THE DIOPHANTINE EQUATION $(X[X-1])^2 = 3Y[Y-1]$

by MANORANJITHAM VELUPPILLAI

(Received 25 March, 1975)

The object of this paper is to prove that the only non-trivial solution in positive integers of the equation of the title is $X = 3$, $Y = 4$.

Substituting $x = 2X-1$, $y = 2Y-1$ gives with a little manipulation

$$y^2-3\left(\frac{x^2-1}{6}\right)^2 = 1.$$

This is of the form

$$u^2-3v^2 = 1, \tag{1}$$

where

$$u = y \quad \text{and} \quad v = \tfrac{1}{6}(x^2-1).$$

Hence we must have

$$x^2 = 1+6v. \tag{2}$$

Now, all the integral solutions of (1) are given by $u = u_n$, $v = v_n$, where n is an integer and

$$u_n \pm \sqrt{3}v_n = (2\pm\sqrt{3})^n. \tag{3}$$

By (3), we have

$$u_n = \frac{\alpha^n+\beta^n}{2}, \quad v_n = \frac{\alpha^n-\beta^n}{2\sqrt{3}}, \tag{4}$$

where $\alpha = 2+\sqrt{3}$ and $\beta = 2-\sqrt{3}$. We easily find from (4), since $\alpha+\beta = 4$, $\alpha-\beta = 2\sqrt{3}$ and $\alpha\beta = 1$, that

$$u_{-n} = u_n, \tag{5}$$

$$v_{-n} = -v_n, \tag{6}$$

$$u_{m+n} = u_m u_n + 3v_m v_n, \tag{7}$$

$$v_{m+n} = u_m v_n + u_n v_m, \tag{8}$$

$$u_{2n} = u_n^2+3v_n^2 = 2u_n^2-1, \tag{9}$$

$$v_{2n} = 2u_n v_n, \tag{10}$$

$$u_{5n} = u_n(16u_n^4-20u_n^2+5), \tag{11}$$

$$v_{5n} = v_n(16u_n^4-12u_n^2+1). \tag{12}$$

We then have, using (7)–(10), that

$$v_{n+2r} \equiv v_n (\text{mod } v_r), \tag{13}$$

$$v_{n+2r} \equiv -v_n (\text{mod } u_r). \tag{14}$$

https://doi.org/10.1017/S0017089500002858 Published online by Cambridge University Press

We have also the following table of values

n	u_n	v_n
0	1	0
1	2	1
2	7	4
3	26	15
4	97	56
5	362	209
6	1351	780
7	5042	2911
8	18817	10864
9	70226	40545
10	262087	151316.

We note that y is odd and hence u is odd. Thus we have to consider only the even values of n. The proof is now accomplished in six stages.

(i) (2) is impossible if $n \equiv \pm 4 \pmod{10}$.

For,

$$\begin{aligned} v_n &\equiv v_{\pm 4} \pmod{v_5} \\ &\equiv \pm v_4 \pmod{v_5}, \text{ using (6),} \\ &\equiv \pm 56 \pmod{209}, \end{aligned}$$

whence $v_n \equiv \pm 1 \pmod{11}$. Then $x^2 = 1 \pm 6v_n \equiv 7$ or $-5 \pmod{11}$, and since $(7/11) = -1$, $(-5/11) = -1$, (2) is impossible.

(ii) (2) is impossible if $n \equiv 8 \pmod{10}$.

For,

$$\begin{aligned} v_n &\equiv v_8 \equiv v_{-2} \pmod{v_5} \\ &\equiv -4 \pmod{209}. \end{aligned}$$

However, then $1+6v_n \equiv -1 \pmod{11}$ and since $(-1/11) = -1$, (2) is impossible.

(iii) (2) is impossible if $n \equiv 12 \pmod{20}$.

For,

$$\begin{aligned} v_n &\equiv v_{12} \equiv v_{-8} \pmod{v_{10}} \\ &\equiv -10864 \pmod{151316}. \end{aligned}$$

Now, $181 \mid 151316$ and $1+6v_n \equiv -23 \pmod{181}$. Since $(-23/181) = -1$, (2) is impossible.

(iv) (2) is impossible if $n \equiv 10 \pmod{20}$.

For,

$$\begin{aligned} v_n &\equiv \pm v_{10} \pmod{u_{10}} \\ &\equiv \pm 151316 \pmod{262087}. \end{aligned}$$

https://doi.org/10.1017/S0017089500002858 Published online by Cambridge University Press

Hence $x^2 \equiv 1 \pm 6.151316 \pmod{7.37441}$. That is, either $x^2 \equiv 907897 \pmod{7.37441}$ or $x^2 \equiv -907895 \pmod{7.37441}$. Since $(907897/37441) = -1$ and $(-907895/7) = -1$, (2) is impossible.

(v) (2) is impossible if $n \equiv 0 \pmod{20}$, $n \neq 0$.

For, if $n \neq 0$, we may write $n = 5.2^t(2l+1)$, where l is an integer, odd or even, and $t \geqq 2$. That is, $n = 5k + 2.5k.l$, where $k = 2^t$. Then by using (14) l times, we obtain

$$\begin{aligned} v_n &\equiv \pm v_{5k} \pmod{u_{5k}} \\ &\equiv \pm v_k(16u_k^4 - 12u_k^2 + 1) \pmod{u_k(16u_k^4 - 20u_k^2 + 5)} \\ &\equiv \pm v_k(8u_k^2 - 4) \pmod{16u_k^4 - 20u_k^2 + 5} \\ &\equiv \pm v_k(24v_k^2 + 4) \pmod{144v_k^4 + 36v_k^4 + 1}. \end{aligned}$$

Hence $x^2 \equiv 1 \pm 6v_k(24v_k^2 + 4) \pmod{144v_k^4 + 36v_k^2 + 1}$. First consider

$$x^2 \equiv 1 + 6v_k(24v_k^2 + 4) \pmod{144v_k^4 + 36v_k^2 + 1}.$$

Now,

$$\begin{aligned} \left(\frac{1 + 6v_k(24v_k^2 + 4)}{144v_k^4 + 36v_k^2 + 1}\right) &= \left(\frac{12v_k^2 - v_k + 1}{144v_k^3 + 24v_k + 1}\right) \\ &= \left(\frac{12v_k^2 + 12v_k + 1}{12v_k^2 - v_k + 1}\right) \\ &= \left(\frac{13v_k}{12v_k^2 - v_k + 1}\right) = \left(\frac{12v_k^2 - v_k + 1}{13}\right). \end{aligned}$$

Similarly

$$\left(\frac{1 - 6v_k(24v_k^2 + 4)}{144v_k^4 + 36v_k^2 + 1}\right) = \left(\frac{12v_k^2 + v_k + 1}{13}\right).$$

Hence

$$\left(\frac{1 \pm 6v_k(24v_k^2 + 4)}{144v_k^4 + 36v_k^2 + 1}\right) = \left(\frac{12v_k^2 \mp v_k + 1}{13}\right).$$

Now $v_k \equiv \pm 4 \pmod{13}$ and so

$$\left(\frac{12v_k^2 \mp v_k + 1}{13}\right) = -1.$$

Hence (2) is impossible.

(vi) (2) is impossible if $n \equiv 2 \pmod{20}$, $n \neq 2$.

For, we can write $n = 2 + 2k.5l$, where $k = 2^t$, $t \geqq 1$ and l is an odd integer.

https://doi.org/10.1017/S0017089500002858 Published online by Cambridge University Press

Using (14) l times, we obtain

$$v_n \equiv -v_2 (\text{mod}\, u_{5k})$$
$$\equiv -4(\text{mod}\, u_k(16u_k^4-20u_k^2+5)).$$

Hence

$$x^2 \equiv -23\ (\text{mod}\ u_k(16u_k^4-20u_k^2+5)).$$

Now $(-23/u_k) = (u_k/23)$ and

$$(-23/16u_k^4-20u_k^2+5) = (16u_k^4-20u_k^2+5/23) = (f(u_k)/23)$$

where $f(u_k) = 16u_k^4-20u_k^2+5$.

The residues of $u_k, f(u_k)$ modulo 23 are periodic and the length of the period is 5. The following table gives these residues and the signs of $(u_k/23)$ and $(f(u_k)/23)$.

$k=2^t$	u_k (mod 23)	$\left(\frac{u_k}{23}\right)$	$f(u_k)$ (mod 23)	$\left(\frac{f(u_k)}{23}\right)$
$t=1$	7	-1		
$=2$	5	-1		
$=3$	3	$+1$	-6	-1
$=4$	-6	-1		
$=5$	2	$+1$	-3	-1
$=6$	7	-1		

From the above table we see that the congruences $x^2 \equiv -23\ (\text{mod}\ u_k)$ and $x^2 \equiv -23\ (\text{mod}\, f(u_k))$ cannot hold simultaneously. Hence (2) is impossible.

Summarizing the results, we see that (2) can hold for n even, only for $n=0$ and $n=2$ and these values do indeed satisfy with $u=1$, $v=0$, $x=1$, $y=1$, and $u=7$, $v=4$, $x=5$, $y=7$. The values $x=1$, $y=1$ give the trivial solution $X=1$, $Y=1$ while the values $x=5$, $y=7$ give the solution $X=3$, $Y=4$.

Acknowledgement. This paper has been prepared under the supervision of Dr. J. H. E. Cohn. The author wishes to express her gratitude to Dr. Cohn for all the help she has received from him.

Royal Holloway College
Englefield Green
Egham
Surrey

https://doi.org/10.1017/S0017089500002858 Published online by Cambridge University Press