Article ID: 1000-5641(2009)05-0138-04

Solutions to some Diophantine equations over $\mathbf{Q}(\sqrt{-3})$

WANG Yong-liang

(*Department of Mathematics, Heze University, Heze* 274015, *China*)

Abstract: By using Fermat's method of descent, this paper proved that Diophantine equations $x^4 - y^4 = z^2$ and $x^4 + 4y^4 = z^2$ have no non-trivial solutions over $\mathbf{Q}(\sqrt{-3})$, which implies that the Fermat Equation also has no non-trivial solutions in this field for $n = 4$.

Key words: Fermat's method of descent; ring of algebraic integers; imaginary quadratic fields

CLC number: O156 **Document code:** A

几个不定方程在$\mathbf{Q}(\sqrt{-3})$中的解

王永亮

(菏泽学院 数学系, 菏泽 274015)

摘要: 应用Fermat下降法，证明了不定方程 $x^4 - y^4 = z^2$ 与 $x^4 + 4y^4 = z^2$ 在$\mathbf{Q}(\sqrt{-3})$ 没有非平凡解, 它表明Fermat方程当 $n = 4$ 时在此域中仍然没有非平凡解.

关键词: Fermat下降法; 代数整数环; 虚二次域

0 Introduction

It is difficult to determine all solutions of a Diophantine equation in a ring of integers of a number field. Now people restrict their attention to the rings of algebraic integers of some quadratic fields, which are a little larger than the ring of rational integers. For example, from the Hilbert theorem 169[1], we know that $x^4 + y^4 = z^2$ has only solutions satisfying $xyz = 0$ in $\mathbf{Z}[\sqrt{-1}]$. Sándor Szabó [2] proved that in $\mathbf{Z}[\sqrt{-2}]$, $x^4 + y^4 = z^2$ has only solutions satisfying $xyz = 0$. In order to deal with a conjecture in the algebraic K-theory, Xu and Qin[3] found out all solutions of $x^4 + y^4 = (-1)^\sigma \omega_1^\mu z^2 (\sigma = 0, 1, \mu = 0, 1$ and $\omega_1 = \sqrt{-2})$ in $\mathbf{Z}[\sqrt{-2}]$. In [4], Xu and Wang discussed several Diophantine equations in rings of integers of some imaginary quadratic fields. In [5], Sándor Szabó investigated the Diophantine equation $x^4 - y^4 = z^2$ in three quadratic fields. However, because there exist third roots of unity in the ring of algebraic

收稿日期: 2008-09

基金项目: 菏泽学院科学基金(XY08SX01)

作者简介: 王永亮, 男, 硕士, 讲师, 研究方向为代数数论. E-mail:wyldxx@yahoo.cn.

integers of quadratic field $\mathbf{Q}(\sqrt{-3})$, the discussion is more difficult than that in the other rings. This note will discuss the special case.

In this note, we determine all solutions of $x^4-\varepsilon y^4=z^2$ in the ring of algebraic integers of $\mathbf{Q}(\sqrt{-3})$, where $\varepsilon=1,-4$, which also implies that the Fermat Equation $x^n+y^n=z^n$ has no non-trivial solutions in this ring when $n=4$. It is very interesting that the equation $x^4+y^4=z^2$ has non-trivial solutions in this ring, for example, $(\sqrt{-3},2,5)$ and $(7,20\sqrt{-3},1201)$. Noting that if the equation $x^4+y^4=z^2$ holds, then the equation $(x^4-y^4)^4+(2xyz)^4=(z^4+4x^4y^4)^2$ also holds. So we can obtain infinitely many solutions of $x^4+y^4=z^2$ in this ring.

1 Diophantine Equations in $\mathbf{Q}(\sqrt{-3})$

In this section, we denote by ω the third root of unity $\frac{-1+\sqrt{-3}}{2}$ and by ω_1 the another $\frac{-1-\sqrt{-3}}{2}$. So we have $\omega^3=\omega_1^3=1$, $\omega=\omega_1^2$ and $\omega_1=\omega^2$. According to algebraic number theory (see [6]), the ring of algebraic integers of $\mathbf{Q}(\sqrt{-3})$ is $\mathbf{Z}[\omega]$, and it is both a unique factorization domain and a valuation ring. In this ring, 2 is inertia, and it is a prime number itself. Also there are congruences as follows for $\forall\alpha\in\mathbf{Z}[\omega]$:

$$\alpha \equiv 0,1,\omega,1+\omega(\mathrm{mod}\ 2) \tag{1.1}$$

$$\alpha^2 \equiv 0,1,1+\omega,\omega(\mathrm{mod}\ 2) \tag{1.2}$$

$$\alpha^2 \equiv 0,1,3+3\omega,\omega(\mathrm{mod}\ 4) \tag{1.3}$$

$$-\alpha^2 \equiv 0,3,1+\omega,3\omega(\mathrm{mod}\ 4) \tag{1.4}$$

$$\alpha^4 \equiv 0,1,\omega,3+3\omega(\mathrm{mod}\ 4) \tag{1.5}$$

They can be checked out easily.

Theorem 1 There do not exist $x,y,z\in\mathbf{Z}[\omega]$ satisfying $x^4-y^4=z^2$ and $xyz\neq 0$.

Proof Suppose that there exist $x,y,z\in\mathbf{Z}[\omega]$ satisfying $x^4-y^4=z^2$ and $xyz\neq 0$. Obviously, we can suppose that they are pairwise relatively prime. We claim:

(I) 2 does not divide x. Otherwise, there must be $-y^4\equiv z^2(\mathtt{mod}\ 4)$. But from (1.5) and (1.2) we have $-y^4\equiv 0,3,3\omega,1+\omega(\mathrm{mod}\ 4)$ and $z^2\equiv 0,1,\omega,3+3\omega(\mathrm{mod}\ 4)$. Comparing them, we have $-y^4\equiv z^2\equiv 0(\mathtt{mod}\ 4)$ which contradicts the assumption of $(y,z)=1$.

(II) 2 divides either y or z. Otherwise, from (1.3) and (1.5) there must be $z^2+y^4\equiv 2,2\omega,2+2\omega,3\omega,1+\omega,3(\mathtt{mod}\ 4)$ and $x^4\equiv 1,3+3\omega,\omega(\mathrm{mod}\ 4)$. Comparing them, we see that $x^4\equiv z^2+y^4(\mathrm{mod}\ 4)$ does not hold, nor does $x^4-y^4=z^2$.

So there are two cases:

(1) If $2|y$, then 2 divides neither x nor z. From $x^4-y^4=z^2$, we have $4|x^4-z^2=(x^2+z)(x^2-z)$. Because 2 is prime, there must be 2 divides either x^2+z or x^2-z. So 2 divides both x^2+z and x^2-z since $x^2+z\equiv x^2-z(\mathrm{mod}\ 2)$. Thus it follows that

$$\frac{x^2+z}{2},\frac{x^2-z}{2}\in\mathbf{Z}[\omega]\quad \texttt{and}\quad (\frac{x^2+z}{2},\frac{x^2-z}{2})=1.$$

Changing $x^4-y^4=z^2$ into $\frac{x^2+z}{2}\cdot\frac{x^2-z}{2}=(\frac{y^2}{2})^2$, we get $x^2+z=2\epsilon a_1^2$, $x^2-z=2\epsilon^{-1}b_1^2$, $y^2=2a_1b_1$, where $a_1,b_1\in\mathbf{Z}[\omega],(a_1,b_1)=1$, and $\epsilon=1,\omega,\omega^{-1},-1,-\omega,-\omega^{-1}$. Note that there are only the six units in this ring. So it comes that

$$x^2 = \epsilon a_1^2 + \epsilon^{-1} b_1^2,\ y^2 = 2a_1b_1,\ z = \epsilon a_1^2 - \epsilon^{-1} b_1^2.$$

Since $y^2 = 2a_1b_1$ and $4|y^2$, we know that $2|a_1$ or $2|b_1$. Without loss of generality, suppose that 2 divides a_1 but not b_1, thus $4|a_1^2$. Consequently, we claim that $x^2 = \epsilon a_1^2 + \epsilon^{-1} b_1^2$ does not hold if $\epsilon = -1, -\omega, -\omega^{-1}$. Otherwise, from $x^2 = \epsilon a_1^2 + \epsilon^{-1} b_1^2$ and $2|a_1$, we have $x^2 \equiv -(\omega_1^i b_1)^2 (\bmod 4)$ with $i = 0, 1, -1$, so $4|x^2$ and $4|b_1^2$ in virtue of (1.3) and (1.4), which is a contradiction since $(x, b_1) = 1$. Thus using $\omega = \omega_1^2$, $\omega_1 = \omega^2$ and a simple substitution, we can suppose that

$$x^2 = a^2 + b^2,\ y^2 = 2ab,\ z = a^2 - b^2.$$

Changing $x^2 = a^2 + b^2$ into $\frac{x+b}{2} \cdot \frac{x-b}{2} = (\frac{a}{2})^2$, we have

$$x = \epsilon c^2 + \epsilon^{-1} d^2,\ a = 2cd,\ b = \epsilon c^2 - \epsilon^{-1} d^2,$$

where $c, d \in \mathbf{Z}[\omega], (c, d) = 1$ and $\epsilon = 1, \omega, \omega^{-1}, -1, -\omega, -\omega^{-1}$. (Noting that $\frac{x+b}{2}, \frac{x-b}{2} \in \mathbf{Z}[\omega]$ and $(\frac{x+b}{2}, \frac{x-b}{2}) = 1$ from $4|x^2 - b^2$ and $x + b \equiv x - b (\bmod 2)$.) It is obvious that $c, d, \epsilon c^2 - \epsilon^{-1} d^2$ are pairwise relatively prime. Putting $a = 2cd, b = \epsilon c^2 - \epsilon^{-1} d^2$ into $y = 2ab$, we get

$$y^2 = 4cd(\epsilon c^2 - \epsilon^{-1} d^2).$$

From $\omega = \omega_1^2$, $\omega_1 = \omega^2$ and the equation above, we conclude that $c, d, \epsilon c^2 - \epsilon^{-1} d^2$ are squares up to a sign. So choosing p, t, q properly, we have two cases:

$$c = \pm p^2,\ d = \pm t^2,\ \epsilon c^2 - \epsilon^{-1} d^2 = q^2 \quad \texttt{and} \quad c = \pm p^2,\ d = \pm t^2,\ \epsilon c^2 - \epsilon^{-1} d^2 = -q^2.$$

Case 1 Putting $c = \pm p^2$ and $d = \pm t^2$ into $\epsilon c^2 - \epsilon^{-1} d^2$, we have $\epsilon p^4 - \epsilon^{-1} t^4 = q^2$. If $\epsilon = 1, \omega,$ or ω^{-1}, then $p^4 - t^4 = q^2,\ \omega p^4 - \omega^{-1} t^4 = q^2$ or $\omega^{-1} p^4 - \omega t^4 = q^2$, that is,

$$p^4 - t^4 = q^2,\ (\omega p)^4 - (\omega^{-1} t)^4 = q^2 \ \texttt{or}\ (\omega^{-1} p)^4 - (\omega t)^4 = q^2.$$

Obviously, 2 does not divide q since 2 does not divide b. So according to claim II, 2 divides t. Thus, we find three solutions (p, t, q), $(\omega p, \omega^{-1} t, q)$ and $(\omega^{-1} p, \omega t, q)$, where p and t are factors of y. If we suppose that the valuation of y at the prime 2 is the least in the beginning, then Fermat's method of descent will lead to a contradiction.

If $\epsilon = -1,\ -\omega$ or $-\omega^{-1}$, then we have $t^4 - p^4 = q^2,\ \omega t^4 - \omega^{-1} p^4 = q^2$ or $\omega^{-1} t^4 - \omega p^4 = q^2$. As similar as the above, Fermat's method of descent will lead to a contradiction.

Case 2 As done in case 1.

(2) If $2|z$, then 2 divides neither x nor y. From $x^4 - y^4 = z^2$, we have $4|x^4 - y^4 = (x^2 + y^2)(x^2 - y^2)$. Because 2 is prime, there must be 2 divides either $x^2 + z$ or $x^2 - z$. So 2 divides both $x^2 + z$ and $x^2 - z$ since $x^2 + z \equiv x^2 + z (\bmod 2)$. Thus it follows that

$$\frac{x^2 + y^2}{2}, \frac{x^2 - y^2}{2} \in \mathbf{Z}[\omega] \quad \texttt{and} \quad (\frac{x^2 + y^2}{2}, \frac{x^2 - y^2}{2}) = 1.$$

As in (1), changing $x^4 - y^4 = z^2$ into $\frac{x^2+y^2}{2} \cdot \frac{x^2-y^2}{2} = (\frac{z}{2})^2$, we get

$$x^2 = \epsilon a^2 + \epsilon^{-1}b^2,\ y^2 = \epsilon a^2 - \epsilon^{-1}b^2,\ z = 2ab,$$

where $a, b \in \mathbf{Z}[\omega]$, $(a, b) = 1$, and $\epsilon = 1, \omega, \omega^{-1}, -1, -\omega$ or $-\omega^{-1}$.

Now multiplying $x^2 = \epsilon a^2 + \epsilon^{-1}b^2$ with $y^2 = \epsilon a^2 - \epsilon^{-1}b^2$, we have $(xy)^2 = \epsilon^2 a^4 - \epsilon^{-2}b^4$, that is, $(\epsilon xy)^2 = (\epsilon a)^4 - b^4$. So we return to (1) since 2 divides neither x nor y. By similar discussion, we know this equation has only trivial solutions. If $xy = 0$, the theorem obviously holds; if $a = 0$, or $b = 0$, we have that $z = 0$ since $z = 2ab$ in this case.

By (1) and (2), the proof is completed.

Corollary 1 There do not exist $x, y, z \in \mathbf{Z}[\omega]$ satisfying $x^4 + 4y^4 = z^2$ and $xyz \neq 0$.

Proof Suppose that there exist $x, y, z \in \mathbf{Z}[\omega]$ satisfying $x^4 + 4y^4 = z^2$ and $xyz \neq 0$. Obviously, we can suppose that they are pairwise relatively prime.

Changing $x^4 + 4y^4 = z^2$ into $z^4 - (2xy)^4 = (x^4 - 4y^4)^2$, we know that $(z, 2xy, x^4 - 4y^4)$ satisfies the equation $x^4 - y^4 = z^2$, which is in contradiction with theorem 1.

Corollary 2 In $\mathbf{Z}[\omega]$, the non-trivial relatively prime solutions of equation $x^4 + y^4 = 2z^2$ is merely $(\pm\epsilon, \pm\epsilon, \pm\epsilon^2)$, where $\epsilon = 1, \omega, \omega^{-1}, -1, -\omega, -\omega^{-1}$. And the equation $x^4 + y^4 = -2z^2$ has no relatively prime solutions.

Proof Suppose that there exist $x, y, z \in \mathbf{Z}[\omega]$ satisfying $x^4 + y^4 = \pm 2z^2$ and $xyz \neq 0$. Obviously, we can suppose that they are pairwise relatively prime.

Changing $x^4 + y^4 = \pm 2z^2$ into

$$(\frac{x^4 - y^4}{2})^2 = z^4 - (xy)^4,$$

we have that $xy = 0, z = 0$ or $x^4 - y^4 = 0$ according to theorem 1 (Note that $x^4 - y^4 \equiv x^4 + y^4 \equiv 0 (\mathrm{mod} 2)$). If $xy = 0$ or $z = 0$, the corollary is true; if $x^4 - y^4 = 0$, then $x = \pm\epsilon, y = \pm\epsilon$ since $(x, y) = 1$. By checking directly, we see that the Diophantine equation $x^4 + y^4 = z^2$ has only solutions $(\pm\epsilon, \pm\epsilon, \pm\epsilon^2)$, where $\epsilon = 1, \omega, \omega^{-1}, -1, -\omega, -\omega^{-1}$. And the equation $x^4 + y^4 = -2z^2$ has no relatively prime solutions. So the results are required.

Acknowledgements The author would show great thanks to reviewers for their helpful comments and suggestions.

[References]

[1] HILBERT D. The theory of Algebraic Number Fields[M]. New York: Springer-Verlag, 1998.

[2] SZABÓ S. The Diophantine equation $x^4+y^4 = z^2$ in $\mathbf{Q}(\sqrt{-2})$[J]. Indian J Pure Appl Math, 1999, 30(9): 857-861.

[3] XU K J, QIN H R. Some Diophantine equations over $\mathbf{Z}[i]$ and $\mathbf{Z}[\sqrt{-2}]$ with applications to K_2 of a field[J]. Communication in Algebra, 2002, 30: 353-367.

[4] XU K J, WANG Y L. Several Diophantine equations in some rings of integers of quadratic imaginary fields[J]. Algebra Colloquium, 2007, 14(4): 661-668.

[5] SZABÓ S. The Diophantine equation $x^4 - y^4 = z^2$ in three quadratic fields[J]. Acta Mathematica Academiae Paedagogicae Nyiregyháziensis, 2004, 20(1): 1-10.

[6] FENG K Q. Algebraic Number Theory[M]. Beijing: Science Press, 2001: 52-53, 219.