MATH. SCAND. 21 (1967), 144–148

THE DIOPHANTINE EQUATION $3x^4 - 2y^2 = 1$

RICHARD T. BUMBY

Diophantine equations of the form $Ax^4 + By^2 = C$ have been studied in great detail in recent decades. In [1], J. H. E. Cohn uses an elementary method to study certain equations of this type. In the course of his study he found that it was necessary to know the solutions of $3x^4 - 2y^2 = 1$ to determine the number of solutions of some of these equations. He conjectured that the only solutions of this equation are $(x,y) = (\pm 1, \pm 1)$ or $(\pm 3, \pm 11)$. This paper is a proof of his conjecture.

Let $\alpha = 5 + 2\cdot 6^{\frac{1}{2}}$ and define

$$U_n = \frac{\alpha^n + \alpha^{1-n}}{\alpha + 1}.$$

Then the solutions of the equation $3u^2 - 2v^2 = 1$ have $u = \pm U_n$ since $(u\,3^{\frac{1}{2}} + v\,2^{\frac{1}{2}})(3^{\frac{1}{2}} + 2^{\frac{1}{2}}) = \pm \alpha^n$.

Thus, in order to solve the equation $3x^4 - 2y^2 = 1$ we must determine when $\pm U_n$ can be a square.

Let us introduce $(-2)^{\frac{1}{2}}$ and $(-3)^{\frac{1}{2}}$. Also, let us agree that $(-2)^{\frac{1}{2}}(-3)^{\frac{1}{2}} = -6^{\frac{1}{2}}$. Then with $\theta = (-2)^{\frac{1}{2}} + (-3)^{\frac{1}{2}}$, we have $\theta^2 = -\alpha$. In addition, we shall use ω to denote $\frac{1}{2}(-1 + (-3)^{\frac{1}{2}})$.

Now

$$U_n = (-1)^n \frac{\theta^{2n} - \theta^{2-2n}}{1 - \theta^2}$$

$$= (-1)^n \frac{\theta^n - \theta^{1-n}}{1-\theta} \, \frac{\theta^n + \theta^{1-n}}{1+\theta}.$$

The two factors of U_n which we have separated are both algebraic integers. A slightly less obvious fact is

LEMMA 1. *The quantity*

$$Y_n = \frac{\theta^n + \theta^{1-n}}{1+\theta}$$

Received October 29, 1966.

This paper contains material presented to the American Mathematical Society under the title "Some Diophantine Equations. Preliminary Report". The research was aided by the National Science Foundation.

is in $Q((-2)^{\frac{1}{2}})$, *and its conjugate is*

$$Y_n' = (-1)^n \frac{\theta^n - \theta^{1-n}}{1-\theta}.$$

PROOF. The field $Q((-2)^{\frac{1}{2}},(-3)^{\frac{1}{2}})$ contains all expressions which are rational combinations of θ and ω. This field is a Galois extension of Q with group $Z_2 \oplus Z_2$. If we label each automorphism by the generator of its fixed field, table 1 gives the effect of these automorphisms on θ and ω.

fixed element	image of θ	image of ω
$(-2)^{\frac{1}{2}}$	θ^{-1}	ω^2
$(-3)^{\frac{1}{2}}$	$-\theta^{-1}$	ω
$6^{\frac{1}{2}}$	$-\theta$	ω^2

table 1

Using table 1 we find that the automorphism fixing $(-2)^{\frac{1}{2}}$ also fixes Y_n and Y_n' while the others interchange these terms. This proves the lemma.

LEMMA 2. *The quantities*

$$\Phi_n = \frac{\omega^2\theta^n - \omega\theta^{1-n}}{\omega^2 - \omega\theta}, \qquad \Psi_n = \omega^2\theta^{2n-1} + \omega\theta^{1-2n}$$

are in $Q((-2)^{\frac{1}{2}})$ *and their conjugates are*

$$\Phi_n' = (-1)^n \frac{\omega\theta^n + \omega^2\theta^{1-n}}{\omega + \omega^2\theta}, \qquad \Psi_n' = -(\omega\theta^{2n-1} + \omega^2\theta^{1-2n}).$$

PROOF. Direct calculation using table 1.

Also note $Y_{1-n} = Y_n$ and $\Psi_{1-n} = -\Psi_n'$. Furthermore

$$\begin{aligned}(\omega^2-\omega\theta)(\omega+\omega^2\theta) &= 1 + (\omega-\omega^2)\theta - \theta^2 \\ &= \theta[(\omega-\omega^2) + (\theta^{-1}-\theta)] = -\theta(-3)^{\frac{1}{2}}.\end{aligned}$$

From this it follows that Φ_n is an algebraic integer. Also Ψ_n is clearly an algebraic integer.

Other calculations we will require are given in table 2.

$$\begin{aligned}1-\theta &= \tfrac{1}{2}[(2-2(-2)^{\frac{1}{2}})-(-3)^{\frac{1}{2}}(2)] \\ \omega^2-\omega\theta &= \tfrac{1}{2}[(2+(-2)^{\frac{1}{2}})-(-3)^{\frac{1}{2}}(-2)^{\frac{1}{2}}] \\ \omega^2\theta-\omega &= \tfrac{1}{2}[(4-(-2)^{\frac{1}{2}})-(-3)^{\frac{1}{2}}(2+(-2)^{\frac{1}{2}})] \\ \omega^2\theta^{-1}-\omega\theta^2 &= \tfrac{1}{2}[(-8+5(-2)^{\frac{1}{2}})-(-3)^{\frac{1}{2}}(-6-(-2)^{\frac{1}{2}})] \\ \Psi_0 &= \omega\theta+\omega^2\theta^{-1} = -3-(-2)^{\frac{1}{2}}\end{aligned}$$

table 2

Among the consequences of table 2 are:

$$\Phi_0 = 1, \quad \Phi_1 = 1-(-2)^{\frac12}, \quad \frac{1-\theta}{\omega^2-\omega\theta} = -(-2)^{\frac12}. \tag{1}$$

Since $\omega^2-\omega\theta \mid (-3)^{\frac12}$, we have $1-\theta \mid 6^{\frac12}$.

LEMMA 3. *$Y_0=Y_1=1$, $Y_2=Y_{-1}=-1+2(-2)^{\frac12}=(1+(-2)^{\frac12})^2$ and $Y_n \equiv Y_{n+4} \pmod{4(-2)^{\frac12}}$. U_n is a unit times a square if and only if Y_n is a square in $Z[(-2)^{\frac12}]$.*

PROOF. The calculation of Y_2 is a special case of the following. If $2n-1=3(2p-1)$, then

$$Y_n = (1+(-2)^{\frac12})\, Y_p\, \Phi_p'\, \Phi_{1-p}'. \tag{2}$$

Since $\theta^2 \equiv 3+2(-2)^{\frac12} \pmod{4(-2)^{\frac12}}$,

$$\theta^4 \equiv 1 \pmod{4(-2)^{\frac12}}.$$

Thus one verifies easily that $Y_n \equiv Y_{n+4} \pmod{4(-2)^{\frac12}}$. Finally Y_n is always odd, so $(Y_n, Y_n')=1$. The domain $Z[(-2)^{\frac12}]$ has unique factorization, so

$$Y_n Y_n' = \text{unit} \times \text{square} \Rightarrow Y_n = \text{unit} \times \text{square}.$$

But modulo $4(-2)^{\frac12}$, the quantity Y_n is always congruent to a square, never to the negative of a square.

Other applications of the calculations modulo $4(-2)^{\frac12}$ are

$$\begin{aligned} \Phi_{n+2} &\equiv (3+2(-2)^{\frac12})\Phi_n \\ \Psi_{n+1} &\equiv (3+2(-2)^{\frac12})\Psi_n \end{aligned} \pmod{4(-2)^{\frac12}}. \tag{3}$$

LEMMA 4. *The quadratic character of $\pm(-2)^{\frac12}$ modulo a prime $\varrho \in Z[(-2)^{\frac12}]$ is given by*

(a) *if $\varrho \equiv \pm 1$ or $\pm 1+2(-2)^{\frac12} \pmod{4(-2)^{\frac12}}$ then both $\pm(-2)^{\frac12}$ are* QR.

(b) *if $\varrho \equiv \pm 3$ or $\pm 3+2(-2)^{\frac12} \pmod{4(-2)^{\frac12}}$ then neither is a* QR.

(c) *if $\varrho \equiv \pm(1+(-2)^{\frac12})$ or $\pm(3+(-2)^{\frac12}) \pmod{4(-2)^{\frac12}}$ then only $-(-2)^{\frac12}$ is a* QR.

(d) *if $\varrho \equiv \pm(1-(-2)^{\frac12})$ or $\pm(3-(-2)^{\frac12}) \pmod{4(-2)^{\frac12}}$ then only $+(-2)^{\frac12}$ is a* QR.

PROOF. This is a consequence of Hilbert's reciprocity law. (See [3, Chapter VII].) This special case can also be obtained by the following elementary method (due to Dirichlet [2]).

The character of an ordinary integer k modulo ϱ in $Z[(-2)^{\frac12}]$ is the same as that of k modulo the norm of ϱ in Z. If $\varrho=r+s(-2)^{\frac12}$, then

$(-2)^{\frac{1}{2}}$ is the root of $sx+r\equiv 0 \pmod{\varrho}$. Hence the quadratic character of $(-2)^{\frac{1}{2}} \bmod \varrho$ is the same as that of $-rs \bmod N(\varrho)$. This is given by the ordinary Legendre symbol

$$\left(\frac{-rs}{r^2+2s^2}\right).$$

The lemma follows from quadratic reciprocity. For example when r, s are both odd, $r^2+2s^2\equiv 3 \pmod 8$ and thus

$$\left(\frac{-rs}{r^2+2s^2}\right) = -(\operatorname{sgn} r)(\operatorname{sgn} s)\left(\frac{-1}{|r|}\right)\left(\frac{-1}{|s|}\right)\left(\frac{2}{|r|}\right) = (-1)^k$$

with

$$k = 1+\tfrac{1}{2}(r-1)+\tfrac{1}{2}(s-1)+\tfrac{1}{8}(r^2-1).$$

THEOREM 1. *If n is even, $(Y_n,3)=1$, and $Y_n=\xi^2$, then $n=0$.*

PROOF. We will show inductively that $n\equiv 0 \pmod{4\cdot 3^a}$ for all $a\geqq 1$.

We have $Y_n+Y_{n+3}\equiv 0 \pmod{\Phi_1'}$. Using the consequences of table 2 (in particular (1) and lemma 3), we have modulo $\Phi_1'=1+(-2)^{\frac{1}{2}}$:

$$Y_{6k}\equiv Y_{6k+1}\equiv 1,\quad Y_{6k+3}\equiv Y_{6k+4}\equiv -1,\quad Y_{6k+2}\equiv Y_{6k+5}\equiv 0.$$

Since Φ_1' has norm 3, -1 is not a quadratic residue. Thus only Y_{6n} can satisfy all hypotheses. Also $\theta^2\equiv -\omega^2 \pmod{\Psi_1}$ since $\Psi_1=\omega^2\theta^{-1}(\theta^2+\omega^2)$. We also have $\Psi_1=-\Psi_0'=3-(-2)^{\frac{1}{2}}$, so it has norm 11. Hence $(1+\theta,\Psi_1)=1$, so that $Y_{12k+6}\equiv -1 \pmod{\Psi_1}$, and -1 is not a quadratic residue $\bmod \Psi_1$. Thus we must have $n\equiv 0 \pmod{4\cdot 3^1}$.

Assume already shown that the hypothesis requires $n\equiv 0 \pmod{4\cdot 3^{a-1}}$ where $a>1$. Let $m=\frac{1}{2}(1+3^{a-1})$. Then $m\equiv 2 \pmod 3$, so $(\Phi_m,3)=1$.

Also $\theta^{2m-1}\equiv\omega^2 \pmod{\Phi_m}$. If $n\equiv -2\cdot 3^{a-1} \pmod{2\cdot 3^a}$, then

$$Y_n'\equiv\frac{\omega^2-\omega\theta}{1-\theta}\equiv\frac{-1}{(-2)^{\frac{1}{2}}} \pmod{\Phi_m}\quad\text{or}\quad Y_n\equiv\frac{1}{(-2)^{\frac{1}{2}}} \pmod{\Phi_m'}.$$

If $n\equiv 2\cdot 3^{a-1}$, then

$$Y_n\equiv\frac{\omega+\omega^2\theta}{1+\theta}\equiv\left(\frac{\omega^2-\omega\theta}{1-\theta}\right)'\equiv\frac{1}{(-2)^{\frac{1}{2}}} \pmod{\Phi_m}.$$

If a is even, then $m\equiv 2 \pmod 4$ so

$$\Phi_m\equiv\Phi_2\equiv 3+2(-2)^{\frac{1}{2}} \pmod{4(-2)^{\frac{1}{2}}}.$$

Now lemma 4 completes this part of the proof.

If a is odd, then $\Phi_m\equiv 1-(-2)^{\frac{1}{2}} \pmod{4(-2)^{\frac{1}{2}}}$. As above, we have that

Y_n is not a quadratic residue mod Φ_m' if $n = -2\cdot 3^{a-1} \pmod{2\cdot 3^a}$. This leaves $n \equiv -4\cdot 3^{a-1} \pmod{4\cdot 3^a}$ to be dealt with. Here we find $Y_n \equiv (-2)^{-\frac{1}{2}} \pmod{\Psi_m'}$. Since $\Psi_m' \equiv 3 + (-2)^{\frac{1}{2}} \pmod{4(-2)^{\frac{1}{2}}}$, lemma 4 comes to the rescue again.

COROLLARY. *The only integer solutions of* $3x^4 - 2y^2 = 1$ *are* $(x,y) = (\pm 1, \pm 1)$ *or* $(\pm 3, \pm 11)$.

PROOF. Using lemma 3 and the fact that $Y_n = Y_{1-n}$, we need only find those n which are even for which Y_n is a square. If $n=0$: $Y_n = 1$, $U_n = 1$, $x = \pm 1$, $y = \pm 1$. By theorem 1, any other solution has $(Y_n, 3) \neq 1$. This requires $3 \mid 2n-1$. Apply (2) and note that Y_p, Φ_p', Φ_{1-p}' are relatively prime in pairs and Y_p cannot be congruent to either $-\xi^2$ or $\pm(1+(-2)^{\frac{1}{2}})\xi^2$. Thus if Y_n is square, so is Y_p. We must then check $n=2$. Here $Y_n = (1+(-2)^{\frac{1}{2}})^2$, $u_n = 9$, $x = \pm 3$, $y = \pm 11$. Looking next at $n = -4$ we find that we do not get a square. Actually

$$\Phi_2' \equiv 3 + 2(-2)^{\frac{1}{2}},\ \Phi_{-1}' \equiv -1 + (-2)^{\frac{1}{2}} \quad \pmod{4(-2)^{\frac{1}{2}}}$$

so they are not congruent to $\pm\xi^2$ or $\pm(1+(-2)^{\frac{1}{2}})\xi^2$. This shows that there are no other solutions.

BIBLIOGRAPHY

1. J. H. E. Cohn, *Eight diophantine equations*, Proc. London Math. Soc. (3) 16 (1966), 153–166.
2. G. Lejeune Dirichlet, *Démonstration d'une propriété analogue a la loi de réciprocité qui extiste entre deux nombres premiers quelconques*, J. Reine Angew. Math. 9 (1832), 379–389 (or Collected Works I, pp. 173–188).
3. O. T. O'Meara, *Introduction to quadratic forms*, Berlin, 1963.

RUTGERS, THE STATE UNIVERSITY, NEW BRUNSWICK, N.J. U.S.A.