Ming, L.
Osaka J. Math.
28 (1991), 747–750

AN ELEMENTARY PROOF OF A THEOREM OF BREMNER

LUO MING

(Received May 7, 1990)

In the paper [1] Bremner proved that the Diophantine equation

$$3x^4-4y^4-2x^2+12y^2-9=0 \tag{1}$$

has only two positive integer solutions $(x, y)=(1, 1)$ and $(3, 3)$, which was suggested by Enomoto, Ito and Noda in their research on tight 4-desings (see [2]). However, he used some of results of Cassels in biquadratic field $\boldsymbol{R}(\sqrt[4]{3})$ and the $\mathfrak{p}$-adic method of Skolem, so his proof is somewhat difficult. In 1983, Ko Chao and Sun Qi indicated that an elementary proof of Bremner's theorem would be significant (see [3]). Now such an elementary proof is given in this paper with nothing deeper than quadratic recipricity used. We describe our method as follows.

Since (1) may be reduced to $(3x^2-1)^2-3(2y^2-3)^2=1$, we have $(3x^2-1)+(2y^2-3)\sqrt{3}=u_n+v_n\sqrt{3}=(2+\sqrt{3})^n$, the latter equation denotes the general solution of the Pell's equation $U^2-3V^2=1$, n is an integer. Thus

$$2y^2=v_n+3\,. \tag{2}$$

First we assume $n=3m$. By

$$u_{3m}+v_{3m}\sqrt{3}=(u_m+v_m\sqrt{3})^3=(u_m^3+9u_m v_m^2)+(3u_m^2 v_m+3v_m^3)\sqrt{3},$$

we get

$$v_{3m}=3v_m(u_m^2+v_m^2)=3v_m(4v_m^2+1)\,,$$

so that

$$2y^2=3(4v_m^3+v_m)+3\,,$$

which leads to

$$6y_1^2=4v_m^3+v_m+1=(2v_m+1)(2v_m^2-v_m+1)\,,$$

where $y=3y_1$, $y_1>0$. Since $(2v_m+1, 2v_m^2-v_m+1)=1$ and $2\nmid(2v_m+1)$, $3\nmid(2v_m^2-v_m+1)$ we have

$$2y_2^2 = 2v_m^2 - v_m + 1\,, \quad y_2 \mid y_1\,, \quad y_2 > 0\,.$$

Thus

$$(4y_2)^2 = (4v_m - 1)^2 + 7\,,$$
$$(4y_2 + 4v_m - 1)(4y_2 - 4v_m + 1) = 7\,,$$
$$4y_2 \pm 4v_m \mp 1 = 7\,, \quad 4y_2 \mp 4v_m \pm 1 = 1\,,$$

which gives $y_2=1$, $v_m=1$. Hence $m=1$, $n=3$. That is, if $3\mid n$ then (2) holds only when $n=3$, this case gives $(x, y)=(3, 3)$, a positive integer solution of (1).

Next we list the following relations which may be derived easily from the general solution of the Pell's equation:

$$u_{n+1} = 4u_n - u_{n-1}\,, \quad u_0 = 1\,, \quad u_1 = 2\,, \tag{3}$$
$$v_{n+1} = 4v_n - v_{n-1}\,, \quad v_0 = 0\,, \quad v_1 = 1\,, \tag{4}$$
$$v_{n+2k} \equiv -v_n \pmod{u_k}\,. \tag{5}$$

If $n \leqslant -2$ then $v_n+3<0$, (2) cannot hold, so we only consider the cases $n \geqslant -1$, Since, by (2), $v_n \equiv 1 \pmod 2$, then $n \equiv 1 \pmod 2$ by (4). Take modulo 8 to (4) we find that if $n \equiv 1 \pmod 4$ then $v_n \equiv 1 \pmod 8$, leads to $2y^2 \equiv 4 \pmod 8$, which is impossible, so that it is necessary for $n \equiv -1 \pmod 4$.

Again, take modulo 37 to (4) we obtain a seqeunce with period 36 as follows (only the terms with foot indices of the form $4k-1$ are listed):

$n \pmod{36}$	-1	3	7	11	15	19	23	27	31
$v_n \pmod{37}$	-1	15	25	25	15	-1	13	7	13
$\left(\frac{v_n+3}{37}\right)$	$-$	$-$	$+$	$+$	$-$	$-$	$+$	$+$	$+$

Since (2) implies $\left(\frac{v_n+3}{37}\right)=\left(\frac{2y^2}{37}\right)=-1$, so according to the above table we can exclude $n \equiv 7, 11, 23, 27, 31 \pmod{36}$. Furthermore $n \equiv 3, 15 \pmod{36}$ belong to the case $3\mid n$, which has been solved in the previous paragraph, then may be exclused, so that there remain the cases $n \equiv -1, 19 \pmod{36}$.

Now by taking modulo 3 to (4) we can exclude $n \equiv 1 \pmod 6$, so also $n \equiv 19 \pmod{36}$, since it implies $v_n \equiv 1 \pmod 3$ and $2y^2 \equiv 1 \pmod 3$, which is impossible. Thus the only case left is $n \equiv -1 \pmod{36}$.

Suppose that $n \equiv -1 \pmod{36}$ and $n \neq -1$, we can write $n=-1+(12k \pm 4)\cdot 3^r$, where $r \geqslant 2$. Let $m=3^r$, by repeated application of (5) and the relations $v_{-n}=-v_n$, $v_{n\pm1}=\pm u_n+2v_n$, we get

$$v_n \equiv v_{-1\pm4m} \pmod{u_{3m}}\,,$$
$$2y^2 \equiv v_{-1\pm4m}+3 \equiv -v_{-1\mp2m}+3 \equiv u_{2m} \pm 2v_{2m}+3 \pmod{u_{3m}}\,.$$

Since $u_{3m}=u_m(u_m^2+9v_m^2)$ and $2\nmid m$ implies $u_m\equiv 2 \pmod 8$, $v_m\equiv \pm 1 \pmod 8$, $u_m^2+9v_m^2\equiv 5 \pmod 8$, so that

$$\left(\frac{u_{2m}\pm 2v_{2m}+3}{u_m^2+9v_m^2}\right)=\left(\frac{2y^2}{u_m^2+9v_m^2}\right)=-1\,. \tag{6}$$

On the other hand, note that $u_{2m}=u_m^2+3v_m^2$, $v_{2m}=2u_m v_m$, $u_m^2-3v_m^2=1$, we have

$$\begin{aligned}\left(\frac{u_{2m}+2v_{2m}+3}{u_m^2+9v_m^2}\right)&=\left(\frac{4u_m^2+4u_m v_m-6v_m^2}{u_m^2+9v_m^2}\right)=\left(\frac{4u_m v_m-42v_m^2}{u_m^2+9v_m^2}\right)=-\left(\frac{2u_m-21v_m}{u_m^2+9v_m^2}\right)\\
&=-\left(\frac{9v_m^2+u_m^2}{21v_m-2u_m}\right)\quad\text{(note that } 21v_m-2u_m>0)\\
&=-\left(\frac{7}{21v_m-2u_m}\right)\left(\frac{126v_m^2+14u_m^2}{21v_m-2u_m}\right)\quad\text{(since } 7\nmid u_m \text{ and } 21v_m-2u_m\equiv\pm 1 \pmod 8))\\
&=-\left(\frac{7}{21v_m-2u_m}\right)\left(\frac{159u_m v_m}{21v_m-2u_m}\right)\\
&=-\left(\frac{21v_m-2u_m}{7\cdot 159}\right)\left(\frac{\frac{1}{2}u_m}{21v_m-2u_m}\right)\left(\frac{v_m}{21v_m-2u_m}\right)\\
&=-\left(\frac{21v_m-2u_m}{53}\right)\left(\frac{2u_m}{21}\right)\left(\frac{\frac{1}{2}u_m}{21v_m}\right)\left(\frac{v_m}{21v_m-2u_m}\right)\\
&=-\left(\frac{2u_m-21v_m}{53}\right)\left(\frac{u_m}{v_m}\right)\left(\frac{v_m}{21v_m-2u_m}\right).\end{aligned}$$

If $v_m\equiv 1 \pmod 8$, then $\left(\frac{v_m}{21v_m-2u_m}\right)=\left(\frac{u_m}{v_m}\right)$; if $v_m\equiv -1 \pmod 8$, then $\left(\frac{v_m}{21v_m-2u_m}\right)=-\left(\frac{21v_m-2u_m}{v_m}\right)=\left(\frac{u_m}{v_m}\right)$, the same as before. Hence, we obtain

$$\left(\frac{u_{2m}+2v_{2m}+3}{u_m^2+9v_m^2}\right)=-\left(\frac{2u_m-21v_m}{53}\right). \tag{7}$$

Similarly we can show

$$\left(\frac{u_{2m}-2v_{2m}+3}{u_m^2+9v_m^2}\right)=-\left(\frac{2u_m+21v_m}{53}\right). \tag{8}$$

Using the recurrent relations (3), (4) we take modulo 53 to $\{2u_n\pm 21v_n\}$, and obtain their residue sequences with the same period 9. Now $m\equiv 0 \pmod 9$ implies both $2u_m\pm 21v_m\equiv 2 \pmod{53}$, so that (7) and (8) lead to

$$\left(\frac{u_{2m}\pm 2v_{2m}+3}{u_m^2+9v_m^2}\right)=-\left(\frac{2}{53}\right)=1\,,$$

which are contrary to (6).

Finally there remains $n=-1$, this case gives $(x, y)=(1, 1)$, another positive integer solution of (1), adding the previous one $(x, y)=(3, 3)$ given by the case $n=3$ we obtain all positive intger solutions of (1). This completes our proof.

Remark: Because in two equations $3x^2-1=u_n$ and $2y^2-3=v_n$ we only use the latter, so actually we have proved that the more general equation $x^2-3(2y^2-3)^2=1$ has only two positive integer solutions $(x, y)=(2, 1)$ and $(26, 3)$.

The auther wishes to thank Professor Sun Qi for his help and encouragement.

References

[1] A. Bremner: *A Diophantine equation arising from tight 4-designs*, Osaka J. Math. **16** (1979), 353–356.

[2] H. Enomoto, N. Ito, R. Noda: *Tight 4-designs*, Osaka J. Math. **16** (1979), 39–43.

[3] Choa. Ko, Qi. Sun: *Some indefinite equation problems in group theory, combinatorial theory and algebraic number theory*, J. Math. Res. Exposition, **3** (1983), 2, 131–134.

Department of Mathemathcs
Chongqing Techers' College
China