THE DIOPHANTINE EQUATION

\[ Y(Y + 1)(Y + 2)(Y + 3) = 2X(X + 1)(X + 2)(X + 3) \]

JOHN H. E. COHN
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

\[
u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad \nu_n = \frac{\alpha^n + \beta^n}{2}
\]

we must have simultaneously

\[
y^2 = 5 + 4\nu_N,
\]

and

\[
x^2 = 5 + 4\nu_N,
\]

where \( N \) is odd and \( N \geq 3 \).

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

\[
\begin{align*}
\nu_{-n} &= (-1)^{n-1}\nu_n \\
v_{-n} &= (-1)^n\nu_n \\
u_{m+n} &= u_mu_n + u_nv_n \\
v_{m+n} &= \nu_mv_n + 2u_nu_n.
\end{align*}
\]

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

\[
\begin{align*}
v_{2k} &= 2v_k^2 - 1 = 4w_k + 1 \\
u_{2k} &= 2u_kv_k \\
v_{4k} &= v_k(8w_k^2 + 1) = v_k(2v_{2k} - 1) \\
u_{4k} &= u_k(8w_k^2 + 3).
\end{align*}
\]

We then have, using (6)—(9) that

331
(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

<table>
<thead>
<tr>
<th>n</th>
<th>u_n</th>
<th>v_n</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>12</td>
<td>17</td>
</tr>
<tr>
<td>5</td>
<td>29</td>
<td>41</td>
</tr>
<tr>
<td>6</td>
<td>70</td>
<td>99</td>
</tr>
<tr>
<td>7</td>
<td>169</td>
<td>239</td>
</tr>
<tr>
<td>8</td>
<td>408</td>
<td>577</td>
</tr>
<tr>
<td>9</td>
<td>985</td>
<td>1393</td>
</tr>
<tr>
<td>10</td>
<td>2378</td>
<td>3363</td>
</tr>
<tr>
<td>11</td>
<td>5741</td>
<td>8119</td>
</tr>
<tr>
<td>12</td>
<td>13860</td>
<td>19601</td>
</tr>
</tbody>
</table>

The proof is now accomplished in eight stages:-

(a). (2) is impossible if \( N \equiv 3 \pmod{6} \).

For,

\[ v_{n+6} = v_n v_6 + 2u_nv_6 \]

by (7)

\[ = 99v_n + 140u_n \]

\[ \equiv -v_n \pmod{5}, \]

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 \( N \equiv -3 \text{ or } -5 \pmod{16} \).

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

\[ v_N \equiv v_{-3} \text{ or } v_{-5} \pmod{v_4} \]

\[ \equiv -v_3 \text{ or } -v_5 \pmod{17}, \text{ using (5)} \]

\[ \equiv -7 \pmod{17}. \]

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

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

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

\[ u_n \equiv \pm u_{\pm 7} \pmod{v_8} \]

\[ \equiv \pm 169 \pmod{577}. \]
Thus we find that
\[ 5 + 4u_N \equiv 681 \text{ or } -671 \pmod{577}, \]
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
\[ u_N \equiv u_{\pm 7} \pmod{v_k} \]
\[ \equiv 169 \pmod{99}, \]
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 \( r \geq 3 \). Then by using (13) \( l \) times
we obtain
\[ 5 + 4u_N = 5 + 4u_{3+2l}, \]
\[ \equiv 5 + (-1)^l 4u_3 \pmod{v_k} \]
\[ \equiv -15 \pmod{v_k}, \]
since \( l \) is odd.

But from (8) we find easily by induction upon \( r \), that if \( k = 2^r \)
with \( r \geq 3 \), 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
(14) \[ N \equiv 1, 5, -1, 37 \pmod{48}, \]
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 \( 5 + 4u_N \equiv 22969 \pmod{19601} \).

But
\[ (22969 \mid 19601) = (3368 \mid 19601) \]
\[ = (2^8 \mid 19601)(421 \mid 19601) \]
\[ = (19601 \mid 421) \]
\[ = (235 \mid 421) \]
\[ = (421 \mid 5)(421 \mid 47) \]
\[ = (-2 \mid 47) = -1, \]
and so (3) is impossible.
(g). (3) is impossible if \( N \equiv 1 \) (mod 48), \( N \neq 1 \) or if \( N \equiv -1 \) (mod 48) and \( N \neq -1 \).

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

\[
\begin{align*}
\quad u_N &= u_{1+3k+21.3k} \\
&
\equiv (-1)^k u_{1+3k} \quad \text{(mod } v_{3k}) \quad \\
&
\equiv \pm (u_{3k} + v_{3k}) \quad \text{(mod } v_{3k}) \quad \text{using (6)} \\
&
\equiv \pm u_{3k} \quad \text{(mod } v_{3k}) \\
&
\equiv \pm u_k(8u_k^2 + 3) \quad \text{mod } v_k(8u_k^2 + 1)),
\end{align*}
\]

using (10) and (11). Thus

\[
u_N \equiv \pm 2u_k \quad \text{mod } 8u_k^2 + 1).
\]

But now, writing \( u = u_k \), we find

\[
(5 + 4u_N | 8u^2 + 1) = (5 \pm 8u | 8u^2 + 1) \\
= (8u \pm 5 | 8u^2 + 1) \\
= (8u^2 + 1 | 8u \pm 5) \\
= (8 | 8u \pm 5)(8u^2 + 8 | 8u \pm 5) \\
= -(33 | 8u \pm 5) \\
= -(8u \pm 5 | 33).
\]

But \( u = u_k \) with \( k = 2^r \) and \( r \geq 4 \), and we find that \( 3 | u_k \), whence \( 3 | u_k \) in view of (9). Also \( v_k \equiv 5 \) (mod 11) whence by induction, using (8), \( v_k \equiv 5 \) (mod 11) for \( n = 2^r \) and \( r \geq 3 \). Thus \( v_{3k} \equiv -u_k \) (mod 11) in view of (9), and so since \( u_k \equiv 1 \) (mod 11), \( u \equiv \pm 1 \) (mod 11). Thus we have \( u \equiv \pm 12 \) (mod 33) whence \( 8u \equiv \mp 3 \) (mod 33). Considering therefore the right hand side of (15), we observe that \( 8u \pm 5 \equiv \pm 2 \) or \( \pm 8 \) (mod 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 \( N \equiv 5 \) (mod 48), \( N \neq 5 \).

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

\[
\begin{align*}
x^2 &= 5 + 4u_N \equiv 5 - 4u_k \equiv -111 \quad \text{(mod } v_{3k}) \quad \\
y^2 &= 5 + 4v_N \equiv 5 - 4v_k \equiv -159 \quad \text{(mod } v_{3k}).
\end{align*}
\]

Now we have from (10) \( v_{3k} = v_k(2v_{2k} - 1) \), and as before \( v_k \equiv 1 \) (mod 12) whence also \( 2v_{2k} - 1 \equiv 1 \) (mod 12). Thus \((-3 | v_k) = (-3 | 2v_{2k} - 1) = 1 \), 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
THE DIOPHANTINE EQUATION $Y(Y+1)(Y+2)(Y+3) = 2X(X+1)(X+2)(X+3)$ 335

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

for some $k = 2^r, r \geq 3$. 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:

<table>
<thead>
<tr>
<th>$k = 2^r$</th>
<th>$r = 3$</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>$v_k \pmod{37}$</td>
<td>$-15$</td>
<td>$5$</td>
<td>$12$</td>
<td>$-9$</td>
<td>$13$</td>
<td>$4$</td>
<td>$-6$</td>
<td>$-3$</td>
<td>$17$</td>
<td>$-15$</td>
</tr>
<tr>
<td>$2v_{2k} - 1 \pmod{37}$</td>
<td>$9$</td>
<td>$-14$</td>
<td>$18$</td>
<td>$-12$</td>
<td>$7$</td>
<td>$-13$</td>
<td>$-7$</td>
<td>$-4$</td>
<td>$6$</td>
<td>$-$</td>
</tr>
<tr>
<td>$v_k \pmod{53}$</td>
<td>$-6$</td>
<td>$18$</td>
<td>$11$</td>
<td>$-24$</td>
<td>$-15$</td>
<td>$25$</td>
<td>$-23$</td>
<td>$-3$</td>
<td>$17$</td>
<td>$-6$</td>
</tr>
<tr>
<td>$2v_{2k} - 1 \pmod{53}$</td>
<td>$-18$</td>
<td>$21$</td>
<td>$4$</td>
<td>$22$</td>
<td>$-4$</td>
<td>$6$</td>
<td>$-7$</td>
<td>$-20$</td>
<td>$-13$</td>
<td>$-$</td>
</tr>
<tr>
<td>$(v_k \mid 37)$</td>
<td>$-1$</td>
<td>$-1$</td>
<td>$+1$</td>
<td>$+1$</td>
<td>$-1$</td>
<td>$+1$</td>
<td>$-1$</td>
<td>$+1$</td>
<td>$-1$</td>
<td>$-$</td>
</tr>
<tr>
<td>$(2v_{2k} - 1 \mid 37)$</td>
<td>$+1$</td>
<td>$-1$</td>
<td>$-1$</td>
<td>$+1$</td>
<td>$+1$</td>
<td>$-1$</td>
<td>$+1$</td>
<td>$+1$</td>
<td>$-1$</td>
<td>$+$</td>
</tr>
<tr>
<td>$(v_k \mid 53)$</td>
<td>$+1$</td>
<td>$-1$</td>
<td>$+1$</td>
<td>$+1$</td>
<td>$+1$</td>
<td>$-1$</td>
<td>$-1$</td>
<td>$-1$</td>
<td>$-1$</td>
<td>$+$</td>
</tr>
<tr>
<td>$(2v_{2k} - 1 \mid 53)$</td>
<td>$-1$</td>
<td>$-1$</td>
<td>$+1$</td>
<td>$-1$</td>
<td>$+1$</td>
<td>$+1$</td>
<td>$+1$</td>
<td>$-1$</td>
<td>$-1$</td>
<td>$+$</td>
</tr>
</tbody>
</table>

Summarising the results, we see that (2) and (3) can hold simultaneously for $N$ odd, $N \geq 3$ 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
Pacific Journal of Mathematics
Vol. 37, No. 2 February, 1971

Charles Compton Alexander, Semi-developable spaces and quotient images of metric spaces ........................................... 277
Ram Prakash Bambah and Alan C. Woods, On a problem of Danzer .................. 295
John A. Beekman and Ralph A. Kallman, Gaussian Markov expectations and related integral equations .................................. 303
Frank Michael Cholewinski and Deborah Tepper Haimo, Inversion of the Hankel potential transform .................................. 319
John H. E. Cohn, The diophantine equation
\[ Y(Y + 1)(Y + 2)(Y + 3) = 2X(X + 1)(X + 2)(X + 3) \] ........................................... 331
Philip C. Curtis, Jr. and Henrik Stetkaer, A factorization theorem for analytic functions operating in a Banach algebra .................. 337
Doyle Otis Cutler and Paul F. Dubois, Generalized final rank for arbitrary limit ordinals ........................................... 345
Keith A. Ekblaw, The functions of bounded index as a subspace of a space of entire functions ........................................... 353
Dennis Michael Girard, The asymptotic behavior of norms of powers of absolutely convergent Fourier series ............................ 357
Paul C. Kainen, Universal coefficient theorems for generalized homology and stable cohomotopy ........................................... 397
Aldo Joram Lazar and James Ronald Retherford, Nuclear spaces, Schauder bases, and Choquet simplexes ........................................... 409
David Lowell Lovelady, Algebraic structure for a set of nonlinear integral operations ....................................................................... 421
John McDonald, Compact convex sets with the equal support property .............. 429
Forrest Miller, Quasivector topologies ........................................... 445
Marion Edward Moore and Arthur Steger, Some results on completability in commutative rings ........................................... 453
A. P. Morse, Taylor’s theorem ........................................... 461
Richard E. Phillips, Derek J. S. Robinson and James Edward Roseblade, Maximal subgroups and chief factors of certain generalized soluble groups ....................................................................... 475
Doron Ravdin, On extensions of homeomorphisms to homeomorphisms .......... 481
John William Rosenthal, Relations not determining the structure of L ............ 497
Prem Lal Sharma, Proximity bases and subbases ........................................... 515
Larry Smith, On ideals in $\Omega^*_u$ ........................................... 527
Warren R. Wogen, von Neumann algebras generated by operators similar to normal operators ........................................... 539
R. Grant Woods, Co-absolutes of remainders of Stone-Čech compactifications ........................................... 545