PACIFIC JOURNAL OF MATHEMATICS
Vol. 37, No. 2, 1971

THE DIOPHANTINE EQUATION $Y(Y+1)(Y+2)(Y+3)=2X(X+1)(X+2)(X+3)$

J. H. E. COHN

It is shown that the only solution in positive integers of the equation of the title is $X=4$, $Y=5$.

Substituting $y = 2Y + 3$, $x = 2X + 3$ gives with a little manipulation

$$\left\{\frac{y^2-5}{4}\right\}^2 - 2\left\{\frac{x^2-5}{4}\right\}^2 = -1\,,$$

and since the fundamental solution of $v^2 - 2u^2 = -1$ is $\alpha = 1 + \sqrt{2}$, we find that if $\beta = 1 - \sqrt{2}$ and

$$(1) \qquad u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}\,; \qquad v_n = \frac{\alpha^n + \beta^n}{2}$$

we must have simultaneously

$$(2) \qquad y^2 = 5 + 4v_N\,,$$

and

$$(3) \qquad x^2 = 5 + 4u_N\,,$$

where N is odd and $N \geqq 3$.

We find easily from (1) since $\alpha\beta = -1$ and $\alpha + \beta = 2$, that

$$(4) \qquad u_{-n} = (-1)^{n-1}u_n$$

$$(5) \qquad v_{-n} = (-1)^n v_n$$

$$(6) \qquad u_{m+n} = u_m v_n + u_n v_m$$

$$(7) \qquad v_{m+n} = v_m v_n + 2u_m u_n\,.$$

Throughout k denotes an even integer, and then we find using (4)—(7) that

$$(8) \qquad v_{2k} = 2v_k^2 - 1 = 4u_k^2 + 1$$

$$(9) \qquad u_{2k} = 2u_k v_k$$

$$(10) \qquad v_{3k} = v_k(8u_k^2 + 1) = v_k(2v_{2k} - 1)$$

$$(11) \qquad u_{3k} = u_k(8u_k^2 + 3)\,.$$

We then have, using (6)—(9) that

(12) $$u_{n+2k} \equiv -u_n \pmod{v_k}$$

and

(13) $$v_{n+2k} \equiv -v_n \pmod{v_k}.$$

We have also the following table of values

n	u_n	v_n
0	0	1
1	1	1
2	2	3
3	5	7
4	12	17
5	29	41
6	70	99
7	169	239
8	408	577
9	985	1393
10	2378	3363
11	5741	8119
12	13860	19601

The proof is now accomplished in eight stages:-

(a). (2) *is impossible if* $N \equiv 3 \pmod 6$.

For,

$$\begin{aligned} v_{n+6} &= v_n v_6 + 2u_n u_6 \qquad \text{by (7)} \\ &= 99v_n + 140u_n \\ &\equiv -v_n \pmod 5, \end{aligned}$$

and so if $N \equiv 3 \pmod 6$, $v_N \equiv \pm v_3 \equiv \pm 2 \pmod 5$, whence $y^2 = 5 + 4v_N$ is impossible modulo 5.

(b). (2) *is impossible if* $N \equiv -3$ *or* $-5 \pmod{16}$.

For, using (13) we find that for such N,

$$\begin{aligned} v_N &\equiv v_{-3} \quad \text{or} \quad v_{-5} && \pmod{v_4} \\ &\equiv -v_3 \quad \text{or} \quad -v_5 && \pmod{17}, \text{ using (5)} \\ &\equiv -7 && \pmod{17}. \end{aligned}$$

But then $5 + 4v_N \equiv -6 \pmod{17}$, and since the Jacobi-Legendre symbol $(-6 \mid 17) = -1$, (2) is impossible.

(c). (3) *is impossible if* $N \equiv \pm 7 \pmod{16}$.

For, using, (12) we find that in this case

$$\begin{aligned} u_n &\equiv \pm u_{\pm 7} && \pmod{v_8} \\ &\equiv \pm 169 && \pmod{577}. \end{aligned}$$

Thus we find that

$5 + 4u_N \equiv 681$ or -671 (mod 577), and since

$$(681 \mid 577) = (-671 \mid 577) = -1\,,$$

(3) is impossible.

(d). (3) *is impossible if* $N \equiv \pm 7 \pmod{24}$.

For then

$$\begin{aligned} u_N &\equiv u_{\pm 7} \qquad &&(\bmod\ v_6) \\ &\equiv 169 &&(\bmod\ 99)\,, \end{aligned}$$

whence $u_N \equiv -2 \pmod 9$, and then $5 + 4u_N \equiv -3 \pmod 9$, and so (3) is impossible.

(e). (2) *and* (3) *together are impossible if* $N \equiv 3 \pmod{16}$.

If $N = 3$, then $5 + 4v_N = 33 \neq y^2$. If $N \neq 3$, then we may write

$$N - 3 = 2lk\,,$$

where l is odd and $k = 2^r$ with $r \geqq 3$. Then by using (13) l times we obtain

$$\begin{aligned} 5 + 4u_N &= 5 + 4u_{3+2lk} && \\ &\equiv 5 + (-1)^l 4u_3 \qquad &&(\bmod\ v_k) \\ &\equiv -15 &&(\bmod\ v_k), \text{ since } l \text{ is odd.} \end{aligned}$$

But from (8) we find easily by induction upon r, that if $k = 2^r$ with $r \geqq 3$, that $v_k \equiv 1 \pmod 4$, $v_k \equiv 1 \pmod 3$ and $v_k \equiv 2 \pmod 5$, whence $(-15 \mid v_k) = -1$ and (3) is impossible.

Combining the results of (a)—(e) we find that we can only have

$$N \equiv 1, 5, -1, 37 \qquad (\bmod\ 48)\,, \tag{14}$$

and we deal with each of these in turn.

(f). (3) *is impossible if* $N \equiv 37 \pmod{48}$.

For then $u_N \equiv u_{-11} \equiv 5741 \pmod{v_{12}}$ and then $5 + 4u_N \equiv 22969$ (mod 19601).

But

$$\begin{aligned} (22969 \mid 19601) &= (3368 \mid 19601) \\ &= (2^3 \mid 19601)(421 \mid 19601) \\ &= (19601 \mid 421) \\ &= (235 \mid 421) \\ &= (421 \mid 5)(421 \mid 47) \\ &= (-2 \mid 47) = -1\,, \end{aligned}$$

and so (3) is impossible.

(g). (3) *is impossible if* $N \equiv 1 \pmod{48}$, $N \neq 1$ *or if* $N \equiv -1 \pmod{48}$ *and* $N \neq -1$.

Since if N is odd, $u_{-N} = u_N$ by (4) it suffices to consider $N \equiv 1 \pmod{48}$, $N \neq 1$. Then we may write $N = 1 + 3k(2l+1)$, where $k = 2^r$ and $r \geqq 4$, and so using (12) we find that

$$\begin{aligned} u_N &= u_{1+3k+2l.3k} \\ &\equiv (-1)^l u_{1+3k} && \pmod{v_{3k}} \\ &\equiv \pm(u_{3k} + v_{3k}) && \pmod{v_{3k}} \text{ using (6)} \\ &\equiv \pm u_{3k} && \pmod{v_{3k}} \\ &\equiv \pm u_k(8u_k^2 + 3) && (\bmod\ v_k(8u_k^2 + 1)), \end{aligned}$$

using (10) and (11). Thus

$$u_N \equiv \pm 2u_k \qquad (\bmod\ 8u_k^2 + 1) .$$

But now, writing $u = u_k$, we find

$$\begin{aligned} (5 + 4u_N \mid 8u^2 + 1) &= (5 \pm 8u \mid 8u^2 + 1) \\ &= (8u \pm 5 \mid 8u^2 + 1) \\ &= (8u^2 + 1 \mid 8u \pm 5) \\ &= (8 \mid 8u \pm 5)(8^2u^2 + 8 \mid 8u \pm 5) \\ &= -(33 \mid 8u \pm 5) \\ &= -(8u \pm 5 \mid 33) . \end{aligned} \tag{15}$$

But $u = u_k$ with $k = 2^r$ and $r \geqq 4$, and we find that $3 \mid u_8$, whence $3 \mid u_k$ in view of (9). Also $v_8 \equiv 5 \pmod{11}$ whence by induction, using (8), $v_n \equiv 5 \pmod{11}$ for $n = 2^r$ and $r \geqq 3$. Thus $u_{2n} \equiv -u_n \pmod{11}$ in view of (9), and so since $u_8 \equiv 1 \pmod{11}$, $u \equiv \pm 1 \pmod{11}$. Thus we have $u \equiv \pm 12 \pmod{33}$ whence $8u \equiv \mp 3 \pmod{33}$. Considering therefore the right hand side of (15), we observe that $8u \pm 5 \equiv \pm 2$ or $\pm 8 \pmod{33}$ and in any one of the four cases the right hand side of (15) equals -1, and accordingly (3) is impossible.

(h). (2) *and* (3) *together are impossible if* $N \equiv 5 \pmod{48}$, $N \neq 5$.

Suppose if possible that (2), (3) hold with $N \equiv 5 \pmod{48}$, $N \neq 5$. Let $N = 5 + 2l.3k$ where $k = 2^r$, $r \geqq 3$ and l is odd. Then we have using (12) and (13)

$$x^2 = 5 + 4u_N \equiv 5 - 4u_5 \equiv -111 \qquad \pmod{v_{3k}} \tag{16}$$

$$y^2 = 5 + 4v_N \equiv 5 - 4v_5 \equiv -159 \qquad \pmod{v_{3k}} . \tag{17}$$

Now we have from (10) $v_{3k} = v_k(2v_{2k} - 1)$, and as before $v_k \equiv 1 \pmod{12}$ whence also $2v_{2k} - 1 \equiv 1 \pmod{12}$. Thus $(-3 \mid v_k) = (-3 \mid 2v_{2k} - 1) = 1$, and so (16) and (17) imply (since as we shall see presently neither v_k nor $2v_{2k} - 1$ is ever divisible by either 37 or 53) that

$$(v_k \mid 37) = (2v_{2k} - 1 \mid 37) = (v_k \mid 53) = (2v_{2k} - 1 \mid 53) = 1\,, \tag{18}$$

for some $k = 2^r$, $r \geqq 3$. We shall demonstrate that (18) occurs for no such k.

In view of (8) it is clear that the residues modulo p for any prime p, of v_k with $k = 2^r$ are eventually periodic with respect to r. It transpires that if $p = 37$ or if $p = 53$, the length of the period is 9, and that the sequence of residues has already become periodic by the time $r = 3$. It is fortunately the case that in no one of the nine cases that arise are all the four conditions of (18) satisfied, and this concludes the proof. A table showing these calculations follows:-

$k = 2^r$	$r = 3$	4	5	6	7	8	9	10	11	12
v_k (mod 37)	-15	5	12	-9	13	4	-6	-3	17	-15
$2v_{2k} - 1$ (mod 37)	9	-14	18	-12	7	-13	-7	-4	6	
v_k (mod 53)	-6	18	11	-24	-15	25	-23	-3	17	-6
$2v_{2k} - 1$ (mod 53)	-18	21	4	22	-4	6	-7	-20	-13	
$(v_k \mid 37)$	-1	-1	$+1$	$+1$	-1	$+1$	-1	$+1$	-1	
$(2v_{2k} - 1 \mid 37)$	$+1$	-1	-1	$+1$	$+1$	-1	$+1$	$+1$	-1	
$(v_k \mid 53)$	$+1$	-1	$+1$	$+1$	$+1$	$+1$	-1	-1	$+1$	
$(2v_{2k} - 1 \mid 53)$	-1	-1	$+1$	-1	$+1$	$+1$	$+1$	-1	$+1$	

Summarising the results, we see that (2) and (3) can hold simultaneously for N odd, $N \geqq 3$ only for $N = 5$, and this value does indeed satisfy (2) and (3) with $x = 11$, $y = 13$. Thus $X = 4$, $Y = 5$ is the only solution of the given equation in positive integers. The complete solution in integers can now be written down; it consists of the sixteen "trivial" pairs of solutions obtained by equating both sides of the given equation to zero, and the four pairs $X = 4$ or -7, $Y = 5$ or -8.

Received October 13, 1970.

ROYAL HOLLOWAY COLLEGE
ENGLEFIELD GREEN, SURREY