TOKYO J. MATH.
VOL. 2, No. 1, 1979

A Note on the Pell Equation

Hideo WADA

Sophia University

For solving the Pell equation $|x^2-my^2|=1$, we usually use the continued fraction expansion of $\sqrt{m}$. We will give here a new geometrical interpretation of the continued fraction expansion, and apply it to solve the Pell equation. Theorem 1 makes the continued fraction expansion of $\sqrt{m}$ more meaningful. Theorem 2 gives the existence of the solution. The proof is simpler and shorter than the usual one.

§1. Let m be a positive integer which is not a square. Then the Pell equation

$$(1)\qquad |x^2-my^2|=1\ , \quad (x, y\in \boldsymbol{Z})$$

can be written as

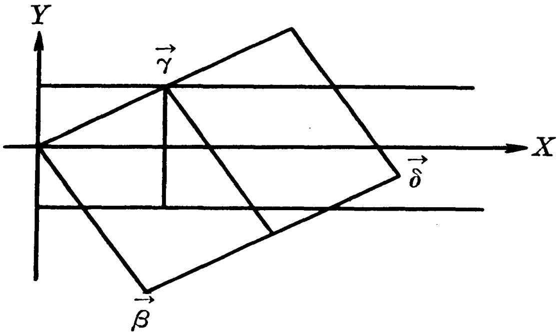
$$(2)\qquad |(x+\sqrt{m}y)(x-\sqrt{m}y)|=1\ .$$

Put $\alpha=x+\sqrt{m}y$, $\alpha'=x-\sqrt{m}y=$ the conjugate of α. Then (2) can be written as $|\alpha\alpha'|=1$. Put $\alpha_0=1$, $\alpha_{-1}=\sqrt{m}$, $L=\{x\alpha_0+y\alpha_{-1}\,|\,x, y\in \boldsymbol{Z}\}=\{x+\sqrt{m}y\,|\,x, y\in\boldsymbol{Z}\}$, and in the X-Y plane, $\vec{\alpha}_0=(1, 1)$, $\vec{\alpha}_{-1}=(\sqrt{m}, -\sqrt{m})$, $\vec{L}=\{x\vec{\alpha}_0+y\vec{\alpha}_{-1}\,|\,x, y\in\boldsymbol{Z}\}=\{(x+\sqrt{m}y, x-\sqrt{m}y)\,|\,x, y\in\boldsymbol{Z}\}=\{(\alpha, \alpha')\,|\,\alpha\in L\}$.

LEMMA 1. *Let $\vec{\beta}=(\beta, \beta')$, $\vec{\gamma}=(\gamma, \gamma')$ be generators of $\vec{L}$ such that $0<\beta$, $0<\gamma$, $\beta'\gamma'<0$, $|\gamma'|<|\beta'|$. Then the smallest number $\delta\in L$ such that $\gamma<\delta$, $|\delta'|<|\gamma'|$ is $\beta+[-\beta'/\gamma']\gamma$, ($[-\beta'/\gamma']$ means the integer part of $-\beta'/\gamma'$). In this case, $\vec{\gamma}$, $\vec{\delta}=(\delta, \delta')$ are generators of $\vec{L}$ such that $0<\gamma$, $0<\delta$, $\gamma'\delta'<0$, $|\delta'|<|\gamma'|$.*

PROOF. We may assume $0<\gamma'<-\beta'$ without any loss of generality. Put $\delta=x\gamma+y\beta$. If $x\leqq 0$ and $y\leqq 0$, then $\delta\leqq 0$. If $x>0$ and $y\leqq 0$, then $\delta'=x\gamma'+y\beta'\geqq\gamma'$. Therefore y must be greater than zero. When $y\geqq 1$, then from the condition $|\delta'|<|\gamma'|$, we have $-\gamma'<x\gamma'+y\beta'<\gamma'$ and $-\gamma'-y\beta'<x\gamma'<\gamma'-y\beta'$. Hence $-1-\beta'/\gamma'\leqq -1-y\beta'/\gamma'<x<1-y\beta'/\gamma'$. From

Received March 3, 1978



the smallestness of δ, we get $y=1$, $x=[-\beta'/\gamma']$. From $\beta=\delta+[-\beta'/\gamma']\gamma$, we get that $\vec{\gamma}$, $\vec{\delta}=(\delta, \delta')$ are generators of $\vec{L}$, and $\gamma'\delta'=\gamma'(\beta'+[-\beta'/\gamma']\gamma')<\gamma'\{\beta'+(-\beta'/\gamma')\gamma'\}=0$.

§2. We want to find positive integers x, y which satisfy (1). Let x_1, y_1 and x_2, y_2 be the positive integer solutions of (1), namely $|x_1^2-my_1^2|=1$, $|x_2^2-my_2^2|=1$, $(0<x_1, y_1, x_2, y_2)$. If $x_1<x_2$, then $my_1^2\leqq x_1^2+1<(x_1+1)^2-1\leqq x_2^2-1\leqq my_2^2$. If $y_1<y_2$, then $x_1^2\leqq my_1^2+1<m(y_1+1)^2-1\leqq my_2^2-1\leqq x_2^2$. Therefore $x_1<x_2 \Leftrightarrow y_1<y_2 \Leftrightarrow x_1+\sqrt{m}\,y_1<x_2+\sqrt{m}\,y_2$. Using Lemma 1, we can calculate the smallest number $\alpha=x+\sqrt{m}\,y$ such that $0<x$, $0<y$, and $|\alpha\alpha'|=1$ as follows.

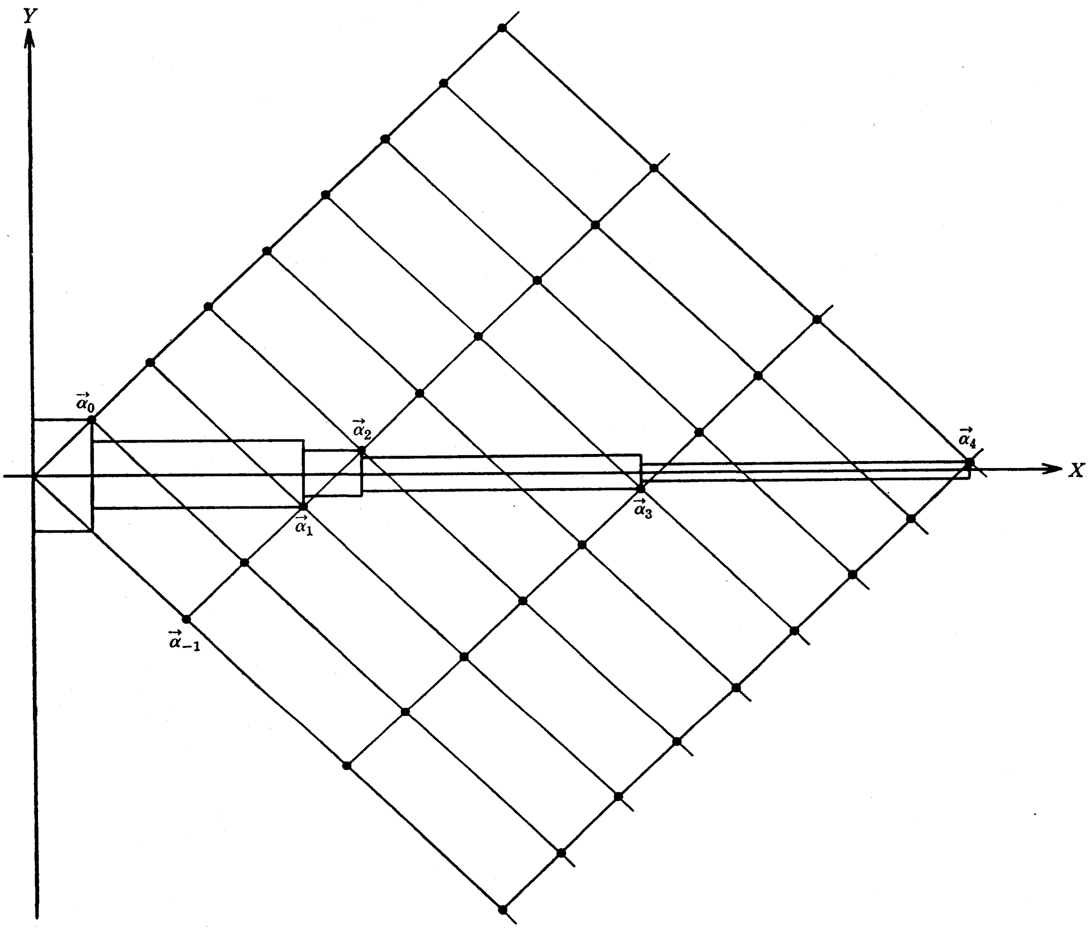
Let $\alpha=x+\sqrt{m}\,y$ be the smallest number such that $0<x$, $0<y$, $|\alpha\alpha'|=1$. Then $1<\alpha$ and $|\alpha'|=1/\alpha<1$. The two points $\vec{\alpha}_{-1}=(\sqrt{m}, -\sqrt{m})$, $\vec{\alpha}_0=(1, 1)$ satisfy the condition of Lemma 1. Therefore the smallest number $\alpha_1\in L$ such that $1=\alpha_0<\alpha_1$, $|\alpha_1'|<|\alpha_0'|=1$ is $\alpha_{-1}+[-\alpha_{-1}'/\alpha_0']\alpha_0=\sqrt{m}+[\sqrt{m}]$. If $|\alpha_1\alpha_1'|=1$, then $\alpha=\alpha_1$. If $|\alpha_1\alpha_1'|>1$, then α must be greater than α_1, and $|\alpha'|=1/\alpha<1/\alpha_1=|\alpha_1'|/|\alpha_1\alpha_1'|<|\alpha_1'|$. From Lemma 1, the two vectors $\vec{\alpha}_0$, $\vec{\alpha}_1=(\alpha_1, \alpha_1')$ satisfy the condition of Lemma 1. Therefore the smallest number $\alpha_2\in L$ such that $\alpha_1<\alpha_2$, $|\alpha_2'|<|\alpha_1'|$ is $\alpha_0+[-\alpha_0'/\alpha_1']\alpha_1$. In general, put $\alpha_{i+1}=\alpha_{i-1}+[-\alpha_{i-1}'/\alpha_i']\alpha_i$. Then this infinite sequence $\{\alpha_i\}$ has the properties: $1=\alpha_0<\alpha_1<\alpha_2<\cdots$, $|\alpha_{-1}'|>|\alpha_0'|>|\alpha_1'|>|\alpha_2'|>\cdots$, and $|\alpha_i'|=(-1)^i\alpha_i'$. If there exists a solution α, then α must be one of α_i. Put $\beta_i=-\alpha_{i-1}'/\alpha_i'$, and $k_i=[\beta_i]$. Then $\beta_0=-(-\sqrt{m})/1=\sqrt{m}$, and

$$\alpha_{i+1}=\alpha_{i-1}+k_i\alpha_i \tag{3}$$

$$\beta_{i+1}=-\alpha_i'/\alpha_{i+1}'=-\alpha_i'/(\alpha_{i-1}'+k_i\alpha_i')=1/(\beta_i-k_i)\,. \tag{4}$$

From (4), we get $\beta_i=k_i+1/\beta_{i+1}$. Therefore we have the continued fraction expansion of $\sqrt{m}$.

$$\sqrt{m}=\beta_0=k_0+1/\beta_1=k_0+\frac{1}{k_1+}\cdots+\frac{1}{k_{n-1}+}\frac{1}{\beta_n}\,.$$



§3. We will give an example. When $m=7$, then

$$\alpha_{-1}=\sqrt{7},\ \alpha_0=1,\ \beta_0=\sqrt{7}=2.6\cdots,$$
$$\alpha_1=\alpha_{-1}+2\alpha_0=\sqrt{7}+2,\ \beta_1=1/(\sqrt{7}-2)=(\sqrt{7}+2)/3=1.5\cdots,$$
$$\alpha_2=\alpha_0+1\alpha_1=\sqrt{7}+3,\ \beta_2=1/\{(\sqrt{7}+2)/3-1\}=(\sqrt{7}+1)/2=1.8\cdots,$$
$$\alpha_3=\alpha_1+1\alpha_2=2\sqrt{7}+5,\ \beta_3=1/\{(\sqrt{7}+1)/2-1\}=(\sqrt{7}+1)/3=1.2\cdots,$$
$$\alpha_4=\alpha_2+1\alpha_3=3\sqrt{7}+8,\ \beta_4=1/\{(\sqrt{7}+1)/3-1\}=(\sqrt{7}+2)/1.$$

In the next section, we will prove that the denominator of β_i is $|\alpha_i\alpha_i'|$. In this example, the dominator of β_4 is one. Therefore $|\alpha_4\alpha_4'|=1$. As a result, the smallest solution of $|x^2-7y^2|=1$ is $x=8,\ y=3$.

§4. **Lemma 2.** *$\alpha_i\alpha_{i-1}'=(-1)^{i-1}(\sqrt{m}+a_i)$ for some $a_i\in \mathbf{Z}$.*

Proof. When $i=0$, then $\alpha_0\alpha_{-1}'=-\sqrt{m}=(-1)^{-1}(\sqrt{m}+0)$, $(a_0=0)$. When $\alpha_i\alpha_{i-1}'=(-1)^{i-1}(\sqrt{m}+a_i)$, then we get $a_i'\alpha_{i-1}=(-1)^{i-1}(-\sqrt{m}+a_i)=(-1)^i(\sqrt{m}-a_i)$ by taking the conjugate. Hence $\alpha_{i+1}\alpha_i'=(\alpha_{i-1}+k_i\alpha_i)\alpha_i'=\alpha_{i-1}\alpha_i'+k_i\alpha_i\alpha_i'=(-1)^i(\sqrt{m}-a_i+(-1)^ik_i\alpha_i\alpha_i')$.

THEOREM 1. *Put* $\alpha_{-1}=\sqrt{m}$, $\alpha_0=1$, $\alpha_{i+1}=\alpha_{i-1}+[-\alpha'_{i-1}/\alpha'_i]\alpha_i$. *Then* $-\alpha'_{i-1}/\alpha'_i=(\sqrt{m}+a_i)/|\alpha_i\alpha'_i|$ *for some* $a_i\in\boldsymbol{Z}$.

PROOF.
$$\begin{aligned}-\alpha'_{i-1}/\alpha'_i&=-\alpha_i\alpha'_{i-1}/(\alpha_i\alpha'_i)\\&=(-1)^i(\sqrt{m}+a_i)/\{(-1)^i|\alpha_i\alpha'_i|\}\\&=(\sqrt{m}+a_i)/|\alpha_i\alpha'_i|\ .\end{aligned}$$

§5. LEMMA 3. $0\leqq a_i<\sqrt{m}$, $|\alpha_i\alpha'_i|<2\sqrt{m}$, $(i\geqq 0)$.

PROOF. $1<-\alpha'_{i-1}/\alpha'_i=(\sqrt{m}+a_i)/|\alpha_i\alpha'_i|$

$$\therefore\quad \alpha_{i-1}/\alpha_i=(\alpha'_{i-1}/\alpha'_i)'=(\sqrt{m}-a_i)/|\alpha_i\alpha'_i|\ .$$

When $i=0$, then $a_0=0$, $|\alpha_0\alpha'_0|=1$. When $i>0$, then $0<\alpha_{i-1}<\alpha_i$.

$$\therefore\quad 0<\alpha_{i-1}/\alpha_i=(\sqrt{m}-a_i)/|\alpha_i\alpha'_i|<1<-\alpha'_{i-1}/\alpha'_i=(\sqrt{m}+a_i)/|\alpha_i\alpha'_i|$$

$$\therefore\quad 0<a_i<\sqrt{m},\ |\alpha_i\alpha'_i|<\sqrt{m}+a_i<2\sqrt{m}\ .$$

THEOREM 2 (Existence of the solution). *Put* $\alpha_{-1}=\sqrt{m}$, $\alpha_0=1$, $\alpha_{i+1}=\alpha_{i-1}+[-\alpha'_{i-1}/\alpha'_i]\alpha_i$. *Then there exists* $i\geqq 1$ *such that* $|\alpha_i\alpha'_i|=1$.

PROOF.
$$\begin{aligned}\alpha_{i+1}/\alpha_i&=\alpha_{i+1}\alpha'_i/(\alpha_i\alpha'_i)=(-1)^i(\sqrt{m}+a_{i+1})/\{(-1)^i|\alpha_i\alpha'_i|\}\\&=(\sqrt{m}+a_{i+1})/|\alpha_i\alpha'_i|\ .\end{aligned}$$

Using Lemma 3, it can be seen the set $\{\alpha_{i+1}/\alpha_i\,|\,i\geqq 0\}$ is a finite set. Consequently, there must exist a certain pair i, j such that $0\leqq i<j$, $\alpha_{i+1}/\alpha_i=\alpha_{j+1}/\alpha_j$. Let i be the smallest integer which satisfies the above condition. Dividing both sides of (3) by α_i, we get $\alpha_{i+1}/\alpha_i=\alpha_{i-1}/\alpha_i+k_i$. If $i>0$, then $0<\alpha_{i-1}/\alpha_i<1$. Therefore $k_i=[\alpha_{i+1}/\alpha_i]$ and

$$\begin{aligned}\alpha_i/\alpha_{i-1}&=\alpha_i/(\alpha_{i+1}-k_i\alpha_i)=1/(\alpha_{i+1}/\alpha_i-[\alpha_{i+1}/\alpha_i])\\&=1/(\alpha_{j+1}/\alpha_j-[\alpha_{j+1}/\alpha_j])=\alpha_j/\alpha_{j-1}\ .\end{aligned}$$

This contradicts the assumption that i is the smallest. Thus we get $i=0$, hence for such j we get $|\alpha_j\alpha'_j|=|\alpha_0\alpha'_0|=1$, jth α_j is a solution of the Pell equation $|x^2-my^2|=1$.

References

[1] O. PERRON, Die Lehre von den Kettenbrüchen, Teubner, 1954 (Chelsea, 1950).

[2] T. TAKAGI, Lectures on the Elementary Theory of Numbers, Kyoritsu Shuppan, Tokyo, 1931 (in Japanese).

Present Address:
DEPARTMENT OF MATHEMATICS
SOPHIA UNIVERSITY
KIOICHO, CHIYODA-KU, TOKYO 102