RESEARCH ARTICLE
doi: 10.2306/scienceasia1513-1874.2017.43.383

ScienceAsia 43 (2017): **383–386**

On some Diophantine equations over complex quadratic number fields

Malinee Chaiya[a], **Somjate Chaiya**[a], **Supawadee Prugsapitak**[b,*]

[a] Department of Mathematics, Faculty of Science, Silpakorn University, Nakhon Pathom 73000 Thailand
[b] Algebra and Applications Research Unit, Department of Mathematics and Statistics, Faculty of Science, Prince of Songkla University, Songkhla 90110 Thailand

[*]Corresponding author, e-mail: supawadee.p@psu.ac.th

Received 15 Jan 2017
Accepted 26 Oct 2017

ABSTRACT: In this paper, we establish a necessary and sufficient condition for two algebraic integers in complex quadratic number fields to be consecutive terms of generalized Fibonacci numbers. We use this result to obtain all solutions of the Diophantine equation $x^2-axy+by^2=c$ over Gaussian integers, where b and c are units in $\mathbb{Z}[\mathrm{i}]$ and $a\in\mathbb{Z}[\mathrm{i}]$ with $|a|^2\geqslant 10$.

KEYWORDS: Fibonacci numbers, second order recurrence, Gaussian integers

MSC2010: 11D09 11B37

INTRODUCTION

The second order recurrence $\{W_n(a,b;p,q)\}$ is defined by

$$W_0=a,\ W_1=b,\quad W_{n+1}=pW_n-qW_{n-1}$$

for $n\geqslant 1$ where a, b, p, q are arbitrary integers. The well-known Fibonacci and Lucas sequences are the sequences $\{W_n(0,1;1,-1)\}$ and $\{W_n(2,1;1,-1)\}$ and are denoted by $\{F_n\}$ and $\{L_n\}$, respectively. Here a generalized Fibonacci sequence means the sequence $\{W_n(0,1;p,q)\}$.

Lucas[1] proved that if x and y are consecutive Fibonacci numbers then

$$y^2-xy-x^2=\pm 1$$

and the converse was proved in Ref. 2. The same results were proved again by Jones[3] and he also concluded that the set of all Fibonacci numbers is identical to the set of positive numbers of the form

$$y(2-(y^2-yx-x^2)^2),$$

as the variables x and y range over the positive integers. Jones[4] proved similar results for a Lucas sequence. He showed that for any positive integer n,

$$L_{n+1}^2-L_{n+1}L_n-L_n^2=5(-1)^n$$

and if two positive integers x and y satisfy

$$y^2-yx-x^2=\pm 5$$

then x and y are two consecutive terms of a Lucas sequence.

Kiss[5] extended the results of Jones and proved that, for given integers p and q such that either $p>0$, $q=-1$ or $p>3$, $q=1$, two nonnegative integers x and y satisfy the equation

$$|x^2-pxy+qy^2|=1$$

if and only if x and y are consecutive terms of a sequence $\{W_n(0,1;p,q)\}$. A similar result was proved in Refs. 6–8 using different approaches. They proved that a pair of positive integers (x,y) is a solution of $y^2-pxy-x^2=\pm 1$ if and only if there exists a positive integer n such that $x=W_n(0,1;p,-1)$ and $y=W_{n+1}(0,1;p,-1)$. Furthermore McDaniel[6] established that for $p>2$, the pair of positive integers (x,y) with $x<y$ is a solution of $y^2-pxy+x^2=1$ if and only if there exists a positive integer n such that $x=W_{n-1}(0,1;p,1)$ and $y=W_n(0,1;p,1)$. The same result but with $p>3$ was proved in Refs. 7, 8.

Motivated by Kiss's result, we will extend his work to the ring of algebraic integers of any complex quadratic number field. Here we establish a sufficient and necessary condition for two algebraic integers in a complex quadratic number field to be consecutive terms of a generalized Fibonacci sequence. As a consequence of our result, we can determine whether an equation

$$x^2-axy+by^2=c$$

has solutions over $\mathbb{Z}[\mathrm{i}]$, when $a \in \mathbb{Z}[\mathrm{i}]$ with $|a|^2 \geqslant 10$ and $b, c \in \{\pm 1, \pm \mathrm{i}\}$. We also show that all solutions to this equation, if there are any, can be expressed in terms of two consecutive generalized Fibonacci numbers.

PRELIMINARY RESULTS

Let K be a complex quadratic number field. Thus $K = \mathbb{Q}(\sqrt{-d})$ for some square-free positive integer d. Let $\mathcal{O}_K$ be a ring of its algebraic integers and U_K be a group of units in K. Thus

(i) if $K = \mathbb{Q}(\sqrt{-1})$ then $\mathcal{O}_K = \mathbb{Z}[\mathrm{i}]$ and $U_K = \{\pm 1, \pm \mathrm{i}\}$;
(ii) if $K = \mathbb{Q}(\sqrt{-3})$ then $\mathcal{O}_K = \mathbb{Z}[\omega]$ and $U_K = \{\pm 1, \pm\omega, \pm\omega^2\}$ where $\omega = \frac{1}{2}(-1+\sqrt{-3})$;
(iii) if $K = \mathbb{Q}(\sqrt{-d})$ where $d \equiv 1,\ 2 \mod 4$ then $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ and $U_K = \{\pm 1\}$;
(iv) if $K = \mathbb{Q}(\sqrt{-d})$ where $d \equiv 3 \mod 4$ then $\mathcal{O}_K = \mathbb{Z}[\frac{1}{2}(-1+\sqrt{d})]$ and $U_K = \{\pm 1\}$.

Lemma 1 *Let K be a complex quadratic number field. Let β and α be elements in $\mathcal{O}_K$ such that $|\beta|^2 = 1$ and $|\alpha|^2 \geqslant 10$. If x and y are in $\mathcal{O}_K$, $|x|^2 > |y|^2 \geqslant 1$, and*

$$|x^2 - \alpha xy + \beta y^2|^2 = 1,$$

then $|\alpha y - x|^2 < |y|^2$.

Proof: Let $z = \beta^{-1}(\alpha y - x)$. We want to show that $|z|^2 < |y|^2$. Since $|x^2 - \alpha xy + \beta y^2|^2 = 1$, we have

$$x^2 - \alpha xy + \beta y^2 = x(-\beta z) + \beta y^2 = \epsilon,$$

for some unit ϵ in $\mathcal{O}_K$. This gives $z = (y^2 - \beta^{-1}\epsilon)/x$. Since $\beta^{-1}\epsilon$ is a unit, we have

$$|z|^2 = \frac{|y^2 - \beta^{-1}\epsilon|^2}{|x|^2} \leqslant \frac{(|y|^2+1)^2}{|x|^2}.$$

Let $|x|^2 = |y|^2 + k$ for some positive integer k. Then

$$|z|^2 \leqslant \frac{(|y|^2+1)^2}{|y|^2+k} = |y|^2 + \frac{1-(k-2)|y|^2}{|y|^2+k}. \quad (1)$$

If either $k \geqslant 4$ or $k = 3$ and $|y|^2 \geqslant 2$, then $(1-(k-2)|y|^2)/(|y|^2+k) < 0$, which implies $|z|^2 < |y|^2$ as needed. We now consider when $k = 3$ and $|y|^2 = 1$. From (1), we have $|z|^2 \leqslant |y|^2 = 1$. However, since $z = \beta^{-1}(\alpha y - x)$ and $|\alpha|^2 \geqslant 10$, we have

$$|z| \geqslant |\alpha y| - |x| \geqslant \sqrt{10} - 2 > 1,$$

a contradiction. Hence the case $k = 3$ and $|y|^2 = 1$ never happens.

It remains to consider when $k = 2$ and $k = 1$. Now let $k \in \{1, 2\}$. Then from (1) we obtain

$$|z|^2 \leqslant |y|^2 + 1. \quad (2)$$

Since $|x|^2 = |y|^2 + k$, $k \in \{1, 2\}$, and $|y|^2 \geqslant 1$, we have

$$|x| = |y|\sqrt{1 + \frac{k}{|y|^2}} \leqslant \sqrt{3}|y|.$$

Since $z = \beta^{-1}(\alpha y - x)$ and $|\alpha| \geqslant \sqrt{10}$,

$$|z| \geqslant |\alpha y| - |x| \geqslant |\alpha y| - \sqrt{3}|y| \geqslant \left(\sqrt{10} - \sqrt{3}\right)|y|.$$

This gives $|z|^2 > 2|y|^2 \geqslant |y|^2 + 1$ which contradicts (2). Hence these cases never happen. □

Let α be a non-zero element in $\mathcal{O}_K$ and β be a unit. From now on, we denote the sequence $\{W_n(0, 1; \alpha, \beta)\}$ by $\{U_n\}$ or $\{U_n(\alpha, \beta)\}$ if the values of α and β are needed in that context. We now prove that $|U_{n+1}^2 - \alpha U_{n+1}U_n + \beta U_n^2| = 1$.

Lemma 2 *For every nonnegative integer n, $|U_{n+1}^2 - \alpha U_{n+1}U_n + \beta U_n^2|^2 = 1$. Indeed,*

$$U_{n+1}^2 - \alpha U_{n+1}U_n + \beta U_n^2 = \beta^n.$$

Proof: Since $U_1^2 - \alpha U_1 U_0 + \beta U_0^2 = 1$, the lemma holds for $n = 0$. For some $n \geqslant 1$, assume that $U_n^2 - \alpha U_n U_{n-1} + \beta U_{n-1}^2 = \beta^{n-1}$. Then

$$\begin{aligned} &U_{n+1}^2 - \alpha U_{n+1}U_n + \beta U_n^2 \\ &\quad = (\alpha U_n - \beta U_{n-1})^2 - \alpha(\alpha U_n - \beta U_{n-1})U_n + \beta U_n^2 \\ &\quad = \beta(U_n^2 - \alpha U_n U_{n-1} + \beta U_{n-1}^2) \\ &\quad = \beta\beta^{n-1} \\ &\quad = \beta^n. \end{aligned}$$

□

MAIN THEOREM

Theorem 1 *Let K be a complex quadratic number field. Let α, β, x and y be algebraic integers such that $|\alpha|^2 \geqslant 10, |\beta|^2 = 1$ and $|x|^2 > |y|^2$. Then x and y satisfy the equation*

$$|x^2 - \alpha xy + \beta y^2|^2 = 1 \quad (3)$$

if and only if there exists a unit u and a positive integer m such that $x = uU_m(\alpha, \beta)$ and $y = uU_{m-1}(\alpha, \beta)$.

Proof: The necessary condition follows from Lemma 2. We prove the sufficient condition as follows. If $y = 0$, then $y = U_0$ and $x = uU_1$ for some unit u. The result holds in this case. Next assume

that $|y|^2 \geqslant 1$. Let $y_0 = x$ and $y_1 = y$ and define $y_n = \beta^{-1}(\alpha y_{n-1} - y_{n-2})$ for $n \geqslant 2$. First we will show that

$$|y_{n-1}^2 - \alpha y_{n-1} y_n + \beta y_n^2|^2 = 1$$

for all $n \geqslant 1$. By the hypothesis, we already have $|y_0^2 - \alpha y_0 y_1 + \beta y_1^2|^2 = 1$. For $n \geqslant 1$,

$$\begin{aligned} y_n^2 - \alpha y_n y_{n+1} + \beta y_{n+1}^2 &= y_n^2 - \alpha y_n(\alpha\beta^{-1} y_n - \beta^{-1} y_{n-1}) \\ &\quad + \beta(\alpha\beta^{-1} y_n - \beta^{-1} y_{n-1})^2 \\ &= y_n^2 - \alpha\beta^{-1} y_{n-1} y_n + \beta^{-1} y_{n-1}^2 \\ &= \beta^{-1}(y_{n-1}^2 - \alpha y_{n-1} y_n + \beta y_n^2). \end{aligned}$$

Since $|\beta^{-1}| = 1$, the result $|y_n^2 - \alpha y_n y_{n+1} + \beta y_{n+1}^2| = 1$ follows by induction.

As a consequence of Lemma 1, there exists a positive integer m such that $|y_m|^2 = 0$ and the sequence $\{|y_j|^2\}_{j=0}^m$ is a strictly decreasing sequence. For $0 \leqslant j \leqslant m$, let $Y_j = y_{m-j}$. Since $y_{n-2} = \alpha y_{n-1} - \beta y_n$ for $2 \leqslant n \leqslant m$, we have

$$Y_j = \alpha Y_{j-1} - \beta Y_{j-2} \tag{4}$$

for $2 \leqslant j \leqslant m$ with $Y_0 = y_m = 0$ and $Y_1 = y_{m-1}$. Since y_m and y_{m-1} satisfy (3), y_{m-1} must be a unit, say u. Since the sequence $\{Y_j\}_{j=0}^m$ satisfies a recurrence relation (4) with $Y_0 = 0$ and $Y_1 = u$, it is easy to see that $Y_j = uU_j$ for $0 \leqslant j \leqslant m$. Hence $x = y_0 = uU_m$ and $y = y_1 = uU_{m-1}$, as desired. □

Notice that the result of Kiss in Ref. 5 is a special case of our main result. Kiss gave an example in Ref. 5 that the condition $|\alpha|^2 \geqslant 10$ is necessary. For instance, if $\alpha = 3$ and $\beta = 1$ then $(x, y) = (2, 1)$ is a solution to (3), but 2 is not in the sequence $\{U_n\}$.

APPLICATIONS

In this section, we will use the results of our main theorem to determine whether the Diophantine equation

$$x^2 - \alpha x y + \beta y^2 = \epsilon \tag{5}$$

has solutions over $\mathbb{Z}[\mathrm{i}]$, where $\alpha, \beta, \epsilon \in \mathbb{Z}[\mathrm{i}]$ with $|\alpha|^2 \geqslant 10$ and $|\beta|^2 = 1 = |\epsilon|^2$. If its solutions exists, we will find all of its solutions. First notice that if (x, y) is a solution to (5), then $|x| \neq |y|$. To see this, suppose that $|x| = |y|$. Then $|x| \geqslant 1$ and because $|\alpha|^2 \geqslant 10$, we must have

$$\begin{aligned} 1 &= |x^2 - \alpha x y + \beta y^2| \\ &\geqslant |\alpha||x||y| - |x|^2 - |y|^2 \\ &= (|\alpha| - 2)|x|^2 \geqslant |\alpha| - 2 > 1, \end{aligned}$$

a contradiction. Hence if (x, y) is a solution, then $|x|^2 \neq |y|^2$. If $|x|^2 > |y|^2$, it follows from Theorem 1 that

$$(x, y) = u\big(U_{n+1}(\alpha, \beta), U_n(\alpha, \beta)\big)$$

for some unit u and some nonnegative integer n. For the case $|x|^2 < |y|^2$, (5) can be written as

$$y^2 - \alpha\beta^{-1} x y + \beta^{-1} x^2 = \epsilon\beta^{-1}.$$

Hence again by Theorem 1, the solution of (5) is of the form

$$(x, y) = u\big(U_n(\alpha\beta^{-1}, \beta^{-1}), U_{n+1}(\alpha\beta^{-1}, \beta^{-1})\big)$$

for some unit u and some nonnegative integer n. It is easy to see that (x, y) is a solution to (5) if and only if $(x\mathrm{i}, y\mathrm{i})$ is a solution to the equation

$$x^2 - \alpha x y + \beta y^2 = -\epsilon.$$

The previous paragraph gives us the idea of the forms of solutions to (5). It leads us to the answer about the existence of the solutions. As a consequence of Lemma 2, we have that

$$U_{n+1}^2 - \alpha U_{n+1} U_n + \beta U_n^2 = \epsilon$$

if and only if $\beta^n = \epsilon$. This give a necessary and sufficient condition for (5) to have solutions over $\mathbb{Z}[\mathrm{i}]$.

Theorem 2 *Let α, β and ϵ be Gaussian integers such that $|\alpha|^2 \geqslant 10$ and $|\beta|^2 = 1 = |\epsilon|^2$. The equation*

$$x^2 - \alpha x y + \beta y^2 = \epsilon$$

has a solution over $\mathbb{Z}[\mathrm{i}]$ if and only if either $\beta^n = \epsilon$ or $\beta^n = -\epsilon$ for some nonnegative integer n. Furthermore, all solutions are given by

$$(x, y) = \begin{cases} \pm\big(U_{n+1}(\alpha, \beta), U_n(\alpha, \beta)\big), & \beta^n = \epsilon, \\ \pm\mathrm{i}\big(U_{n+1}(\alpha, \beta), U_n(\alpha, \beta)\big), & \beta^n = -\epsilon, \\ \pm\big(U_n(\alpha\beta^{-1}, \beta^{-1}), & \\ \quad U_{n+1}(\alpha\beta^{-1}, \beta^{-1})\big), & \beta^{1-n} = \epsilon, \\ \pm\mathrm{i}\big(U_n(\alpha\beta^{-1}, \beta^{-1}), & \\ \quad U_{n+1}(\alpha\beta^{-1}, \beta^{-1})\big), & \beta^{1-n} = -\epsilon, \end{cases}$$

with $n \geqslant 0$.

The following is an immediate consequence of Theorem 2.

Corollary 1 *For any Gaussian integer α with $|\alpha|^2 \geqslant 10$, the equations*

$$x^2 - \alpha x y + y^2 = \pm\mathrm{i}, \quad x^2 - \alpha x y - y^2 = \pm\mathrm{i}$$

have no solutions over $\mathbb{Z}[\mathrm{i}]$.

We end this section with some explicit examples of the solutions to (5). First consider the equation

$$x^2 - \alpha xy + y^2 = 1. \tag{6}$$

Here $\beta = 1$ and $\epsilon = 1$, so $\beta^n = \epsilon$ for all nonnegative integers n. Hence all solutions of (6) over $\mathbb{Z}[\mathrm{i}]$ are given by

$$(x, y) = \pm\big(U_{n+1}(\alpha, 1), U_n(\alpha, 1)\big), \\ \pm\big(U_n(\alpha, 1), U_{n+1}(\alpha, 1)\big)$$

for all nonnegative integers n.

Next consider the equation

$$x^2 - \alpha xy + y^2 = -1. \tag{7}$$

In this case $\beta = 1$ and $\epsilon = -1$. It is clear that $\beta^n \neq \epsilon$ for any integer n, but $\beta^n = -\epsilon$ for all nonnegative integers n. Thus all solutions of (7) over $\mathbb{Z}[\mathrm{i}]$ are given by

$$(x, y) = \pm\mathrm{i}\big(U_{n+1}(\alpha, 1), U_n(\alpha, 1)\big), \\ \pm\mathrm{i}\big(U_n(\alpha, 1), U_{n+1}(\alpha, 1)\big)$$

with $n \geqslant 0$.

We next solve the equation

$$x^2 - \alpha xy - y^2 = 1. \tag{8}$$

Since here $\beta = -1$ and $\epsilon = 1$, $\beta^n = \epsilon$ and $\beta^{1-n} = -\epsilon$ when n is even. Furthermore, $\beta^n = -\epsilon$ and $\beta^{1-n} = \epsilon$ if n is odd. Hence the solutions to (8) over $\mathbb{Z}[\mathrm{i}]$ are given by $(x, y) = \pm(U_{2n+1}(\alpha, -1), U_{2n}(\alpha, -1))$, $\pm\mathrm{i}(U_{2n+2}(\alpha, -1), U_{2n+1}(\alpha, -1))$, $\pm(U_{2n+1}(-\alpha, -1), U_{2n+2}(-\alpha, -1))$, $\pm\mathrm{i}(U_{2n}(-\alpha, -1), U_{2n+1}(-\alpha, -1))$, with $n \geqslant 0$.

For the last example, let us consider the equation

$$x^2 - \alpha xy + \mathrm{i}y^2 = 1. \tag{9}$$

In this case $\beta = \mathrm{i}$ and $\epsilon = 1$. So we have

$$\beta^n = \begin{cases} \epsilon, & n \equiv 0 \mod 4, \\ -\epsilon, & n \equiv 2 \mod 4, \end{cases}$$

$$\beta^{1-n} = \begin{cases} \epsilon, & n \equiv 1 \mod 4, \\ -\epsilon, & n \equiv 3 \mod 4. \end{cases}$$

Hence the solutions to (9) over $\mathbb{Z}[\mathrm{i}]$ are given by $(x, y) = \pm(U_{4n+1}(\alpha, \mathrm{i}), U_{4n}(\alpha, \mathrm{i}))$, $\pm\mathrm{i}(U_{4n+3}(\alpha, \mathrm{i}), U_{4n+2}(\alpha, \mathrm{i}))$, $\pm(U_{4n+1}(-\alpha\mathrm{i}, -\mathrm{i}), U_{4n+2}(-\alpha\mathrm{i}, -\mathrm{i}))$, $\pm\mathrm{i}(U_{4n+3}(-\alpha\mathrm{i}, -\mathrm{i}), U_{4n+4}(-\alpha\mathrm{i}, -\mathrm{i}))$, with $n \geqslant 0$.

REFERENCES

1. Lucas E (1876) Sur l'emploi calcul symbolique, dans la théorie des séries récurrentes *Nouv Corresp Math* **2**, 201–6.
2. Wasteels MJ (1902) Quelques propriétés des nombres de Fibonacci. *Mathesis, troisième série, tome II*, 60–2.
3. Jones JP (1975) Diophantine representations of the Fibonacci numbers. *Fibonacci Quart* **13**, 84–8.
4. Jones JP (1976) Diophantine representations of the Lucas numbers. *Fibonacci Quart* **14**, 134.
5. Kiss P (1979) Diophantine representations of generalized Fibonacci numbers. *Elem Math* **34**, 129–32.
6. McDaniel WL (1995) Diophantine representation of Lucas sequence. *Fibonacci Quart* **33**, 59–63.
7. Keskin R (2010) Solutions of some quadratic Diophantine equations. *Comput Math Appl* **60**, 2225–30.
8. Keskin R, Demirturk B (2013) Solutions of some Diophantine equations using generalized Fibonacci and Lucas sequences. *Ars Combinatoria* **111**, 161–79.