Acta Mathematica Academiae Paedagogicae Nyíregyháziensis
20 (2004), 1–10
www.emis.de/journals

THE DIOPHANTINE EQUATION $x^4 - y^4 = z^2$ IN THREE QUADRATIC FIELDS

SÁNDOR SZABÓ

ABSTRACT. Each solution of the equation $x^4 - y^4 = z^2$ in the integers of the quadratic field $Q(\sqrt{d})$ is also a solution of the equation $xyz = 0$, where $d = -2, -1, 2$.

1. Introduction

The solution (x_0, y_0, z_0) of the equation $x^4 - y^4 = z^2$ is called *trivial* if $x_0 = 0$ or $y_0 = 0$ or $z_0 = 0$. It is a classical result that the equation $x^4 - y^4 = z^2$ has only trivial solutions in integers. (See for example [2] or [3].) The purpose of this paper is to show that the equation $x^4 - y^4 = z^2$ has only trivial solutions in some larger domains, namely in the integers of $Q(\sqrt{d})$, where $d = -2, -1, 2$.

The proof is a standard application of the infinite decent. The details are depending on the arithmetical properties of $Q(\sqrt{d})$. As a matter of fact the three values of d are singled out because these are the cases in which the rational prime 2 is an associate of a square in $Q(\sqrt{d})$. Let ω be a prime divisor of 2 in $Q(\sqrt{d})$. Thus $2 = \mu\omega^2$, where μ is a unit in $Q(\sqrt{d})$. The corresponding values of d, μ, ω are listed in the table below.

d	μ	ω
-2	-1	$\sqrt{-2}$
-1	$-\sqrt{-1}$	$1+\sqrt{-1}$
2	1	$\sqrt{2}$

TABLE 1

We will use the principal ideals formed by the algebraic integer multiples of ω^n for $1 \leq n \leq 4$. However, usually we will prefer to formulate our statements in terms of congruences instead of ideals. Clearly, ω^2, ω^4 are associates of 2, 4 respectively and so they span the same principal ideals. Similarly, ω, ω^3 are associates of ω, 2ω and so they span the same ideals. We will use the next observation several times. If an integer α of $Q(\sqrt{d})$ and $\alpha \equiv 1 \pmod{\omega}$, then $\alpha^2 \equiv 1 \pmod{\omega^2}$ and $\alpha^4 \equiv 1$

2000 *Mathematics Subject Classification.* Primary 11F06; Secondary 11E08.
Key words and phrases. Diophantine equations, Quadratic fields.

(mod ω^4). Indeed, α can be written in the form $\alpha = k\omega + 1$, where k is an integer of $Q(\sqrt{d})$. Then computing α^2 and α^4

$$\alpha^2 = (k\omega)^2 + 2(k\omega) + 1,$$

$$\alpha^4 = (k\omega)^4 + 4(k\omega)^3 + 6(k\omega)^2 + 4(k\omega) + 1$$

show that $\alpha^2 \equiv 1 \pmod{\omega^2}$ and $\alpha^4 \equiv 1 \pmod{\omega^4}$.

2. The equation in $Q(\sqrt{-1})$

We list the properties of $Q(\sqrt{-1})$ which play part later. Let $i = \sqrt{-1}$ and $\omega = 1 + i$. The ring of integers of $Q(i)$ is $Z[i] = \{u + vi : u, v \in Z\}$ which is a unique factorization domain. The units of $Z[i]$ are 1, i, -1, $-i$. The norm of ω is 2 and consequently ω is a prime in $Z[i]$. The prime factorization of 2 is $(-i)\omega^2$.

Theorem 1. *The equation $x^4 - y^4 = z^2$ has only trivial solutions in $Z[i]$.*

Proof. We divide the proof into (6) smaller steps.

(1) If (x_0, y_0, z_0) is a nontrivial solution of the equation $x^4 - y^4 = z^2$, then we may assume that x_0, y_0, z_0 are pairwise relatively primes.

Let g be the greatest common divisor of x_0 and y_0 in $Z[i]$. As $x_0 \neq 0$, it follows that $g \neq 0$. Dividing $x_0^4 - y_0^4 = z_0^2$ by g^4 we get $(x_0/g)^4 - (y_0/g)^4 = (z_0/g^2)^2$. This equation holds in $Q(i)$. The left hand side of the equation is an element of $Z[i]$. Consequently the right hand side of the equation belongs to $Z[i]$. Thus $(x_0/g, y_0/g, z_0/g^2)$ is also a nontrivial solution of the equation $x^4 - y^4 = z^2$ in $Z[i]$. Hence we may assume that x_0 and y_0 are relatively primes in $Z[i]$. If there is a prime q of $Z[i]$ such that $q|x_0$ and $q|z_0$, then $q|y_0$. This violates that x_0 and y_0 are relatively primes. Similarly, if $q|y_0$ and $q|z_0$, then $q|x_0$ violating again that x_0 and y_0 are relatively primes. Thus we may assume that x_0, y_0, z_0 are pairwise relatively primes.

(2) Let (x_0, y_0, z_0) be a nontrivial solution of the equation $x^4 - y^4 = z^2$ in $Z[i]$ such that x_0, y_0, z_0 are pairwise relatively primes. Note that at most one of x_0, y_0, z_0 can be congruent to 0 modulo ω. We consider the following four cases. None of x_0, y_0, z_0 is congruent to 0 modulo ω and three cases depending on one of x_0, y_0, z_0 is congruent to 0 modulo ω respectively. Table 2 summarizes the cases.

	$x_0 \equiv$	$y_0 \equiv$	$z_0 \equiv$	
case 1	1	1	1	(mod ω)
case 2	0	1	1	(mod ω)
case 3	1	0	1	(mod ω)
case 4	1	1	0	(mod ω)

Table 2

In case 1 the equation $x_0^4 - y_0^4 = z_0^2$ leads to the contradiction $1 - 1 \equiv 1 \pmod{\omega}$.

Note that if (x_0, y_0, z_0) is a nontrivial solution of the equation $x^4 - y^4 = z^2$, then (y_0, x_0, iz_0) is also a nontrivial solution of the equation. This observation reduces case 2 to case 3.

(3) In case 3 let $(x_1, \omega^r y_1, z_1)$ be a solution of the equation $x^4 - y^4 = z^2$, where $r \geq 1$, $x_1 \equiv y_1 \equiv z_1 \equiv 1 \pmod{\omega}$ and x_1, y_1, z_1 are pairwise relatively primes. We will show that $z_1 \equiv 1 \pmod{\omega^2}$.

In order to prove this claim write z_1 in the form $z_1 = k\omega^2 + l$, $k, l \in Z[i]$ and compute z_1^2.

$$z_1^2 = k^2\omega^4 + 2k\omega^2 l + l^2.$$

From this it follows that $z_1^2 \equiv l^2 \pmod{\omega^4}$ Since the elements 0, 1, i, $1+i$ form a complete set of representatives modulo ω^2 and since $z_1 \equiv 1 \pmod{\omega}$ we may choose l to be 1 or i. Consequently, z_1^2 is congruent to 1 or -1 modulo ω^4. The equation $x_1^4 - \omega^{4r}y_1^4 = z_1^2$ gives that $1 \equiv z_1^2 \pmod{\omega^4}$ and so $z_1 \equiv 1 \pmod{\omega^2}$.

(4) In case 3 let $(x_1, \omega^r y_1, z_1)$ be a solution of the equation $x^4 - y^4 = z^2$, where $r \geq 1$, $x_1 \equiv y_1 \equiv z_1 \equiv 1 \pmod{\omega}$ and x_1, y_1, z_1 are pairwise relatively primes. We will show that there are pairwise relatively prime elements x_2, y_2, z_2 of $Z[i]$ such that $x_2 \equiv y_2 \equiv z_2 \equiv 1 \pmod{\omega}$ and $(x_2, \omega^{r-1}y_2, z_2)$ is a solution of the equation $x^4 - y^4 = z^2$.

In order to verify the claim write the equation $x_1^4 - \omega^{4r}y_1^4 = z_1^2$ in the form $\omega^{4r}y_1^4 = (x_1^2 - z_1)(x_1^2 + z_1)$ and compute the greatest common divisor of $(x_1^2 - z_1)$ and $(x_1^2 + z_1)$. Let g be this greatest common divisor. As $g | \omega^{4r}y_1^4$ it follows that $g \neq 0$. $g | (x_1^2 - z_1)$, $g | (x_1^2 + z_1)$ implies that $g | 2x_1^2$, $g | 2z_1$ If q is a prime divisor of g with $q \not| \omega$, then we get $q | x_1$, $q | z_1$. But we know that this is not the case as x_1 and z_1 are relatively primes. Thus $g = \omega^s$ and $0 \leq s \leq 2$ since $g | 2$. By step (3) $z_1 \equiv 1 \pmod{\omega^2}$. This together with $x_1^2 \equiv 1 \pmod{\omega^2}$ gives that $(x_1^2 - z_1) \equiv 0 \pmod{\omega^2}$, $(x_1^2 + z_1) \equiv 0 \pmod{\omega^2}$. Therefore $g = \omega^2$. The unique factorization property in $Z[i]$ gives that there are relatively prime elements $a, b \in Z[i]$ such that

$$x_1^2 - z_1 = \omega^2 a, \qquad x_1^2 + z_1 = \omega^2 b.$$

Let $a = \omega^u a_1$, $b = \omega^v b_1$. So $\omega^{4r}y_1^4 = \omega^{u+v+4}a_1 b_1$. By the unique factorization property in $Z[i]$ there are elements a_2, b_2 and a unit ε in $Z[i]$ for which

$$x_1^2 - z_1 = \omega^{u+2}\varepsilon a_2^4, \qquad x_1^2 + z_1 = \omega^{v+2}\varepsilon^{-1}b_2^4,$$

$$4r = u + v + 4, \qquad a_2^4 b_2^4 = y_1^4.$$

Here a_2, b_2 are prime to ω. It follows that $a_2 \equiv b_2 \equiv 1 \pmod{\omega}$. By addition we get

$$2x_1^2 = \omega^{v+2}\varepsilon^{-1}b_2^4 + \omega^{u+2}\varepsilon a_2^4.$$

After dividing by ω^2 it gives

$$\mu x_1^2 = \omega^v \varepsilon^{-1}b_2^4 + \omega^u \varepsilon a_2^4,$$

where $\mu = -i$. We distinguish two cases depending on either $u = 0$, $v = 4r - 4$ or $v = 0$, $u = 4r - 4$. When $u = 0$, $v = 4r - 4$ we get

$$-ix_1^2 = \omega^{4r-4}\varepsilon^{-1}b_2^4 + \varepsilon a_2^4.$$

If $4r - 4 = 0$, then this reduces to

$$-i \equiv \varepsilon^{-1} + \varepsilon \pmod{\omega^2}.$$

But this is not possible as $\varepsilon^{-1} + \varepsilon \equiv 0 \pmod{\omega^2}$. The computation is summarized in Table 3.

Thus $4r - 4 \neq 0$. Now

$$-i \equiv \varepsilon \pmod{\omega^2}.$$

From this it follows that $\varepsilon = \pm i$. By multiplying by $-\varepsilon$ we get

$$(i\varepsilon)x_1^2 = \omega^{4r-4}(-\varepsilon^{-1}\varepsilon)b_2^4 + (-\varepsilon^2)a_2^4.$$

Note that $i\varepsilon$ is a square of an element of $Z[i]$, say $i\varepsilon = \sigma^2$. Thus $(a_2, \omega^{r-1}b_2, \sigma x_1)$, $t \geq 2$ is a nontrivial solution of the equation $x^4 - y^4 = z^2$.

When $v = 0$, $u = 4r - 4$ we get

$$-ix_1^2 = \varepsilon^{-1}b_2^4 + \omega^{4r-4}\varepsilon a_2^4.$$

ε	ε^{-1}	$\varepsilon^{-1}+\varepsilon$
1	1	2
i	$-i$	0
-1	-1	-2
$-i$	i	0

TABLE 3

If $4r-4=0$, then this reduces to

$$-i \equiv \varepsilon^{-1}+\varepsilon \pmod{\omega^2}.$$

But this is not possible as $\varepsilon^{-1}+\varepsilon \equiv 0 \pmod{\omega^2}$. Thus $4r-4 \neq 0$. Now

$$-i \equiv \varepsilon \pmod{\omega^2}.$$

From this it follows that $\varepsilon = \pm i$. By multiplying by ε^{-1} we get

$$(-i\varepsilon^{-1})x_1^2 = (\varepsilon^{-2})b_2^4 + \omega^{4r-4}(\varepsilon^{-1}\varepsilon)a_2^4.$$

Note that $-i\varepsilon^{-1}$ is a square of an element of $Z[i]$, say $-i\varepsilon^{-1}=\sigma^2$. Thus

$$(\omega^{r-1}a_2, b_2, \sigma x_1), \qquad r \geq 2$$

is a nontrivial solution of the equation $x^4-y^4=z^2$.

(5) In case 4 let $(x_1, y_1, \omega^s z_1)$ be a solution of the equation $x^4-y^4=z^2$, where $s \geq 1$, $x_1 \equiv y_1 \equiv z_1 \equiv 1 \pmod{\omega}$ and x_1, y_1, z_1 are pairwise relatively primes. We will show that there are pairwise relatively prime elements x_2, y_2, z_2 of $Z[i]$ such that $x_2 \equiv y_2 \equiv z_2 \equiv 1 \pmod{\omega}$ and either $(\omega^{s-2}x_2, y_2, z_2)$ or $(x_2, \omega^{s-2}y_2, z_2)$ is a solution of the equation $x^4-y^4=z^2$.

In order to verify the claim write the equation $x_1^4-y_1^4=\omega^{2s}z_1^2$ in the form $\omega^{2s}z_1^2=(x_1^2-y_1^2)(x_1^2+y_1^2)$ and compute the greatest common divisor of $(x_1^2-y_1^2)$ and $(x_1^2+y_1^2)$. Let g be this greatest common divisor. As $g|\omega^{2s}z_1^2$ it follows that $g \neq 0$. $g|(x_1^2-y_1^2)$, $g|(x_1^2+y_1^2)$ implies that $g|2x_1^2$, $g|2y_1^2$. If q is a prime divisor of g with $q \not| \omega$, then we get $q|x_1$, $q|y_1$. But we know that this is not the case as x_1 and y_1 are relatively primes. Thus $g=\omega^s$ and $0 \leq s \leq 2$ since $g|2$. As $(x_1^2-y_1^2) \equiv 0 \pmod{\omega^2}$, $(x_1^2+y_1^2) \equiv 0 \pmod{\omega^2}$. It follows that $g=\omega^2$. The unique factorization property in $Z[i]$ gives that there are relatively prime elements $a, b \in Z[i]$ such that

$$x_1^2-y_1^2=\omega^2 a, \qquad x_1^2+y_1^2=\omega^2 b.$$

Let $a=\omega^u a_1$, $b=\omega^v b_1$. So $\omega^{2s}z_1^2=\omega^{u+v+4}a_1b_1$. By the unique factorization property in $Z[i]$ there are elements a_2, b_2 and a unit ε in $Z[i]$ for which

$$x_1^2-y_1^2=\omega^{u+2}\varepsilon a_2^2, \qquad x_1^2+y_1^2=\omega^{v+2}\varepsilon^{-1}b_2^2,$$
$$2s=u+v+4, \qquad a_2^2b_2^2=z_1^2.$$

Here a_2, b_2 are prime to ω. It follows that $a_2 \equiv b_2 \equiv 1 \pmod{\omega}$. By addition and subtraction we get

$$2x_1^2=\omega^{v+2}\varepsilon^{-1}b_2^2+\omega^{u+2}\varepsilon a_2^2,$$
$$2y_1^2=\omega^{v+2}\varepsilon^{-1}b_2^2-\omega^{u+2}\varepsilon a_2^2.$$

After dividing by ω^2 it gives

$$\mu x_1^2=\omega^{v}\varepsilon^{-1}b_2^2+\omega^{u}\varepsilon a_2^2,$$
$$\mu y_1^2=\omega^{v}\varepsilon^{-1}b_2^2-\omega^{u}\varepsilon a_2^2,$$

where $\mu = -i$. By multiplying the two equations together and multiplying by ε^2 we get

$$\mu^2\varepsilon^2x_1^2y_1^2 = \omega^{2v}b_2^4 - \omega^{2u}\varepsilon^4a_2^4.$$

We distinguish two cases depending on either $u = 0$, $v = 2s-4$ or $v = 0$, $u = 2s-4$. When $u = 0$, $v = 2s-4$ we get

$$\mu^2\varepsilon^2x_1^2y_1^2 = \omega^{4s-8}b_2^4 - \varepsilon^4a_2^4.$$

Thus $(\omega^{s-2}b_2, \varepsilon a_2, \mu\varepsilon x_1y_1)$, is a nontrivial solution of the equation $x^4 - y^4 = z^2$.

When $v = 0$, $u = 2s-4$ we get

$$\mu^2\varepsilon^2x_1^2y_1^2 = b_2^4 - \omega^{4s-8}\varepsilon^4a_2^4.$$

Thus $(b_2, \omega^{s-2}\varepsilon a_2, \mu\varepsilon x_1y_1)$, is a nontrivial solution of the equation $x^4 - y^4 = z^2$.

(6) Let (x_0, y_0, z_0) be a nontrivial solution of the equation $x^4 - y^4 = z^2$ in $Z[i]$. Either $y_0 \equiv 0 \pmod{\omega}$ or $z_0 \equiv 0 \pmod{\omega}$. In other words there is a solution $(x_1, \omega^r y_1, z_1)$ or $(x_1, y_1, \omega^s z_1)$ with $x_1, y_1, z_1 \equiv 1 \pmod{\omega}$, $r, s \geq 1$. By step (5) the second case reduces to the first one. In the first case choose a solution for which r is minimal. According to step (4) there is a solution $(x_2, \omega^{r-1}y_2, z_2)$, where $x_2, y_2, z_2 \equiv 1 \pmod{\omega}$, $r \geq 2$. This contradicts the choice of r and so completes the proof. $\square$

3. The equation in $Q(\sqrt{-2})$

Let $\omega = \sqrt{-2}$. The ring of integers of $Q(\sqrt{-2})$ is $Z[\omega] = \{u + v\omega : u, v \in Z\}$ and $Z[\omega]$ is a unique factorization domain. The units in $Z[\omega]$ are -1, 1. The prime factorization of 2 is $2 = (-1)\omega^2$.

Theorem 2. *The equation $x^4 - y^4 = z^2$ has only trivial solutions in $Z[\sqrt{-2}]$.*

Proof. We divide the proof into (7) steps many of them similar to the corresponding steps in the proof of Theorem 1.

(1) If (x_0, y_0, z_0) is a nontrivial solution of the equation $x^4 - y^4 = z^2$, then we may assume that x_0, y_0, z_0 are pairwise relatively primes.

(2) Let (x_0, y_0, z_0) be a nontrivial solution of the equation $x^4 - y^4 = z^2$ in $Z[\omega]$ such that x_0, y_0, z_0 are pairwise relatively primes. We face with four cases listed in Table 2.

In case 1 the equation $x_0^4 - y_0^4 = z_0^2$ gives the contradiction $1 - 1 \equiv 1 \pmod{\omega}$.

Next we show that case 2 is not possible either. From the equation $x_0^4 - y_0^4 = z_0^2$ it follows that $-1 \equiv z_0 \pmod{\omega^4}$. Writing z_0 in the form $z_0 = k\omega^2 + l$, $k, l \in Z[\omega]$ and computing z_0^2

$$z_0^2 = k^2\omega^4 + 2k\omega^2 l + l^2$$

we can see that $z_0^2 \equiv l^2 \pmod{\omega^4}$. Note that 0, 1, ω, $1 + \omega$ is a complete set of representatives modulo ω^2 and $z_0 \equiv 1 \pmod{\omega}$ we can choose l to be either 1 or $1 + \omega$. These lead to the following contradictions

$$-1 \equiv 1 \pmod{\omega^4},$$

$$-1 \equiv (1 + \omega)^2 \equiv -1 + 2\omega \pmod{\omega^4}$$

respectively.

(3) In case 3 let $(x_1, \omega^r y_1, z_1)$ be a solution of the equation $x^4 - y^4 = z^2$, where $r \geq 1$, $x_1 \equiv y_1 \equiv z_1 \equiv 1 \pmod{\omega}$ and x_1, y_1, z_1 are pairwise relatively primes. We will show that $z_1 \equiv 1 \pmod{\omega^2}$.

The equation $x_1^4 - \omega^{4r}y_1^4 = z_1^2$ gives that $1 \equiv z_1^2 \pmod{\omega^4}$ and so $z_1 \equiv 1 \pmod{\omega^2}$. From step (2) we know that if z_1 is in the form $z_1 = k\omega^2 + l$, $k, l \in Z[\omega]$, then $z_1^2 \equiv l^2 \pmod{\omega^4}$ and we may choose l to be 1 or $1 + \omega$. Since the second choice leads to the contradiction $1 \equiv (1 + \omega)^2 \equiv -1 + 2\omega \pmod{\omega^4}$ we left with the $l = 1$ possibility and so $z_1 \equiv 1 \pmod{\omega^2}$.

(4) In case 3 let $(x_1, \omega^r y_1, z_1)$ be a solution of the equation $x^4 - y^4 = z^2$, where $r \geq 1$, $x_1 \equiv y_1 \equiv z_1 \equiv 1 \pmod{\omega}$ and x_1, y_1, z_1 are pairwise relatively primes. We will show that there are pairwise relatively prime elements x_2, y_2, z_2 of $Z[\omega]$ such that $x_2 \equiv y_2 \equiv z_2 \equiv 1 \pmod{\omega}$ and $(x_2, \omega^{r-1} y_2, z_2)$ is a solution of the equation $x^4 + y^4 = z^2$.

A similar argument we used in the proof of Theorem 1 gives that from $x_1^4 - \omega^{4r} y_1^4 = z_1^2$ it follows that

$$\mu x_1^2 = \omega^v \varepsilon^{-1} b_2^4 + \omega^u \varepsilon a_2^4,$$

where $\mu = -1$. We distinguish two cases depending on either $u = 0$, $v = 4r - 4$ or $v = 0$, $u = 4r - 4$. When $u = 0$, $v = 4r - 4$ we get

$$-x_1^2 = \omega^{4r-4} \varepsilon^{-1} b_2^4 + \varepsilon a_2^4.$$

If $4r - 4 = 0$, then this reduces to

$$-1 \equiv \varepsilon^{-1} + \varepsilon \pmod{\omega^2}.$$

But this is not possible as $\varepsilon^{-1} + \varepsilon \equiv 0 \pmod{\omega^2}$. Thus $4r - 4 \neq 0$. Now

$$x_1^2 = \omega^{4r-4} b_2^4 + a_2^4$$

or

$$-x_1^2 = \omega^{4r-4} b_2^4 + a_2^4$$

depending on $\varepsilon = -1$ or $\varepsilon = 1$. The second alternative is impossible modulo ω^4 and so $(a_2, \omega^{r-1} b_2, x_1)$, $r \geq 2$ is a nontrivial solution of the equation $x^4 + y^4 = z^2$ in $Z[\omega]$.

When $v = 0$, $u = 4r - 4$ we get

$$-x_1^2 = \varepsilon^{-1} b_2^4 + \omega^{4r-4} \varepsilon a_2^4.$$

If $4r - 4 = 0$, then this reduces to

$$-1 \equiv \varepsilon^{-1} + \varepsilon \pmod{\omega^2}.$$

But clearly this is not the case.

Thus $4r - 4 \neq 0$. Now

$$x_1^2 = b_2^4 + \omega^{4r-4} a_2^4$$

or

$$-x_1^2 = b_2^4 + \omega^{4r-4} a_2^4$$

depending on $\varepsilon = -1$ or $\varepsilon = 1$. The second alternative is impossible modulo ω^4 and so $(b_2, \omega^{r-1} a_2, x_1)$, $r \geq 2$ is a nontrivial solution of the equation $x^4 + y^4 = z^2$ in $Z[\omega]$.

(5) If $(x_1, \omega^r y_1, z_1)$ is a solution of the equation $x^4 + y^4 = z^2$, where $r \geq 1$, $x_1 \equiv y_1 \equiv z_1 \equiv 1 \pmod{\omega}$ and x_1, y_1, z_1 are pairwise relatively primes, then there are pairwise relatively prime elements x_2, y_2, z_2 of $Z[\omega]$ such that $x_2 \equiv y_2 \equiv z_2 \equiv 1 \pmod{\omega}$ and $(x_2, \omega^{r-1} y_2, z_2)$ is a solution of the equation $x^4 - y^4 = z^2$.

From the equation $\omega^{4r} y_1^4 = (z_1 - x_1^2)(z_1 + x_1^2)$ by the standard argument it follows that

$$-x_1^2 = \omega^v \varepsilon^{-1} b_2^4 - \omega^u \varepsilon a_2^4.$$

We distinguish two cases according to $u = 0$, $v = 4r - 4$ or $v = 0$, $u = 4r - 4$. When $u = 0$, $v = 4r - 4$ we have

$$-x_1^2 = \omega^{4r-4} \varepsilon^{-1} b_2^4 - \varepsilon a_2^4.$$

If $4r - 4 = 0$, then $-1 \equiv \varepsilon^{-1} - \varepsilon \pmod{\omega^2}$ follows which is not possible so $4r - 4 \neq 0$. Now

$$x_1^2 = \omega^{4r-4} b_2^4 - a_2^4 \quad \text{or} \quad x_1^2 = -\omega^{4r-4} b_2^4 + a_2^4$$

depending on $\varepsilon = -1$ or $\varepsilon = 1$. In the first case $(\omega^{r-1}b_2, a_2, x_1)$ is a solution of $x^4 - y^4 = z^2$ which is not possible modulo ω^4. In the second case $(a_2, \omega^{r-1}b_2, x_1)$ is a solution of $x^4 - y^4 = z^2$.

Let us turn to the $v = 0$, $u = 4r - 4$ case when we have

$$-x_1^2 = \varepsilon^{-1}b_2^4 - \omega^{4r-4}\varepsilon a_2^4.$$

The $4r - 4 = 0$ subcase leads to the $-1 \equiv \varepsilon^{-1} - \varepsilon \pmod{\omega^2}$ contradiction and so $4r - 4 \neq 0$. Now

$$x_1^2 = b_2^4 - \omega^{4r-4}a_2^4 \quad \text{or} \quad x_1^2 = -b_2^4 + \omega^{4r-4}a_2^4$$

depending on $\varepsilon = -1$ or $\varepsilon = 1$. In the first case $(b_2, \omega^{r-1}a_2, x_1)$ is a solution of $x^4 - y^4 = z^2$. In the second case $(\omega^{r-1}a_2, b_2, x_1)$ is a solution of $x^4 - y^4 = z^2$ which is not possible modulo ω^4.

(6) In case 4 let $(x_1, y_1, \omega^s z_1)$ be a solution of the equation $x^4 - y^4 = z^2$, where $s \geq 1$, $x_1 \equiv y_1 \equiv z_1 \equiv 1 \pmod{\omega}$ and x_1, y_1, z_1 are pairwise relatively primes. It follows that there are pairwise relatively prime elements x_2, y_2, z_2 of $Z[\omega]$ such that $x_2 \equiv y_2 \equiv z_2 \equiv 1 \pmod{\omega}$ and either $(\omega^{s-2}x_2, y_2, z_2)$ or $(x_2, \omega^{s-2}y_2, z_2)$ is a solution of the equation $x^4 - y^4 = z^2$.

The proof of this claim can follow the same lines as step 5 in the proof of Theorem 1.

(7) Let (x_0, y_0, z_0) be a nontrivial solution of the equation $x^4 - y^4 = z^2$ in $Z[\omega]$. Either $y_0 \equiv 0 \pmod{\omega}$ or $z_0 \equiv 0 \pmod{\omega}$. It means that there is a solution in one of the forms $(x_1, \omega^r y_1, z_1)$ or $(x_1, y_1, \omega^s z_1)$, where $r, s \geq 1$, $x_1 \equiv y_1 \equiv z_1 \equiv 1 \pmod{\omega}$ and x_1, y_1, z_1 are pairwise relatively primes. By step (6) the second case reduces to the first one. In the first case choose a solution for which r is minimal. By step (4) this leads to a solution $(x_2, \omega^{r-1}y_2, z_2)$, $r \geq 2$ of the equation $x^4 + y^4 = z^2$. By step (5) there is a solution $(x_2, \omega^{r-2}y_2, z_2)$, $r \geq 2$ of the equation $x^4 - y^4 = z^2$. This contradicts the minimality of r and so completes the proof. □

4. The equation in $Q(\sqrt{2})$

Let $\omega = \sqrt{2}$. The ring of integers of $Q(\sqrt{-2})$ is $Z[\omega] = \{u + v\omega : u, v \in Z\}$ and $Z[\omega]$ is a unique factorization domain. The units in $Z[\omega]$ are $\pm\eta^n$, where $\eta = 1 + \omega$ and $n \in Z$. The prime factorization of 2 is $2 = \omega^2$. Setting $\eta^n = a_n + b_n\omega$, $\eta^{-n} = A_n + B_n\omega$ we can see that a_n, b_n, A_n, B_n can be computed using the formulas

$$\begin{aligned} a_0 &= 1, & b_0 &= 0, \\ a_n &= a_{n-1} + 2b_{n-1}, & b_n &= a_{n-1} + b_{n-1}, \\ A_0 &= 1, & B_0 &= 0, \\ A_n &= -A_{n-1} + 2B_{n-1}, & B_n &= A_{n-1} - B_{n-1}. \end{aligned}$$

The sequences η^{-n}, η^n are periodic modulo ω^2 and the length of the period is 4. It follows that $\varepsilon + \varepsilon^{-1} \equiv 0 \pmod{\omega^2}$ for each unit of $Z[\omega]$ and if $\varepsilon \equiv 1 \pmod{\omega^2}$, then $\varepsilon = \eta^{2n}$ or $\varepsilon = -\eta^{2n}$ for some $n \in Z$.

Theorem 3. *The equation $x^4 - y^4 = z^2$ has only trivial solutions in $Z[\sqrt{2}]$.*

Proof. We divide the proof into (7) steps many of them similar to the corresponding steps in the proof of Theorem 2.

(1) If (x_0, y_0, z_0) is a nontrivial solution of the equation $x^4 - y^4 = z^2$, then we may assume that x_0, y_0, z_0 are pairwise relatively primes.

(2) Let (x_0, y_0, z_0) be a nontrivial solution of the equation $x^4 - y^4 = z^2$ in $Z[\omega]$ such that x_0, y_0, z_0 are pairwise relatively primes. We face with four cases listed in Table 2.

In case 1 the equation $x_0^4 - y_0^4 = z_0^2$ gives the contradiction $1 - 1 \equiv 1 \pmod{\omega}$.

We claim that case 2 is not possible either. From the equation $x_0^4 - y_0^4 = z_0^2$ it follows that $-1 \equiv z_0 \pmod{\omega^4}$. Writing z_0 in the form $z_0 = k\omega^2 + l$, $k, l \in Z[\omega]$ and computing z_0^2

$$z_0^2 = k^2\omega^4 + 2k\omega^2 l + l^2$$

we can see that $z_0^2 \equiv l^2 \pmod{\omega^4}$. Note that 0, 1, ω, $1+\omega$ is a complete set of representatives modulo ω^2 and $z_0 \equiv 1 \pmod{\omega}$ we can choose l to be either 1 or $1+\omega$. These lead to the following contradictions

$$-1 \equiv 1 \pmod{\omega^4},$$

$$-1 \equiv (1+\omega)^2 \equiv 3 + 2\omega \pmod{\omega^4}$$

respectively.

(3) In case 3 let $(x_1, \omega^r y_1, z_1)$ be a solution of the equation $x^4 - y^4 = z^2$, where $r \geq 1$, $x_1 \equiv y_1 \equiv z_1 \equiv 1 \pmod{\omega}$ and x_1, y_1, z_1 are pairwise relatively primes. We will show that $z_1 \equiv 1 \pmod{\omega^2}$.

The equation $x_1^4 - \omega^{4r} y_1^4 = z_1^2$ gives that $1 \equiv z_1^2 \pmod{\omega^4}$ and so $z_1 \equiv 1 \pmod{\omega^2}$. From step (2) we know that if z_1 is in the form $z_1 = k\omega^2 + l$, $k, l \in Z[\omega]$, then $z_1^2 \equiv l^2 \pmod{\omega^4}$ and we may choose l to be 1 or $1+\omega$. Since the second choice leads to the contradiction $1 \equiv (1+\omega)^2 \equiv 3 + 2\omega \pmod{\omega^4}$ we left with the $l = 1$ possibility and so $z_1 \equiv 1 \pmod{\omega^2}$.

(4) In case 3 let $(x_1, \omega^r y_1, z_1)$ be a solution of the equation $x^4 - y^4 = z^2$, where $r \geq 1$, $x_1 \equiv y_1 \equiv z_1 \equiv 1 \pmod{\omega}$ and x_1, y_1, z_1 are pairwise relatively primes. We will show that there are pairwise relatively prime elements x_2, y_2, z_2 of $Z[\omega]$ such that $x_2 \equiv y_2 \equiv z_2 \equiv 1 \pmod{\omega}$ and $(x_2, \omega^{r-1} y_2, z_2)$ is a solution of the equation $x^4 + y^4 = z^2$.

A similar argument we used in the proof of Theorem 1 gives that from $x_1^4 - \omega^{4r} y_1^4 = z_1^2$ it follows that

$$\mu x_1^2 = \omega^v \varepsilon^{-1} b_2^4 + \omega^u \varepsilon a_2^4,$$

where $\mu = 1$. We distinguish two cases depending on either $u = 0$, $v = 4r - 4$ or $v = 0$, $u = 4r - 4$. When $u = 0$, $v = 4r - 4$ we get

$$x_1^2 = \omega^{4r-4} \varepsilon^{-1} b_2^4 + \varepsilon a_2^4.$$

If $4r - 4 = 0$, then this reduces to

$$1 \equiv \varepsilon^{-1} + \varepsilon \pmod{\omega^2}.$$

But this is not possible as $\varepsilon^{-1} + \varepsilon \equiv 0 \pmod{\omega^2}$. Thus $4r - 4 \neq 0$. Now

$$1 \equiv \varepsilon \pmod{\omega^2}$$

and so $\varepsilon = \eta^{2n}$ or $\varepsilon = -\eta^{2n}$. In the first case

$$x_1^2 = \omega^{4r-4} \eta^{-2n} b_2^4 + \eta^{2n} a_2^4.$$

Multiplying by η^{2n} we get

$$\eta^{2n} x_1^2 = \omega^{4r-4} b_2^4 + \eta^{4n} a_2^4.$$

Therefore $(\eta^n a_2, \omega^{r-1} b_2, \eta^n x_1)$ is a solution of the equation $x^4 - y^4 = z^2$ and $r \geq 2$. In the second case we get

$$x_1^2 = \omega^{4r-4}(-\eta^{-2n}) b_2^4 + (-\eta^{2n}) a_2^4.$$

Then

$$-\eta^{2n} x_1^2 = \omega^{4r-4} b_2^4 + \eta^{4n} a_2^4.$$

Hence $(\eta^n a_2, \omega^{r-1} b_2, \eta^n x_1)$ is a solution of the equation $x^4 - y^4 = -z^2$ and $r \geq 2$. But this is impossible modulo ω^4.

When $v = 0$, $u = 4r - 4$ we get

$$x_1^2 = \varepsilon^{-1} b_2^4 + \omega^{4r-4} \varepsilon a_2^4.$$

If $4r-4=0$, then this reduces to

$$1 \equiv \varepsilon^{-1} + \varepsilon \pmod{\omega^2}$$

which is not the case. Thus $4r-4 \neq 0$. Now

$$1 \equiv \varepsilon^{-1} \pmod{\omega^2}$$

and so $\varepsilon = \eta^{2n}$ or $\varepsilon = -\eta^{2n}$. In the first case

$$x_1^2 = \omega^{4r-4}\eta^{-2n}b_2^4 + \eta^{2n}a_2^4.$$

Multiplying by η^{2n} we get

$$\eta^{2n}x_1^2 = \omega^{4r-4}b_2^4 + \eta^{4n}a_2^4.$$

Therefore $(\eta^n a_2, \omega^{r-1}b_2, \eta^n x_1)$ is a solution of the equation $x^4 - y^4 = z^2$ and $r \geq 2$. In the second case we get

$$x_1^2 = \omega^{4r-4}(-\eta^{-2n})b_2^4 + (-\eta^{2n})a_2^4.$$

Then

$$-\eta^{2n}x_1^2 = \omega^{4r-4}b_2^4 + \eta^{4n}a_2^4.$$

Hence $(\eta^n a_2, \omega^{r-1}b_2, \eta^n x_1)$ is a solution of the equation $x^4 - y^4 = -z^2$ and $r \geq 2$. But this is impossible modulo ω^4.

(5) If $(x_1, \omega^r y_1, z_1)$ is a solution of the equation $x^4 + y^4 = z^2$, where $r \geq 1$, $x_1 \equiv y_1 \equiv z_1 \equiv 1 \pmod{\omega}$ and x_1, y_1, z_1 are pairwise relatively primes, then there are pairwise relatively prime elements x_2, y_2, z_2 of $Z[\omega]$ such that $x_2 \equiv y_2 \equiv z_2 \equiv 1 \pmod{\omega}$ and $(x_2, \omega^{r-1}y_2, z_2)$ is a solution of the equation $x^4 - y^4 = z^2$.

From the equation $\omega^{4r}y_1^4 = (z_1 - x_1^2)(z_1 + x_1^2)$ in the known way we can deduce

$$x_1^2 = \omega^v \varepsilon^{-1} b_2^4 - \omega^u \varepsilon a_2^4$$

and in the usual way we distinguish two cases depending on either $u=0$, $v=4r-4$ or $v=0$, $u=4r-4$. In the $u=0$, $v=4r-4$ case

$$x_1^2 = \omega^{4r-4}\varepsilon^{-1}b_2^4 - \varepsilon a_2^4.$$

If $4r-4=0$ we get the $1 \equiv \varepsilon^{-1} - \varepsilon \pmod{\omega^2}$ contradiction. Thus $4r-4 \neq 0$ and we get $1 \equiv -\varepsilon \pmod{\omega^2}$ which in turn implies that $\varepsilon = \eta^{2n}$ or $\varepsilon = -\eta^{2n}$. In the first subcase

$$\eta^{2n}x_1^2 = \omega^{4r-4}b_2^4 - \eta^{4n}a_2^4$$

shows that $(\omega^{r-1}b_2, \eta^n a_2, \eta^n x_1)$ is a solution of the equation $x^4 - y^4 = z^2$. This is impossible modulo ω^4 as $r \geq 2$. In the second subcase

$$\eta^{2n}x_1^2 = -\omega^{4r-4}b_2^4 + \eta^{4n}a_2^4$$

shows that $(\eta^n a_2, \omega^{r-1}b_2, \eta^n x_1)$ is a solution of the equation $x^4 - y^4 = z^2$.

Let us turn to the $v=0$, $u=4r-4$ case. Now

$$x_1^2 = \varepsilon^{-1}b_2^4 - \omega^{4r-4}\varepsilon a_2^4.$$

If $4r-4=0$ we get the $1 \equiv \varepsilon^{-1} - \varepsilon \pmod{\omega^2}$ contradiction and so $4r-4 \neq 0$. Consequently we get $1 \equiv \varepsilon^{-1} \pmod{\omega^2}$ which gives that $\varepsilon = \eta^{2n}$ or $\varepsilon = -\eta^{2n}$. In the first subcase

$$\eta^{2n}x_1^2 = b_2^4 - \omega^{4r-4}\eta^{4n}a_2^4$$

shows that $(b_2, \omega^{r-1}\eta^n a_2, \eta^n x_1)$ is a solution of the equation $x^4 - y^4 = z^2$ and $r \geq 2$.

This is impossible modulo ω^4 as $r \geq 2$. In the second subcase

$$\eta^{2n}x_1^2 = -b_2^4 + \omega^{4r-4}\eta^{4n}a_2^4$$

shows that $(\omega^{r-1}\eta^n a_2, b_2, \eta^n x_1)$ is a solution of the equation $x^4 - y^4 = z^2$. But this is impossible modulo ω^4 as $r \geq 2$.

(6) In case 4 let $(x_1, y_1, \omega^s z_1)$ be a solution of the equation $x^4 - y^4 = z^2$, where $s \geq 1$, $x_1 \equiv y_1 \equiv z_1 \equiv 1 \pmod{\omega}$ and x_1, y_1, z_1 are pairwise relatively primes.

It follows that there are pairwise relatively prime elements x_2, y_2, z_2 of $Z[\omega]$ such that $x_2 \equiv y_2 \equiv z_2 \equiv 1 \pmod{\omega}$ and either $(\omega^{s-2}x_2, y_2, z_2)$ or $(x_2, \omega^{s-2}y_2, z_2)$ is a solution of the equation $x^4 - y^4 = z^2$.

The proof of this claim can follow the same lines as step 5 in the proof of Theorem 1.

(7) Let (x_0, y_0, z_0) be a nontrivial solution of the equation $x^4 - y^4 = z^2$ in $Z[\omega]$. Either $y_0 \equiv 0 \pmod{\omega}$ or $z_0 \equiv 0 \pmod{\omega}$. It means that there is a solution in one of the forms $(x_1, \omega^r y_1, z_1)$ or $(x_1, y_1, \omega^s z_1)$, where $r, s \geq 1$, $x_1 \equiv y_1 \equiv z_1 \equiv 1 \pmod{\omega}$ and x_1, y_1, z_1 are pairwise relatively primes. By step (6) the second case reduces to the first one. In the second case choose a solution for which r is minimal. By step (4) this leads to a solution $(x_2, \omega^{r-1}y_2, z_2)$, $r \geq 2$ of the equation $x^4 + y^4 = z^2$. By step (5) there is a solution $(x_2, \omega^{r-2}y_2, z_2)$, $r \geq 2$ of the equation $x^4 - y^4 = z^2$. This contradicts the minimality of r and so completes the proof. $\square$

References

[1] J. T. Cross. In the Gaussian integers, $\alpha^4 + \beta^4 \neq \gamma^4$. *Math. Mag.*, 66(2):105–108, 1993.

[2] L. J. Mordell. *Diophantine equations.* Pure and Applied Mathematics, Vol. 30. Academic Press, London, 1969.

[3] T. Nagell. *Introduction to Number Theory.* John Wiley & Sons Inc., New York, 1951.

Received September 05, 2003.

Department of Mathematics,
University of Bahrain,
P.O. Box 32038
State of Bahrain
E-mail address: sszabo7@hotmail.com