements of $K$, so is $t$.

---

[1] D. K. Faddeev, *Group of divisor classes on the curve defined by the equation* $x^4+y^4=1$, Amer. Math. Soc. Trans. Soviet Math. Dokl. 1 (1961), pp. 1149-1151.

Suppose first that $t$ is rational. Then $x^2$ and $y^2$ are rational, and on excluding (2), $K$ is a quadratic field, and so $x^2|y^2$ or $y^2|x^2$ is a perfect square. It is well known on noting (5), that this occurs only when $t = 0, \pm 1, \infty$.

This gives apart from (2),

$$x^2 = -1,\ y^2 = 0; \quad x^2 = 0,\ y^2 = -1,$$

and this is in accordance with part of (3).

We now consider the case when $K$ is a quadratic field. We may suppose that $t$ is a non-rational element of $K$.

Put

$$X = (1+t^2)xy, \quad Y = (1+t^2)y. \tag{6}$$

Then

$$X^2 = 2t(1-t^2), \quad Y^2 = 2t(1+t^2). \tag{7}$$

We may suppose that $t$ is a root of the quadratic equation

$$F(t) = t^2+Bt+C = 0, \tag{8}$$

where $B, C$ are rational constants and so $K = Q(t)$. Then

$$X = a+bt, \quad Y = a_1+b_1t, \tag{9}$$

where $a, b, a_1, b_1$, are rational constants. From (7), we deduce the two identities in a variable $z$,

$$(a+bz)^2-2z(1-z^2) = F(z)(P+Qz), \tag{10}$$

$$(a_1+b_1z)^2-2z(1+z^2) = F(z)(P_1+Q_1z), \tag{11}$$

where $P, Q, P_1, Q_1$ are rational constants. Clearly $QQ_1 \neq 0$, and so the left hand sides of (10), (11) must vanish for rational values of $z$. For (10), this is possible only when $z = 0, z = \pm 1$, and for (11), only when $z = 0, 1$. On combining these, we have six possibilities for the linear factors in (10), (11). These correspond to cases $(z_1, z_2)$ where $z_1$ refers to the $z = 0, \pm 1$ in (10), and $z_2$ to the $z = 0, 1$ in (11). We consider the cases in turn.

(I) $(0, 0)$. Here $P = 0,\ a = 0,\ P_1 = 0,\ a_1 = 0$, and

$$b^2z-2(1-z^2) = QF(z),$$
$$b_1^2z-2(1+z^2) = Q_1F(z).$$

The two left hand sides are the same except for a constant factor and this is obviously impossible.

(II) $(1, 0)$. Here $P+Q = 0,\ a+b = 0,\ P_1 = 0,\ a_1 = 0$, and

$$a^2(1-z)-2z(1+z) = PF(z),$$
$$b_1^2z-2(1+z^2) = Q_1F(z).$$

On subtracting, $a^2 = -2$ which is impossible.



(III) $(-1, 0)$. Here $a-b = 0,\ a_1 = 0$, and

$$a^2(1+z)-2z(1-z) = PF(z),$$
$$b_1^2z-2(1+z^2) = Q_1F(z).$$

Addition gives $a^2-2 = 0$.

(IV) $(0, 1)$. Here $P = 0,\ a = 0,\ P_1+Q_1 = 0,\ (a_1+b_1)^2-4 = 0$. Since the sign of $a_1$ is at our disposal, we may take $a_1+b_1 = 2$. Then

$$b^2z-2(1+z^2) = QF(z),$$
$$(2-b_1+b_1z)^2-2z-2z^3 = P_1(1-z)F(z).$$

Multiply the first equation by $1-z$. On comparing constant terms and coefficients of $z^3$,

$$\frac{-2}{(2-b_1)^2} = \frac{2}{-2}.$$

(V) $(1, 1)$. Here $a+b = 0,\ P+Q = 0,\ a_1+b_1 = 2,\ P_1+Q_1 = 0$, and

$$a^2(1-z)^2-2z(1-z^2) = PF(z)(1-z),$$
$$\big(2-b_1(1-z)\big)^2-2z(1+z^2) = P_1F(z)(1-z).$$

On comparing the constant terms and coefficients of $z^3$

$$\frac{a^2}{(2-b_1)^2} = \frac{2}{-2}$$

and so $a = 0,\ b_1 = 2$ and can be rejected.

(VI) $(-1, 1)$. Here $a = b,\ P-Q = 0,\ a_1+b_1 = 2,\ P_1+Q_1 = 0$.

$$a^2(1+z)-2z(1-z) = PF(z).$$

From the second equation in (V), on dividing out by $1-z$,

$$(2-b_1)^2+(2-b_1^2)z+2z^2 = P_1F(z).$$

Since the coefficients of $z^2$ are the same,

$$a^2 = (2-b_1)^2, \quad a^2+b_1^2 = 4.$$

Then either $a = 0,\ b_1 = 2$ which is obviously impossible since $F(z)$ is irreducible, or $a = \pm 2,\ b_1 = 0$. Then $b = \pm 2,\ a_1 = \pm 2$. This gives

$$F(z) = z^2+z+2,$$

and so

$$t = \frac{-1 \pm \sqrt{-7}}{2} \quad \text{and} \quad K = Q(\sqrt{-7}).$$

Then

$$X = \pm 2(1+t), \quad Y = \pm 2,$$

and from (6)

$$y = \pm \frac{2t}{t^2+1}, \quad x = \pm(1+t),$$

with independent signs. Hence

$$x = \varepsilon_1 \frac{(1+\varepsilon\sqrt{-7})}{2}, \quad y = \varepsilon_2 \frac{(1-\varepsilon\sqrt{-7})}{2}, \quad \varepsilon^2 = \varepsilon_1^2 = \varepsilon_2^2 = 1.$$

We now consider the case when $K$ is a cubic field $Q(t)$ where $t$ is a root of the irreducible equation

$$F(t) = t^3+Bt^2+Ct+D = 0.$$

We have now in (7),

$$X = a+bt+ct^2, \quad Y = a_1+b_1t+c_1t^2,$$

and then the two identities in $z$,

$$(a+bz+cz^2)^2-2z(1-z^2) = F(z)(P+Qz), \tag{12}$$

$$(a_1+b_1z+c_1z^2)^2-2z(1+z^2) = F(z)(P_1+Q_1z). \tag{13}$$

We have as before six cases to consider, namely $(0, 0)$, $(1, 0)$, $(-1, 0)$, $(0, 1)$ $(1, 1)$ $(-1, 1)$.

There is now however the further possibility that $QQ_1 = 0$. Suppose first that $Q = 0$. We have then three cases which we can write as $(-, -)$, $(-, 0)$ $(-, 1)$.

(I) $(-, -)$. Here $c = c_1 = 0$, $Q = Q_1 = 0$. Then

$$\frac{a^2}{a_1^2} = \frac{2}{-2},$$

and so $a = a_1 = 0$, obviously impossible.

(II) $(-, 0)$. Here $c = 0$, $Q = 0$, $a_1 = 0$, $P_1 = 0$. Then

$$(a+bz)^2-2z(1-z^2) = PF(z),$$
$$z(b_1+c_1z)^2-2(1+z^2) = Q_1F(z).$$

Hence

$$\frac{a^2}{-2} = \frac{2}{c_1^2}.$$

(III) $(-, 1)$. Here $c = 0$, $Q = 0$, $a_1+b_1+c_1 = \pm 2$, $P_1+Q_1 = 0$. Then

$$(1-z)(a+bz)^2-2z(1-z)(1-z^2) = P(1-z)F(z),$$
$$(a_1+b_1z+c_1z^2)^2-2z(1+z^2) = P_1(1-z)F(z).$$



Hence

$$\frac{a^2}{a_1^2} = -\frac{2}{c_1^2},$$

and $a = a_1 = 0$ or $a_1 = c_1 = 0$, and then $F(z)$ is divisible by $z$.

Suppose next $Q_1 = 0$. We have three cases $(0, -)$, $(1, -)$, $(-1, -)$.

(IV) $(0, -)$. Here

$$z(b+cz)^2-2(1-z^2) = QF(z),$$
$$(a_1+b_1z)^2-2z(1+z^2) = P_1F(z).$$

Hence

$$\frac{-a_1^2}{2} = \frac{-2}{c^2} = \frac{2a_1b_1-2}{b^2} = \frac{b_1^2}{2bc+2}. \tag{14}$$

From these two equations, replacing $z$ by $t$, and multiplying, we deduce another identity,

$$(a_1+b_1z)^2(b+cz)^2-4(1-z^4) = F(z)(P_2+Q_2z).$$

Hence the left hand side vanishes for a rational value of $z$. This can only be $z = 0, \pm 1$.

When $z = 0$, $a_1b = \pm 2$ and since $a_1c = \pm 2$, and $a_1 \neq 0$, we have $b \pm c = 0$, and then $F(z)$ is not irreducible. When $z = \pm 1$, $(a_1 \pm b_1)(b \pm c) = 0$ and so $a_1 \pm b_1 = 0$.

Then from (14), $bc = -2$ and

$$\frac{-a_1^2}{2} = (\pm 2a_1^2-2)\frac{c^2}{4},$$
$$-a_1^2 = (\pm a_1^2-1)\frac{1}{a_1^2}$$

and gives no value for $a_1$.

(V) $(1, -)$. Here

$$(a+bz+cz^2)^2-2z(1-z^2) = P(1-z)F(z),$$
$$(a_1+b_1z)^2-2z(1+z^2) = P_1F(z).$$

Divide the first equation by $1-z$. Then

$$\frac{a^2}{a_1^2} = \frac{c^2}{2},$$

and so $a = 0$, and this is impossible.

(VI) $(-1, -)$. Here

$$(a+bz+cz^2)^2-2z(1-z^2) = P(1+z)F(z),$$
$$(a_1+b_1z)^2-2z(1+z^2) = F(z).$$

Divide the first equation by $1+z$. Then

$$\frac{a^2}{a_1^2} = -\frac{c^2}{2}.$$

This disposes of the cases when $QQ_1 = 0$.

We now consider the six cases when $QQ_1 \neq 0$.

(I′) $(0, 0)$. Here $a = 0$, $P = 0$, $a_1 = 0$, $P_1 = 0$. Hence

$$z(b+cz)^2-2(1-z^2) = QF(z),$$
$$z(b_1+c_1z)^2-2(1+z^2) = Q_1F(z).$$

The two left hand sides must be equal. Hence

$$b^2 = b_1^2, \quad c^2 = c_1^2, \quad bc-b_1c_1 = -2,$$

and so

$$b = \pm b_1, \quad c = \mp c_1, \quad bc = -1.$$

Then

$$F(z) = c^2z^3+b^2z-2.$$

Then from (6),

$$y = \pm\frac{bt-ct^2}{1+t^2}, \quad x = \pm\frac{b+ct}{b-ct}, \quad bc = -1.$$

It suffices to take the $+$ signs. Then $x+1 = by$ since this gives

$$\frac{2b}{b-ct} = \frac{b(b-ct)t}{1+t^2},$$

or

$$2(1+t^2) = t(b-ct)^2,$$

and this is $F(t) = 0$.

(II′) $(1, 0)$. Here $a+b+c = 0$, $P+Q = 0$, $a_1 = 0$, $P_1 = 0$, and so

$$(-b-c+bz+cz^2)^2-2z(1-z^2) = P(1-z)F(z),$$
$$z(b_1+c_1z)^2-2(1+z^2) = Q_1F(z).$$

Dividing out by $1-z$, we have

$$\frac{(b+c)^2}{-2} = \frac{-c^2}{c_1^2}.$$

Hence either $b = c = 0$ or $c = c_1 = 0$ which are obviously impossible.



(III′) $(-1, 0)$. Here

$$(b-c+bz+cz^2)^2-2z(1-z^2) = P(1+z)F(z),$$
$$z(b_1+c_1z)^2-2(1+z^2) = Q_1F(z).$$

Now

$$\frac{(b-c)^2}{-2} = \frac{c^2}{c_1^2},$$

and this is impossible.

(IV′) $(0, 1)$. Here

$$z(b+cz)^2-2(1-z^2) = QF(z),$$
$$(a_1+b_1z+c_1z^2)^2-2z(1+z^2) = P_1(1-z)F(z).$$

Dividing out by $1-z$, we find

$$\frac{a_1^2}{-2} = \frac{-c_1^2}{c^2},$$

and so $a_1 = c_1 = 0$ or $c_1 = c = 0$ which are both impossible.

(V′) $(-1, 1)$. $a-b+c = 0$, $a_1+b_1+c_1 = 0$,

$$(a+bz+cz^2)^2-2z(1-z^2) = P(1+z)F(z),$$
$$(a_1+b_1z+c_1z^2)^2-2z(1+z^2) = P_1(1-z)F(z).$$

On dividing out by $1+z$ and $1-z$, we have

$$\frac{a^2}{a_1^2} = \frac{-c^2}{c_1^2}.$$

Hence $a = a_1 = 0$ or $a = c = 0$ or $a_1 = c_1 = 0$ or $c = c_1 = 0$. These are all impossible since $F(z)$ is irreducible.

(VI′) $(1, 1)$. A solution arises in this case. Here $a+b+c = 0$, $P+Q = 0$, $a_1+b_1+c_1 = 2$, $P_1+Q_1 = 2$ by choice of sign for $a_1$. Hence

$$(-b-c+bz+cz^2)^2-2z(1-z^2) = P(1-z)F(z), \tag{15}$$
$$(2-b_1-c_1+b_1z+c_1z^2)^2-2z(1+z^2) = P_1(1-z)F(z). \tag{16}$$

In (15), (16), compare the constant terms, the coefficients of $z^4$, and insert the values $z = -1$, and $z = 1$. We find

$$\frac{(b+c)^2}{(b_1+c_1-2)^2} = \frac{c^2}{c_1^2} = \frac{1}{b_1+2c_1-2} = \frac{b^2}{(b_1-1)^2+1}. \tag{17}$$

Then

$$\frac{c}{b+c} = \pm\frac{c_1}{b_1+c_1-2}, \quad \frac{b}{b+c} = \left(\frac{(b_1-1)^2+1}{(b_1+c_1-2)^2}\right)^{1/2}.$$

Hence

$$\left(1\pm\frac{c_1}{b_1+c_1-2}\right)^2=\frac{(b_1-1)^2+1}{(b_1+c_1-2)^2},$$

$$(b_1+c_1-2\mp c_1)^2=(b_1-1)^2+1. \tag{18}$$

Take first the $-$ sign. Then $b_1=1$ and from (17),

$$b^2=\frac{1}{2c_1-1},\quad c_1=\frac{b^2+1}{2b^2},\quad c=\pm\frac{b^2+1}{2b}.$$

Further

$$\frac{(b+c)^2}{(c_1-1)^2}=\frac{c^2}{c_1^2},\quad \left(\frac{b+c}{b}\right)^2=\left(\frac{b^2-1}{2b^2}\right)^2.$$

We cannot have $c=\dfrac{b^2+1}{2b}$ for this would give

$$\frac{3b^2+1}{2b^2}=\pm\frac{(b^2-1)}{2b^2},$$

and gives no value for $b$.

Hence $c=-(1+b^2)/2b$. Then from (6),

$$y=\left(\frac{b^2-1}{2b^2}+z+\frac{b^2+1}{2b^2}z^2\right)\Big/(1+z^2),$$

$$x=\left(\frac{1-b^2}{2b}+bz-\frac{b^2+1}{2b}z^2\right)\Big/\left(\frac{b^2-1}{2b}+z+\frac{b^2+1}{2b^2}z^2\right).$$

Hence

$$\frac{x}{b}+1=2z\Big/\left(\frac{b^2-1}{2b^2}+z+\frac{b^2+1}{2b^2}z^2\right)=y$$

from equation (16) provided $z$ satisfies the equation derived from (15), namely,

$$(1-z)\left(\frac{b^2-1}{2b}-\frac{b^2+1}{2b}z\right)^2-z(1+z)=0.$$

We now take the $+$ sign in (18) and show that no solution arises. Now

$$(b_1+2c_1-2)^2=(b_1-1)^2+1,$$

and so

$$b_1=-\frac{(2c_1^2-4c_1+1)}{2c_1-1}.$$



Then

$$b^2=\frac{(b_1-1)^2+1}{b_1+2c_1-2}=\left(\frac{2c_1^2-2c_1}{2c_1-1}\right)^2+1\Big/\frac{-2c_1^2+4c_1-1}{2c_1-1}+2c_1-2$$

$$=\frac{(2c_1^2-2c_1)^2+(2c_1-1)^2}{(2c_1^2-2c_1+1)(2c_1-1)}=\frac{2c_1^2-2c_1+1}{2c_1-1}.$$

Since $2b^2=\dfrac{(2c_1-1)^2+1}{2c_1-1}$, the only rational solution is given by $c_1=1$, $b=\pm1$, $b_1=1$. Then $z$ is a factor of $F(z)$ in (16). This completes the proof.

The present method fails when $K$ is an algebraic number field of degree $n>3$. There is a possibility that solutions of $x^4+y^4=1$ exist in many fields.

When $n=4$, obvious solutions are given by

$$x=a+bt,\quad y=a_1+b_1t,$$

where $a, b, a_1, b_1$, are rational, and $K$ is defined by

$$(a+bt)^4+(a_1+b_1t)^4=1.$$

On noting (7), it is suggested that solutions are given by

$$x=a+bt+ct^2,\quad y=a_1+b_1t+c_1t^2,$$

where $t$ is a root of the equation $F(t)=0$ below.

For instead of (10), (11), we have now

$$(a+bz+cz^2)^2-2z(1-z^2)=PF(z),$$

$$(a_1+b_1z+c_1z^2)^2-2z(1+z^2)=P_1F(z).$$

It is not difficult to impose conditions on the constants such that these two relations are consistent.

Addendum (April 22, 1968). Professor Ljunggren informs me that the result for quadratic fields is due to Aigner. His proof is different from mine and is contained in his paper, *Über die Möglichkeit von $x^4+y^4=z^2$ in quadratische Körper*, Jahresbericht der deutschen Math. Verein. 43(1934), pp. 226-228.

ST. JOHN'S COLLEGE,
CAMBRIDGE, ENGLAND

*Reçu par la Rédaction le 16. 8. 1967*